REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

“PLAN DE SEGURIDAD INFORMATICO BASADO EN LA NORMA ISO/IEC 27002:2022 PARA LA EMPRESA ADLINK S.A. DE LA PROVINCIA DE IMBABURA”.

Trabajo de Investigación para la obtención del Título de Magister en Computación Mención Seguridad Informática

AUTOR:

Maribel Jacqueline Medina Picuasi

DIRECTOR:

MSc. Evelin Guadalupe Enríquez Huaca

Ibarra, junio 2024

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

DIRECCIÓN DE BIBLIOTECA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	1003357900		
APELLIDOS Y NOMBRES	Medina Picuasi Maribel Jacqueline		
DIRECCIÓN	Av. La Gasca y Alejandro Andrade		
EMAIL	mjmedinap@utn.edu.ec		
TELÉFONO FIJO	X	**TELÉFONO MÓVIL:**	0939896002

DATOS DE LA OBRA		
TÍTULO:	PLAN DE SEGURIDAD INFORMATICO BASADO EN LA NORMA ISO/IEC 27002:2022 PARA LA EMPRESA ADLINK S.A. DE LA PROVINCIA DE IMBABURA	
AUTOR (ES):	Medina Picuasi Maribel Jacqueline	
FECHA: DD/MM/AAAA	26/06/2024	
SOLO PARA TRABAJOS DE GRADO		
PROGRAMA:	☐ **PREGRADO**	☒ **POSTGRADO**
TITULO POR EL QUE OPTA:	Magíster en Computación con mención en Seguridad Informática	
ASESOR /DIRECTOR:	MSc. Evelin Guadalupe Enríquez Huaca, PhD. Yoo Sang Guun	

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 26 días del mes de junio de 2024.

EL AUTOR: 

Firma

Nombre: Maribel Jacqueline Medina Picuasi

APROBACIÓN DEL TUTOR

Yo, MSc. Evelin Enríquez Huaca, en calidad de directora de la tesis titulada: “Plan de seguridad informático basado en la Norma ISO/IEC 27002:2022 para la empresa ADLINK S.A. de la provincia de Imbabura.” de autoría de la Ing. Maribel Jacqueline Medina Picuasi, para optar por el grado de Magister en Computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que designe.

En la ciudad de Ibarra, a los 26 días del mes de junio de 2024.

Lo certifico

MSc. Evelin Guadalupe Enríquez Huaca

DIRECTORA DE TESIS

AGRADECIMIENTO

A la Gloriosa Universidad Técnica del Norte; y a los profesionales que hicieron posible la apertura de la maestría. A los maestros que con su conocimiento y experticia han sabido dirigir el aprendizaje a nuevos horizontes sembrando la semilla de innovación en nuestra vida profesional. A mis padres y hermanos por su cariño y apoyo en el trascurso de mi vida. A mi directora MSc. Evelin Enríquez Huaca y a mi asesor PhD. Yoo Sang Guun por su tiempo, paciencia y conocimientos para la elaboración de este proyecto. A mis amigos que con su respaldo y ánimo constante han sabido impulsar la meta tan anhelada. A todos un agradecimiento sincero y fraterno.

Jacqueline Medina

INDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSTGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

PLAN DE SEGURIDAD INFORMATICO BASADO EN LA NORMA ISO/IEC 27002:2022 PARA LA EMPRESA ADLINK S.A. DE LA PROVINCIA DE IMBABURA

Autor: Maribel Jacqueline Medina Picuasi

Directora: MSc. Evelin Enríquez Huaca

Año: 2024

RESUMEN

El presente trabajo tiene como finalidad desarrollar un plan de seguridad informático para la empresa ADLINK S.A, con el objetivo de salvaguardar la información de los activos críticos identificados, inicialmente se realiza una encuesta, la misma que permite conocer la situación actual de la empresa en cuestión de seguridad de información, dando como resultado una aplicación baja de controles de seguridad informática. La metodología aplicada es Magerit, la misma que permite a través de sus fases identificar los activos críticos y de mayor relevancia, la evaluación de riesgos, amenazas y vulnerabilidades. Una vez realizado el estudio de riesgos se realiza un Plan de Seguridad Informático basado en la Norma ISO/IEC 27002:2022, que incluye pasos y actividades específicas para mejorar la seguridad informática de ADLINK S.A, el plan proporciona una guía clara y estructurada para implementar medidas de seguridad eficientes y mitigar los riesgos identificados. El diseño del Plan de Seguridad Informático basado en la Norma ISO/IEC 27002:2022 demuestra el compromiso y responsabilidad de ADLINK S.A. con las mejores prácticas y estándares internacionales en seguridad de la información. El utilizar la última versión hace que la empresa tenga un marco sólido y

actualizado en materia de seguridad de información brindando, confianza a sus clientes y salvaguardando su activo más preciado que es la información.

Palabras clave: plan de seguridad informático, riesgos, vulnerabilidades, norma, ISO 27002.

ABSTRACT

The purpose of this work is to develop an information security plan for the company ADLINK S.A., with the aim of safeguarding the information of the identified critical assets. Initially, a survey is conducted to assess the current situation of the company in terms of information security, resulting in a low implementation of computer security controls. The applied methodology is Magerit, which allows the identification of critical and most relevant assets, risk assessment, threats, and vulnerabilities through its phases. Once the risk study is completed, an Information Security Plan based on ISO/IEC 27002:2022 is developed, which includes specific steps and activities to improve the computer security of ADLINK S.A. The plan provides a clear and structured guide to implementing efficient security measures and mitigating identified risks. The design of the Information Security Plan based on ISO/IEC 27002:2022 demonstrates the commitment and responsibility of ADLINK S.A. to the best practices and international standards in information security. Using the latest version ensures that the company has a solid and updated framework in information security, providing confidence to its customers and safeguarding its most precious asset, which is information.

Keywords: computer security plan, risks, vulnerabilities, standard, ISO 27002.

CAPITULO I

EL PROBLEMA

1.1. Planteamiento del Problema

La creciente dependencia de las organizaciones en entornos digitales y la constante evolución de las amenazas cibernéticas han destacado la imperiosa necesidad de implementar medidas efectivas de seguridad informática. En este contexto, la empresa ADLINK S.A., proveedora de servicios de internet en la provincia de Imbabura, se encuentra expuesta a diversos riesgos, amenazas y vulnerabilidades que podrían comprometer la confidencialidad, integridad y disponibilidad de la información crítica que maneja.

El presente trabajo de investigación busca abordar la problemática de seguridad informática en ADLINK S.A. a través de un enfoque integral fundamentado en la Norma ISO/IEC 27002:2022. La ausencia de un plan de seguridad informática personalizado y bien estructurado según los requerimientos específicos de la organización representa una brecha significativa que podría exponerla a vulnerabilidades en la gestión de sus activos informáticos.

En primer lugar, se llevará a cabo un diagnóstico preliminar de la seguridad informática de ADLINK S.A. para identificar las áreas susceptibles de mejora y los posibles puntos de vulnerabilidad. Esta evaluación proporcionará una visión clara del estado actual de la seguridad dentro de la empresa, lo que permitirá establecer los cimientos para futuras acciones correctivas.

La metodología MAGERIT fue utilizada por la organización para llevar a cabo la caracterización y análisis de los riesgos, amenazas y vulnerabilidades relacionados con su infraestructura informática. Este enfoque riguroso permitió una evaluación detallada de los riesgos potenciales, lo que a su vez facilitó la selección de medidas de seguridad adecuadas y la asignación eficiente de recursos para su implementación. De esta manera, la empresa pudo

fortalecer su postura de seguridad y reducir el riesgo de posibles incidentes.

Finalmente, se desarrollará un Plan de Seguridad Informática específico para ADLINK S.A., detallando los pasos y actividades necesarios para fortalecer la protección de la información sensible. Este plan estará alineado con las directrices establecidas en la Norma ISO/IEC 27002:2022, Ofreciendo un sólido marco internacionalmente reconocido para la implementación de medidas de seguridad efectivas.

La ejecución efectiva de este plan de acción no solo reforzará la posición de seguridad de ADLINK S.A., sino que también ayudará a preservar la confianza de los clientes y garantizar la continuidad de los servicios de internet proporcionados por la empresa en la provincia de Imbabura.

1.2. Interrogantes de la investigación

- ¿Cuál es el diagnóstico preliminar de la seguridad informática de la empresa ADLINK S.A. mediante inspecciones de campo?
- ¿Cómo generar un Plan de Seguridad Informático basado en las Normas ISO 27002:2022, detallando los pasos y actividades a seguir para la empresa ADLINK S.A. de la provincia de Imbabura?

1.3. Objetivo de la investigación

1.3.1. Objetivo general

Diseñar un Plan de Seguridad Informático basado en la Norma ISO/IEC 27002:2022 para la empresa ADLINK S.A. de la provincia de Imbabura.

1.3.2. Objetivos específicos

- Realizar un diagnóstico preliminar de la seguridad informática de la empresa ADLINK S.A mediante inspecciones de campo
- Evaluar los riesgos, amenazas y vulnerabilidades informáticos a través, de la metodología MAGERIT.

- Elaborar un Plan de Seguridad Informático basado en las Normas ISO 27002:2022, detallando los pasos y actividades a seguir para la empresa ADLINK S.A. de la provincia de Imbabura.

1.4. Justificación

Este trabajo de investigación surge de la necesidad imperante de abordar las crecientes amenazas cibernéticas que enfrentan las organizaciones en la era digital actual. En particular, la empresa ADLINK S.A., dedicada a la provisión de servicios de internet en la provincia de Imbabura, se encuentra en un contexto altamente dinámico y vulnerable, donde la seguridad de la información es crucial para garantizar la confianza de sus clientes y la continuidad de sus operaciones.

La importancia estratégica de la seguridad informática en la actualidad se ve acentuada por la naturaleza crítica de la información que maneja ADLINK S.A., incluyendo datos de sus clientes y operaciones propias. La falta de un plan de seguridad informático integral adaptado a las particularidades de la organización deja a la empresa expuesta a riesgos significativos, como pérdida de datos, interrupciones en los servicios, y deterioro de la reputación empresarial.

La elección de la Norma ISO/IEC 27002:2022 como marco de referencia para el desarrollo del plan de seguridad se justifica por su reconocimiento internacional. La aplicación de este estándar permitirá a ADLINK S.A. establecer controles y procedimientos robustos, alineados con las mejores prácticas de la industria, para mitigar los riesgos y garantizar un entorno seguro para la información crítica.

El diagnóstico preliminar, la evaluación de riesgos mediante la metodología MAGERIT y la posterior elaboración del plan de seguridad, no solo abordarán las vulnerabilidades actuales de la empresa, sino que, también sentarán las bases para una cultura de seguridad informática continua. Además, la ejecución de esta investigación no solo

beneficiará a ADLINK S.A., sino que también contribuirá al cuerpo de conocimientos en el área de seguridad informática, proporcionando un caso de estudio valioso que puede ser referente para otras organizaciones que buscan fortalecer su seguridad en un entorno digital cada vez más complejo y desafiante.

La línea de investigación se basará en el proyecto de seguridad informática mediante el diseño de un plan informático de seguridad de la información basada en la norma ISO/IEC 27002:2022.

CAPITULO II

MARCO REFERENCIAL

2.1. Antecedentes

Tsung-Han et al., (2016) en su artículo publicado en una revista especializada, el autor resalta la importancia crítica de un Sistema de Gestión de Seguridad de la Información (SGSI). El principal objetivo de esta labor consistió en establecer un sistema completo de gestión de seguridad de la información, diseñado de manera específica para afrontar los desafíos previamente detectados. Para lograrlo, se aplicaron enfoques y normativas actualizadas, con el fin de asegurar la protección adecuada de los activos de información y mitigar los riesgos potenciales.

Dada la trascendental relevancia de evaluar el impacto en los negocios y valorar los riesgos en este ámbito, se llevaron a cabo minuciosas evaluaciones para seleccionar las metodologías más apropiadas para esta investigación. Este enfoque metodológico permitió identificar de manera precisa y exhaustiva los riesgos potenciales y sus posibles impactos en las operaciones del negocio. Además, facilitó la adopción de medidas preventivas y correctivas efectivas para mitigar estos riesgos y certificar la resguardo adecuado de los activos de información de la organización.

Al desarrollar un sistema integrado de gestión de seguridad de la información basado en enfoques y estándares contemporáneos, la investigación contribuyó significativamente al fortalecimiento de la postura de seguridad de la empresa y a la protección de sus activos críticos. Este enfoque unificado proporcionó una base sólida para la implementación de prácticas de seguridad de vanguardia y la mejora continua del SGSI en línea con las necesidades y desafíos cambiantes del entorno empresarial actual.

Huamani (Huamani, 2021) en su estudio realizado en la Corte Superior de Justicia de Lima tuvo como propósito identificar los riesgos y vulnerabilidades existentes, Con el

propósito último de instaurar un plan integral de Seguridad Informática en la institución, se ha tomado como referencia la normativa internacional ISO/IEC 27002:2013. Esta norma establece políticas y directrices destinadas a mejorar el nivel de seguridad de la información y a fomentar una cultura adecuada en este ámbito. Para obtener un diagnóstico preciso de la situación tecnológica, se empleó la técnica de encuesta para recabar información sobre las fallas recurrentes en los sistemas informáticos, lo cual facilitó la evaluación de la necesidad de implementar dicho plan de seguridad.

Los resultados obtenidos de la encuesta han puesto de manifiesto diversas deficiencias en materia de seguridad informática en la institución. Se ha identificado la ausencia de una política interna de seguridad informática, la falta de controles permanentes en la infraestructura tecnológica y un desconocimiento generalizado sobre la normativa ISO 27002:2013. Ante la frecuencia de vulnerabilidades y riesgos en los sistemas de información de la Corte Superior de Justicia de Lima, es crucial implementar políticas y estrategias apropiadas para hacer frente de manera efectiva a posibles eventualidades o ataques futuros. Se reconoce la importancia crítica de la información para cualquier institución, ya sea pública o privada, y se busca garantizar su protección y seguridad mediante acciones concretas.

Carvajal (2018), En su trabajo de investigación, el autor sostiene que, debido a la naturaleza crucial de los activos de información en una organización, surge una necesidad tanto legal como organizativa de implementar estándares de protección en el ámbito de la Seguridad Informática (SI), con el fin de salvaguardar el dominio de la información. Esta afirmación subraya la importancia de establecer medidas de seguridad adecuadas para garantizar la integridad, confidencialidad y disponibilidad de la información crítica de la organización.

Esta adopción de la norma ISO/IEC 27001 por parte del gobierno colombiano no solo demuestra su compromiso con la seguridad de la información, sino que también establece un

marco sólido para la implementación de prácticas de seguridad coherentes y efectivas en todas las entidades gubernamentales. Al seguir las mejores prácticas establecidas por la ISO/IEC 27001, el gobierno puede fortalecer su postura de seguridad, proteger la información sensible y fomentar la confianza en sus servicios en línea.

Figueroa (2018), en su trabajo de investigación cuyo objetivo fue la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma NTC-ISO-IEC 27001:2013 se destaca por su impacto favorable en la seguridad de la información (SI). Este enfoque se respalda mediante la valoración de las exigencias institucionales, la identificación de las expectativas de los interesados y la consideración de sus requisitos.

Un estudio realizado en Colombia subraya la categoría de que las instituciones cuenten con un sistema de Seguridad de la Información (SI), dado que se reconocen más de 542,000 ciberataques diarios, con más de 198 millones de incidentes documentados el año pasado, los cuales tenían el potencial de afectar a empresas de diversas magnitudes, tanto del ámbito público como del privado, además de a individuos particulares.

En Colombia, el sector financiero ha sido notablemente afectado por los ataques cibernéticos, ocupando la posición principal en términos de frecuencia de estos eventos, seguido por el sector gubernamental y luego por el sector de las telecomunicaciones. Los tipos de ataques más comunes incluyen malware, phishing, denegación de servicio (DoS) y ataques basados en la web.

2.2. Marco Teórico

2.2.1. Seguridad

Cuando hablamos de seguridad, a menudo asociamos este término con la idea de eliminar riesgos o desconfiar de algo o alguien. No obstante, la percepción de este concepto puede cambiar dependiendo del contexto en el que se aplique. Para estudiar y administrar los riesgos a los que estamos suceptibles, es crucial comprender esta variabilidad en la

percepción de la seguridad (Raffino, 2017).

En la era actual, la información se ha convertido en un recurso invaluable para cualquier tipo de organización o institución. Desde datos confidenciales de clientes hasta estrategias comerciales, la información es la columna vertebral sobre la cual se construyen y operan las empresas. En consecuencia, la seguridad de esta información se ha vuelto una prioridad crítica. Con el avance de la tecnología y la creciente digitalización de los procesos empresariales, las amenazas a la seguridad de la información han evolucionado y se han multiplicado. Las organizaciones enfrentan una amplia gama de amenazas, que van desde ataques cibernéticos sofisticados hasta errores humanos inadvertidos. Los ciberataques pueden provenir de hackers externos, pero también pueden surgir de actores internos malintencionados o de acciones inadvertidas de los propios empleados. Además, el aumento del almacenamiento y la transmisión de datos a través de redes digitales expone a las organizaciones a riesgos de robo, manipulación o pérdida de información en tránsito (Garcia, 2016).

A pesar de estos desafíos, muchas organizaciones encuentran que el apoyo recibido de las instituciones gubernamentales o de seguridad cibernética es insuficiente. La rápida evolución de las amenazas y la complejidad del panorama de seguridad cibernética hacen que sea difícil para las instituciones mantenerse al día con las últimas técnicas y tecnologías de protección de datos. Como resultado, las empresas deben asumir cada vez más la responsabilidad de proteger su propia información, desarrollando estrategias de seguridad de la información integrales y proactivas (Garcia, 2016).

En este contexto, la sostenibilidad emerge como un pilar fundamental de la gestión empresarial. La habilidad de una organización para proteger sus activos de información resulta esencial para asegurar la continuidad y seguridad de sus operaciones y asi, adaptarse a los cambios en el entorno tecnológico determinará su éxito y su capacidad para mantener la

confianza de los clientes y socios comerciales. Por lo tanto, la seguridad de la información se ha convertido en un componente esencial de la estrategia empresarial y requiere una atención constante y un enfoque proactivo para garantizar la seguridad y la sostenibilidad de la organización (Garcia, 2016).

2.2.2. Información

Los datos organizados que tienen valor para una entidad, conocidos como información, puede presentarse en diversas formas y medios, entre los cuales se incluyen:

- En medios impresos, tales como libros, revistas, folletos o documentos impresos.
- Integrada en imágenes, como en fotografías, gráficos o diagramas.
- Transmitida mediante expresión oral, a través de conversaciones, conferencias o presentaciones.
- Impresa en papel o en formato digital, en documentos electrónicos o archivos PDF.
- Almacenada electrónicamente mediante tecnología, en bases de datos, sistemas informáticos o servidores.
- Utilizada en dispositivos de proyección, como presentaciones de diapositivas o pantallas interactivas.
- Enviada como anexo en faxes o correos electrónicos, adjuntando archivos o documentos.
- Mostrada y compartida en reuniones, mediante material impreso o presentaciones multimedia.
- Durante interacciones personales o virtuales, en conversaciones cara a cara o en plataformas de comunicación en línea.
- Guardada en servicios de almacenamiento en la nube, como Dropbox, Google Drive o Microsoft OneDrive, para acceder a ella desde cualquier lugar y

dispositivo con conexión a internet.

Estas diversas formas de manifestación de la información reflejan la amplia gama de contextos y situaciones en los cuales puede ser utilizada y compartida en el ámbito personal, profesional y empresarial.

2.2.3. Seguridad de la información

La seguridad de la información, en su función central, desempeña un papel esencial al asegurar la confidencialidad, integridad y disponibilidad de los datos y sistemas interconectados dentro de una organización. Esto implica proteger la data susceptible contra accesos no acreditados, garantizar que los sistemas estén disponibles y operativos cuando se necesiten para el procesamiento de información, y asegurar que los datos no sean modificados de manera no deseada (Aguasanta, 2024).

Esta definición encapsula los tres pilares esenciales de la seguridad de la información:

- Confidencialidad: Se refiere a resguardar la información confidencial frente a accesos no permitidos, asegurando que únicamente individuos o entidades autorizadas puedan acceder a ella y evitando su divulgación a personas no autorizadas. Este aspecto de la seguridad de la información se centra en proteger la privacidad y la confidencialidad de los datos sensibles, lo que es fundamental para mantener la integridad y la reputación de una organización.
- Integridad: Se trata de asegurar que la información mantenga su precisión, integridad y no sea modificada sin autorización. Esto implica proteger los datos contra cualquier tipo de alteración no deseada, ya sea deliberada o accidental, durante su procesamiento, almacenamiento o transmisión. Preservar la integridad de la información es esencial para garantizar su confiabilidad y utilidad para la organización.
- Disponibilidad: Se refiere a asegurar que la información esté disponible y

accesible cuando sea necesario para las operaciones comerciales o la toma de decisiones. Esto implica prevenir interrupciones no planificadas en el acceso a la información debido a fallos técnicos, ataques cibernéticos u otros eventos adversos.

El propósito de la Seguridad de la Información es mitigar las amenazas latentes y reducir los riesgos a un nivel aceptable para los interesados. Dado que la información puede existir en diversas formas y estados, es necesario implementar medidas de protección apropiadas de acuerdo con su importancia y criticidad, independientemente de su forma o estado. Este es el ámbito central de la Seguridad de la Información (Huamani, 2021).

La seguridad de la información se puede definir como el estado en el que un sistema o conjunto de datos, ya sea de naturaleza informática u otro, se encuentra protegido de peligros, daños o riesgos, estando estrechamente ligada a la certeza y a la reducción de riesgos y contingencias. Cualquier elemento que tenga el potencial de impactar directamente en la acción o los efectos derivados se supone una amenaza o un riesgo.

En este contexto, el objetivo primordial de la seguridad de la información es salvaguardar los activos de una organización ante diversos riesgos, que pueden incluir desde ciberataques hasta errores humanos o desastres naturales. Esta protección busca asegurar la confidencialidad, integridad y disponibilidad de la información, así como mantener la funcionalidad y continuidad del sistema en todo momento.

Al mantener un entorno seguro para la información, las organizaciones pueden mitigar los riesgos y proteger aspectos críticos como datos sensibles, propiedad intelectual y la confianza de los clientes. Esto les permite operar de manera eficiente y competitiva, minimizando interrupciones y maximizando la confianza de las partes interesadas (García, 2015).

Las empresas se enfrentan a diversas contingencias en relación con la seguridad de

sus activos más preciados, y una forma efectiva de mitigar estos riesgos es involucrar a la gerencia y a expertos multidisciplinarios, así como a la tecnología y la aplicación de políticas, entre otros recursos disponibles. Una estrategia para abordar estas contingencias podría ser la realización de una evaluación interna de aspectos tales como la disponibilidad de recursos, la capacitación del personal y otros elementos similares (Najar, 2017).

En este enfoque, la gerencia desempeña un papel crucial al establecer políticas y directrices que promuevan una cultura de seguridad dentro de la organización. Los expertos multidisciplinarios, por su parte, pueden aportar conocimientos especializados en áreas como seguridad cibernética, gestión de riesgos y cumplimiento normativo, contribuyendo así a la identificación y mitigación de vulnerabilidades. La tecnología también juega un papel fundamental al proporcionar herramientas y soluciones para proteger los activos de la organización contra amenazas externas e internas. Esto puede incluir el uso de firewalls, sistemas de detección de intrusiones, cifrado de datos y software de gestión de seguridad de la información (Najar, 2017).

Brindar capacitación tanto a los administradores como a los usuarios es una medida importante, ya que implica una inversión significativa en la adquisición de hardware, licencias de software y el mantenimiento de estos recursos. Esto puede reducir la necesidad de inversión adicional y permitir la optimización de los recursos existentes (Forum, Council, & Management, 2013).

Esto no solo contribuye a mejorar la seguridad de la organización, sino que también puede ayudar a minimizar los riesgos asociados con posibles brechas de seguridad. Además, proporcionar a los usuarios una comprensión clara del porqué detrás de las políticas de seguridad, en lugar de simplemente imponerlas, puede ser más efectivo en términos de aceptación y cumplimiento. Esto puede evitar la resistencia y el rechazo por parte de los usuarios, ya que se sienten más involucrados y comprenden la importancia de su papel en la

protección de los activos de la organización (Forum, Council, & Management, 2013).

2.2.4. Clasificación de la Seguridad

Activa

Diversos riesgos acechan a los sistemas informáticos, entre ellos el acceso no autorizado a los datos. Aunque las contraseñas son una medida común de protección, existen otras estrategias de resguardo (Garcia et al., 2014).

Sin embargo, la simple utilización de contraseñas no es suficiente, especialmente ante la creciente sofisticación de las amenazas cibernéticas. Por consiguiente, se recomienda recurrir al cifrado de datos, el cual convierte la información en un formato ilegible para personas no autorizadas, dificultando así su acceso incluso si se logra penetrar las primeras barreras de seguridad (Garcia et al., 2014).

Además, los programas antivirus y otras herramientas de seguridad informática pueden detectar y prevenir la instalación de software malicioso y la ejecución de acciones perjudiciales en los sistemas, contribuyendo de esta manera a proteger la integridad de los datos. Por último, efectuar copias de respaldo de las contraseñas y otros datos esenciales es una práctica crítica para asegurar la disponibilidad y la recuperación de la información en caso de pérdida, robo o corrupción de los datos (Garcia et al., 2014).

Pasiva

Realizar copias de seguridad periódicas de los datos importantes es una forma efectiva de implementar seguridad pasiva, que se centra en reducir las consecuencias y el impacto de los incidentes y desastres. Un ejemplo común de esto es la protección contra el malware en sistemas informáticos (Garcia et al., 2014)..

El malware, como los virus informáticos, gusanos, troyanos y ransomware, puede causar daños significativos a los sistemas informáticos al infectar archivos, robar información confidencial o bloquear el acceso a los datos hasta que se pague un rescate. Si bien es

importante tener medidas activas para prevenir la infección por malware, como el uso de software antivirus y firewalls, la seguridad pasiva implica también prepararse para la posibilidad de que ocurra un incidente (Garcia et al., 2014).

2.2.5. Categoría de la seguridad de la información

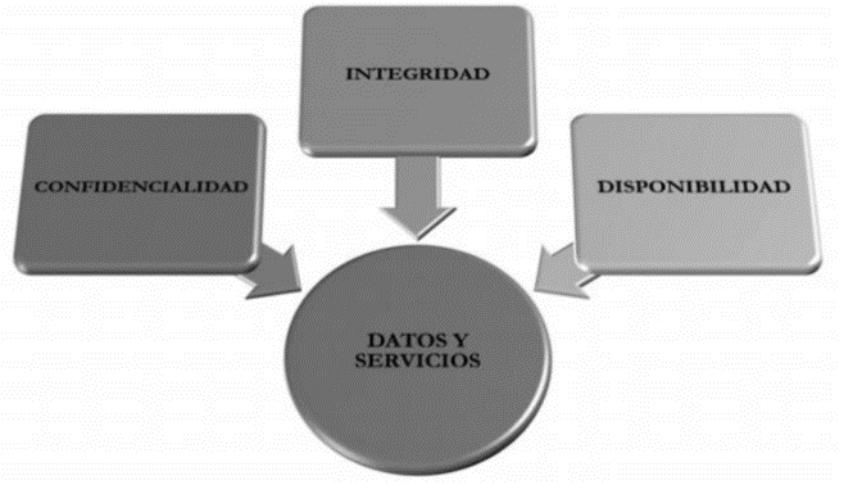
Al asegurar la integridad de la información, se garantiza que esta sea precisa, completa y esté libre de modificaciones no autorizadas. Esto implica proteger los datos contra cualquier forma de manipulación, ya sea intencional o accidental, que pueda comprometer su exactitud o confiabilidad. Una organización confía en la integridad de su información para la toma de decisiones, la prestación de servicios, la satisfacción de clientes y socios comerciales, y el cumplimiento de sus objetivos estratégicos. Por lo tanto, la seguridad de la información es un aspecto crucial de la gestión empresarial moderna y requiere una atención diligente y proactiva para mantener la confianza y el buen funcionamiento de la organización en su conjunto.

En el corazón de cualquier estrategia de seguridad de la información yace la conservación de la confiabilidad, la rectitud y la reserva de los datos. Este enfoque integral no solo abarca la protección de la información sensible contra accesos no autorizados, manipulaciones maliciosas o pérdidas accidentales, sino que también garantiza su accesibilidad cuando sea necesario para los procesos operativos críticos de la organización.

2.2.6. Metas de la seguridad informática

Las metas implican no solo asegurar que la información esté accesible cuando se necesite, sino también protegerla contra accesos no autorizados o divulgación no deseada, así como garantizar que los datos no sean alterados de manera no autorizada. Estos objetivos son fundamentales para preservar la funcionalidad y la fiabilidad de los sistemas de información, así como para mantener la confianza tanto de los usuarios internos como de los externos en la seguridad de los datos (Romero et al., 2019).

Figura 1. *Metas de la seguridad informática*



Fuente: Tomado de (Aguasanta, 2024)

2.2.6.1. Confiabilidad de la Información

Esta medida de seguridad garantiza que las partes acreditadas logren acceder a datos sensibles o confidenciales. Para lograrlo, se implementan mecanismos de control de acceso robustos, como sistemas de autenticación multifactor, roles y permisos específicos, y políticas de acceso basadas en el principio de necesidad mínima. Estos controles ayudan a prevenir accesos no autorizados y a proteger la privacidad y la integridad de la información. Además, es crucial realizar una supervisión continua y auditorías de acceso para detectar y mitigar cualquier actividad sospechosa o no autorizada (normaiso 27002, 2022).

2.2.6.2. Integridad de la Información

Esta condición de la información garantiza que los datos permanezcan inalterados y sin perturbaciones desde su origen, lo que valida su autenticidad y originalidad. Además, se realizan verificaciones y validaciones periódicas para detectar y corregir posibles alteraciones o modificaciones no autorizadas en los datos. Esto ayuda a preservar la integridad y la confianza en la información, esencial en cualquier entorno empresarial o de gestión de datos (normaiso 27002, 2022).

2.2.6.3. Accesibilidad de la información

El acceso y uso oportunos de la información, conforme a los procedimientos y canales adecuados, son fundamentales para garantizar su eficaz aprovechamiento y protección. Este principio asegura que la información esté disponible cuando se necesite y se utilice de acuerdo con las normativas establecidas, minimizando así los riesgos asociados con accesos indebidos o uso inapropiado. Para cumplir con este principio, se implementan sistemas de gestión de acceso y protocolos claros que determinan quién puede acceder a qué información y bajo qué circunstancias. Además, se promueve la formación y la concienciación del personal sobre las políticas y procedimientos relacionados con el acceso y uso de la información. De esta manera, se fomenta una cultura de seguridad de la información que protege tanto los activos como los intereses de la organización (normaiso 27002, 2022).

2.2.6.4. Fiabilidad de la información

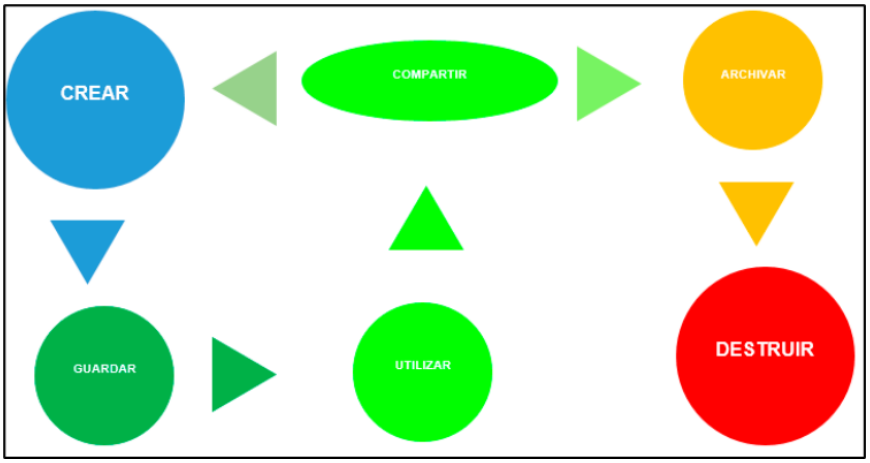
La fiabilidad de la información se vincula estrechamente con la confianza y la fiabilidad percibida en la fuente que la suministra. En esencia, se trata de evaluar hasta qué punto se puede confiar en dicha fuente y en la veracidad de la información que ofrece. Esta confiabilidad es esencial para respaldar la toma de decisiones informadas y para sustentar la validez de los datos utilizados en cualquier contexto. Evaluar la credibilidad de la información implica considerar la reputación, la experiencia, la imparcialidad y la precisión histórica de la fuente. Además, la transparencia en la presentación de la información y la documentación de las fuentes y métodos utilizados pueden reforzar aún más la credibilidad percibida. En última instancia, la credibilidad de la información influye significativamente en la confianza del público y en la aceptación de los mensajes transmitidos (normaiso 27002, 2022).

2.2.7. Ciclo de vida de la información

La información, al igual que otros activos de una empresa, atraviesa diversos ciclos

desde su compra inicial hasta su eventual culminación. Es esencial garantizar la calidad de este proceso en cada etapa del ciclo. Desde la recopilación inicial de datos hasta su almacenamiento, uso y eventual eliminación, cada paso debe ser gestionado con cuidado para conservar la rectitud, confiabilidad y reserva de la información. Esto implica implementar controles y instrucciones adecuadas para asegurar la precisión de los datos desde su origen, protegerlos contra accesos no autorizados o pérdidas, y asegurar su eliminación segura cuando ya no sean necesarios. Al mantener altos estándares de calidad en todo el ciclo de vida de la información, las organizaciones pueden maximizar el valor de sus activos de información y mitigar los riesgos asociados con su gestión (Aguasanta, 2024).

Figura 2. *Ciclo de vida de la información*



Fuente: Tomado de normaiso 27002 (2022).

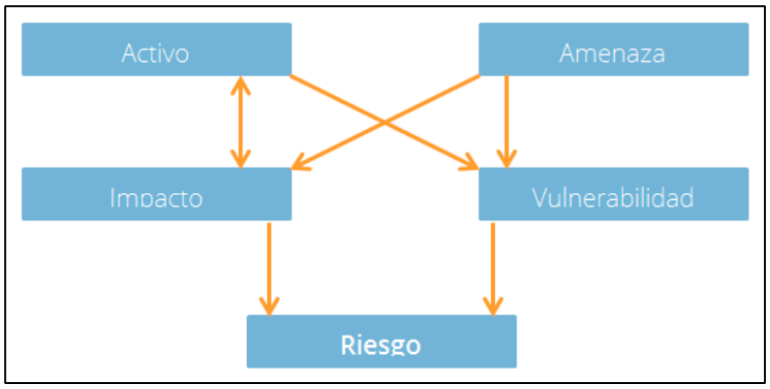
2.2.8. Activos

Los recursos de datos son elementos esenciales dentro del ámbito de la seguridad de la información. El término "activo" en el contexto empresarial o institucional hace referencia al conjunto de bienes, derechos y recursos que una entidad, sea esta pública o privada, posee. Esta definición engloba una variedad de elementos que van desde muebles, oficinas y equipos informáticos hasta datos, servicios, aplicaciones (software), hardware, comunicaciones, recursos administrativos, físicos y humanos. También se incluyen aquellos elementos que se

espera proporcionen beneficios en el futuro (Huamani, 2021).

Esto recursos de información representan la base sobre la cual se construyen y operan los sistemas y procesos de la organización. Desde la gestión eficiente de archivos y bases de datos hasta la implementación segura de software y aplicaciones, cada elemento desempeña un papel crucial en la operatividad y la seguridad de la empresa. La protección de estos recursos contra amenazas internas y externas se convierte en una prioridad para garantizar la continuidad del negocio y la preservación de la integridad y confidencialidad de la información. Por lo tanto, la adecuada gestión y protección de estos activos son elementos clave dentro de cualquier estrategia de seguridad de la información (Aguasanta, 2024).

Figura 3. *Activos*



Fuente: Tomado de normaiso 27002 (2022).

2.2.9. Amenaza

Una amenaza se caracteriza como un origen latente de sucesos no esperados que tienen el potencial de causar daño a un sistema o una organización. Estos eventos no deseados pueden surgir de diversas fuentes y pueden manifestarse de varias maneras, comprometiendo los recursos de información (Forum, Council, & Management, 2013):

2.2.9.1. Amenaza lógica

Esta categoría de amenazas se centra específicamente en aquellas que afectan la información almacenada en los activos de una organización. Esto puede incluir una variedad de riesgos potenciales, como acceso no autorizado a datos confidenciales, pérdida de

información debido a errores humanos o fallas técnicas, robo de datos, ataques de malware que comprometen la integridad de los archivos, entre otros.

- Amenaza estructurada: Generado a través de una metodología formal, respaldado por un potencial patrocinador y, lo que es crucial, ejecutado por alguien con un objetivo bien definido, este tipo de amenaza representa un peligro significativo. Un ejemplo ilustrativo es el notorio espionaje industrial. Esta amenaza no solo busca infiltrarse en sistemas con el propósito de obtener información sensible, sino que también pretende hacerlo de manera prolongada y sin ser detectada, evitando así levantar sospechas mediante indicadores de ataque evidentes (Aguasanta, 2024).
- Amenaza no estructurada: Los atacantes suelen carecer de metodología formal, patrocinadores claros y objetivos definidos. En su mayoría, se trata de intrusos "oportunistas", influencias de malware o incluso empleados descontentos. Esta amenaza se caracteriza por su falta de restricciones y su objetivo principal suele ser causar daño o conseguir beneficios sin importar las consecuencias. Este tipo de amenaza es implacable en dejar un rastro, ya que busca notoriedad y suele manifestarse mediante actividades como la manipulación del contenido de un sitio web público (Aguasanta, 2024).

2.2.9.2. Amenaza física

La ausencia de una adecuada protección de documentos sensibles puede desencadenar situaciones problemáticas, permitiendo que posibles agresores accedan físicamente a distintas áreas de la empresa. Por ejemplo, podrían buscar información confidencial en contenedores de basura, resaltando así la importancia de establecer medidas sólidas de seguridad física para resguardar la información crítica. Además, es factible que alguien se infiltre en las instalaciones haciéndose pasar por un colega y siguiendo a un empleado, aprovechando la

falta de supervisión en la entrada. Estos ejemplos subrayan cómo incluso las formas más simples de acceso físico pueden representar una amenaza considerable para la seguridad de la información y la integridad empresarial (Aguasanta, 2024).

2.2.10. Vulnerabilidad

Estas vulnerabilidades pueden ser aprovechadas para comprometer la confidencialidad, la integridad, el control de acceso, la disponibilidad o la integridad de los datos y aplicaciones almacenados en dicho sistema. Esencialmente, una vulnerabilidad representa una puerta abierta que los atacantes pueden utilizar para acceder ilegalmente a un sistema o para llevar a cabo acciones maliciosas que pongan en peligro la seguridad de la información. Por lo tanto, identificar y remediar las vulnerabilidades es una parte fundamental de mantener la seguridad de los sistemas y proteger los datos contra posibles ataques (Alvarez, 2019).

Estas vulnerabilidades en los sistemas informáticos pueden facilitar el acceso, el control o la exploración de información sensible almacenada en las bases de datos de cualquier empresa por parte de personas no autorizadas. Es importante reconocer que incluso los sistemas más seguros pueden contener vulnerabilidades que podrían ser explotadas por individuos malintencionados. Consecuentemente, es fundamental realizar acciones de seguridad proactivas, como actualizaciones de software, parches de seguridad y auditorías regulares. (Aguasanta, 2024).

2.2.11. Riesgos

El riesgo es un término en el mundo de la informática cuando hay una exposición o posibilidad de pérdida de información o datos, por atentados o amenazas a los sistemas dela información (Huamani, 2021). Es importante destacar que una amenaza por sí sola no constituye un riesgo si no existe una vulnerabilidad en el sistema que pueda ser explotada por esa amenaza. Por lo tanto, para que exista un riesgo real, debe haber tanto una amenaza como

una vulnerabilidad que puedan ser explotadas (López, 2010).

En otras palabras, una amenaza representa el potencial de un evento no deseado que pudiera causar daño, mientras que una vulnerabilidad es una debilidad en un sistema que podría ser aprovechada por esa amenaza. El riesgo se materializa cuando una amenaza explota una vulnerabilidad, lo que resulta en un impacto negativo en la seguridad del sistema. Por lo tanto, la gestión del riesgo implica identificar y mitigar tanto las amenazas como las vulnerabilidades para reducir la probabilidad de que ocurran incidentes de seguridad (López, 2010).

Cuando una organización se enfrenta a un riesgo específico, tiene varias opciones:

- Optar por no tomar acción y simplemente aceptar el riesgo. Esto puede ser válido si el daño esperado no justifica la inversión en medidas de prevención o si el costo de remediar el riesgo supera el posible daño.
- Implementar acciones para reducir o eliminar el riesgo. Esto implica tomar medidas concretas para disminuir la probabilidad o el impacto del riesgo identificado.
- Transferir el riesgo, por ejemplo, a través de la contratación de un seguro. Esta opción puede ser útil cuando el riesgo es demasiado grande para ser manejado internamente.

Cuando nos referimos a los "riesgos" en lugar de la "seguridad", estamos reconociendo la importancia de identificar y comprender estos riesgos. Esta perspectiva nos permite tomar medidas concretas para mitigarlos o eliminarlos por completo (Aguasanta, 2024).

2.2.11.1. Clases de Riesgo

Figura 4. *Clases de riesgo*

Fuente: Aguasanta (2024)

Una de las principales causas de los riesgos que enfrentan las organizaciones en el campo de la seguridad informática es la falta de conocimiento en esta área. Al no estar al tanto de las capacidades y tácticas de los ciberdelincuentes, muchas organizaciones subestiman las amenazas y no implementan medidas de seguridad adecuadas. Esto puede llevar a que los atacantes exploten vulnerabilidades fácilmente identificables y causen daños significativos. Es crucial que las organizaciones inviertan en educación y capacitación en seguridad informática para estar mejor preparadas y protegidas contra las crecientes amenazas cibernéticas (Alvarez, 2019).

En la era digital actual, la gestión de riesgos en tecnologías de la información se erige como un pilar fundamental para las compañías que manejan sistemas técnicos en sus procesos e información. Esta gestión no solo es esencial para el funcionamiento eficiente y seguro de estas entidades, sino que también desempeña un papel crucial en la protección de la integridad, confidencialidad y disponibilidad de la información crítica. Al reconocer, valorar y aminorar los riesgos concernientes con la seguridad de los datos y sistemas informáticos, las organizaciones pueden garantizar la continuidad de sus operaciones y preservar la confianza de sus clientes y partes interesadas en un entorno digitalmente complejo

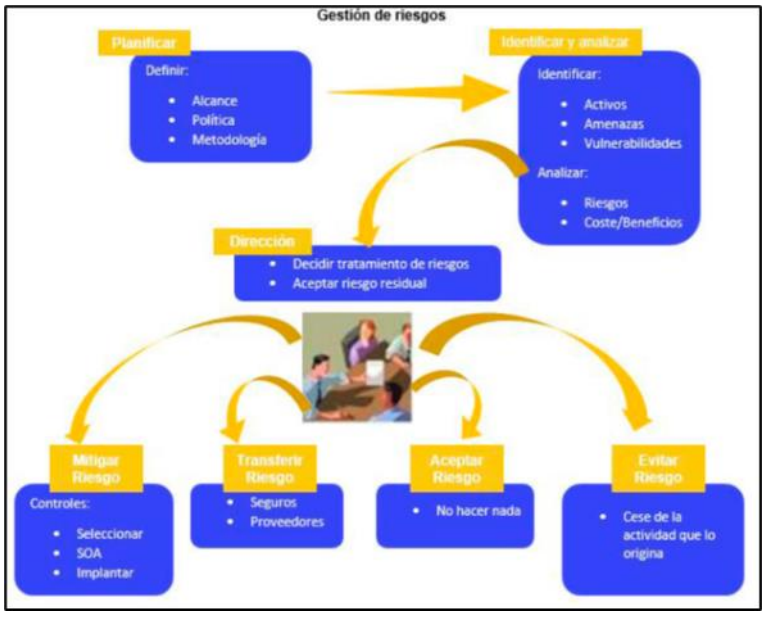
(Aguasanta, 2024).

2.2.12. Gestión de Riesgos en la Seguridad de la Información

Este sistema se refiere a un enfoque integral para gestionar la seguridad de la información en una organización, que incluye políticas, procedimientos, controles y otros elementos diseñados para proteger la confiabilidad, rectitud y disponibilidad de la información crítica. Implementar un ISMS ayuda a las organizaciones a identificar y gestionar los riesgos de seguridad de la información de manera sistemática y eficaz (Aguasanta, 2024).

Los análisis y debates actuales indican que las empresas a menudo se ven confrontadas con diversos riesgos. Estos riesgos subrayan la necesidad de que las organizaciones aborden aspectos específicos de su comunicación interna, incluida la identificación, el examen y la evaluación de si estos riesgos solicitan cuidado o solución (Aguasanta, 2024).

Figura 5. *Gestión de riesgos*



Fuente: Aguasanta (2024).

2.2.13. Normativas para gestionar la seguridad y los riesgos de la información

Se han desarrollado estándares que establecen las mejores prácticas para asegurar que

la información sea manejada de manera adecuada y segura. Estos estándares proporcionan un marco de referencia que ayuda a las organizaciones a establecer y mantener medidas de seguridad robustas y a cumplir con los requisitos legales y regulatorios pertinentes. Estos estándares proporcionan un marco de contexto y orientación para la ejecución de medidas de seguridad de la información consistentes y efectivas, lo que ayuda a las organizaciones a proteger sus activos de información y a mantener la confianza de sus clientes y partes interesadas (Méndez, 2020).

2.2.14. ISO 27000

Es un estándar, que incluye varios principios de seguridad de la información que brindan pautas para desarrollar un sistema de gestión de la información. Por lo que se enumera el conjunto de normas que componen dicha familia.

Tabla 1. *Conjunto de normas de la familia ISO 2700*

Norma	Detalle
ISO/IEC 27000	Este es la principal normativa SGSI, en el que se crean todos los estándares existentes.
ISO/IEC 27001	Es una normativa internacional, de gestión de seguridad institucional, la cual es considerada, como el estándar más importante de la familia ya que promueve la mejora continua de cada proceso. La cual fue publicada en octubre de 2005.
ISO/IEC 27002	Fue publicada el 1 de julio de 2007, donde el objetivo primordial, es establecer diversos lineamientos para mantener la integridad, confidencialidad y disponibilidad de la información.
ISO/IEC 27003	Este es una normativa internacional diseñada para guiar la implementación de SGSI. Por lo que fue publicado el 7 de diciembre de 2009 en apoyo de la norma ISO 27001.
ISO/IEC 27004	Es un estándar que facilita métricas de gestión de la información. Define quién, cómo y cuándo se deben tomar las medidas contra los parámetros dados. Por lo que fue publicada el 7 de diciembre de 2009.
ISO/IEC 27005	Es un estándar útil para la gestión de riesgos. Por lo que establece un

Norma	Detalle
	conjunto de recomendaciones, útiles para evaluar la seguridad de la información. Por lo que es el soporte de riesgo para la norma ISO 27001; la cual fue publicada en junio de 2008.
ISO/IEC 27006	Incluye requisitos para la acreditación de organizaciones. Por lo que es responsable de proporcionar los requisitos y la orientación para la certificación SGSI, es decir, útil para comprobar el cumplimiento de la norma ISO 27001 generada en 2011.
ISO/IEC 27007	Esta es una guía para organizaciones certificadas, una guía para gestionar auditorías de SGSI.
ISO/IEC 27799:2008	Es un estándar regulatorio para la industria médica.

Fuente: Tomado de Gavidia, 2022, pág. 8

El orden de jerarquía de los dominios según las ISO/IEC 27002:2022, son:

Figura 6. *Jerarquía de dominios ISO*

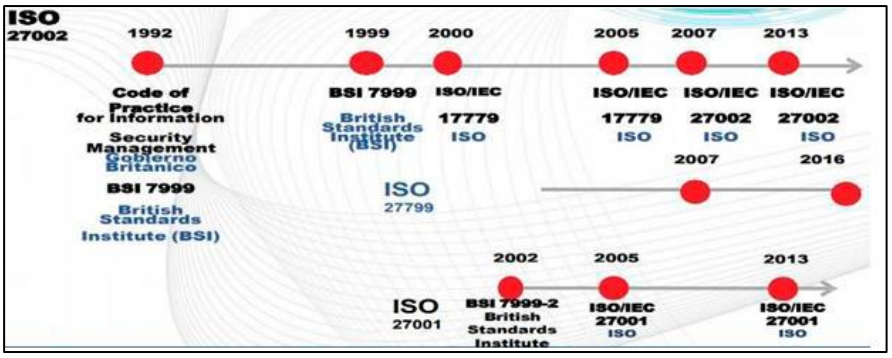
Fuente: Tomado de Nicolao, 2022, pág. 27

Según la Escuela Europea de Excelencia (2022), los nuevos controles según la actualización de las normas ISO 27002:2022 son:

- Información sobre amenazas.
- Seguridad de la información en la nube.

- Prolongación del negocio.
- La seguridad física y su control.
- Configuración.
- Eliminación de la información.
- Encriptación de datos.
- Prevención de fugas de datos.
- Seguimiento y monitoreo.
- Filtrado web.
- Codificación segura.

Figura 7. *Avance de la norma ISO/IEC 27000 en el tiempo*



Fuente: Aguasanta (2024).

Un Sistema de Gestión de Seguridad de la Información (SGSI) se configura como una estructura integral que engloba políticas, prácticas, recursos y procedimientos, coordinados de manera conjunta por una entidad, con el fin primordial de proteger sus activos de información. Este sistema requiere un enfoque holístico que abarque desde la planificación hasta la mejora continua, abordando aspectos como la identificación de riesgos, la implementación de medidas de seguridad, la vigilancia constante y la adaptación a los cambios del entorno. Además, debe estar adaptado a las necesidades específicas y los

objetivos de la organización, con el propósito de garantizar una gestión eficaz de la seguridad de la información en todos los niveles (Valencia, 2021).

Así, dentro de las prácticas de seguridad de la información se encuentran la implementación de controles de seguridad, la gestión de riesgos, la capacitación del personal y la evaluación de la conformidad, entre otros aspectos relevantes. Al adherirse a estas normas y directrices, las organizaciones pueden fortalecer su postura de seguridad y disminuir el riesgo de incidentes que podrían impactar negativamente en su operatividad y reputación:

2.2.15. ISO 27001

El despliegue de un Sistema de Gestión de Seguridad de la Información (SGSI) va más allá de una simple implementación inicial; implica un compromiso continuo con el mantenimiento y la mejora constante de las prácticas de seguridad. En este sentido, la norma ISO/IEC 27001 establece un marco que fomenta una cultura de mejora continua, destacando la importancia de la evaluación regular de los riesgos asociados a los activos de información y la adaptación de las medidas de seguridad en manifestación a los alteraciones del ambiente empresarial y las nuevas amenazas (Aguasanta, 2024):

- Planificar (Plan): En esta etapa, se establecen los objetivos y procesos necesarios para lograr los resultados deseados. Esto incluye la identificación de riesgos y la definición de medidas de seguridad adecuadas para mitigarlos.
- Hacer (Do): En esta etapa, se implementan los planes y procesos establecidos en la fase de planificación. Esto implica poner en práctica los controles de seguridad y procedimientos definidos para proteger la información.
- Verificar (Check): En esta etapa, se lleva a cabo la supervisión y evaluación de los procesos implementados para garantizar que estén funcionando según lo

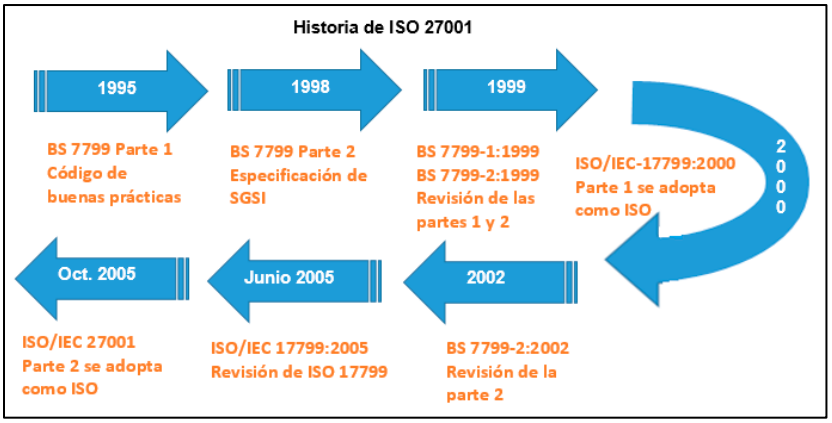
previsto. Se realizan auditorías internas y revisiones periódicas para identificar posibles desviaciones o áreas de mejora.

- Actuar (Act): En esta etapa, se toman acciones correctivas y preventivas basadas en los resultados de la fase de verificación.

Este ciclo de mejora continua es fundamental en la implementación y gestión de la seguridad de la información, ya que proporciona un enfoque estructurado y sistemático para identificar, implementar, monitorear y mejorar continuamente los controles de seguridad en una organización (Conexion ESAN, 2016).

Aunque la norma ISO/IEC 27001 no proporciona procedimientos específicos para la implementación, es pertinente para organizaciones de diversos ámbitos, incluyendo el sector privado, público y sin fines de lucro, independientemente de su tamaño o industria.

Figura 8. *Avance de la norma ISO/IEC 27001en el tiempo*



Fuente: Aguasanta (2024)

Una vez identificados estos riesgos, se procede a desarrollar planes de acción para mitigarlos, lo que implica la elaboración y aplicación de procedimientos específicos y la capacitación del personal en temas de seguridad de la información. La verificación del SGSI comprende la evaluación continua de su desempeño, la eficacia de los controles implementados y la realización de auditorías internas para garantizar el cumplimiento de los estándares establecidos. Este procedimiento es esencial para asegurar que el SGSI funcione

de manera efectiva en la protección de los datos sensibles de la organización (ISO27001, 2014).

2.2.16. Norma ISO/IEC 27002

ISO/IEC 27002, un conjunto de directrices de seguridad de la información, ofrece recomendaciones para la gestión eficaz de la seguridad de la información en una variedad de contextos organizativos. Estas directrices están diseñadas para ayudar a las organizaciones a proteger la información y a abordar los riesgos asociados con la gestión de la seguridad de la información (Huamani, 2021).

A continuación, se muestran de forma general algunos dominios de la norma ISO/IEC 27002

2.2.16.1. Políticas de seguridad

Es crucial que esta política sea aprobada por los directivos de mayor nivel y luego comunicada a todo el personal. Además, es fundamental revisar y actualizar regularmente esta política, especialmente cuando se producen cambios significativos, para garantizar su pertinencia y eficacia en la protección de la información de la entidad (Aguasanta, 2024).

2.2.16.2. Gestión de activos

Según lo establecido en la norma, un activo se define como cualquier elemento que posea valor para la organización y requiera protección. Sin embargo, para garantizar esta protección, es necesario identificar y clasificar los activos, lo que permite la creación de un inventario estructurado y su mantenimiento continuo. Además, es crucial establecer reglas documentadas que definan los tipos de uso permitidos para cada activo, asegurando así su manejo adecuado y seguro en la organización (Velepucha, 2022).

2.2.16.3. Control de accesos

Establecer un control de acceso adecuado para los activos de información, en conformidad con los requisitos del negocio, es de suma importancia. El propósito primordial

radica en asegurar que únicamente los usuarios autorizados dispongan de acceso a estos activos, lo cual contribuye a prevenir posibles daños o incidentes de seguridad. Este enfoque es esencial para proteger tanto la integridad como la confidencialidad de la información de la organización (Aguasanta, 2024).

2.2.16.4. Seguridad física y ambiental

La preservación física y ambiental es un aspecto crítico en la protección de los activos de información contra amenazas externas y condiciones desfavorables. Para lograr esta protección, se implementan estrategias y dispositivos físicos en áreas designadas como seguras. Estas estrategias pueden abarcar desde sistemas de acceso hasta equipos contra incendios (Aguasanta, 2024).

2.2.16.5. Seguridad en las telecomunicaciones.

Implementar normativas formales para regular el intercambio de información es crítico para asegurar la seguridad tanto en transferencias físicas como digitales. Estas normas establecen procedimientos y protocolos específicos que garantizan un intercambio seguro y protegido de datos entre sistemas, dispositivos o individuos. Al adherirse a estas normativas, se reduce el riesgo de exposición de la información a amenazas como la interceptación no autorizada, la manipulación de datos o la pérdida de confidencialidad. Además, el cumplimiento de estas normas contribuye a mantener la integridad y la disponibilidad de la información durante todo el proceso de transferencia (Alvarez, 2019).

2.2.16.6. Procura, progreso y preservación de los sistemas informáticos.

Esto se puede lograr estableciendo acuerdos contractuales claros que incluyan cláusulas de seguridad y privacidad. Además, es importante realizar evaluaciones periódicas de la seguridad de los proveedores y asegurarse de que cumplan con los estándares y regulaciones de seguridad pertinentes. Esto ayuda a mitigar el riesgo de compromiso de la información confidencial y garantiza la integridad y la confidencialidad de los datos en todo

momento. (Alvarez, 2019).

2.2.16.7. Gestión de incidentes en la seguridad de la información.

La comunicación efectiva a través de estos informes facilita la toma de medidas correctivas oportunas para abordar los problemas de seguridad identificados. Al registrar los eventos de seguridad de manera adecuada, se crea un historial que permite realizar un seguimiento de las tendencias y patrones de seguridad, lo que puede ser útil para reconocer espacios de progreso y tomar disposiciones informadas sobre la seguridad de la información.

Es importante establecer procedimientos claros y bien definidos para la evaluación y gestión de eventos de seguridad. Esto incluye la asignación de responsabilidades, la clasificación y priorización de los eventos, la respuesta ante incidentes y la implementación de medidas correctivas y preventivas (Alvarez, 2019).

2.2.16.8. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Crear, documentar y poner en marcha planes de continuidad del negocio es fundamental para asegurar la resiliencia de una organización ante posibles incidentes que puedan interrumpir sus operaciones. Estos planes tienen como objetivo principal prevenir la interrupción de las actividades empresariales y garantizar una rápida recuperación en caso de que ocurran eventos adversos.

Los planes de continuidad del negocio deben incluir medidas para identificar y evaluar los riesgos potenciales, así como estrategias para mitigarlos y gestionarlos eficazmente. Esto puede implicar la implementación de medidas de seguridad física y lógica, la creación de procedimientos de respuesta ante incidentes, la realización de copias de seguridad de datos críticos y la implementación de sistemas de redundancia y recuperación de desastres.

Esto garantiza que la organización esté preparada para hacer frente a cualquier

situación de emergencia y pueda continuar operando de manera efectiva incluso en las circunstancias más adversas. Además, la revisión constante de los planes permite identificar y corregir posibles deficiencias antes de que se conviertan en problemas graves (Alvarez, 2019).

2.2.16.9. Cumplimiento.

La implementación de procedimientos adecuados para garantizar la conformidad con los requisitos legales, regulaciones y contratos es fundamental para asegurar el cumplimiento normativo y evitar posibles sanciones legales o pérdidas financieras. Esto es especialmente relevante, donde el uso indebido puede resultar en demandas por infracción de derechos de autor o violación de patentes.

Estos controles pueden incluir la implementación de políticas y procedimientos internos, la realización de auditorías periódicas para verificar el cumplimiento, y la capacitación del personal sobre las leyes y regulaciones pertinentes.

La ejecución de estas revisiones se fundamenta en los requerimientos de seguridad reconocidos y los recursos utilizables en la compañia. Es importante asignar los recursos adecuados para garantizar la efectividad de los controles y asegurar el cumplimiento continuo con los requisitos legales y regulatorios. Además, es necesario mantenerse al tanto de los cambios en las leyes y regulaciones para actualizar los procedimientos en consecuencia y asegurar la conformidad en todo momento (Alvarez, 2019).

2.3. Marco legal

La Normativa ISO/IEC 27002:2022, que aborda la ciberseguridad, la seguridad de la información y la protección de la privacidad, se desarrolló para proporcionar orientación sobre la implementación de los 114 controles definidos en la norma ISO/IEC 27001. A diferencia de la versión anterior de 2013, esta normativa no es certificable y ha experimentado una evolución notable (ISO, 2022).

2.3.1. Ley orgánica de telecomunicaciones

En el Tercer Suplemento del Registro Oficial No. 439, se publicó la Ley Orgánica de Telecomunicaciones, el 18 de febrero del 2015, dice:

En el capítulo I, en Consideraciones Preliminares, en el Artículo I, se detalla el objeto, que dice que se debe desarrollar, el régimen general de telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajo los principios y derechos constitucionalmente establecidos (Asamblea Nacional, 2015).

Mientras que en el capítulo I, en establecimientos y explotación de redes, en el artículo

Se entiende por redes de telecomunicaciones a los sistemas y demás recursos que permiten la transmisión, emisión y recepción de voz, vídeo, datos o cualquier tipo de señales, mediante medios físicos o inalámbricos, con independencia del contenido o información cursada (Asamblea Nacional, 2015).

2.3.2. Ley de comercio electrónico

Mientras que en el Registro Oficial Suplemento 557 del 17 de abril del 2002, se determina la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, como título preliminar en el artículo 1, el objeto de la Ley abarca la regulación de diversos aspectos relacionados con el ámbito digital, como los encargos de datos, la firma electrónica, los servicios de certificación, el convenio electrónico y telemático, así como la prestación de servicios electrónicos mediante redes de información. Esta regulación abarca áreas como el comercio electrónico y establece medidas de protección para los usuarios de estos sistemas, garantizando la seguridad y confianza en las transacciones realizadas en el entorno digital (Congreso Nacional, 2002).

En el Capítulo I, en Principios Generales, en el artículo 5, detalla que, en la intimidad y discreción, instituyen los compendios de confiabilidad para los encargos de datos. Toda

infracción a estos principios, primariamente aquellas concernientes a la infracción electrónica, traspaso ilegal de mensajes de datos o quebrantamiento del secreto profesional, será penada acorde a lo prevenido en esta ley y demás normas que rigen la materia (Congreso Nacional, 2002).

CAPITULO III

MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

El área de estudio de esta tesis se centró en la seguridad informática, un campo de vital importancia en el contexto empresarial, caracterizado por la creciente digitalización y la interconexión de sistemas y datos. Específicamente, la investigación se enfocó en la aplicación de un Plan de Seguridad Informático basado en la Norma ISO/IEC 27002:2022 para la empresa ADLINK S.A., una entidad dedicada a la provisión de servicios de internet en la provincia de Imbabura.

La empresa ADLINK S.A. se encontraba inmersa en un entorno altamente tecnológico y conectado, lo que la hacía especialmente vulnerable a posibles amenazas cibernéticas. Por lo tanto, la implementación de un plan de seguridad informática sólido y basado en estándares reconocidos era fundamental para garantizar la protección de sus sistemas y datos, así como para mantener la confianza de sus clientes y asegurar el éxito continuo de sus operaciones. En este trabajo de investigación, se exploraron en detalle los procesos y estrategias necesarios para llevar a cabo esta implementación, así como los posibles beneficios que podía aportar a la empresa en términos de mitigación de riesgos y mejora de la resiliencia frente a posibles ataques cibernéticos.

3.2. Enfoque y tipo de investigación

3.2.1. Enfoque

La presente investigación adopta un enfoque mixto que integra métodos cualitativos y cuantitativos para lograr una comprensión holística y detallada de la seguridad informática en la empresa ADLINK S.A. y la aplicación del Plan de Seguridad basado en la Norma ISO/IEC 27002:2022.

3.2.2. Tipo de investigación

3.2.2.1. Investigación Mixta

Este tipo de investigación busca aprovechar las fortalezas de diferentes enfoques de investigación, tanto cualitativos como cuantitativos, para obtener una comprensión más completa y profunda del fenómeno estudiado, especialmente en el ámbito de la seguridad y los procesos informáticos.

Este enfoque de investigación permite combinar métodos como la revisión documental, encuestas, entrevistas, observaciones, análisis estadísticos, entre otros, según las necesidades y objetivos específicos de la investigación. En este caso, en relación a los planes de seguridad informática, la normativa ISO 27002:2022 y otras documentaciones relevantes. Al recopilar y analizar esta información, se busca respaldar el trabajo de investigación y proporcionar un marco sólido para abordar aspectos como las incertidumbres y los desafíos en la seguridad informática. Al mismo tiempo se aplicó un trabajo de campo para un análisis cualitativo oportuno de la situación y la problemática actual de la empresa a través, de una encuesta a los trabajadores de la empresa y una entrevista para el director general.

3.3. Procedimiento de investigación

Fase 1:

Durante esta etapa, se llevó a cabo la identificación de los riesgos de seguridad del sistema informático de la empresa ADLINK S.A., utilizando la metodología MAGERIT v.3. El proceso se inició con la determinación de los activos, los cuales representaban recursos con un valor institucional. Posteriormente, se identificaron las amenazas existentes, se definieron los riesgos específicos y se evaluaron las posibilidades de circunstancia de las amenazas y el impacto potencial que podrían tener en los activos de la compañía.

Una vez identificados los riesgos, se aplicaron medidas de salvaguarda adecuadas para mitigarlos o eliminarlos en la medida de lo posible. Estas medidas incluyeron la

ejecución de controles de seguridad, políticas y procedimientos específicos, así como la aceptación de tecnologías de protección convenientes.

Finalmente, se llevó a cabo una evaluación del riesgo residual, es decir, el riesgo que permanecía después de la implementación de las medidas de salvaguarda. Esta evaluación permitió determinar los riesgos que aún requerían atención y posibles mejoras en el sistema de seguridad informática de la empresa ADLINK S.A.

Fase 2:

En esta fase, se llevó a cabo un análisis de la norma ISO/IEC 27002:2022 mediante la selección de controles. El objetivo era minimizar los riesgos coligados a la seguridad de la gestión de activos en la empresa ADLINK S.A. Para lograr esto, se revisaron y evaluaron los diferentes controles de seguridad propuestos por la norma ISO/IEC 27002:2022 en relación con la gestión de activos de la organización.

Se realizó una cuidadosa consideración de cada control para determinar su relevancia y aplicabilidad al contexto específico de ADLINK S.A. Esto implicó evaluar la efectividad de cada control para abordar los riesgos identificados anteriormente en el análisis de riesgos. Se seleccionaron aquellos controles que se consideraron más adecuados y efectivos para mitigar los riesgos de seguridad asociados a la gestión de activos de la empresa.

Fase 3:

Posteriormente, se procedió al desarrollo de las políticas de seguridad de la información, fundamentadas en los controles seleccionados de la norma ISO/IEC 27002:2022. Este paso se ejecutó con el objetivo específico de fortalecer la seguridad en la gestión de activos dentro de la empresa ADLINK S.A.

Para llevar a cabo este proceso, se tomó como base los controles previamente seleccionados durante el análisis de la norma ISO/IEC 27002:2022. Estos controles sirvieron como punto de referencia para establecer directrices y procedimientos claros que abordaran

los riesgos identificados y garantizaran la protección adecuada de los activos de información de la organización.

Se trabajó en estrecha colaboración con los responsables de cada área relevante dentro de la empresa para desarrollar políticas específicas que se alinearan con las necesidades y objetivos del negocio.

Además, se enfatizó la importancia de la concientización y capacitación del personal en relación con estas políticas de seguridad. Se implementaron programas de formación para garantizar que todos los empleados comprendieran las políticas y procedimientos establecidos, así como su papel en la protección de los activos de información de la empresa.

CAPITULO IV

RESULTADOS Y DISCUSION

4.1. Análisis e Interpretación de Resultados

4.1.1. Encuesta

A través, de la implementación de un sondeo en forma de encuesta de seguridad o cumplimiento IT entre todos los empleados de ADLINK S.A donde, este instrumento fue dirigido a todo el personal administrativo y personal de TI conformado por un total de 15 colaboradores. Utilizando un método de recolección de datos previamente establecido y diseñado para evaluar y comprender los aspectos de seguridad de la información y las tecnologías de información en una empresa u organización. Los resultados obtenidos reflejan el grado de aplicación de medidas de seguridad en la empresa.

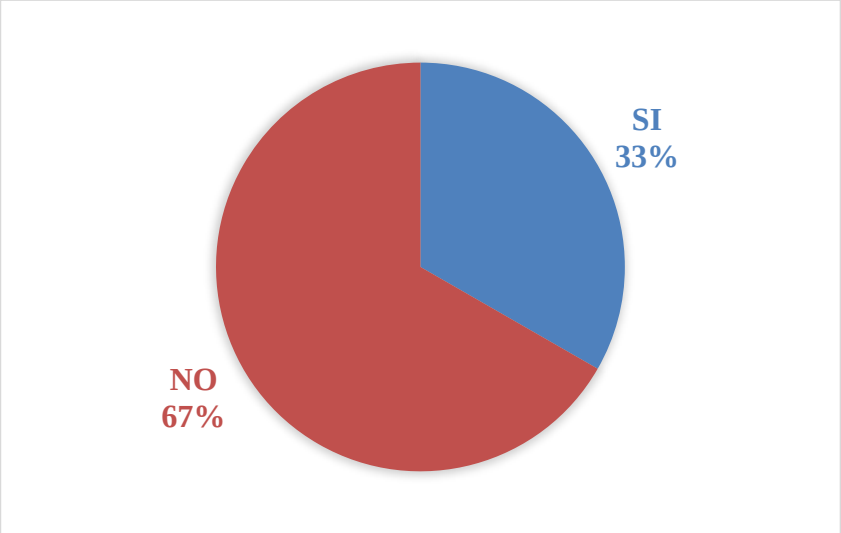
Pregunta 1. ¿La compañía en este momento maneja políticas de seguridad para la apropiada administración de la información que se trabaja en los pertinentes espacios?

Tabla 2. *Políticas de Seguridad*

¿La compañía en este momento maneja políticas de seguridad para la apropiada administración de la información que se trabaja en los pertinentes espacios?

		Frecuencia	Porcentaje
Válido	SI	5	33.3
	NO	10	66.7
	Total	15	100

Figura 9. *Referente Pregunta 1*



Interpretación

El 67% de los encuestados indicó que la empresa no aplica políticas de seguridad para gestionar adecuadamente la información en las áreas correspondientes, lo que refleja una percepción generalizada de falta de implementación de medidas de seguridad. Por otro lado, solo el 33% de los encuestados afirmó que la empresa sí implementa políticas de seguridad, lo que sugiere que una minoría percibe que se están aplicando medidas adecuadas en este sentido.

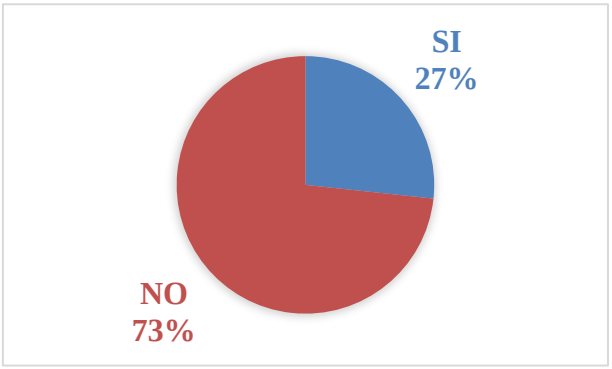
Este resultado pone de manifiesto una posible área de mejora en la implementación de políticas de seguridad de la información en la empresa. Sería pertinente investigar más a fondo las razones detrás de esta percepción predominante y tomar medidas correctivas en consecuencia.

Pregunta 2. ¿El personal de la organización posee algún tipo de conocimiento respecto a los protocolos a seguir en caso de detectar el uso no autorizado de dispositivos informáticos?

Tabla 3. I*ngreso de individuos no autorizados a los dispositivos*

		Frecuencia	Porcentaje
Válido	SI	4	26.7
	NO	11	73.3
	Total	15	100

Figura 10. *Referente Pregunta 2*



Interpretación

El 73% de los encuestados indicó que no está al tanto de los protocolos establecidos para abordar el uso no autorizado de dispositivos informáticos, lo que sugiere una falta general de familiaridad con estos procedimientos dentro del personal. Por otro lado, solo el 27% de los encuestados afirmó conocer los procedimientos, lo que indica que una minoría está informada sobre cómo actuar en tales situaciones.

Estos hallazgos resaltan una brecha significativa en el conocimiento y la comprensión del personal sobre los procedimientos de seguridad relacionados con el uso no autorizado de dispositivos informáticos. Es crucial proporcionar una capacitación adecuada y mejorar la comunicación sobre estos protocolos para fortalecer la seguridad de la información en la organización.

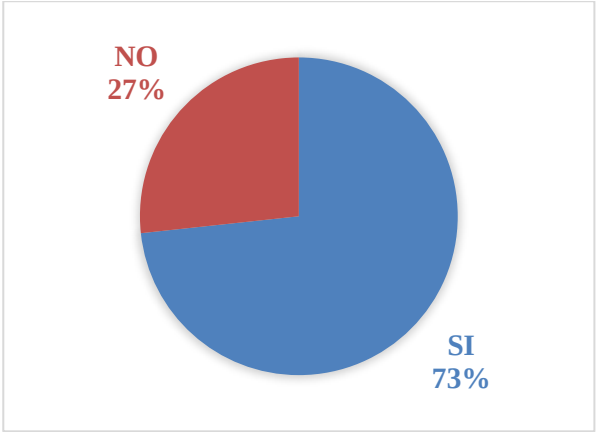
Pregunta 3. ¿La empresa cuenta con un plan para manejar situaciones de emergencia debido a desastres naturales?

Tabla 4. *Procedimiento a seguir en caso de emergencias derivadas de desastres naturales.*

		Frecuencia	Porcentaje

Válido	SI	11	73.3
	NO	4	26.7
	Total	15	100

Figura 11. *Referente Pregunta 3*



Interpretación

El 73% de los encuestados respondió "SI", lo que indica que la mayoría de la empresa cuenta con un plan establecido para manejar situaciones de emergencia debido a desastres naturales.

El 27% de los encuestados respondió "NO", lo que sugiere que una minoría de la empresa no tiene un plan específico para hacer frente a tales situaciones.

Estos resultados muestran que la mayoría de la empresa ha tomado medidas para prepararse y responder ante desastres naturales, lo que refleja una conciencia y preparación adecuadas en términos de gestión de emergencias. Sin embargo, aún queda espacio para mejorar y garantizar que todos los empleados estén completamente informados y preparados para enfrentar tales eventualidades.

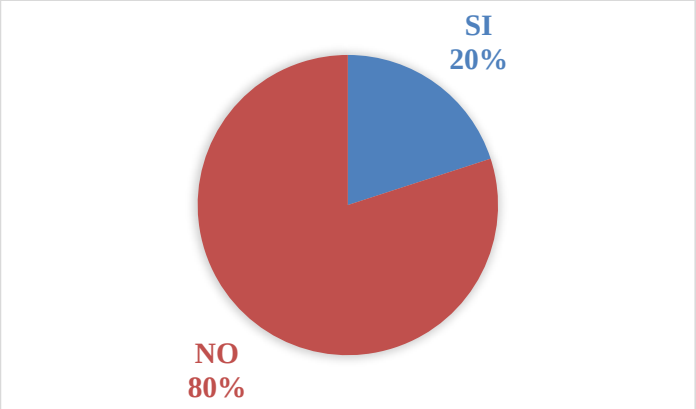
Pregunta 4. ¿Opina que sería beneficioso que la compañía elabore un Manual de Procedimientos para el Departamento de Tecnologías de la Información con el fin de facilitar la realización ordenada de cada tarea?

Tabla 5. *Procedimientos para el departamento de tecnologías de la información que faciliten*

la ejecución ordenada de cada tarea.

		Frecuencia	Porcentaje
Válido	SI	3	20
	NO	12	80
	Total	15	100

Figura 12. *Referente Pregunta 4*



Interpretación

El 80% de los encuestados indicó su negativa a la elaboración de un Manual de Procedimientos para el Departamento de Tecnologías de la Información, lo que sugiere una oposición generalizada a esta propuesta. Por otro lado, solo el 20% de los encuestados expresó su apoyo a la idea de desarrollar dicho manual, lo que indica que solo una minoría considera beneficioso implementarlo.

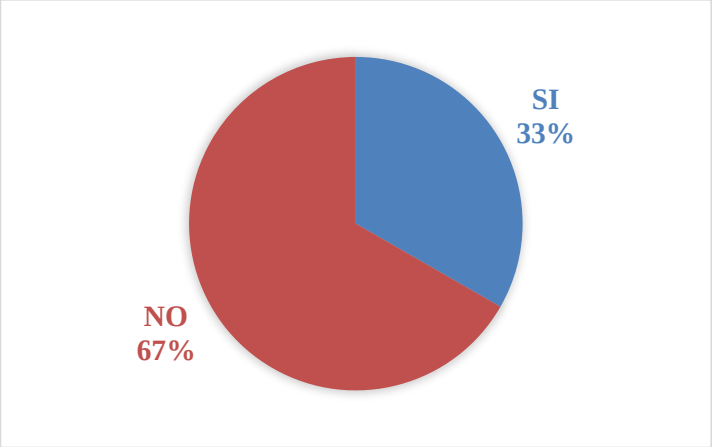
Estos resultados evidencian una clara discrepancia entre la mayoría de los encuestados y la propuesta de crear un manual de procedimientos para el Departamento de Tecnologías de la Información. Sería necesario indagar más a fondo para comprender las razones detrás de esta oposición y explorar alternativas para mejorar la eficiencia y la organización en el departamento.

Pregunta 5. ¿La organización cuenta con protocolos para mitigar los riesgos en sus actividades operativas?

Tabla 6. *Resúmenes de remisión de riesgos.*

		Frecuencia	Porcentaje
Válido	SI	5	33.3
	NO	10	66.7
	Total	15	100

Figura 13. *Referente Pregunta 5*



Interpretación

El 67% de los encuestados respondió "NO", lo que indica que la mayoría de la organización no cuenta con protocolos para mitigar riesgos en sus actividades operativas.

Solo el 33% de los encuestados respondió "SI", lo que sugiere que una minoría tiene protocolos establecidos para mitigar riesgos en sus actividades operativas.

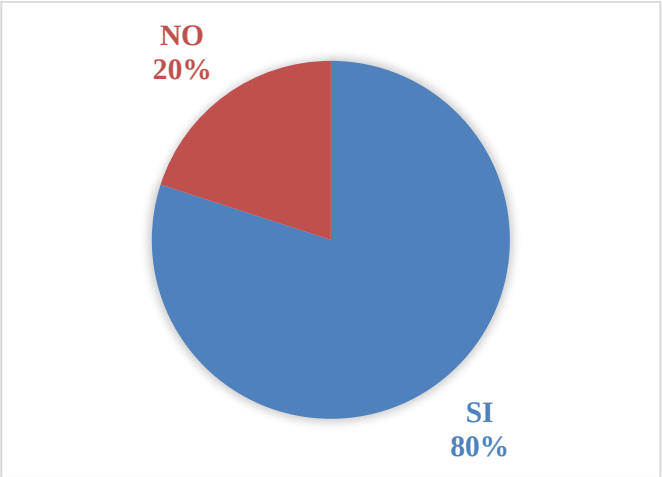
Estos resultados revelan una falta de protocolos estructurados para abordar y mitigar los riesgos en las actividades operativas de la organización. Esta situación podría exponer a la empresa a una mayor vulnerabilidad frente a posibles riesgos y pérdidas.

Pregunta 6. ¿Se han registrado los recursos informáticos bajo su supervisión?

Tabla 7. *Supervisión de los activos informáticos.*

		Frecuencia	Porcentaje
Válido	SI	12	80
	NO	3	20
	Total	15	100

Figura 14. *Referente Pregunta 6*



Interpretación

El 80% de los encuestados afirmó que sí, lo que refleja que la mayoría de los recursos informáticos bajo su responsabilidad están correctamente registrados. Sin embargo, el 20% restante respondió "NO", lo que sugiere que una minoría de los recursos informáticos aún no han sido registrados.

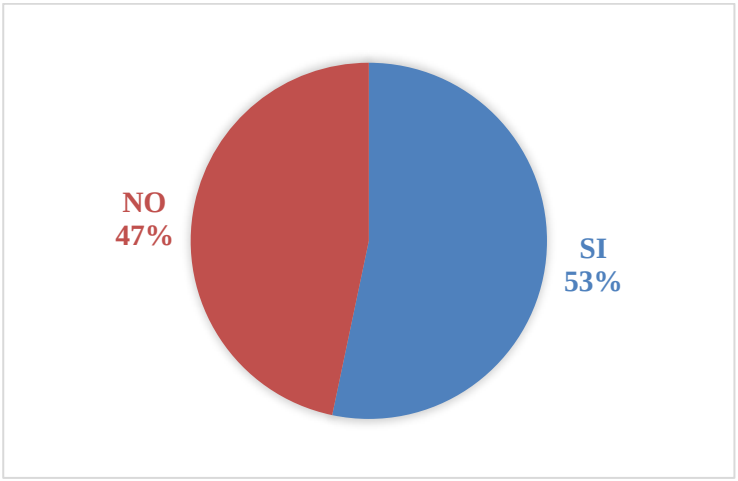
Estos resultados señalan una buena práctica en la mayoría de los casos, pero también destacan una oportunidad para mejorar la gestión de los activos informáticos mediante un registro completo y preciso de todos los recursos.

Pregunta 7. ¿Se implementa un sistema de control para evitar alteraciones no acreditadas en los elementos materiales de las instalaciones informáticas por parte del personal?

Tabla 8. *Medidas de seguridad para prevenir la modificación de tanto el hardware como el software por parte del personal.*

		Frecuencia	Porcentaje
Válido	SI	8	53.3
	NO	7	46.7
	Total	15	100

Figura 15. *Referente Pregunta 7*



Interpretación

El 53% de los encuestados indicó que no cuentan con un sistema de control para evitar alteraciones no autorizadas en los dispositivos informáticos, lo que sugiere una carencia generalizada en la organización. Por otro lado, el 47% restante afirmó haber implementado un sistema de control para este propósito, lo que indica que una minoría ha tomado medidas para proteger la integridad de los dispositivos.

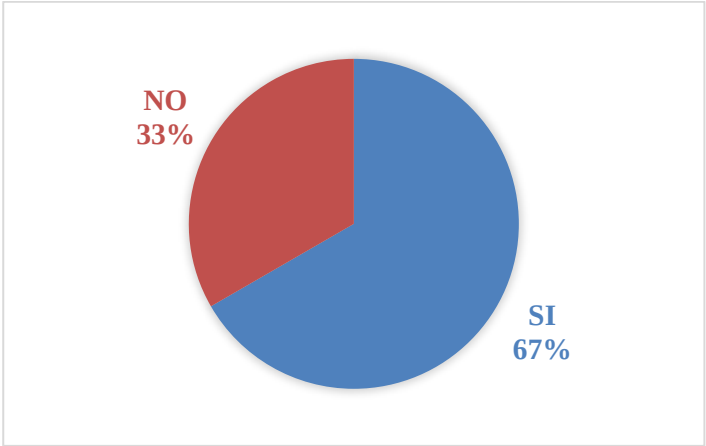
Estos hallazgos resaltan la necesidad de mejorar las medidas de control para prevenir manipulaciones no autorizadas, lo que podría comprometer la seguridad de la información. Implementar controles adecuados y supervisar activamente los dispositivos informáticos puede ayudar a mitigar este riesgo y fortalecer la seguridad en la organización.

Pregunta 8. ¿Se programa regularmente el mantenimiento preventivo de los equipos informáticos dentro de la organización?

Tabla 9. *Mantenimientos preventivos.*

		Frecuencia	Porcentaje
Válido	SI	10	66.7
	NO	5	33.3
	Total	15	100

Figura 16. *Referente Pregunta 8*



Interpretación

El 67% de los encuestados respondió "SI", lo que muestra que la colectividad de la organización planifica labores de mantenimiento preventivo para los equipos informáticos.

El 33% de los encuestados respondió "NO", lo que insinúa que una minoría no realiza esta planificación.

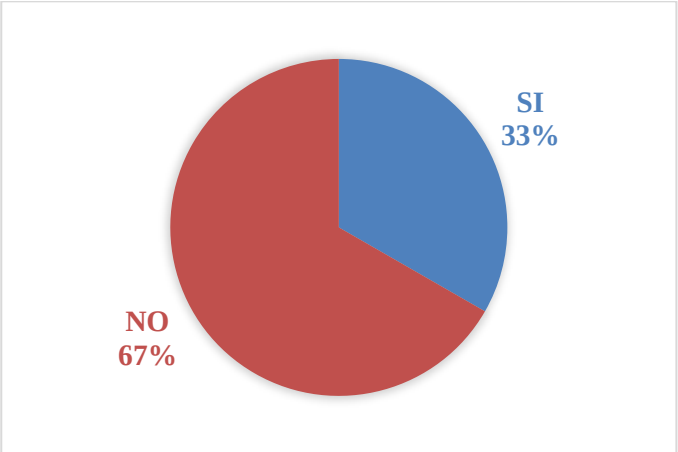
Estos resultados muestran que la mayoría de la organización reconoce la importancia de realizar labores de mantenimiento preventivo para los equipos informáticos. Este enfoque puede contribuir significativamente a la prolongación de la vida útil de los equipos, así como a reducir la probabilidad de fallas y mejorar el rendimiento general del sistema. Sin embargo, sería importante abordar las razones detrás de la falta de planificación en el 40% restante y considerar la implementación de un enfoque más proactivo hacia el mantenimiento de los equipos informáticos.

Pregunta 9. ¿Se realiza un seguimiento de las instalaciones informáticas remitidos a mantenimiento desde cada departamento?

Tabla 10. *Supervisión de los equipos de cómputo.*

		Frecuencia	Porcentaje
Válido	SI	5	33.3
	NO	10	66.7
	Total	15	100

Figura 17. *Referente Pregunta 9*



Interpretación

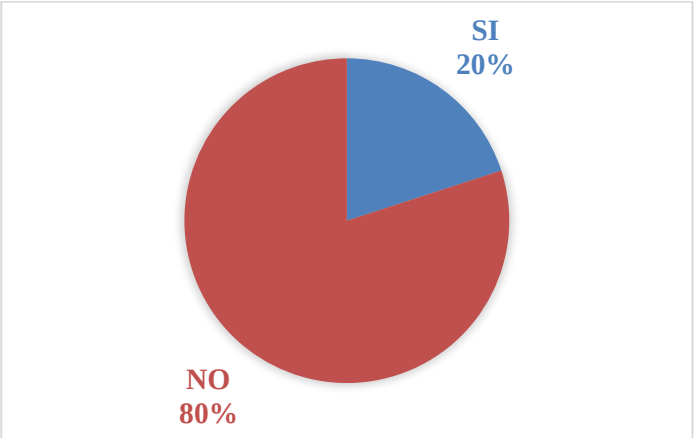
El 67% de los encuestados indicó que no se lleva a cabo un seguimiento de los dispositivos informáticos enviados a mantenimiento desde cada departamento, lo que refleja una falta de sistema para monitorear esta actividad en la mayoría de la organización. Por otro lado, solo el 33% respondió afirmativamente, lo que sugiere que una minoría realiza este seguimiento de manera sistemática. Estos hallazgos destacan la necesidad de establecer un proceso de seguimiento más riguroso para los dispositivos en mantenimiento, lo que podría mejorar la gestión de los recursos informáticos y reducir posibles retrasos en la resolución de problemas. Implementar un sistema de seguimiento efectivo podría ser crucial para optimizar la eficiencia en la gestión de activos informáticos y garantizar una atención oportuna a las necesidades de mantenimiento.

Pregunta 10. ¿Tiene usted conocimiento sobre los pasos a alcanzar en caso de comprobar algún inconveniente o riesgo en las instalaciones informáticas?

Tabla 11. *Supervisión de los dispositivos informáticos.*

		Frecuencia	Porcentaje
Válido	SI	3	20
	NO	12	80
	Total	15	100

Figura 18. *Referente Pregunta 10*



Interpretación

El 80% de los encuestados indicó no estar familiarizado con el procedimiento a seguir en caso de detectar fallos o amenazas en dispositivos informáticos, lo que insinúa un fallo generalizado de conocimiento al respecto. Solo el 20% afirmó estar familiarizado con dicho proceso. Estos resultados destacan la necesidad de proporcionar capacitación y aumentar la conciencia sobre los procedimientos de respuesta a incidentes de seguridad para garantizar una gestión eficiente de posibles amenazas o fallos en los dispositivos informáticos.

4.1.2. Entrevista

En el marco de la evolución constante de la tecnología y la creciente importancia de la seguridad de la información, se llevó a cabo una entrevista al Director/Gerente General de la compañía con el propósito de explorar y comprender más profundamente los desafíos y las

estrategias relacionadas con la gestión de la seguridad de la información en Empresa ADLINK S.A. Fundamentada en las buenas prácticas de recolección de información para el diseño de planes de seguridad informática de la norma ISO/IEC 27002, Estándar de ciberseguridad del Instituto Nacional de Estándares y Tecnología de EE. UU (NIST), Guías y mejores prácticas de seguridad informática (SANS), entre otras. Esta entrevista representó una oportunidad para destacar las iniciativas existentes, identificar áreas de mejora y trazar un camino hacia un futuro más seguro y resiliente. A través de un diálogo abierto y constructivo, se buscaba obtener una visión clara de las prácticas pasadas, las necesidades y las aspiraciones de la organización en materia de seguridad de la información.

Pregunta 1: ¿Cuál es la importancia de la seguridad informática en empresa ADLINK S.A.?

Respuesta: Considero que la seguridad informática es de suma importancia para nuestra empresa. La protección de los activos de información y la salvaguarda de la integridad de nuestros sistemas son fundamentales para certificar la continuación del negocio y la certeza de nuestros clientes.

Pregunta 2: ¿Ha enfrentado la empresa alguna pérdida de información?

Respuesta: puedo confirmar que, en el pasado, hemos enfrentado algunos incidentes de pérdida de información, Estos incidentes nos han servido como lecciones valiosas para fortalecer aún más nuestra postura de seguridad y mejorar continuamente nuestros sistemas y procedimientos para proteger nuestros activos de información.

Pregunta 3: ¿Empresa ADLINK S.A. realiza políticas de seguridad en sus métodos informáticos?

Respuesta: Actualmente no disponemos de unas políticas de seguridad.

Pregunta 4: ¿Los dispositivos informáticos cuentan con acceso a internet y una apropiada corriente de aire?

Respuesta: Los equipos informáticos están equipados con acceso a internet, así como con medidas de seguridad adecuadas para proteger nuestra red y datos. Esto incluye firewalls, sistemas de detección de intrusiones y antivirus actualizados regularmente para prevenir y mitigar posibles amenazas cibernéticas. Además, nos aseguramos de que los equipos informáticos estén ubicados en áreas con una adecuada ventilación para garantizar un funcionamiento óptimo y prevenir el sobrecalentamiento, lo que podría afectar el rendimiento y la vida útil de los equipos.

Pregunta 5: ¿La compañía tiene mano de obra concretamente determinado a la seguridad informática y el soporte técnico?

Respuesta: En ADLINK S.A., reconocemos la importancia crítica de la seguridad informática y el soporte técnico para garantizar el funcionamiento eficiente y seguro de nuestros sistemas informáticos. Por lo tanto, contamos con personal específicamente asignado a estas áreas clave. Tenemos un equipo dedicado de expertos en seguridad informática que monitorean constantemente nuestra red, identifican posibles amenazas y toman medidas proactivas para proteger nuestros sistemas y datos contra ataques cibernéticos.

Pregunta 6: ¿Empresa ADLINK S.A. realiza mantenimiento informático regular en sus computadoras?

Respuesta: En ADLINK S.A., aseguramos un mantenimiento informático regular en nuestras computadoras como parte de nuestras prácticas operativas estándar. Este mantenimiento incluye actividades planificadas, como revisiones periódicas, actualizaciones de software y hardware, así como la limpieza y optimización de sistemas. Esta estrategia proactiva nos permite anticipar y abordar posibles problemas antes de que se conviertan en inconvenientes importantes, garantizando así la fiabilidad y el rendimiento óptimo de nuestras computadoras.

Pregunta 7: ¿La compañía dispone de un servidor exclusivo para sus operaciones?

Respuesta: No.

Pregunta 8: ¿Se han implementado salvaguardas en las computadoras para prevenir daños causados por cortes de energía y picos de voltaje?

Respuesta: Actualmente esta fuera de servicio el sistema de protección que teníamos disponible.

Pregunta 9: ¿La empresa cuenta con mecanismos de copia de seguridad para prevenir la pérdida de datos?

Respuesta: No, la organización no cuenta con sistemas de respaldo para evitar la pérdida de información.

Durante la entrevista, el director de ADLINK S.A. discutió varios aspectos relacionados con la seguridad informática y la gestión de sistemas de información en la empresa. Se destacó la importancia de implementar políticas de seguridad informática, así como la asignación de personal específico para esta tarea. Sin embargo, se reconoció una falta de un plan de seguridad informática eficiente, así como la ausencia de un servidor exclusivo y medidas de protección contra apagones y sobretensiones. Estas deficiencias indican áreas críticas que deben abordarse para mejorar la protección de los activos de información y garantizar el funcionamiento eficiente de los sistemas informáticos en ADLINK S.A.

4.1.3. Resumen de las principales debilidades.

Falta de un plan de seguridad informática eficiente: Se reconoce la necesidad de implementar políticas y procedimientos sólidos para garantizar la seguridad de la información, pero existe una discrepancia entre la percepción de la dirección y la realidad experimentada por el personal en cuanto a la implementación efectiva de estas políticas.

Ausencia de un servidor exclusivo: No se dispone de un servidor dedicado para respaldar las operaciones de la empresa, lo que puede afectar la eficiencia y la confiabilidad

de los servicios informáticos.

Carencia de medidas de protección contra apagones y sobretensiones: La falta de dispositivos de respaldo y protección eléctrica puede aumentar el riesgo de pérdida de datos y daños en el hardware durante eventos imprevistos.

Deficiencias en el mantenimiento informático regular: Aunque se reconoce la importancia del mantenimiento preventivo de los equipos informáticos, no se llevan a cabo actividades regulares para garantizar su óptimo funcionamiento y seguridad.

4.1.4. Gestión de Riesgos.

Dentro de la gestión de riesgos empresariales, es de vital importancia analizar detalladamente las posibles repercusiones que estos riesgos puedan tener para la empresa, especialmente en lo que concierne a los procesos que implican información crítica. La identificación de riesgos constituye el primer paso crucial en este proceso. Implica identificar todas las posibles amenazas que podrían afectar a la empresa, abarcando riesgos como la seguridad informática, operativos, financieros, legales, regulatorios y otros que puedan surgir. Este análisis exhaustivo proporciona una base sólida para la posterior evaluación y gestión efectiva de los riesgos empresariales.

- Evaluación de riesgos: Una vez identificados los riesgos, se evalúa su impacto potencial y la probabilidad de ocurrencia. Esto permite priorizar los riesgos y determinar qué amenazas son las más críticas para la empresa.
- Desarrollo de estrategias de mitigación: Una vez que se han identificado y evaluado los riesgos, se desarrollan estrategias para mitigarlos. Esto puede implicar implementar controles de seguridad adicionales, transferir el riesgo a través de seguros, evitar ciertas actividades o aceptar el riesgo si sus impactos son mínimos o gestionables.
- Implementación y monitoreo: Una vez que se han establecido las estrategias

de mitigación, se implementan y se monitorean de manera continua para garantizar su efectividad. Además, se revisan regularmente los riesgos para adaptarse a los cambios en el entorno empresarial y tecnológico.

- Cultura de gestión de riesgos: Es importante fomentar una cultura organizacional que promueva la conciencia y la responsabilidad sobre la gestión de riesgos en todos los niveles de la empresa. Esto implica la participación activa de los empleados en la identificación y mitigación de riesgos, así como la comunicación abierta sobre los desafíos y las estrategias de gestión de riesgos.

4.1.4.1. Identificación de activos

a) Reconocer la importancia de cada activo en posesión de la empresa es fundamental, dado que estos contienen información crítica.
b) Esta priorización se fundamenta en la excelencia de estos activos para los ordenamientos de la compañía.
c) Subsecuentemente, identificamos las amenazas y fragilidades afines con estos activos prioritarios. Este proceso nos consiente valorar el posible impacto que podrían experimentar los activos de la compañía.

4.1.4.2. Inventario de Activos Informáticos

El propósito primordial de un Inventario de Activos Informáticos radica en brindar una visión completa y detallada de todos los recursos tecnológicos y de información que posee una organización. Al permitir un conocimiento claro y actualizado de los activos, incluyendo hardware, software, datos y recursos de red, el inventario facilita una gestión eficiente de estos elementos, minimizando costos, optimizando su uso y evitando duplicidades. Además, contribuye a la seguridad de la información al identificar riesgos y permitir la implementación de medidas de protección adecuadas, garantiza el cumplimiento

normativo al documentar los activos de manera precisa, y sirve como base para la planificación estratégica de tecnología de la información, al proporcionar información sobre la infraestructura existente y las necesidades futuras de la organización en términos de tecnología y recursos informáticos.

4.1.5. Utilización de la metodología MAGERIT para llevar a cabo el análisis y la valoración del riesgo

4.1.5.1. Comprobar los activos notables para la empresa.

- [D] Datos: La información constituye el elemento central para brindar sus productos.
  - Base de datos de: proveedores, compradores, comercializaciones y empleados.
- [SW] Software: Entre las aplicaciones encontramos:
  - De desarrollo propio (Control de ventas e inventarios)
  - Sistema de gestión de abonados
  - Sistema de gestión de OLTs
  - Sistema de gestión de equipos MIMOSA
  - Sistema de geolocalización de infraestructura GPON.
  - Microsoft Office (Word y Excel).
- [HW] hardware:
  - Ordenadores (3): DELL LATTITUDE 34075 SFF I7-1200 16GB 2TB WIN11 PRO, con monitor DELL de 15.6.
  - 60 km de infraestructura GPON
  - Equipos de gestión de red: OLTs TPLINK-CDATA-VSQL
  - Router (1): Mikrotik, SWITCH MIKROTIK-UBIQUITI.
  - (800) CPE TPLINK, HUAWEI, CDATA-
  - Puntos de acceso (60): MiKROTIK, TPLINK-UBIQUITI

- Respaldo de Energía (1): UPS batería
- Fusionadoras (2): SUMITOMO-SIGNALFIRE

- [PERSONAL] Personal: Se considera como personal aquellos colaboradores relacionados con la gestión de información:
- Personal Administrativo
- Personal TIC

A continuación, se ofrece un resumen conciso de los distintas propiedades o discernimientos de un activo:

- Confidencialidad: Garantizar que la información esté restringida únicamente a las personas con los permisos apropiados es crucial para evitar posibles consecuencias negativas. ¿Qué perjuicio ocasionaría si la información fuera conocida por alguien que no debería tener acceso a ella?
- Integridad: Asegurar la integridad de los activos de información implica mantenerlos libres de alteraciones no autorizadas. ¿Qué consecuencias negativas acarrearía si estos activos estuvieran dañados o corruptos?
- Disponibilidad: Garantizar la disponibilidad y usabilidad de los activos para los usuarios que los requieran es esencial. ¿Qué consecuencias negativas resultarían si estos activos no estuvieran disponibles o no pudieran ser utilizados?

Tabla 12. *Factores para evaluar los activos*

DESCRIPCION	VALOR	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
EXTREMO	5	¿Qué perjuicio ocasionaría si la información fuera conocida por alguien que no debería tener acceso a ella?	¿Qué consecuencias negativas acarrearía si estos activos estuvieran dañados o corruptos?	¿Qué consecuencias negativas resultarían si estos activos no estuvieran disponibles o no pudieran ser utilizados?
MUY ALTO	4			
ALTO	3			
MEDIO	2			
BAJO	1			
DEPRECIABLE	0			

Fuente: Cevallos (2019)

La valoración de activos se llevó a cabo mediante una combinación de una escala cuantitativa y una escala cualitativa. En esta evaluación, se utilizaron criterios que van desde el nivel 5 hasta el nivel 0. En el nivel 5, se considera que la valoración ante una pérdida de un activo debido a una amenaza es alta y crítica para el área de Tecnologías de la Información y Comunicación (TICS). Por otro lado, en el nivel 0, se representan pérdidas despreciables o nulas para el área de TICS. Esta combinación de escalas permite una evaluación exhaustiva de los activos, teniendo en cuenta tanto aspectos cuantitativos como cualitativos, lo que proporciona una visión más completa de la importancia y el impacto de los activos en el área de TICS.

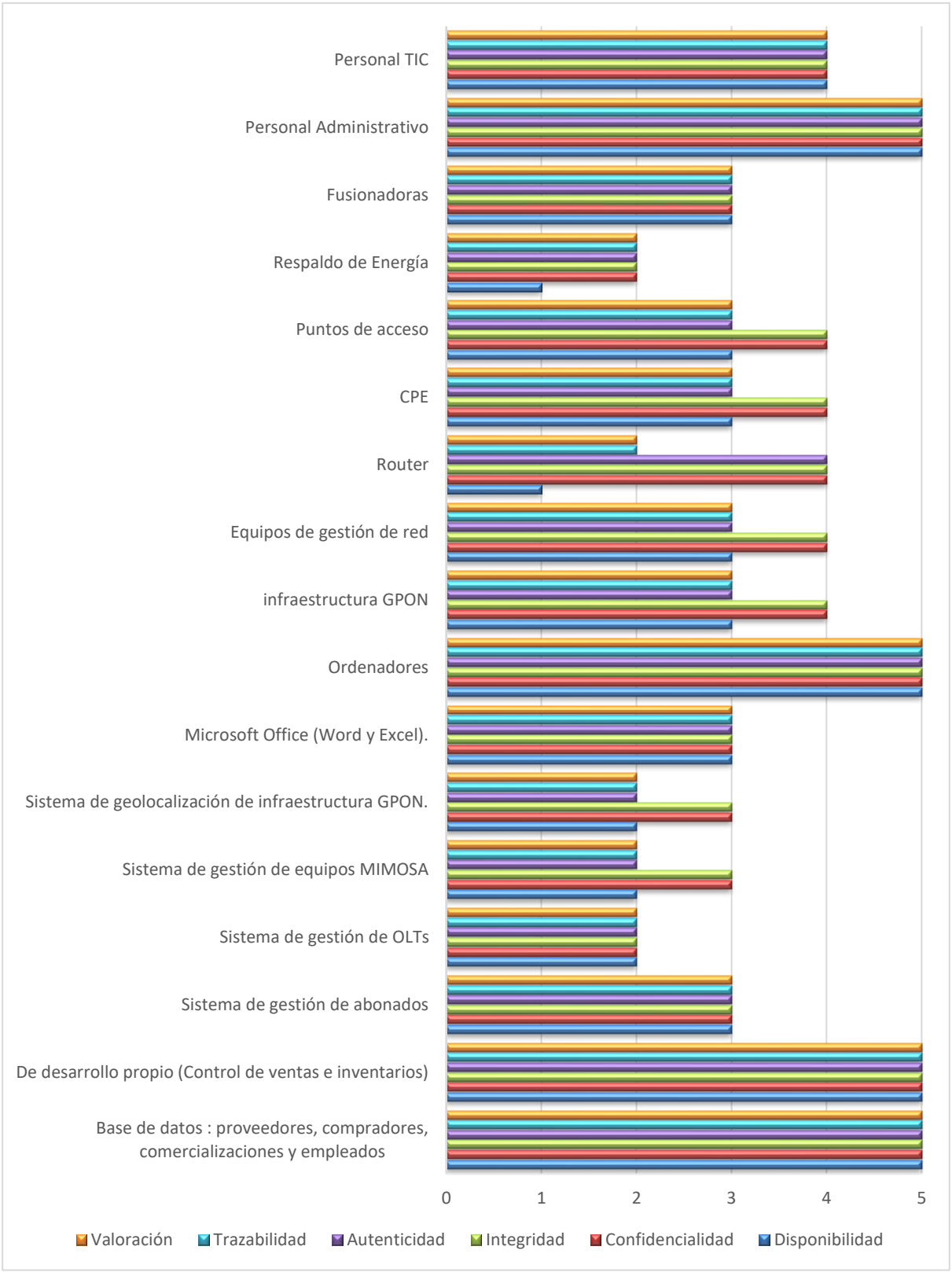
Tabla 13. *Valoración de Activos*

	Disponibilidad	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Valoración
[D] Datos:						
Base de datos: proveedores, compradores, comercializaciones y empleados	5	5	5	5	5	5
[SW] Software						
De desarrollo propio (Control de ventas e inventarios)	5	5	5	5	5	5
Sistema de gestión de abonados	3	3	3	3	3	3

Sistema de gestión de OLTs	2	2	2	2	2	2
Sistema de gestión de equipos MIMOSA	2	3	3	2	2	2
Sistema de geolocalización de infraestructura GPON.	2	3	3	2	2	2
Microsoft Office (Word y Excel).	3	3	3	3	3	3
[HW] hardware:						
Ordenadores	5	5	5	5	5	5
infraestructura GPON	3	4	4	3	3	3
Equipos de gestión de red	3	4	4	3	3	3
Router	1	4	4	4	2	2
CPE	3	4	4	3	3	3
Puntos de acceso	3	4	4	3	3	3
Respaldo de Energía	1	2	2	2	2	2
Fusionadoras	3	3	3	3	3	3
[PERSONAL] Personal						

Personal Administrativo	5	5	5	5	5	5
Personal TIC	4	4	4	4	4	4

Figura 19. *Identificación y Valoración de activos*



La Gráfica 19 muestra el estado actual de la Seguridad de la Información (SI) de la

empresa, utilizando una escala de valoración del 1 al 5. Esta evaluación revela que la mayoría de los activos tienen un nivel alto de valoración de pérdida, lo que sugiere una situación preocupante. Esta evaluación se alinea con los hallazgos presentados a lo largo de la investigación, que destacan la falta de un plan de gestión de SI en la empresa.

Los activos más afectados, según la Gráfica 19, incluyen al Personal, las Bases de Datos, los Ordenadores y algunos softwares, especialmente aquellos desarrollados internamente por la empresa. Estos activos parecen ser los más vulnerables a riesgos y amenazas debido a la ausencia de un plan de gestión de SI, lo que sugiere la necesidad urgente de implementar medidas para protegerlos y mitigar los riesgos asociados.

4.1.5.2. Comprobar las amenazas y vulnerabilidades

- **Amenazas**

Tabla 14. *Aspectos a considerar en la evaluación de activos:*

AMENAZA	DESCRIPCION
(N) DESASTRES NATURALES	Ocasionada de manera directa o indirecta por desastres naturales, como terremotos o inundaciones.
(I) DE ORIGEN INDUSTRIAL	Eventos resultantes de la actividad humana, como la contaminación o fallos eléctricos, de naturaleza industrial.
"E" ERRORES Y FALLOS NO INTENCIONADOS	Errores no deliberados provocados por individuos con acceso al sistema de información
(A) ATAQUES INTENCIONADOS	Sabotajes o ataques intencionados perpetrados por individuos con acceso al sistema de información

Fuente: Aguasanta (2024)

Tabla 15. *Evaluación de las Amenazas y Dimensiones Afectadas*

ACTIVO	CODIGO	AMENAZA	DIMENSIONES AFECTADAS
[D] Datos:			
Base de datos: proveedores, compradores, comercializaciones y empleados			
	[E.1]	errores cometidos por los usuarios.	Disponibilidad, Confidencialidad, Integridad, Autenticidad, Trazabilidad, Valoración
	[E.2]	Los errores cometidos por el administrador del sistema.	
	[E.15]	Cambios no intencionados en la información	
	[E.18]	La eliminación o destrucción de la información	
	[E.19]	La filtración o divulgación no autorizada de información.	
	[A.5]	La suplantación de identidad de un usuario en el sistema	

	[A.6]	Acceso no autorizado	
	[A.11]	La alteración intencionada de la información	
	[I.5]	Daño causado por un fallo físico o lógico	
	[I.5]	Daño causado por un fallo físico o lógico	
ACTIVO	CODIGO	AMENAZA	DIMENSIONES AFECTADAS
[SOFTWARE]			
De desarrollo propio, Sistema de gestión de abonados, Sistema de gestión de OLTs, Sistema de gestión de equipos MIMOSA, Sistema de geolocalización de infraestructura GPON, Microsoft Office (Word y Excel).			
	[E.1]	Error de uso	Disponibilidad, Confidencialidad, Integridad, Autenticidad, Trazabilidad, Valoración

	[E.20]	Defectos o vulnerabilidades en los programas de software	
	[A.6]	El uso no autorizado o la copia ilegal de software	
	[I.6]	Interrupción del suministro eléctrico	
	[E.2]	Los errores cometidos por el administrador del sistema o por personas responsables de la instalación y operación	
ACTIVO	CODIGO	AMENAZA	DIMENSIONES AFECTADAS
[HARDWARE]			
Ordenadores, infraestructura GPON, Equipos de gestión de red, Router, CPE, Puntos de acceso, Respaldo de Energía			
	[E.2]	Las equivocaciones o errores cometidos por individuos con responsabilidades de instalación y operación, como administradores del sistema	Disponibilidad, Confidencialidad, Integridad, Autenticidad, Trazabilidad, Valoración
	E.23]	Los errores durante el mantenimiento o la actualización del hardware	

	[A.11]	La suplantación de identidad de un usuario en el sistema	
	[A.6]	Ingreso sin autorización	
	[I.6]	Interrupción del suministro eléctrico	
ACTIVO	CODIGO	AMENAZA	DIMENSIONES AFECTADAS
[PERSONAL]			
Personal Administrativo, Personal TIC			
	[E.7]	Deficiencias en la organización	Disponibilidad, Confidencialidad, Integridad, Autenticidad, Trazabilidad, Valoración
	[E.19]	Fugas de información	

En la Tabla 15 se evidencia la presencia de amenazas de diversos tipos, incluyendo ataques intencionados [A], errores y fallos no intencionados [E], y amenazas de origen industrial [I]. Estas amenazas afectan principalmente la confidencialidad y disponibilidad de los activos. Para mitigar el impacto de estas amenazas y garantizar la protección de los activos, es crucial implementar controles efectivos que aborden adecuadamente las dimensiones

afectadas.

Estos controles deben diseñarse con el objetivo de reducir o eliminar la posibilidad de que estas amenazas comprometan la confidencialidad y disponibilidad de los activos. Esto podría implicar la implementación de medidas de seguridad, como firewalls, sistemas de detección de intrusiones, políticas de acceso y autenticación robustas, sistemas de respaldo de datos, capacitación del personal en seguridad informática, entre otros.

- **Vulnerabilidades**

Las vulnerabilidades representan las probabilidades de que una amenaza pueda materializarse y afectar un activo específico. Es importante reconocer que no todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos pueden ser vulnerables a la acción de hackers que intentan acceder de manera no autorizada, mientras que una instalación eléctrica puede ser vulnerable a un cortocircuito debido a un mal funcionamiento o falta de mantenimiento.

Cuando se realiza un análisis de riesgos, es esencial considerar la vulnerabilidad de cada activo. Esto implica evaluar la susceptibilidad de cada activo a las diferentes amenazas que pueden afectarlo. Al comprender las vulnerabilidades específicas de cada activo, se pueden desarrollar estrategias y medidas de seguridad adecuadas para mitigar los riesgos y proteger los activos de manera efectiva.

Tabla 16. *Amenazas y Vulnerabilidades:*

ACTIVO	AMENAZA	VULNERABILIDAD
BASE DE DATOS: proveedores, compradores, comercializaciones y empleados	errores cometidos por los usuarios.	La ausencia de fundamentos de empleo y procedimientos para la administración del sistema
	Los errores cometidos por el administrador del sistema.	La habilitación de tipologías y ocupaciones de base de datos que no son necesarias
	Cambios no intencionados en la información	Configuraciones débiles y/o predeterminadas.
	La eliminación o destrucción de la información	La ausencia de controles en la disolución o alteración de responsabilidades
	La filtración o divulgación no autorizada de información.	La activación de características y funciones en la base de datos que no son necesarias.

	La suplantación de identidad de un usuario en el sistema	El uso de contraseñas débiles o inseguras.
	Acceso no autorizado	El uso de contraseñas débiles o inseguras
	La alteración intencionada de la información	La ausencia de supervisión de los privilegios de acceso
	Daño causado por un fallo físico o lógico	La carencia de una definición clara de los requisitos de seguridad
	Daño causado por un fallo físico o lógico	Fallo de ensayos al software
	Error de uso	Falla de recopilaciones de usanza y administración del sistema
SOFTWARE: De desarrollo propio (Control de ventas e inventarios) Sistema de gestión de abonados Sistema de gestión de OLTs, Sistema de gestión de equipos MIMOSA Sistema de geolocalización de infraestructura GPON.	Defectos o vulnerabilidades en los programas de software	La ausencia de observaciones para un progreso innegable de software.
	El uso no autorizado o la copia ilegal de software	La carencia de un control adecuado durante el proceso de desarrollo.

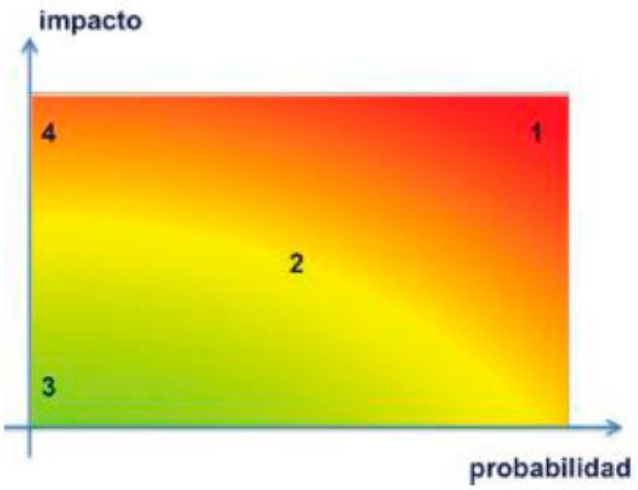
Microsoft Office (Word y Excel).	Interrupción del suministro eléctrico	La ausencia de equipos que proporcionen energía ininterrumpida (UPS)
	Los errores cometidos por el administrador del sistema o por personas responsables de la instalación y operación	La habilitación de puertos USB
	Las equivocaciones o errores cometidos por individuos con responsabilidades de instalación y operación, como administradores del sistema	La carencia de un software antivirus con licencia
	Los errores durante el mantenimiento o la actualización del hardware	La ausencia de mantenimiento tanto del hardware como del software
HARDWARE: Ordenadores infraestructura GPON Equipos de gestión de red Router	La suplantación de identidad de un usuario en el sistema	La falta de capacitación en seguridad de la información

CPE Puntos de acceso Respaldo de Energía Fusionadoras	Ingreso sin autorización	La ausencia de controles de bloqueo
[PERSONAL] Personal Personal Administrativo Personal TIC	Fugas de información	Falta de controles en la vinculación

4.1.5.3. Estimación del riesgo

El riesgo crece con el impacto y la posibilidad, lo que sugiere la existencia de diferentes áreas a considerar en la gestión del riesgo

Figura 20. *Estimación del Riesgo*



Fuente: Aguasanta (2024)

Tabla 17. *Estimación del Riesgo*

IMPACTO	PROBABILIDAD	RIESGO
MA: MUY ALTO	MA: PRACTICAMENTE SEGURO	MA; CRITICO, DAÑO EXTREMADAMENTE GRAVE
A: ALTO	A: PROBABLE	A: IMPORTANTE, DAÑO GRAVE
M: MEDIO	M: POSIBLE	M: APRECIABLE, DAÑO IMPORTANTE
B: BAJO	B: POCO PROBABLE	B: BAJO, DAÑO MENOR
MB: MUY BAJO	MB: MUY ALTO	MB: DESPRECIABLE, IRRELEVANTE A EFECTOS PRACTICOS

Fuente: Aguasanta (2024)

Figura 21. *Mapa de calor de la estimación impacto*

Impacto		Degradación				
		1 (MB)	10% (B)	50% (M)	90% (A)	100% (MA)
Probabilidad	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Aguasanta (2024)

ACTIVO	AMENAZA	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	AUTENTICIDAD	TRAZABILIDAD	DEGRADACIÓN
BASE DE DATOS: proveedores, compradores, comercializaciones y empleados	errores cometidos por los usuarios.	MA	MB	B	B	B	M
	Los errores cometidos por el administrador del sistema.	B	MB	B	B	B	B
	Cambios no intencionados en la información	A	B	A	A	A	A
	La eliminación o destrucción de la información	B	MB	B	B	B	B
	La filtración o divulgación no autorizada de información.	A	B	A	A	A	A
	La suplantación de identidad de un usuario en el sistema	B	MB	B	B	B	B
	Acceso no autorizado	MA	M	M	M	M	M
	La alteración intencionada de la información	B	B	B	B	B	B
	Avería de origen físico o lógico	A	B	A	A	A	A

	Avería de origen físico o lógico	MA	A	MA	MA	MA	MA
SOFTWARE: De desarrollo propio (Control de ventas e inventarios)	Error de uso	MA	M	M	M	M	M
Sistema de gestión de abonados	Defectos o vulnerabilidades en los programas de software	MA	M	M	M	M	M
Sistema de gestión de OLTs, Sistema de gestión de equipos MIMOSA	El uso no autorizado o la copia ilegal de software	MA	M	M	M	M	M
Sistema de geolocalización de infraestructura GPON	Interrupción del suministro eléctrico	B	MB	B	B	B	B
	Los errores cometidos por el administrador del sistema o por personas responsables de la instalación y operación	B	MB	B	B	B	B
HARDWARE: Ordenadores	Las equivocaciones o errores cometidos	A	A	MA	MA	MA	MA

infraestructura GPON	por individuos con responsabilidades de instalación y operación, como administradores del sistema						
Equipos de gestión de red							
Router							
CPE							
Puntos de acceso	Los errores durante el mantenimiento o la actualización del hardware	MA	M	M	M	M	M
Respaldo de Energía	La suplantación de identidad de un usuario en el sistema	M	M	M	M	M	M
Fusionadoras	Ingreso sin autorización	M	M	M	M	M	M
	Interrupción del suministro eléctrico	M	M	M	M	M	M
[PERSONAL] Personal	Escapes de información	MA	MA	MA	MA	MA	MA
Personal Administrativo							
Personal TIC							

Tabla 18. *Matriz de Riesgo*

Activo	Código	Código Riesgo	Amenaza	Vulnerabilidad	Impacto	Probabilidad de ocurrencia	Evaluación del riesgo	Degradación
BASE DE DATOS: proveedores, compradores, comercializaciones y empleados	[E.1]	R1	errores cometidos por los usuarios.	La ausencia de manuales de uso y procedimientos para el manejo del sistema	M	A	A	M
	[E.2]	R2	Los errores cometidos por el administrador del sistema.	La habilitación de características y funciones de base de datos que no son necesarias	B	A	M	B

	[E.15]	R3	Cambios no intencionados en la información	Configuraciones débiles y/o predeterminadas.	A	B	A	A
	[E.18]	R4	La eliminación o destrucción de la información	La ausencia de controles en la desvinculación o cambio de responsabilidades	B	MB	MB	B
	[E.19]	R5	La filtración o divulgación no autorizada de información.	La activación de características y funciones en la base de datos que no son necesarias.	A	MB	M	A

	[A.5]	R6	La suplantación de identidad de un usuario en el sistema	El uso de contraseñas débiles o inseguras.	B	MB	MB	B
	[A.6]	R7	Acceso no autorizado	El uso de contraseñas débiles o inseguras	M	MB	B	M
	[A.11]	R8	La alteración intencionada de la información	La ausencia de supervisión de los privilegios de acceso	B	MB	MB	B
	[I.5]	R17	Avería de origen físico o lógico	Falta de claridad en la definición de requerimientos de seguridad	A	B	A	A

	[I.5]	R18	Avería de origen físico o lógico	Falta de pruebas al software	MA	B	MA	MA
SOFTWARE: De desarrollo propio (Control de ventas e inventarios) Sistema de gestión de abonados Sistema de gestión de OLTs, Sistema de gestión de equipos MIMOSA Sistema de geolocalización de infraestructura GPON	[E.1]	R19	Error de uso	Falta de manuales de uso y manejo del sistema	M	M	M	M
	[E.20]	R20	Defectos o vulnerabilidades en los programas de software	La ausencia de consideraciones para un desarrollo seguro de software.	M	B	M	M
	[A.6]	R21	El uso no autorizado o la copia ilegal de software	La carencia de un control adecuado durante el proceso de desarrollo.	M	MB	B	M

	I.6]	R23	Interrupción del suministro eléctrico	La ausencia de equipos que proporcionen energía ininterrumpida (UPS)	B	MB	MB	B
	[E.2]	R24	Los errores cometidos por el administrador del sistema o por personas responsables de la instalación y operación	La habilitación de puertos USB	B	B	MB	B

HARDWARE: Ordenadores infraestructura GPON Equipos de gestión de red Router CPE Puntos de acceso Respaldo de Energía Fusionadoras	[E.2]	R25	Las equivocaciones o errores cometidos por individuos con responsabilidades de instalación y operación, como administradores del sistema	La carencia de un software antivirus con licencia	MA	B	MA	MA
	E.23]	R26	Los errores durante el mantenimiento o la actualización del hardware	La ausencia de mantenimiento tanto del hardware como del software	M	B	M	M

	[A.6]	R27	La suplantación de identidad de un usuario en el sistema	La falta de capacitación en seguridad de la información	M	B	M	M
	[A.11]	R28	Ingreso sin autorización	La ausencia de controles de bloqueo	M	MB	B	M
	[I.6]	R29	Interrupción del suministro eléctrico	La carencia de dispositivos que proporcionen energía ininterrumpida (UPS)	M	MB	B	M
[PERSONAL] Personal Personal Administrativo Personal TIC	[E.19]	R38	Escapes de información	Falla de revisiones en la vinculación	MA	B	MA	MA

El mapa de calor se utiliza para visualizar y analizar datos en función de su distribución espacial o temporal. Se representa gráficamente mediante colores para resaltar áreas con valores altos o bajos en un conjunto de datos. Este tipo de visualización ayuda a identificar patrones, tendencias y áreas de concentración, lo que facilita la toma de decisiones informadas. En el contexto de la gestión de riesgos, un mapa de calor puede utilizarse para identificar y priorizar áreas de alto riesgo en función de la probabilidad y el impacto de los riesgos, como una herramienta para asignar recursos y desarrollar estrategias de mitigación eficaces.

Tabla 19. *Mapa de Calor*

<table>
<tr><td></td><td colspan="5">PROBABILIDAD</td></tr>
<tr><td>Riesgo</td><td>MB</td><td>B</td><td>M</td><td>A</td><td>MA</td></tr>
<tr><td>MA</td><td colspan="2">R30, R31, R32</td><td colspan="2">R18, R25, R38</td><td></td></tr>
<tr><td>A</td><td colspan="2">R5, R9</td><td colspan="2">R3, R17</td><td></td></tr>
<tr><td>M</td><td colspan="2" rowspan="3">R7, R21, R28, R29</td><td>R20, R26, R27</td><td>R19</td><td>R1</td></tr>
<tr><td>B</td><td colspan="2" rowspan="2">R11, R24, R37,</td><td></td><td>R2</td></tr>
<tr><td>MB</td><td colspan="2">R4, R6, R8, R10, R12, R13, R14, 15, R16, R22, R23, R33, R34, R35, R36</td><td></td><td></td></tr>
</table>

Es evidente que es de suma importancia abordar los activos que se encuentran en riesgo extremo, trabajando para reducirlos al menos a un nivel moderado. Además, es esencial dirigir nuestra atención hacia los activos críticos que actualmente presentan un riesgo moderado, con el objetivo de disminuirlos hasta alcanzar un nivel de riesgo bajo. Esta estrategia nos permitirá fortalecer la seguridad de nuestros activos más valiosos y mitigar las posibles amenazas que puedan afectarlos.

Tabla 20. *Tolerancia del riesgo*

B	Baja	Vigilar y examinar según sea requerido. Riesgos poco probables y de impacto mínimo
M	Moderada	Evaluar el riesgo y determinar la adecuación y eficacia de los controles implementados.
A	Alta	Es crucial prestar la atención adecuada a los riesgos poco probables, pero de impacto muy alto.
MA	Extrema	Necesita una respuesta y atención inmediatas. Riesgos altamente probables y de impacto muy alto

4.1.5.4. Determinación de las salvaguardas aplicables frente al riesgo

El objetivo de las salvaguardas o controles es reducir la probabilidad de una amenaza y limitar la posible degradación que un activo puede sufrir.

Para desarrollar esta sección, a la norma de seguridad ISO/IEC 27002:2022. Así, en función al activo, la amenaza y la vulnerabilidad identificados, así como al resultado obtenido del análisis de riesgo, se establecen los controles respectivos.

Este enfoque permite diseñar e implementar medidas específicas que mitiguen los riesgos identificados, garantizando la protección adecuada de los activos de información y fortaleciendo la seguridad de la organización en su conjunto

Tabla 21. *Salvaguardas o controles aplicables*

Control	Aplicable	No Aplicable	descripción
5.37 Procedimientos operativos documentados	✓		Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información
5.15 Control de acceso	✓		garantizar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.
5.18 Derechos de acceso	✓		garantizar que el acceso a la información y otros activos asociados se defina y autorice de acuerdo con los requisitos comerciales
6.3 Sensibilización, educación y formación en materia de seguridad de la información	✓		Asegurar que el personal y las partes interesadas relevantes conozcan y cumplan con sus responsabilidades de seguridad de la información
8.32 Gestión del cambio	✓		Preservar la seguridad de la información al ejecutar cambios

8.5 Autenticación segura	✓	garantizar que un usuario o una entidad se autentica de forma segura cuando se otorga acceso a sistemas, aplicaciones y servicios
8.29 Pruebas de seguridad en el desarrollo y la aceptación	✓	validar si se cumplen los requisitos de seguridad de la información cuando las aplicaciones o el código se implementan en el entorno de producción.
8.31 Separación de los entornos de desarrollo, prueba y producción	✓	proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba
7.11 Servicios públicos de apoyo	✓	evitar la pérdida, el daño o el compromiso de la información y otros activos asociados, o la interrupción de las operaciones de la organización debido a fallas e interrupciones de los servicios públicos de apoyo
5.17 Información de autentificación	✓	asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión, incluido el

		asesoramiento al personal sobre el manejo adecuado de la información de autenticación
6.8 Informes de eventos de seguridad de la información	✓	respaldar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que pueden ser identificados por el personal
5.26 Respuesta a los incidentes de seguridad de la información	✓	Garantizar una respuesta eficiente y eficaz a los incidentes de seguridad de la información
8.7 Protección contra el malware	✓	garantizar que la información y otros activos asociados estén protegidos contra malware
7.13 Mantenimiento de los equipos	✓	operaciones de la organización causada por la falta de mantenimiento
7.7 Escritorio y pantalla despejados	✓	Reducir los riesgos de acceso no autorizado, pérdida y daño de la información en escritorios, pantallas y en otros lugares accesibles durante y fuera del horario normal de trabajo

4.1.5.5. Riesgo Residual

La tabla 22 proporciona una evaluación detallada de los riesgos asociados con diferentes activos, como bases de datos, software, hardware y personal, antes y después de la implementación de controles específicos. Cada riesgo se identificó mediante un código y se evalúa en términos de impacto, probabilidad de ocurrencia y la evaluación general del riesgo.

Antes de aplicar los controles, se realizó una evaluación inicial de los riesgos, clasificándolos según su impacto y probabilidad de ocurrencia. Esto proporcionó una visión general de los riesgos asociados con cada activo, desde aquellos con impacto moderado y baja probabilidad de ocurrencia hasta aquellos con impacto significativo y alta probabilidad de ocurrencia.

Después de implementar los controles, se llevó a cabo una reevaluación de los riesgos para estimar los aquellos residuales y la efectividad de las medidas tomadas. Los cambios en la estimación del riesgo revelo la eficacia de los controles implementados, lo que sugiere una reducción en el impacto o la probabilidad de ocurrencia del riesgo. Los resultados de la evaluación de riesgos proporcionan una base sólida para tomar decisiones informadas sobre medidas adicionales que puedan ser necesarias para mitigar los riesgos restantes. Esto podría incluir la revisión y mejora de los controles existentes, la implementación de nuevos controles o la asignación de recursos adicionales para abordar los riesgos identificados.

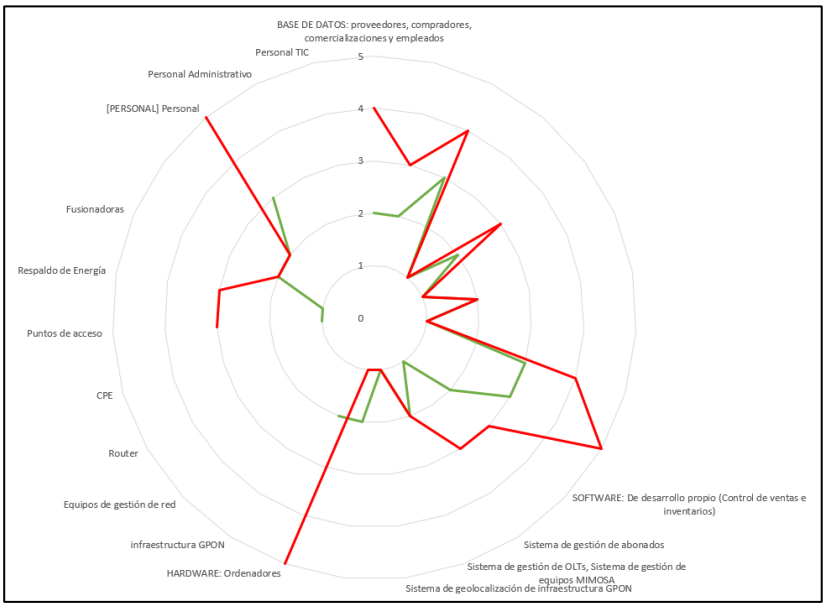
Tabla 22. *Estimación del efecto del riesgo residual con la aplicación de los controles ISO/IEC 27002:2022*

				Antes de Aplicar los controles		Después de Implementar los Controles	
Activo	Código	Código Riesgo	Impacto	Probabilidad de ocurrencia	Evaluación del riesgo	Probabilidad de ocurrencia	Evaluación del riesgo residual
BASE DE DATOS: proveedores, compradores,	[E.1]	R1	M	A	A	B	B

comercializaciones y empleados	[E.2]	R2	B	A	M	B	B
	[E.15]	R3	A	B	A	B	M
	[E.18]	R4	B	MB	MB	MB	MB
	[E.19]	R5	A	MB	M	MB	B
	[A.5]	R6	B	MB	MB	MB	MB
	[A.6]	R7	M	MB	B	MB	B
	[A.11]	R8	B	MB	MB	MB	MB
	[I.5]	R17	A	B	A	B	M
	[I.5]	R18	MA	B	MA	B	M
SOFTWARE: De desarrollo propio (Control de ventas e inventarios)	[E.1]	R19	M	M	M	M	B
Sistema de gestión de abonados	[E.20]	R20	M	B	M	B	MB
Sistema de gestión de OLTs, Sistema de gestión de equipos MIMOSA	[A.6]	R21	M	MB	B	MB	B
Sistema de geolocalización de infraestructura GPON	I.6]	R23	B	MB	MB	MB	MB

	[E.2]	R24	B	B	MB	B	MB
HARDWARE: Ordenadores infraestructura GPON Equipos de gestión de red Router CPE	[E.2]	R25	MA	B	MA	B	B
Puntos de acceso	E.23]	R26	M	B	M	B	MB
Respaldo de Energía	[A.6]	R27	M	B	M	B	MB
Fusionadoras	[A.11]	R28	M	MB	B	MB	B
	[I.6]	R29	M	MB	B	MB	B
[PERSONAL] Personal Administrativo Personal TIC	[E.19]	R38	MA	B	MA	B	M

Figura 22. *Evolución del Riesgo*



En la figura 22, se puede observar la evolución del riesgo en función de la estimación de la efectividad de los controles o salvaguardas efectuadas, la línea roja representa el riesgo previo a la implementación y la verde muestra el nuevo nivel del riesgo calculado después de la implementación.

4.1.5.6. Resultados.

Una vez realizado un minucioso análisis del contexto actual de ADLINK S.A., se ha identificado una serie de debilidades en la gestión de activos de la empresa. A pesar de su constante crecimiento y su incursión exitosa en el comercio en línea, ADLINK S.A. ha mostrado una falta de atención significativa hacia la seguridad informática, lo que ha expuesto vulnerabilidades en la protección de sus activos digitales. Esta falta de enfoque ha resultado en problemas recurrentes, como la pérdida de información valiosa y fallos en el sistema, que podrían haberse evitado con una gestión más efectiva de los activos. Por tanto, es imperativo que ADLINK S.A. priorice la implementación de un sólido Plan de Seguridad Informática que aborde estas debilidades y proteja adecuadamente sus activos digitales frente a amenazas potenciales.

CAPITULO V

PROPUESTA

5.1. Políticas de Seguridad de la Información para Empresa ADLINK S.A.

Las políticas de seguridad de la información en Empresa ADLINK S.A. están diseñadas como un conjunto de directrices y reglamentos específicos que orientan el manejo adecuado de los datos utilizados por la organización y su personal.

5.1.1. Política de Seguridad Informática Específica

- Objetivo:

El objetivo es establecer un protocolo efectivo para la administración conveniente de los activos de información, con el fin de reducir los riesgos asociados con pérdidas, modificaciones no autorizadas, accesos indebidos, divulgación no controlada, duplicación y alteraciones intencionadas de datos.

- Disposiciones facilitadas por la administración

La aprobación del responsable del departamento de Tecnologías de la Información y Comunicación (TICS) es necesaria para la política de seguridad de la información.

La política de seguridad debe ser revisada y comunicada regularmente al personal de TICS.

- Consideraciones sobre la organización de la seguridad informática:

- Propósito:

Elaborar un grupo de pautas de administración que utilicen como punto de referencia y control para dirigir y supervisar la aplicación de medidas de seguridad de la información dentro de la organización, con el fin de fortalecer la protección de los activos de datos y sistemas.

- Organización interna:

El responsable del departamento de TICS puede asignar responsabilidades por escrito

afines con la seguridad de la información a asociados competentes del equipo.

Es responsabilidad del responsable del departamento de TICS garantizar la adecuada ejecución de todas las actividades relacionadas con la seguridad de la información.

- Seguridad relacionada con el factor humano:

- Objetivo:

Garantizar que los usuarios estén adecuadamente informados sobre las medidas de seguridad de la información para reducir los riesgos de robos, fraudes o usos inapropiados de la misma.

- Proceso de pre-contratación:

Los miembros del equipo de TICS deben comprometerse mediante un acuerdo de confidencialidad antes de ser contratados.

- Durante el empleo:

Se llevarán a cabo charlas periódicas para educar y generar conciencia sobre las políticas de seguridad de la información.

Se designarán usuarios competentes en seguridad de la información para impartir capacitaciones.

- Cese de puesto de trabajo:

El departamento de Recursos Humanos debe notificar al área de TICS cuando un empleado deje la empresa para desactivar su acceso a los sistemas informáticos.

- Control de accesos:

- Objetivo:

Restringir y limitar el acceso a la información y sistemas de la empresa.

Requisitos de Negocio para el Control de Accesos:

Se proporcionará un manual de usuario para el uso adecuado y la gestión de los sistemas académicos.

Las contraseñas serán almacenadas de forma segura utilizando cifrado.

Se llevarán a cabo monitoreos en las cuentas de usuarios con actividad sospechosa.

- Responsabilidades del usuario:

Los usuarios deben proteger sus equipos de cómputo cuando no estén en uso.

Se prohíbe el acceso a las aplicaciones académicas utilizando las credenciales de otro usuario.

- Control de acceso a sistemas:

Se utilizarán métodos adecuados de autenticación y roles de privilegios de usuario.

Se asignarán cuentas de usuario y contraseñas, que deberán ser cambiadas en el primer inicio de sesión.

- Seguridad en los equipos:

Los equipos de cómputo deben contar con fuentes de energía ininterrumpida.

Se implementarán medidas de protección para el cableado de datos.

Se llevará a cabo mantenimiento preventivo y correctivo de los equipos utilizados por el personal administrativo.

- Auditoría interna:

Se implementarán revisiones internas periódicas para verificar el nivel de adhesión a los estándares de seguridad de la información.

Se establecerán programas de auditoría interna para planificar y llevar a cabo auditorías periódicas.

- Gestión de incidentes en la seguridad de la información y mejoras:

Se establecerá un proceso para notificar y responder a las vulnerabilidades de seguridad.

Se documentarán y comunicarán adecuadamente los informes sobre incidentes de

seguridad.

5.1.1.1. Guía de Instrucciones para la Capacitación de Usuarios en la Empresa

El propósito es proporcionar a los empleados una referencia detallada y estructurada sobre cómo utilizar eficazmente las herramientas, sistemas y recursos tecnológicos disponibles en la organización. Esta guía tiene como objetivo facilitar la formación y el desarrollo de habilidades entre los usuarios, permitiéndoles familiarizarse con los procedimientos operativos estándar, las mejores prácticas de seguridad, y las funcionalidades específicas de los sistemas informáticos utilizados en la empresa. En resumen, la guía tiene como propósito mejorar la eficiencia, la productividad y la seguridad de los empleados al proporcionarles la información necesaria para aprovechar al máximo los recursos tecnológicos disponibles en su entorno laboral.

Tabla 23. *Guía de Instrucciones para la Capacitación de Usuarios*

ACTIVIDADES	RESPONSABLES
Elaborar un plan de capacitación con fechas y horarios establecidos	Departamento de Informática
Es necesario gestionar el espacio físico para llevar a cabo las capacitaciones	Departamento de Informática
Debes enviar una invitación con la fecha de la capacitación	Departamento de Informática
Llevar a cabo la capacitación según lo previsto	Departamento de Informática
Es necesario elaborar un acta de participación	Departamento de Informática
FIN DEL PROCEDIMIENTO	

5.1.1.2. Manual para la Gestión de Hardware en la Empresa

la gestión eficiente de los recursos tecnológicos es fundamental para garantizar el óptimo funcionamiento de nuestras operaciones. Reconociendo la importancia del hardware en nuestros procesos diarios, hemos elaborado este Manual de Procedimientos para la

Administración de Hardware. Este manual tiene como objetivo establecer pautas claras y prácticas para la adquisición, instalación, mantenimiento y disposición de los activos de hardware de la empresa. Al seguir estas directrices, no solo optimizaremos el rendimiento de nuestros equipos, sino que también garantizaremos la seguridad de la información y la continuidad operativa en toda la organización.

Tabla 24. *Guía de Instrucciones para Administración de Hardware en la Empresa*

ACTIVIDADES	RESPONSABLES
Es necesario crear una partición en los equipos informáticos.	Departamento de Informática
Se requiere establecer una estructura para el almacenamiento de la información, de acuerdo con las directrices establecidas por la empresa	Departamento de Informática
Comunicar o impartir capacitaciones a los empleados sobre la ubicación de la información almacenada.	Departamento de Informática
FIN DEL PROCEDIMIENTO	

5.1.2. El Ciclo PDCA (Plan-Do-Check-Act) con la norma ISO 27002.

El ciclo PDCA (Planificar, Hacer, Verificar y Actuar) se utiliza en la creación y planificación de un Sistema de Gestión de la Seguridad de la Información conforme a las directrices de la norma ISO/IEC 27002. A continuación, se presenta un cronograma que detalla las actividades realizadas en las diferentes etapas del proyecto, junto con los plazos estimados para su implementación:

Planificación: Se diseña la estructura del Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con los lineamientos establecidos en la norma ISO/IEC 27002, definiendo los objetivos de seguridad específicos para Empresa ADLINK S.A.

Ejecución: Se implementaron los controles de seguridad de acuerdo con la normativa ISO 27002, lo que garantizó la confidencialidad, integridad y disponibilidad de los sistemas y datos interconectados. Además, se llevó a cabo un programa de concientización para los empleados con el fin de mejorar su comprensión y compromiso con las prácticas de seguridad

de la información. Asimismo, se inició la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a los estándares establecidos por la normativa ISO 27002, lo que permitió gestionar eficazmente la seguridad de los activos de información.

Evaluación: Se monitorea el funcionamiento del SGSI para evaluar su eficacia en la implementación de los controles de seguridad conforme a las normas ISO. Se realiza una evaluación para determinar su alineación con los objetivos de Empresa ADLINK S.A. establecidos por estas normas.

Acción: Se llevan a cabo acciones correctivas y preventivas para abordar cualquier desviación detectada durante la fase de evaluación. Se busca mejorar continuamente el SGSI de Empresa ADLINK S.A. de acuerdo con los estándares ISO 27002.

El objetivo de la propuesta es establecer un Sistema de Gestión de Seguridad de la Información (SGSI) en Empresa ADLINK S.A., basado en la norma ISO/IEC 27002, con el fin de garantizar la protección adecuada de la información sensible y los activos de la organización. La propuesta busca implementar controles de seguridad eficaces, concienciar a los usuarios sobre las experiencias seguras de manejo de la información y asegurar la alineación con los esquemas internacionales de seguridad de la información.

CONCLUSIONES

- El diagnóstico preliminar realizado mediante inspecciones de campo ha permitido identificar áreas de fortaleza y debilidad en el sistema de seguridad informática de ADLINK S.A. Este análisis proporciona una base sólida para la elaboración de un plan de seguridad informática efectivo.
- La evaluación de riesgos, amenazas y vulnerabilidades utilizando la metodología MAGERIT ha proporcionado una comprensión detallada de los posibles peligros que enfrenta la empresa en términos de seguridad informática. Esto incluye la identificación de activos críticos, amenazas potenciales y las posibles consecuencias de los incidentes de seguridad.
- Se ha elaborado un Plan de Seguridad Informático detallado, basado en la Norma ISO/IEC 27002:2022, que incluye pasos y actividades específicas para mejorar la seguridad informática de ADLINK S.A. Este plan proporciona una hoja de ruta clara y estructurada para implementar medidas de seguridad efectivas y mitigar los riesgos identificados. El diseño del Plan de Seguridad Informático basado en la Norma ISO/IEC 27002:2022 demuestra el compromiso de ADLINK S.A. con las mejores prácticas y estándares internacionales en seguridad de la información. Esta actualización a la última versión de la norma garantiza que la empresa esté alineada con las últimas recomendaciones y enfoques en materia de seguridad cibernética, lo que fortalece su capacidad para proteger sus activos digitales.

RECOMENDACIONES

- Se recomienda que ADLINK S.A. proceda con la implementación del Plan de Seguridad Informático diseñado, siguiendo cuidadosamente los pasos y actividades delineados. Esto garantizará una mejora significativa en la seguridad de la información de la empresa y la protección de sus activos digitales.
- Es fundamental que se brinde capacitación y concienciación adecuadas al personal de ADLINK S.A. sobre las políticas y procedimientos de seguridad informática establecidos. Esto incluye la formación sobre buenas prácticas de seguridad, la identificación de amenazas potenciales y el manejo adecuado de la información sensible.
- Se sugiere que la empresa realice evaluaciones periódicas de su sistema de seguridad informática para identificar nuevas amenazas y vulnerabilidades, así como para asegurarse de que el Plan de Seguridad Informático esté actualizado y sea efectivo en todo momento. La seguridad de la información es un proceso continuo que requiere una atención constante y una mejora continua.

REFERENCIAS

Alvarez. (2019). *PLAN INFORMÁTICO BASADO EN LA NORMA ISO 27001-2013 PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN Y LA INFRAESTRUCTURA TECNOLÓGICA EN LA EMPRESA "CALZADO CARLÍN" DE SANTO DOMINGO.* Santo Domingo: UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES.

Asamblea Nacional. (2015, febrero 12). LEY ORGÁNICA DE TELECOMUNICACIONES. *Última Reforma: Cuarto Suplemento del Registro Oficial 508. Última Reforma: Cuarto Suplemento del Registro Oficial 508*. Quito. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/02/Reglamento-Ley-Organica-de-Telecomunicaciones.pdf

Asamblea Nacional. (2021, mayo 26). LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. *Ley 0, Registro Oficial Suplemento 459, Estado: Vigente*. Quito. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Cardona Londoño, & Carvajal Portilla. (2018). *Diseño del sistema de gestión de seguridad de la información basado en la familia de normas de la serie ISO/IEC 27000 para una entidad pública colombiana.* Colombia: Universidad Autónoma de Manizales. Obtenido de https://repositorio.autonoma.edu.co/handle/11182/1003

Cevallos. (2019). *Diseño de una política de seguridad de la información para el área de TICS del Instituto Técnológico Superior Central Técnico , basado en la norma de seguridad ISO/IEC 27002:2013.* Ecuador: Universidad Internacional SEK. Obtenido de https://repositorio.uisek.edu.ec/handle/123456789/3320

Chapellin. (2023). NIST SP 800-53: Controles de Seguridad NIST. *tecnetone.com*. Retrieved

from https://blog.tecnetone.com/nist-sp-800-53-controles-de-seguridad-nist

Cheng-Yuan Ku, Tsung-Han Yang, Cheng-Yuan Ku, & Man-Nung Liu. (2016). Case Study: Application of Enhanced Delphi Method for Software Development and Evaluation in Medical Institutes. *Kybernetes, 45*, 637-649. Obtenido de https://imf.nctu.edu.tw/en/30/40101/per1/Case-Study-Application-of-Enhanced-Delphi-Method-for-Software-Development-and-Evaluation-in-Medical-Institutes-83181779

Conexion ESAN. (16 de mayo de 2016). La norma ISO 27001 y la mejora continua en la gestión de seguridad de la información. *ESAN*. Obtenido de https://www.esan.edu.pe/conexion-esan/norma-iso-27001-mejora-continua-en-la-gestion-de-seguridad-informacion

Congreso Nacional. (2002, abr 17). LEY DE COMERCIO ELECTRÓNICO. *Ley -67, Registro Oficial Suplemento 557, Estado: Vigente*. Quito. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Cubillos, F. (2018). *Diseño de un sistema de gestión de seguridad de la información para el Colegio Germán Arciniegas I.E.D., bajo la norma técnica colombiana NTC ISO/IEC 27001:2013.* Bogota: Universidad Abierta y a Distancia. Obtenido de https://repository.unad.edu.co/handle/10596/25633

ESAN. (2016, mayo 11). Importancia y beneficios de contar con un Sistema de Gestión de Seguridad de Información. *ESAN*. Retrieved from https://www.esan.edu.pe/apuntes-empresariales/2016/05/importancia-y-beneficios-de-contar-con-un-sistema-de-gestion-de-seguridad-de-informacion/

Forum, Council, & Security y Management. (2013). Conceptos de seguridad informática y su

reflejo en la Cámara de Cuentas de Andalucía. 111–117.

García. (2015, enreo 9). ¿Qué es la Seguridad Informática? Retrieved from http://www.integracanarias.com/blog/35-seguridad-informatica-que-es#targetText=No%20debes%20confundir%20Seguridad%20Inform%C3%A1tica,e%20integridad%20de%20la%20misma.

Garcia. (2016, junio 11). Análisis de situación ISO 27001 en las organizaciones., ISO 27001:2013. Retrieved julio 12, 2023, from https://www.eoi.es/blogs/ciberseguridad/2016/06/11/analisis-de-situacion-iso27001-en-las-organizaciones-3/.

García, Delgado, & Rodríguez. (2014). Seguridad activa y pasiva. Recuperado el 15 de julio de 2023, de https://sites.google.com/site/seguridadinformaticasjn/seguridad-activa-y-pasiva.

Grupo CYNTHUS. (2023, marzo 5). ISO 27002: QUÉ ES Y DIFERENCIAS CON LA ISO 27001. *CYNTHUS*. Retrieved from https://www.cynthus.com.mx/iso-27002-diferencias-con-iso-27001/

ISO27001. (2 de octubre de 2014). Sistema de Gestión de la Seguridad. Obtenido de www.ISO27001.es

López, A. (2010). *Seguridad informática.* Madrid: Editex. Obtenido de https://books.google.co.ve/books/about/Seguridad_inform%C3%A1tica.html?hl=es&id=Mgvm3AYIT64C&redir_esc=y

Méndez. (2020). *DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS.* Pimentel: Universidad Señor de Sipan.

Moreno. (2016, junio 11). ANÁLISIS DE SITUACIÓN ISO27001 EN LAS ORGANIZACIONES. Retrieved from

https://www.eoi.es/blogs/ciberseguridad/2016/06/11/analisis-de-situacion-iso27001-en-las-organizaciones-3/.

Najar. (enero-junio de 2017). Exposici on del activo m as valioso de la organizacion, la“informacion”. *Vision Electronica, 11*(1).

normaiso 27001. (2017). *ISO 27001 AL COMPLETO*. Obtenido de https://normaiso27001.es/referencias-normativas-iso-27000/

normaiso 27002. (2022). *ISO 27001 AL COMPLETO*. Obtenido de https://normaiso27001.es/referencias-normativas-iso-27000/

ONOFA. (2022, JUNIO 30). Ataques cibernéticos amenazan seguridad en Ecuador. *Dialogo Americas*. Retrieved from https://dialogo-americas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/

Orrego. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Pensamiento Americano, 4*(6), 21–23. Obtenido de https://doi.org/10.21803/penamer.4.6.57

Raffino. (2017, septiembre 5). ¿Qué es Seguridad? Retrieved from https://concepto.de/seguridad/

Romero, Araujo, Mestre, & Galindo. (2019). *TECNOLOGÍA INTERCULTURALIDAD Y NATURALEZA.* Bogota, Colombia: UNIEDICIONES. Retrieved from https://www.researchgate.net/publication/338194813_TECNOLOGIA_INTERCULTURALIDAD_Y_NATURALEZA

Torres. (2020). *PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A.* Ambato: UNIVERSIDAD TÉCNICA DE AMBATO.

Viteri. (2022). *Linkedin* . Retrieved from ANÁLISIS DE LA NORMA ISO 27002:2022: https://www.linkedin.com/pulse/an%C3%A1lisis-de-la-norma-iso-270022022-

c%C3%A9sar-paul-viteri-pe%C3%B1afiel/?originalSubdomain=es