UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

ABRIL 2023 - SEPTIEMBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERA EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS Y DISEÑO DE UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN EL ESTÁNDAR ISO 27001:2022 PARA LA EMPRESA PC SOLUCIONES DE LA CIUDAD DE BABAHOYO.

ESTUDIANTE:

ERICK ALEXIS FUENTES POZO

TUTOR:

ING. OMAR RODRIGO MONTECE MORENO

AÑO 2023

ÍNDICE

RESUMEN

La Empresa PC Soluciones, ubicada en la ciudad de Babahoyo, se ha consolidado como una empresa que ofrece un servicio de excelente calidad en el sector de soluciones tecnológicas y servicios informáticos. La ausencia de un modelo de gestión de seguridad de la información integral y estandarizado ha dejado a la organización vulnerable a una amplia gama de riesgos potenciales, desde ataques de ciberdelincuentes hasta errores internos que podrían resultar en la filtración de datos valiosos.

El estándar ISO 27001:2022 proporciona un marco sólido para la gestión de la seguridad de la información en organizaciones de todo tipo. Sin embargo, cada empresa tiene características únicas que deben ser consideradas al implementar este estándar. Pc Soluciones debe adaptar los requisitos y controles del estándar ISO 27001 a su propio contexto operativo y a los servicios que ofrece.

La combinación de los métodos deductivos e inductivos en este marco metodológico permitirá desarrollar una comprensión integral de la situación actual de seguridad de la información en la empresa, fundamentar decisiones con base en evidencia teórica y empírica, y diseñar un modelo de gestión de seguridad de la información efectivo y adaptado a las necesidades específicas de Pc Soluciones.

El análisis de la situación revela graves deficiencias en la seguridad de la empresa, incluyendo vulnerabilidades en la red, ataques de ingeniería social efectivos y violaciones graves de la privacidad y la seguridad. Esto destaca la urgente necesidad de implementar un modelo de gestión de seguridad de la información basado en ISO 27001:2022. Este estándar proporcionará una estructura sólida para abordar estos

problemas, fortalecer la concienciación en seguridad y proteger adecuadamente los activos de la empresa.

Palabras claves: Ciberdelincuentes, Implementar, Seguridad, Vulnerabilidades

ABSTRACT

The PC Solutions Company, located in the city of Babahoyo, has established itself as a company that offers an excellent quality service in the sector of technological solutions and computer services. The absence of a comprehensive and standardized information security management model has left the organization vulnerable to a wide range of potential risks, from attacks by cybercriminals to internal errors that could result in the leakage of valuable data.

The ISO 27001:2022 standard provides a solid framework for information security management in organizations of all types. However, each company has unique characteristics that must be considered when implementing this standard. Pc Soluciones must adapt the requirements and controls of the ISO 27001 standard to its own operational context and the services it offers.

The combination of deductive and inductive methods in this methodological framework will allow the development of a comprehensive understanding of the current situation of information security in the company, base decisions based on theoretical and empirical evidence, and design an information security management model. information effective and adapted to the specific needs of Pc Soluciones.

The analysis of the situation reveals serious deficiencies in the security of the company, including vulnerabilities in the network, effective social engineering attacks and serious violations of privacy and security. This highlights the urgent need to implement an information security management model based on ISO 27001:2022. This

standard will provide a solid framework to address these issues, strengthen security awareness, and adequately protect company assets.

Key words: Cybercriminals, Implement, Security, Vulnerabilities

PLANTEAMIENTO DEL PROBLEMA

En un mundo cada vez más interconectado y digitalizado, la seguridad de la información se ha convertido en un aspecto crítico para la supervivencia y el éxito de las organizaciones. Las amenazas cibernéticas, los ataques maliciosos y la filtración de datos confidenciales pueden tener consecuencias devastadoras para la integridad, la reputación y la operatividad de las empresas. En este contexto, la adopción de estándares y marcos de seguridad de la información, como ISO 27001:2022, se ha vuelto esencial para garantizar la protección adecuada de los activos de información.

La Empresa PC Soluciones, ubicada en la ciudad de Babahoyo, se ha consolidado como una empresa que ofrece un servicio de excelente calidad en el sector de soluciones tecnológicas y servicios informáticos. Sin embargo, este progreso no está exento de desafíos, ya que la empresa se enfrenta a la necesidad apremiante de asegurar su entorno de información contra amenazas cibernéticas en constante evolución. La ausencia de un modelo de gestión de seguridad de la información integral y estandarizado ha dejado a la organización vulnerable a una amplia gama de riesgos potenciales, desde ataques de ciberdelincuentes hasta errores internos que podrían resultar en la filtración de datos valiosos.

A pesar de la creciente conciencia sobre la importancia de la seguridad de la información, la Empresa PC Soluciones ha recurrido a enfoques ad hoc para abordar la cuestión. Esta aproximación fragmentada ha dado lugar a la implementación inconsistente de medidas de seguridad, dejando brechas en su postura general de seguridad. La falta de una estructura formal y unificada para abordar la seguridad de la

información ha obstaculizado la identificación precisa de riesgos, la implementación de controles adecuados y la adaptación a las cambiantes circunstancias de seguridad. Esto no solo pone en riesgo la información crítica de la empresa, sino que también impacta negativamente en la confianza de los clientes que confían en la seguridad de los servicios y soluciones brindados por la empresa.

En este contexto, la adopción del estándar ISO 27001:2022 surge como una solución viable para la Empresa PC Soluciones. Sin embargo, la implementación exitosa de este estándar requiere un enfoque meticuloso y personalizado que se ajuste a las necesidades y características específicas de la empresa. Por lo tanto, el problema central radica en la carencia de un modelo de gestión de seguridad de la información que no solo cumpla con los requisitos del estándar ISO 27001:2022, sino que también resuelva las deficiencias de seguridad actuales de la Empresa.

Este modelo debe abordar la falta de estructura, la fragmentación de enfoques y la falta de conciencia sobre riesgos dentro de la organización. Asimismo, debe ser flexible y adaptable para anticipar y mitigar las amenazas emergentes en el horizonte de la seguridad cibernética. Solo a través de un enfoque integral y estratégico se podrá proteger adecuadamente la información valiosa, garantizar la continuidad del negocio y mantener la confianza de todas las partes interesadas involucradas.

JUSTIFICACIÓN

El desafío radica en adaptar este estándar a las características y necesidades específicas de la Empresa Pc Soluciones, considerando su variedad de servicios y la dinámica propia de su entorno empresarial La implementación exitosa de este modelo debería mejorar la seguridad de la información, fortalecer la posición competitiva de la empresa y brindar tranquilidad tanto a sus clientes como a sus operaciones internas.

El estándar ISO 27001:2022 proporciona un marco sólido para la gestión de la seguridad de la información en organizaciones de todo tipo. Sin embargo, cada empresa tiene características únicas que deben ser consideradas al implementar este estándar. Pc Soluciones debe adaptar los requisitos y controles del estándar ISO 27001 a su propio contexto operativo y a los servicios que ofrece.

Esto implica identificar y evaluar los riesgos específicos para la empresa, diseñar controles de seguridad apropiados y establecer procesos efectivos de monitoreo y mejora continua para garantizar la eficacia del sistema de gestión de seguridad de la información.

La implementación de un modelo de gestión de seguridad de la información basado en ISO 27001:2022 conlleva múltiples beneficios. En primer lugar, mejora la seguridad y protege la confidencialidad, integridad y disponibilidad de los datos, lo que reduce el riesgo de filtraciones y ataques cibernéticos. Además, la adopción de un estándar reconocido como ISO 27001 ayuda a la empresa a cumplir con regulaciones y requisitos normativos relacionados con la seguridad de la información.

Esto a su vez fortalece la confianza de los clientes y socios comerciales en la capacidad de la empresa para manejar de manera segura la información. Asimismo, la implementación del estándar promueve una cultura de seguridad en toda la organización, involucrando a empleados y directivos en la protección de la información crítica.

OBJETIVOS DEL ESTUDIO

Objetivo general:

Analizar y Desarrollar un modelo de gestión de seguridad de la información, fundamentado en el estándar ISO 27001:2022, específicamente adaptado a las necesidades y contextos de la Empresa Pc Soluciones en Babahoyo.

Objetivos específicos:

- Analizar las diferentes etapas y requisitos del estándar ISO 27001:2022 y cómo pueden ser adaptados de manera efectiva a la realidad operativa de la Empresa Pc Soluciones.
- Fundamentar las bases teóricas sobre la seguridad de la información y el estándar ISO 27001:2022, así como su aplicabilidad en empresas que ofrecen servicios tecnológicos.
- Evaluar el impacto potencial de la implementación del modelo de seguridad en términos de mejora de la protección de la información, cumplimiento normativo y confianza del cliente.

LÍNEAS DE INVESTIGACIÓN

En la elaboración del presente caso de estudio se basó en las líneas de investigación de la carrera de sistema de información de la facultad de administración, finanzas e informática reconociendo como pertinente tema de "Análisis y Diseño de un modelo de gestión de seguridad de la información basado en el estándar ISO 27001:2022 para la Empresa Pc Soluciones de la ciudad de Babahoyo".

- **Línea de investigación**

Sistemas de información y comunicación, emprendimiento e innovación.

- **Sub línea de investigación**

Redes y tecnologías inteligentes de software y hardware.

ARTICULACIÓN

La articulación de mi estudio de caso se basa en el análisis y diseño de un modelo de gestión de seguridad de información ya que durante mis prácticas en la empresa Pc Soluciones pude notar la necesidad de mejorar la seguridad de la información tanto como del cliente y de los artículos que se ingresan en la impresa.

Me pareció buena idea reforzar la seguridad con lo que he aprendido dentro de la carrera de sistema de información, ya que el sistema con el que cuenta la empresa es un poco vulnerable y se podría filtrar información en algún momento.

MARCO CONCEPTUAL

Un Sistema de Gestión de Seguridad de la Información (SGSI)

Explica (Federico Hurtado, 2018) que un Sistema de Gestión de Seguridad de la Información (SGSI) representa una estructura organizativa esencial para salvaguardar la información crucial en una empresa. Su propósito fundamental radica en la identificación, evaluación y mitigación de los riesgos de seguridad, permitiendo así una gestión efectiva de la integridad, confidencialidad y disponibilidad de los datos. (pag.14)

También se compone de etapas clave, entre las cuales destaca la identificación de los activos de información más críticos y valiosos para la organización. A continuación, se procede con la evaluación de riesgos, analizando detalladamente las posibles amenazas y vulnerabilidades que podrían afectar estos activos. Con base en esta evaluación, se implementan controles y medidas de seguridad adecuadas, estableciendo políticas, procedimientos que minimicen los riesgos y fortalezcan la seguridad. (pag.15)

La ciberseguridad

Menciona (Lewis, 2020) que la ciberseguridad se enfoca en salvaguardar sistemas informáticos, redes y datos contra amenazas cibernéticas. Su propósito es prevenir accesos no autorizados y ataques que puedan comprometer la seguridad y la disponibilidad de los recursos digitales. La gestión de identidad y acceso controla quiénes pueden acceder a sistemas y en qué medida, mientras que la identificación y solución de vulnerabilidades en aplicaciones y sistemas es esencial. (pag.5)

El cifrado protege la confidencialidad de los datos al convertirlos en formato ilegible. Los firewalls, sean hardware o software, supervisan el tráfico de red para bloquear posibles amenazas. La monitorización constante detecta comportamientos anómalos, y la respuesta a incidentes define cómo afrontar y mitigar ataques. (pag.8)

El estándar ISO 27001:2022

Comenta (Watkins, 2022) que el estándar ISO 27001:2022 es una norma internacional que establece los requisitos para la creación, implementación y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). Su enfoque radica en resguardar la información sensible de una organización, gestionando eficazmente los riesgos de seguridad. Esta norma ofrece un marco integral basado en un ciclo de vida, abarcando desde la planificación hasta la mejora de los controles de seguridad. (pag.45)

Dice (Sánchez, 2019) que el proceso de implementación del ISO 27001 involucra identificar el contexto y las partes interesadas, definir compromisos de liderazgo, establecer objetivos de seguridad, implementar controles, monitorear el desempeño y buscar mejoras. Cumplir con ISO 27001:2022 demuestra el compromiso de una organización con la seguridad de la información ante socios, clientes y partes interesadas. Ayuda a gestionar los riesgos y proteger la confidencialidad, integridad y disponibilidad de la información. (pag.22)

Según (Calder, 2023) en el contexto de empresas de servicios tecnológicos, la aplicabilidad del estándar ISO 27001:2022 es especialmente relevante. Estas empresas manejan y procesan grandes volúmenes de información sensible y valiosa, lo que las convierte en objetivos potenciales de ciberataques y amenazas cibernéticas. Implementar ISO 27001 en una empresa de servicios tecnológicos puede ayudar a:

Proteger Datos Sensibles: En un entorno donde los datos son activos críticos, la norma ISO 27001 ayuda a identificar y clasificar la información sensible y valiosa. Mediante la implementación de controles de seguridad adecuados, como el cifrado de datos, el control de acceso y la segmentación de redes, las empresas de servicios tecnológicos pueden salvaguardar información confidencial, minimizando el riesgo de exposición a amenazas internas y externas. (pag.35)

Gestionar Riesgos: La norma ISO 27001 se basa en un enfoque de gestión de riesgos. Esto significa que las empresas pueden identificar los riesgos específicos que enfrentan, evaluar su impacto y probabilidad, y luego implementar medidas para mitigarlos. En el caso de empresas tecnológicas, esto podría abarcar desde vulnerabilidades de software hasta riesgos relacionados con la protección de datos de clientes y la interrupción de servicios críticos. (pag.36)

Fortalecer la Resiliencia: En un mundo digital donde los ciberataques y las interrupciones son cada vez más comunes, la norma ISO 27001 establece la necesidad de planes de respuesta a incidentes y de continuidad del negocio. Estos planes aseguran que la organización esté preparada para manejar crisis y restaurar la normalidad operativa de manera eficiente, reduciendo los impactos negativos en la operación. (pag.36)

Cumplimiento Normativo: Las empresas de servicios tecnológicos a menudo están sujetas a regulaciones estrictas sobre la privacidad de los datos y la seguridad de la información, como el GDPR en la Unión Europea. La implementación de ISO 27001 puede ayudar a demostrar el cumplimiento con estas regulaciones, al establecer medidas de seguridad y controles que se alinean con los estándares internacionales. (pag.37)

Ganar Confianza: La adopción de ISO 27001 puede marcar una diferencia significativa en la percepción de los clientes, socios y reguladores. Al obtener una certificación ISO 27001, las empresas de servicios tecnológicos pueden demostrar su compromiso con la seguridad de la información y la privacidad de los datos. Esto puede influir en la toma de decisiones de los clientes y socios comerciales, fortaleciendo las relaciones y construyendo una reputación de confiabilidad en el mercado. (pag.37)

Amenazas cibernéticas

Señala (Andrés Cosialls, 2020) que las amenazas cibernéticas son riesgos que afectan la seguridad de sistemas, redes y datos digitales. Estas amenazas buscan explotar vulnerabilidades en la seguridad para acceder a información valiosa o causar daño. Entre las amenazas cibernéticas más comunes se encuentran el malware, software malicioso que roba información; el phishing, correos fraudulentos para con el fin de obtener datos confidenciales; y el ransomware, que bloquea datos hasta que se paga un rescate. (pag.54)

También existen los ataques DDoS, que sobrecargan servicios; la inyección de código, manipulación de aplicaciones; y ataques de hombre en el medio, donde se interceptan comunicaciones. La ingeniería social manipula psicológicamente a personas para obtener información, mientras que las fugas de datos involucran la divulgación no autorizada. (pag.55)

Pentesting (Pruebas de Penetración)

Menciona (Price, 2018) que las Pruebas de Penetración, comúnmente conocidas como Pentesting, representan una estrategia fundamental en ciberseguridad para identificar y evaluar las vulnerabilidades en sistemas, redes y aplicaciones. Estas

pruebas simulan ataques controlados por profesionales de seguridad con el objetivo de detectar y corregir brechas en la seguridad antes de que los atacantes reales las aprovechen.

El Pentesting sigue un proceso que incluye varias etapas esenciales. Comienza con la fase de reconocimiento y planificación, donde se obtiene información sobre el sistema objetivo. Luego sigue la enumeración y escaneo, que involucra un análisis detallado de la infraestructura para identificar activos y servicios disponibles. En la etapa de explotación, se intenta aprovechar las vulnerabilidades descubiertas. (pag.11)

Hacking Ético

Explica (Peña, 2020) que el Ethical hacking", es una práctica legítima que involucra la evaluación de la seguridad de sistemas, redes y aplicaciones para identificar y solucionar vulnerabilidades antes de que sean explotadas por atacantes maliciosos. A diferencia de los hackers no éticos, los hackers éticos trabajan de manera profesional y autorizada para mejorar la seguridad de los sistemas. Esta actividad engloba diversas acciones como pruebas de penetración, análisis de vulnerabilidades, evaluaciones de seguridad. (pag.50)

Los hackers éticos emplean técnicas similares a las de los hackers maliciosos, pero su finalidad es fortalecer la seguridad en lugar de comprometerla, estas se llevan a cabo con el consentimiento del propietario del sistema o la red que se está evaluando, también cuentan con un profundo conocimiento de técnicas y herramientas de seguridad, así como metodologías para identificar y resolver vulnerabilidades. (pag.51)

Política de Seguridad de la Información

Según (Bertolin, 2018) que una Política de Seguridad de la Información es un conjunto de directrices esenciales que establecen el marco general para garantizar la

seguridad de la información en una organización. Esta política proporciona una guía coherente y alineada con los objetivos de seguridad, orientando las decisiones y acciones relacionadas con la protección de la información. La gestión de riesgos es un componente vital, ya que describe cómo se identifican, evalúan los riesgos de seguridad. (pag.42)

La política también regula el acceso y control a sistemas y datos, estableciendo los procedimientos de autenticación, autorización y niveles de acceso adecuados. La protección de datos es otro aspecto destacado, delineando las medidas para proteger datos sensibles a través de prácticas como el cifrado y la clasificación de información. (pag.42)

Confidencialidad, Integridad y Disponibilidad (CIA)

Confidencialidad: Según (Veiga, 2020) Este principio se refiere a la protección de la información para evitar su divulgación a personas no autorizadas. Implica garantizar que solo aquellos que tienen permiso puedan acceder a ciertos datos, evitando así fugas de información y violaciones de privacidad. Se pretende lograr mediante el control de acceso y el cifrado de datos.

Integridad: Asegura que los datos no sean alterados de manera no autorizada. Garantiza que la información permanezca precisa, completa y sin manipulaciones indebidas. Se pretende lograr mediante la implementación de medidas para prevenir la modificación no autorizada de datos y la detección temprana de cambios no autorizados.

Disponibilidad: Garantiza que la información esté disponible y accesible cuando sea necesaria por parte de los usuarios autorizados. Implica mantener la funcionalidad de sistemas y redes para evitar interrupciones no planificadas que puedan afectar la disponibilidad de los recursos y la continuidad de las operaciones. (pag.22)

Dice (Aguilar, 2021) que estos tres principios de CIA son interdependientes y forman la base de una estrategia sólida de seguridad de la información. Cuando se implementan de manera efectiva, ayudan a garantizar que la información se maneje y proteja de manera adecuada, salvaguardando los datos críticos para una empresa. (pag.24)

Cumplimiento normativo

Indica (Ruiz, 2022) que el cumplimiento normativo se refiere al proceso de asegurarse de que una organización siga y cumpla con las leyes, regulaciones y estándares relevantes en su industria o ubicación geográfica. Este proceso es fundamental para garantizar que la organización opere de manera ética y legal, y evite posibles sanciones o consecuencias adversas. (pag.45)

El cumplimiento normativo abarca varias áreas, como la privacidad de datos, la seguridad de la información, la protección al consumidor, la salud y seguridad en el trabajo, entre otros. Algunos ejemplos notables incluyen el Reglamento General de Protección de Datos, la Ley de Portabilidad y Responsabilidad de Seguros. (pag.46)

Análisis de Riesgos

Explica (Roi Naveiro Flores, 2022) que el Análisis de Riesgos es un proceso esencial que busca identificar, evaluar y gestionar los posibles riesgos que una organización podría enfrentar. Su objetivo principal es comprender y evaluar las amenazas y vulnerabilidades que podrían afectar los activos y objetivos de la organización. Este proceso implica varios pasos clave. En primer lugar, se identifican los activos valiosos de la organización, como datos, sistemas e infraestructura. (pag.55)

A continuación, se evalúan las debilidades y vulnerabilidades que podrían ser explotadas por las amenazas identificadas. Además, se estiman el posible impacto y la

probabilidad de que ocurra un riesgo. Estos factores se combinan para calcular el nivel de riesgo y priorizar las acciones a tomar. Una vez que se cuantifican los riesgos, se desarrollan estrategias de gestión que pueden incluir, evitación de los riesgos. (pag.57)

Controles de Seguridad

Comenta (Martha Romero, 2018) que los Controles de Seguridad son medidas y prácticas cruciales que las organizaciones implementan para salvaguardar sus sistemas, activos y datos contra amenazas y riesgos de seguridad. Estos controles desempeñan un papel crucial en la protección de la información y la gestión de riesgos. Los controles administrativos involucran políticas, procedimientos en seguridad para establecer prácticas seguras y manejar el acceso. Los controles físicos se centran en la protección de activos físicos. (pag.31)

Amenazas Internas y Externas

Amenazas Internas: Menciona (Soto, 2023) que estas amenazas provienen de individuos que ya tienen acceso autorizado a los sistemas y activos de la empresa, como empleados, contratistas o socios. Pueden ser intencionales o no intencionales. Ejemplos de amenazas internas intencionales incluyen el robo de datos por parte de un empleado descontento o la divulgación de información confidencial. Para abordar estas amenazas, las organizaciones deben implementar medidas de control de acceso, monitorizar el comportamiento de los empleados y aplicar políticas de uso aceptable. (pag.6)

Amenazas Externas: Estas amenazas provienen de fuentes fuera de la organización y buscan explotar vulnerabilidades en sistemas y redes para obtener acceso no autorizado. Los atacantes externos pueden ser individuos maliciosos, grupos de hackers o incluso organizaciones criminales. Contra estas amenazas, las organizaciones

deben implementar soluciones de seguridad como firewalls, sistemas de detección de intrusiones y soluciones de prevención de malware. (pag.6)

La Auditoría de Seguridad

Argumenta (Arantes, 2023) que la Auditoría de Seguridad es un proceso esencial que implica la revisión y evaluación sistemática de sistemas y procedimientos en una organización para identificar debilidades que podrían comprometer la seguridad de la información. El objetivo principal es asegurarse de que las políticas de seguridad sean cumplidas, los controles sean efectivos y se detecten problemas potenciales. (pag.65)

Este proceso involucra varios pasos clave. Comienza con la planificación, estableciendo los objetivos y el alcance de la auditoría. Luego, se recopila información sobre los sistemas y políticas de seguridad existentes. A través de la evaluación y pruebas técnicas, se identifican debilidades y vulnerabilidades. (pag.66)

La criptografía

Según (Manuel J. Prieto, 2020) la criptografía es un campo esencial en la protección de la información, enfocado en convertir datos en un formato ininteligible llamado "cifrado", que solo puede ser revertido por aquellos con la clave adecuada. Su objetivo primordial es asegurar la confidencialidad, integridad y autenticidad de los datos, salvaguardándolos de accesos no autorizados. Es importante considerar que la efectividad de la criptografía depende de su correcta implementación y de la seguridad de las claves.

Existen dos categorías principales de criptografía. La criptografía simétrica utiliza una única clave compartida entre remitente y receptor para cifrar y descifrar datos. La criptografía asimétrica, o de clave pública, emplea un par de claves: una

pública para cifrar y una privada para descifrar. Esto permite compartir claves públicas sin comprometer la privacidad. (pag.10)

La resiliencia cibernética

Menciona (Gómez, 2019) que la resiliencia cibernética se refiere a la capacidad de una organización para anticipar, resistir, adaptarse y recuperarse de los impactos de ciberataques y eventos adversos relacionados con la seguridad de la información. Implica mantener la continuidad de las operaciones y minimizar daños en situaciones de crisis. La preparación incluye implementar medidas preventivas para diversos casos.

La detección rápida es crucial para identificar incidentes y anomalías en sistemas y redes. La respuesta efectiva activa planes y procedimientos para manejar incidentes en tiempo real, minimizando el impacto. La recuperación es esencial para restablecer la operación normal y reconstruir sistemas y datos tras un ciberataque. La adaptación implica aprender de los incidentes y ajustar estrategias de seguridad para prevenir problemas similares. (pag.24)

Protección de datos personales

Explica (Álvarez, 2023) que la protección de datos personales se refiere a la salvaguardia de la información que identifica o se relaciona con individuos, preservando su privacidad y control sobre cómo se recopila, utiliza y comparte dicha información. Esta protección es esencial para garantizar la confianza de las personas y cumplir con regulaciones de privacidad. En este contexto, la recolección y tratamiento de datos personales debe ser transparente. (pag.45)

La protección de datos personales implica respetar los derechos de privacidad de las personas, permitiéndoles controlar su información y proporcionando mecanismos para ejercer esos derechos. Esto es fundamental en una era digital donde los datos

personales son cada vez más valiosos y susceptibles a mal uso. La protección de datos no solo es un requisito legal, sino también un componente crucial para mantener la confianza. (pag.46)

Política de Respuesta a Incidentes

Dice (Wilson, 2019) que una política de respuesta a incidentes es un conjunto crucial de directrices que una organización establece para gestionar incidentes de seguridad de la información de manera eficaz. Su objetivo principal es reducir el impacto de los incidentes, minimizar riesgos y garantizar una respuesta organizada y coordinada. Esta política involucra diversas etapas esenciales. La preparación establece roles y responsabilidades del equipo de respuesta, protocolos de comunicación y métodos de detección de incidentes. (pag.4)

La contención y mitigación define acciones concretas para limitar el alcance y minimizar los efectos del incidente, como desconectar sistemas afectados y aplicar medidas correctivas. La notificación establece cómo y cuándo se debe informar a las partes relevantes, como afectados y reguladores, siguiendo pautas legales. (pag.4)

Cumplimiento de Regulaciones

Argumenta (Jackson, 2019) que el cumplimiento de regulaciones se refiere a la adhesión de una organización a las normativas y leyes pertinentes en su industria o jurisdicción. Estas regulaciones pueden abarcar aspectos como seguridad de la información, privacidad de datos, prácticas comerciales éticas y más. Cumplir con estas regulaciones es esencial para evitar sanciones legales, mantener la confianza del público y operar de manera ética. El cumplimiento implica conocer y comprender las regulaciones relevantes, implementar prácticas y medidas para cumplirlas, y llevar a cabo auditorías periódicas para asegurarse de que se mantenga la conformidad. (pag.11)

Gestión de Incidentes de Seguridad

Comenta (Tejada, 2023) que la gestión de incidentes de seguridad se refiere a la planificación, coordinación y respuesta ante eventos que afectan la seguridad de la información y los sistemas de una organización. El objetivo principal es minimizar el impacto de los incidentes, restaurar la normalidad operativa y prevenir futuras ocurrencias similares. Esta gestión implica varias fases esenciales. La preparación involucra la creación de políticas y procedimientos, la asignación de roles y la formación de equipos de respuesta. La detección y evaluación se enfoca en identificar y analizar incidentes para comprender su alcance y gravedad. (pag.45)

MARCO METODOLÓGICO

Para abordar el análisis y diseño del modelo de gestión de seguridad de la información basado en el estándar ISO 27001:2022 para la Empresa Pc Soluciones, se empleará una combinación de métodos deductivos e inductivos. Estos métodos permitirán establecer una base teórica sólida y recopilar datos empíricos que respalden la implementación exitosa del modelo de seguridad.

En la fase deductiva, se realizará una revisión bibliográfica exhaustiva sobre la seguridad de la información, el estándar ISO 27001:2022 y su aplicabilidad en empresas de servicios tecnológicos. Esta revisión permitirá comprender los conceptos

fundamentales, identificar buenas prácticas y establecer los fundamentos teóricos para el diseño del modelo de seguridad. A partir de esta revisión, se derivarán hipótesis iniciales que guiarán la investigación empírica.

En la fase inductiva, el objetivo principal es recopilar datos empíricos que reflejan la situación actual de seguridad de la información en la empresa y sus necesidades específicas. Para ello, se utilizará una combinación de métodos, incluida una encuesta dirigida a miembros de la empresa con conocimientos en seguridad de la información.

Encuesta:

La encuesta se realizó con el fin de obtener percepciones y experiencias concretas sobre la seguridad de la información y la necesidad de un modelo de gestión basado en ISO 27001:2022. Las preguntas están diseñadas para comprender la magnitud de la amenaza de ataques de malware, además de la opinión sobre su relevancia en la seguridad de la empresa.

¿Su empresa ha experimentado pérdida de datos debido a ataques de malware?

¿Está familiarizado con el estándar ISO 27001:2022 y sus requisitos?

¿Cree que la implementación de un modelo de gestión de seguridad basado en ISO 27001:2022 sería beneficiosa para su empresa?

¿Considera importante la capacitación del personal para prevenir ataques cibernéticos?

¿Ha notado comportamientos sospechosos en los sistemas de la empresa que podrían indicar posibles ataques de malware?

Análisis de Datos:

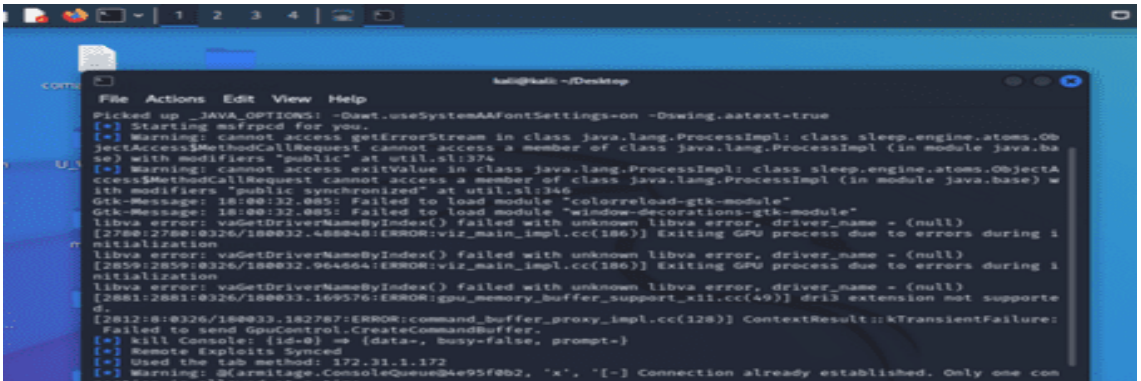
Los datos recopilados a través de la encuesta se analizarán cualitativamente para identificar patrones, tendencias y opiniones clave. Estos hallazgos ayudarán a contextualizar la necesidad y el potencial impacto de la implementación del modelo de seguridad basado en ISO 27001:2022 en la Empresa.

La combinación de los métodos deductivos e inductivos en este marco metodológico permitirá desarrollar una comprensión integral de la situación actual de seguridad de la información en la empresa, fundamentar decisiones con base en evidencia teórica y empírica, y diseñar un modelo de gestión de seguridad de la información efectivo y adaptado a las necesidades específicas de Pc Soluciones.

Resultados

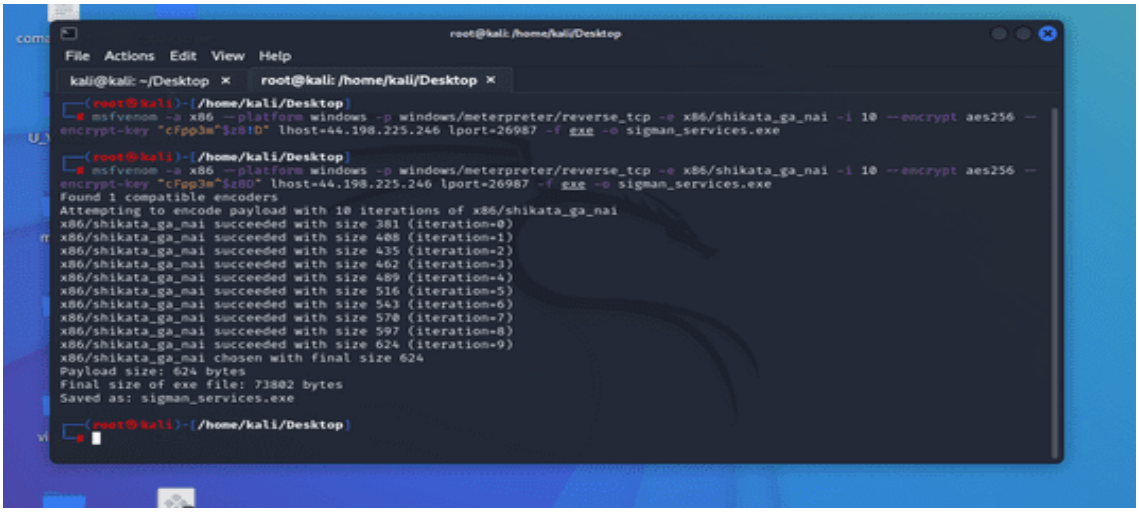
En las siguientes imágenes se puede observar el proceso del uso de la herramienta Cobalt Strike la cual sirve para realizar penetración y evaluación de seguridad. se pretende simular un ataque y evaluar la efectividad de los controles de seguridad implementados en el Sistema de Gestión de Seguridad de la Información.

Ilustración 1. Iniciación del Cobalt strike.



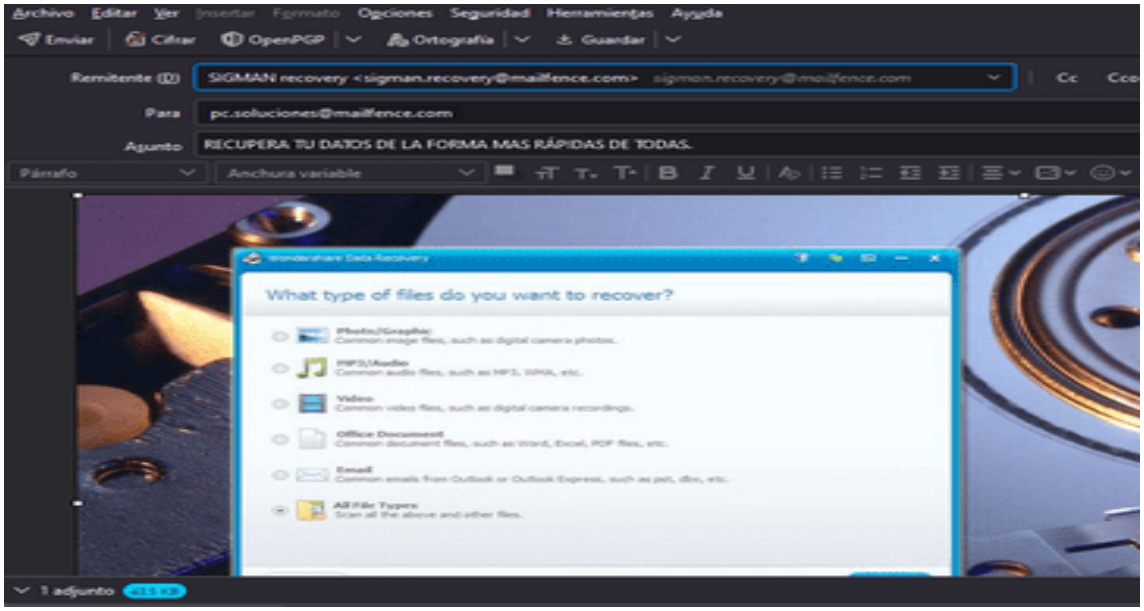
Elaborado por: Erick Alexis Fuentes Pozo

Ilustración 2. En esta línea de código se establece una conexión con un servidor remoto utilizando una dirección IP específica y un puerto en modo de escucha. Esta acción procederá a la creación de un archivo ejecutable llamado "sigman_services.exe", el cual es un virus con una intención perjudicial.



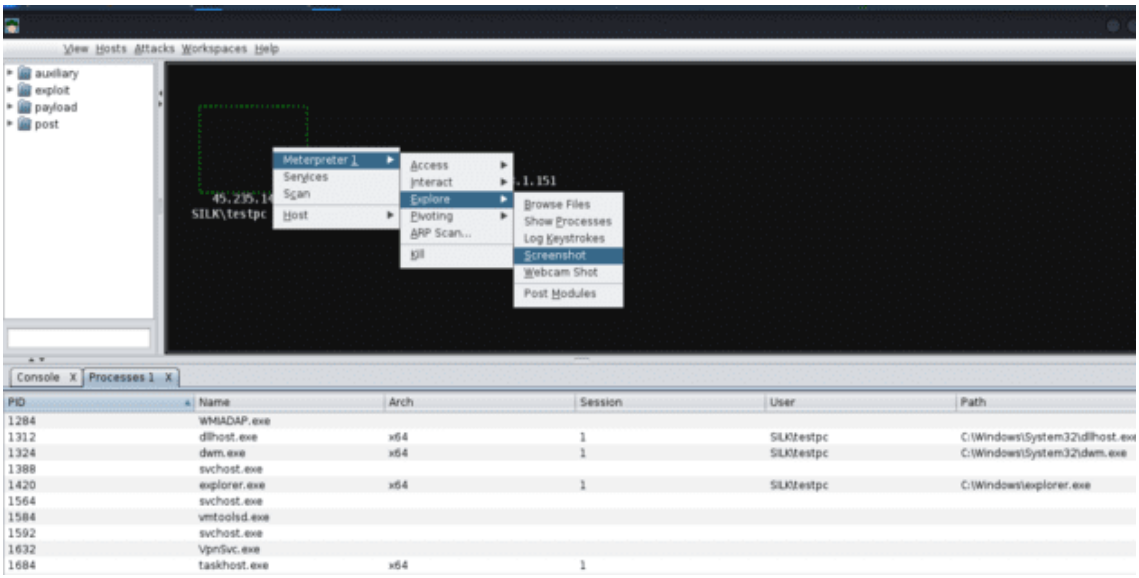
Elaborado por: Erick Alexis Fuentes Pozo

Ilustración 3. A través de un servidor de correo privado se utilizaba una estrategia engañosa que implicaba realizar una promoción de un software de recuperación de



Elaborado por: Erick Alexis Fuentes Pozo

Ilustración 4. En la computadora objetivo, se estableció una sesión de Metasploit Meterpreter, el cual es un framework de exploración que brinda una variedad de capacidades de espionaje. Podemos acceder a opciones que nos permiten supervisar su sistema, como visualizar los procesos en ejecución, explorar archivos, capturar la pantalla de la computadora accediendo así a toda su información.



Elaborado por: Erick Alexis Fuentes Pozo

DISCUSIÓN DE RESULTADOS

En primer lugar, se ejecutó la herramienta Cobalt Strike, aprovechando una vulnerabilidad en un puerto abierto de la red de la empresa. Esto permitió a los atacantes establecer una conexión y acceder a la interfaz gráfica de Cobalt Strike, lo que indica una grave vulnerabilidad en la infraestructura de seguridad de la empresa.

Posteriormente, se procedió a crear un virus, denominado "sigman_services.exe", el cual se configuró para conectarse a una dirección IP

específica y un puerto en modo de escucha. Este virus se distribuyó a través de un servidor de correo privado, utilizando una estrategia de ingeniería social efectiva. Esta acción refleja una seria deficiencia en los filtros y políticas de seguridad de correo electrónico de la empresa.

Una vez que el virus se infiltró en la computadora de la víctima, los atacantes obtuvieron un control total. Tuvieron la capacidad de espiar los procesos en ejecución, explorar archivos y tomar capturas de pantalla. Además, pudieron activar la cámara de la máquina, lo que representa una violación significativa de la privacidad y la seguridad.

Los resultados de esta práctica son motivo de preocupación y resaltan una serie de debilidades críticas en la seguridad de la empresa donde se refleja una falta de filtros y políticas de seguridad efectivas de la empresa debido a que los atacantes pudieron ejercer un control total, accediendo a información confidencial.

Por lo cual se destaca la necesidad imperante de desarrollar un modelo de gestión de seguridad de la información basado en el estándar ISO 27001:2022. Este marco proporcionará a la empresa una estructura sólida para abordar la gestión de riesgos, la concienciación en seguridad, la respuesta a incidentes y la mejora continua de la seguridad de la información y de esta forma proteger adecuadamente los activos de la empresa

CONCLUSIONES

Se ha comprobado que el estándar ISO 27001:2022 puede ser adaptado de manera efectiva a la realidad operativa de la Empresa Pc Soluciones. La identificación de procesos y activos críticos para la empresa ha permitido personalizar el modelo de seguridad de la información de manera adecuada, asegurando que se ajuste a las necesidades específicas de la organización.

La base teórica proporcionada sobre seguridad de la información y el estándar ISO 27001:2022 es esencial para comprender la importancia de la gestión de la seguridad de la información en empresas que ofrecen servicios tecnológicos como Pc Soluciones. Esta comprensión facilita la aceptación y compromiso de los empleados y directivos en la implementación del modelo.

La implementación de un modelo de gestión de seguridad de la información según ISO 27001:2022 envía un mensaje claro a los clientes y socios comerciales de Pc Soluciones. Demuestra un compromiso firme con la protección de la información confidencial y la privacidad de los datos, lo que, a su vez, mejora la confianza y la percepción de la empresa en el mercado.

RECOMENDACIONES

- Se recomienda desarrollar un plan de implementación detallado y realista que incluya un cronograma claro y asignación de responsabilidades para garantizar una transición suave hacia el modelo de seguridad ISO 27001:2022.

- Se sugiere proporcionar capacitación y concienciación a todo el personal de Pc Soluciones para garantizar que comprendan la importancia de la seguridad de la información y su papel en su implementación.
- Se sugiere realizar auditorías internas periódicas para verificar el cumplimiento de los controles y procedimientos de seguridad, identificando áreas de mejora.

REFERENCIAS

Aguilar, L. J. (2021). Un futuro hiperconectado: 5G, inteligencia artificial, Big Data, Cloud, Blockchain y ciberseguridad. Madrid. Obtenido de https://www.google.com.ec/books/edition/Internet_de_las_cosas/HE1OEAAAQB

AJ?hl=es-419&gbpv=1&dq=Confidencialidad,+Integridad+y+Disponibilidad+(CIA)&pg=PA320&printsec=frontcover

Álvarez, J. L. (2023). Tratado de protección de datos personales. España. Obtenido de https://www.google.com.ec/books/edition/Tratado_de_protecci%C3%B3n_de_datos_personal/tTC5zwEACAAJ?hl=es-419

Andrés Cosialls, J. G. (2020). ciberseguridad y desarrollo sostenible. España. Obtenido de https://www.google.com.ec/books/edition/Sector_agroalimentario_Ciberseguridad_y/3BE5EAAAQBAJ?hl=es-419&gbpv=0

Arantes, S. c. (2023). Auditoría de seguridad informática. Madrid. Obtenido de https://www.google.com.ec/books/edition/Auditor%C3%ADa_de_seguridad_inform%C3%A1tica/VcK_EAAAQBAJ?hl=es-419&gbpv=0

Bertolin, J. (2018). Seguridad de la información. Redes, informática y sistemas de información. Madrid. Obtenido de https://www.google.com.ec/books/edition/Seguridad_de_la_informaci%C3%B3n_Redes_infor/_z2GcBD3deYC?hl=es-419&gbpv=1&dq=Pol%C3%ADtica+de+Seguridad+de+la+Informaci%C3%B3n&pg=PA42&printsec=frontcover

Calder, A. (2023). Cyber Essentials: una guía para las certificaciones Cyber Essentials y Cyber Essentials Plus. New York. Obtenido de https://www.google.com.ec/books/edition/Cyber_Essentials_A_guide_to_the_Cyber_Es/dpLKEAAAQBAJ?hl=es-419&gbpv=0

Federico Hurtado, R. B. (2018). Sistema de gestión integral. Una sola gestión, un solo equipo. Madrid. Obtenido de https://www.google.com.ec/books/edition/Sistema_de_gesti%C3%B3n_integral_Una_sola_ge/15nVyh1Fn6MC?hl=es-419&gbpv=1&dq=Sistema+de+Gesti%C3%B3n+de+Seguridad+de+la+Informaci%C3%B3n+(SGSI)&pg=PA31&printsec=frontcover

Gómez, M. O. (2019). En busca de un modelo de resiliencia cibernética basado en las experiencias de la OTAN. España. Obtenido de https://www.google.com.ec/books/edition/En_busca_de_un_modelo_de_resilienc ia_cib/0Y2-DwAAQBAJ?hl=es-419&gbpv=0

Jackson, C. (2019). PLAN GENERAL PARA EL CUMPLIMIENTO DE LA REGULACIÓN DE LA PROTECCIÓN DELOS DATOS. España. Obtenido de https://www.google.com.ec/books/edition/PLAN_GENERAL_PARA_EL_CUMP LIMIENTO_DE_LA/R2O-DwAAQBAJ?hl=es-419&gbpv=1&dq=Cumplimiento+de+Regulaciones&printsec=frontcover

Lewis, E. (2020). Guía completa para principiantes aprende todo de la ciberseguridad. Madrid. Obtenido de https://www.google.com.ec/books/edition/Ciberseguridad/7ruHzQEACAAJ?hl= es-419

Manuel J. Prieto, M. J. (2020). Historia de la criptografía. Madrid. Obtenido de https://www.google.com.ec/books/edition/Historia_de_la_criptograf%C3%ADa/ GJDHDwAAQBAJ?hl=es-419&gbpv=1&dq=La+criptograf%C3%ADa&printsec=frontcover

Martha Romero, G. F. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. Madrid. Obtenido de https://www.google.com.ec/books/edition/INTRODUCCI%C3%93N_A_LA_SEGURIDAD_INFORM%C3%81TIC/5Z9yDwAAQBAJ?hl=es-419&gbpv=0

Peña, C. (2020). Entorno de pruebas - Sistemas vulnerables - Uso de Nmap. Madrid. Obtenido de https://www.google.com.ec/books/edition/Hacking_Etico_Vol_1/mqEJEAAAQBAJ?hl=es-419&gbpv=1&dq=Hacking+%C3%89tico&printsec=frontcover

Price, M. (2018). Guía Completa Del Principiante a la Piratería Informática y Pruebas De Penetración. Madrid. Obtenido de https://www.google.com.ec/books/edition/Hacking/VU56swEACAAJ?hl=es-419

Roi Naveiro Flores, D. R. (2022). Análisis de riesgos. Madrid. Obtenido de https://www.google.com.ec/books/edition/An%C3%A1lisis_de_riesgos/cGJwEAAAQBAJ?hl=es-419&gbpv=1&dq=An%C3%A1lisis+de+Riesgos&printsec=frontcover

Ruiz, J. A. (2022). Derecho del cumplimiento normativo y análisis regulatorio de la empresa. España. Obtenido de https://www.google.com.ec/books/edition/Derecho_del_cumplimiento_normativo_y_an/8Gx4zwEACAAJ?hl=es-419

Sánchez, M. B. (2019). Ingeniería de instrumentación de plantas de proceso. Madrid. Obtenido de https://www.google.com.ec/books/edition/Ingenier%C3%ADa_de_instrumentaci%C3%B3n_de_plant/eGGNDwAAQBAJ?hl=es-419&gbpv=0

Soto, M. G. (2023). Ciberinteligencia de la amenaza en entornos corporativos. España. Obtenido de https://www.google.com.ec/books/edition/Ciberinteligencia_de_la_amenaza_en_entor/3OPGEAAAQBAJ?hl=es-419&gbpv=0

Tejada, E. C. (2023). Gestión de incidentes de seguridad informática. IFCT0109. Madrid. Obtenido de https://www.google.com.ec/books/edition/Gesti%C3%B3n_de_incidentes_de_seguridad_info/rxPLEAAAQBAJ?hl=es-419&gbpv=1&dq=Gesti%C3%B3n+de+Incidentes+de+Seguridad&printsec=frontcover

Veiga, J. M. (2020). Curso superior en dirección de seguridad privada. Madrid. Obtenido de https://www.google.com.ec/books/edition/Asesor_Gestor_en_seguridad_privada_integ/suXJDwAAQBAJ?hl=es-419&gbpv=0

Watkins, S. (2022). ISO/IEC 27001:2022 - An introduction to information security and the ISMS standard. New york. Obtenido de https://www.google.com.ec/books/edition/ISO_IEC_27001_2022_An_introduction_to_in/LtWbEAAAQBAJ?hl=es-419&gbpv=1&dq=El+est%C3%A1ndar+ISO+27001:2022&printsec=frontcover

ANEXO 1

ENCUESTAS

1. ¿Su empresa ha experimentado pérdida de datos debido a ataques de malware?

SI  NO 

2. ¿Está familiarizado con el estándar ISO 27001:2022 y sus requisitos?

SI ☐ NO ■

3. ¿Cree que la implementación de un modelo de gestión de seguridad basado en ISO 27001:2022 sería beneficiosa para su empresa?

SI ■ NO ☐

4. ¿Considera importante la capacitación del personal para prevenir ataques cibernéticos?

SI ■ NO ☐

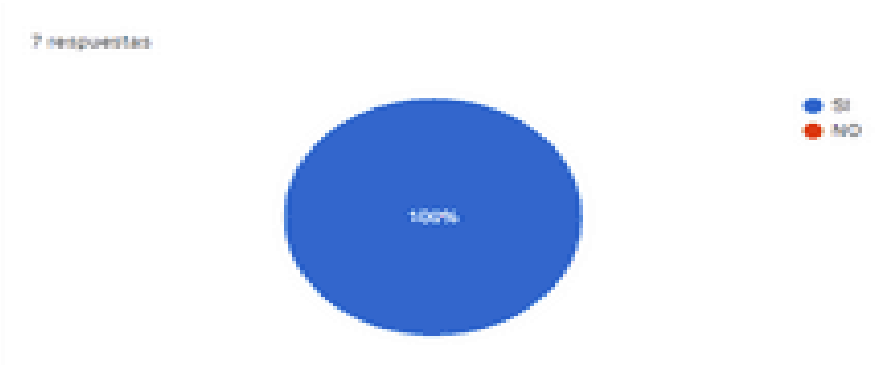
5. ¿Ha notado comportamientos sospechosos en los sistemas de la empresa que podrían indicar posibles ataques de malware?

SI ■ NO ☐

RESULTADOS DE LAS ENCUESTAS

1. **¿Su empresa ha experimentado pérdida de datos debido a ataques de malware?**

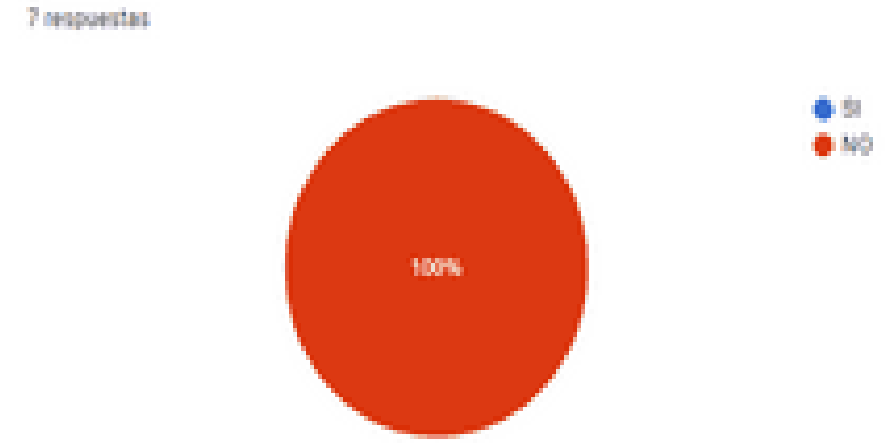
Se puede concluir que el total de personas encuestadas mencionan que si han experimentado perdidas de información debido a ataques maliciosos ejecutados por ciberdelincuentes.



Elaborado por: Erick Alexis Fuentes Pozo

2. ¿Está familiarizado con el estándar ISO 27001:2022 y sus requisitos?

Como resultado se obtuvo que el total de personas encuestadas afirman que no han conocen a fondo sobre el funcionamiento del estándar ISO 27001:2022 o lo requisitos para ponerlos en práctica.



Elaborado por: Erick Alexis Fuentes Pozo

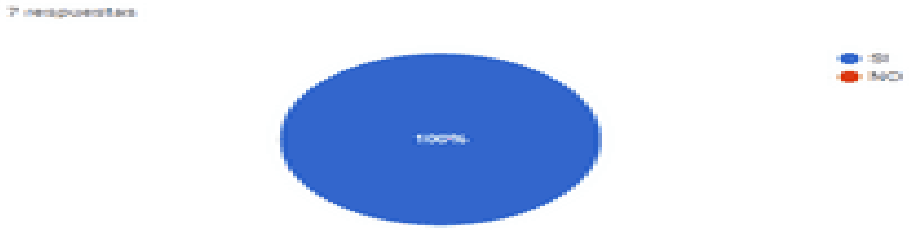
3. ¿Cree que la implementación de un modelo de gestión de seguridad basado en ISO 27001:2022 sería beneficiosa para su empresa?

Como resultado se obtuvo que el total de personas encuestadas afirman que, si este estándar proporciona un enfoque sólido ya que podría ayudar a fortalecer la protección de los activos de la empresa, reducir riesgos de seguridad.

Elaborado por: Erick Alexis Fuentes Pozo

4. ¿Considera importante la capacitación del personal para prevenir ataques cibernéticos?

Se puede concluir que el total de personas encuestadas mencionan que, si es importante la capacitación del personal porque, en muchos casos, los ataques cibernéticos comienzan con errores humanos.



Elaborado por: Erick Alexis Fuentes Pozo

5. ¿Ha notado comportamientos sospechosos en los sistemas de la empresa que podrían indicar posibles ataques de malware?

Como resultado se obtuvo que el total de personas encuestadas afirman que esta herramienta es esencial para evitar estos ataques a la seguridad del sistema de su

Elaborado por: Erick Alexis Fuentes Pozo

ANEXOS 2

OFICIO A EMPRESA

Babahoyo, 16 de agosto del 2023

Sr(a)
FRANCISCO JAVIER AVILES ARCOS
GERENTE DE LA EMPRESA PC SOLUCIONES
En su despacho.

De mis consideraciones:

Yo: **FUENTES POZO ERICK ALEXIS**, con cédula de identidad 125009547-6, estudiante de la Universidad Técnica de Babahoyo de la Facultad de Administración, finanzas e informática, carrera de **SISTEMAS DE INFORMACION**, matriculado(a) en el proceso de titulación periodo JUNIO 2023 – OCTUBRE 2023, le solicito a usted de la manera más comedida se sirva autorizar a quien corresponda se proceda otorgarme el permiso respectivo para realizar mi estudio de caso denominado **ANÁLISIS Y DISEÑO DE UN MODELO DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN EL ESTANDAR ISO 27001:2022 PARA LA EMPRESA PC SOLUCIONES DE LA CIUDAD DE BABAHOYO**, el cual es requisito indispensable para poder titularme.

Esperando una respuesta favorable quedo de usted muy agradecido(a).

Muy atentamente

ERICK ALEXIS FUENTES POZO
1250095476

Recibido
16/08/2023

PC Soluciones

ANEXOS 3

OFICIO A DECANO

Babahoyo, 16 de agosto del 2023

Magister
Eduardo Galeas Guijarro
DECANO DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA
En su despacho.

Reciba un cordial saludo de quienes conformamos **ACTIVIDADES DE MANTENIMIENTO Y REPARACIÓN DE MAQUINARIA DE INFORMÁTICA Y EQUIPO PERIFÉRICO CONEXO, VENTA AL POR MENOR DE COMPUTADORAS** de la ciudad de **BABAHOYO** del cantón **LOS RÍOS**

Por medio de la presente me dirijo a usted para comunicarle que se ha **AUTORIZADO** al estudiante **ERICK ALEXIS FUENTES POZO** de la carrera de **SISTEMAS DE INFORMACION** de la Facultad de Administración Finanzas e Informática de la Universidad Técnica de Babahoyo para que realice el estudio de caso con el tema: **ANÁLISIS Y DISEÑO DE UN MODELO DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN EL ESTANDAR ISO 27001:2022 PARA LA EMPRESA PC SOLUCIONES DE LA CIUDAD DE BABAHOYO,** el cual es requisito indispensable para poder titularse.

Sin otro particular me suscribo de usted

Atentamente

JAVIER FRANCISCO AVILES ARCOS
1716711435
pcsoluciones2005@gmail.com , 0990640528