UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE COMPUTACION

SISTEMA DE GESTIÓN PARA LA PROTECCIÓN DE DATOS CRÍTICOS DE UNA EMPRESA DE TRANSPORTE PESADO

Trabajo de titulación previo a la obtención del

Titulo de Ingeniero en Ciencias de la Computación

AUTOR: RICHARD ENRIQUE CAMACHO CABRERA

TUTOR: JOSÉ LUIS AGUAYO MORALES

Quito – Ecuador

2023

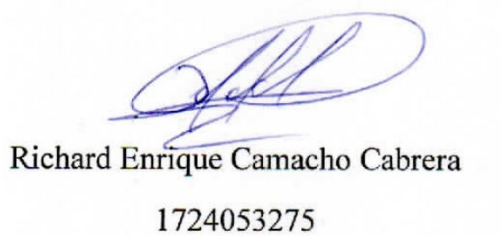
CERTIFICADO DE RESPONSABILIDAD Y AUDITORÍA DEL TRABAJO DE TITULACION

Yo, Richard Enrique Camacho Cabrera con documento de identificación N° 1724053275; manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 14 de agosto del 2023

Atentamente,



Richard Enrique Camacho Cabrera

1724053275

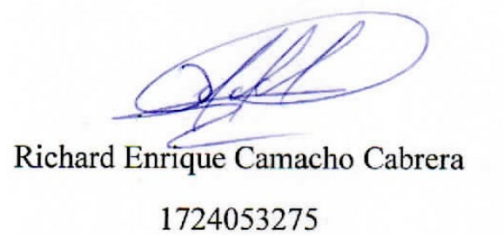
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALEAIANA

Yo, Richard Enrique Camacho Cabrera con documentación N° 1724053275, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: "Sistema de gestión para la protección de datos críticos de una empresa de transporte pesado", el cual ha sido desarrollado para optar por el título de: Ingeniero en Ciencias de la Computación en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 14 de agosto del 2023

Atentamente,



Richard Enrique Camacho Cabrera

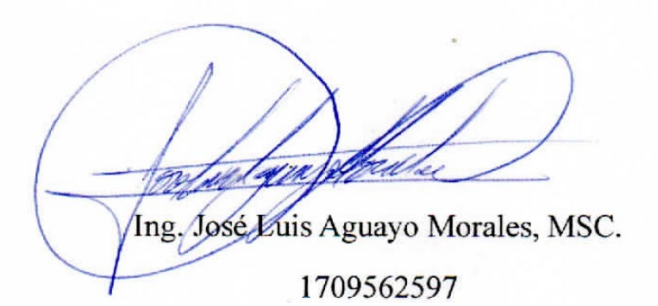
1724053275

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, José Luis Aguayo Morales con documento de identificación N.º 1709562597, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: SISTEMA DE GESTIÓN PARA LA PROTECCIÓN DE DATOS CRÍTICOS DE UNA EMPRESA DE TRANSPORTE PESADO, realizado por Richard Enrique Camacho Cabrera con documento de identificación N.º 1724053275, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 14 de agosto del 2023

Atentamente,



SISTEMA DE GESTIÓN PARA LA PROTECCIÓN DE DATOS CRÍTICOS DE UNA EMPRESA DE TRANSPORTE PESADO

MANAGEMENT SYSTEM FOR THE PROTECTION OF CRITICAL DATA OF A HEAVY TRANSPORTATION COMPANY

Richard Enrique Camacho[1], José Luis Aguayo[2]

Resumen – Este estudio propone un sistema de gestión para la protección de datos críticos en una empresa de transporte pesado, el objetivo es fortalecer la integridad, confidencialidad y disponibilidad de la información adaptada a las necesidades del sector. Se utilizó la metodología MAGERIT, que proporciona un marco estructurado para identificar y gestionar los riesgos de seguridad de la información. Asimismo, se consideraron los requisitos establecidos por la Ley Orgánica de Protección de Datos Personales. El sistema propuesto responde a las principales amenazas de seguridad, incluyendo el análisis de riesgos y la protección adecuada de los activos de información. La implementación de una política de seguridad mejorará la protección de los datos críticos. Se recomienda capacitación sobre esta política, además, será objeto de revisión periódica y mejora para adaptarse a las nuevas amenazas y desafíos del entorno tecnológico en evolución. En conclusión, este estudio muestra que la implementación de la metodología MAGERIT con herramientas tecnológicas permitirá identificar y gestionar los riesgos de manera efectiva, estableciendo controles y procedimientos adecuados. Se recomienda su aplicación en otras organizaciones, brindando un enfoque integral y robusto para proteger la información y mantener la confianza de las partes interesadas. Es importante mantener una política de seguridad de la información en constante revisión y mejora para adaptarse a los cambios del entorno y conseguir una mejor protección de los activos de la empresa.

Palabras claves: Magerit, Gestión de Riesgos, Sistema de gestión, Protección de Datos, Datos Críticos, Política de Seguridad.

Abstract - This study proposes a management system for the protection of critical data in a heavy transport companies, the objective is to strengthen the integrity, confidentiality and availability of information adapted to the needs of the sector. The MAGERIT methodology was used, which provides a structured framework to identify and manage information security risks. In addition, the requirements established by the Organic Law of Protection of Personal Data were considered, too. The proposed system answers the main security threats, including risk analysis and adequate protection of information assets. The implementation of a security policy will improve the protection of critical data. Training is recommended about this policy, besides, it will be subject to periodic review, and improvement to adapt to the new threats and challenges of the evolving technological environment. In conclusion, this study shows that the implementation of the MAGERIT methodology with technology tools will make it possible to identify and manage risks effectively, establishing adequate controls and procedures. Its application in other organizations is recommended, providing a comprehensive and robust approach to protect information and maintain the trust of interested parties. The maintaining an information security policy in constant review, and improvement to adapt to changes in the environment and get a better protection of company assets is importants.

Keywords: Magerit, Risk Management, Management System, Data Protection, Critical Data, Security Policy.

I. INTRODUCCIÓN

En la actualidad, la protección de datos se ha convertido en un tema crítico en la era digital en la que se vive, y las empresas de transporte pesado no son la excepción, ya que manejan información sensible y crítica para su operación [9]. La confidencialidad, integridad y disponibilidad (C.I.A.) de la información son elementos esenciales para el éxito de cualquier organización, y en el caso de las empresas de transporte pesado, la pérdida, robo o filtración de información puede tener consecuencias graves para su funcionamiento y para la seguridad de sus operaciones [10].

Ante este contexto, se presenta un sistema de gestión para la protección de datos críticos de una empresa de transporte pesado, con el objetivo de aumentar la C.I.A. en todo momento. El sistema propuesto aborda las principales amenazas a la información y ofrece un conjunto de medidas e inspecciones para reducir las amenazas asociados con su manejo.

Este sistema de gestión se basa en las mejores prácticas y estándares internacionales, adaptados a las

[1] Estudiante de Ingeniería en Ciencias de la Computación - Universidad Politécnica Salesiana, Egresado - UPS - sede Quito. Autor para correspondencia: rcamachoc@est.ups.edu.ec

[2] Magister en Redes de Comunicaciones, Ingeniero en Electrónica y Telecomunicaciones, Profesor de Ingeniería en Sistemas y Computación - UPS - sede Quito. Email: aguayo@ups.edu.ec

necesidades específicas de una empresa de transporte pesado. Entre las medidas y controles que se proponen se encuentran: la implementación de políticas de seguridad de la información, la formación y concientización de los empleados, el control de acceso a los datos, la gestión de vulnerabilidades, la realización de auditorías y pruebas de penetración.

Es importante destacar que la implementación de un sistema de gestión para la protección de datos críticos no solo minimiza los riesgos y aumenta la confianza de los clientes y stakeholders de la empresa, sino que también es un requisito legal en muchos países. Por lo tanto, la implementación del sistema propuesto no solo mejora la seguridad de la información de la empresa, sino que también apoya con el cumplimiento legal y su sostenibilidad a largo plazo.

Por tanto, este trabajo tiene como objetivo presentar un sistema de gestión para la protección de datos críticos de una empresa de transporte pesado, que permita incrementar la CIA, minimizando los riesgos asociados con su manejo y cumpliendo con los requisitos legales pertinentes. La implementación de este sistema permitirá a la empresa aumentar la seguridad de sus operaciones, mejorar la confianza de sus clientes y stakeholders, permitirá su sostenibilidad a largo plazo en un entorno cada vez más digitalizado.

II. MATERIALES Y MÉTODOS

1. Metodología MAGERIT.

La investigación se emplea en la metodología de desarrollo denominada "MAGERIT 3", que se elaboró por el Consejo Superior de Administración Electrónica de España, la cual se encuentra en sintonía con la norma ISO-27001 en lo que concierne a la evaluación de procesos y gestión de riesgos [1]. Su propósito es brindar recomendaciones sobre las medidas pertinentes que deben ser implementadas con la finalidad de controlar y minimizar los riesgos de manera efectiva.

Teniendo identificadas las variables de la problemática que se ha dispuesto, se establece la conexión causa y efecto entre las partes que forman la investigación [6]. La metodología MAGERIT 3.0 para la detección de activos. Esta metodología ayuda a determinar los valores de probabilidad e impacto de un evento, los cuales se multiplican para obtener un valor integral que representa el riesgo a gestionar [7]. Es fundamental tener conocimiento en cuanto a los riesgos a los que están expuestos los elementos de trabajo, ya que esto resulta esencial para poder llevar a cabo su gestión de manera efectiva.

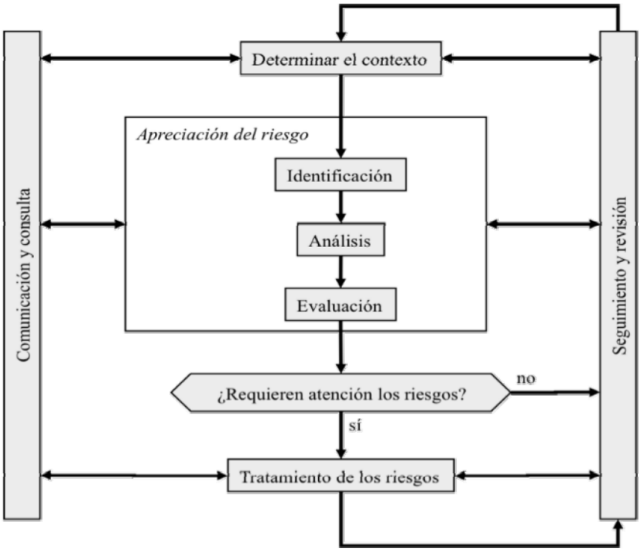


Figura 1. Proceso de gestión de riesgos
Fuente: Libro I de MAGERIT V3 [1].

2. Ley Orgánica de Protección de Datos Personales (LOPDP).

Durante la administración del Expresidente Lenin Moreno, se empezó a desarrollar el Plan Nacional de la Sociedad de la Información y el Conocimiento, donde uno de los objetivos centrales del eje estratégico No. 6 fue la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP). Se presentó el proyecto de ley ante la Asamblea Nacional en el 2019, con el propósito principal de establecer medidas y garantías para asegurar que el derecho a la protección de la información personal sea respetado y mantenido en un nivel aceptable [11].

Posteriormente, los días 9 y 11 de febrero de 2021, se llevaron a cabo debates en la Asamblea Nacional sobre esta ley. En donde en el 2021, la LOPDP fue publicada en el Registro Oficial No. 459. Esta legislación consta de 12 partes principales, que a su vez están divididas en 77 secciones individuales. Además, incluye 9 disposiciones generales que establecen principios y directrices adicionales, así como 4 disposiciones transitorias que se aplican durante un período de tiempo específico [12].

La ley da protección a la información personal en cualquier formato o medio. Sin embargo, no se extiende al tratamiento de datos personales en entornos domésticos, a datos que han sido anonimizados o a la información relacionada con personas que ocupan cargos públicos.

En términos de su ámbito territorial se aplica: 1) cuando el método de los datos se realice dentro del territorio nacional, 2) cuando el responsable o encargado del tratamiento tenga domicilio en Ecuador, y 3) cuando la entidad o individuo que no tiene

residencia en Ecuador, pero que lleva a cabo el procesamiento de datos de personas que se encuentran en el territorio nacional. [12].

En relación con la legislación existente, la LOPDP elimina los enunciados proporcionados por la Ley de Compra Electrónica, Mensajes y Firmas Electrónicas en relación a la privacidad. Además, se sustituye la definición de accesibilidad y confidencialidad establecida en la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, siendo esta última un pilar fundamental en la protección de los datos personales.

III. ANÁLISIS DE RIESGOS:

Dentro del desarrollo de análisis de riesgos, se procede a identificar y evaluar los diferentes elementos que conforman el riesgo, permitiendo obtener una estimación de los umbrales asociados a cada uno de ellos. Esta metodología nos brinda la capacidad de comprender y valorar la magnitud de los riesgos a los que estamos expuestos, así como su nivel de impacto en nuestras operaciones [1].
Al evaluar y asignar valores a cada componente del riesgo, se puede decidir sobre las medidas de mitigación y control necesarias para reducir su probabilidad de ocurrencia o minimizar sus consecuencias [2]. De esta manera, nos aseguramos de contar con una visión integral y fundamentada que nos permita gestionar los riesgos de manera efectiva y proteger nuestros activos de información de manera adecuada.

1. Inventario de activos

Los activos tienen una importancia crucial en el funcionamiento y la continuidad de una organización, ya que representan elementos de valor y utilidad [3]. Por lo tanto, resulta de vital importancia salvaguardar estos activos con el fin de mantener el adecuado desarrollo de las operaciones comerciales.

Es esencial contar con la participación de los propietarios de los activos clave en este equipo multidisciplinario. Se considera propietario de un activo a aquella persona que tiene la responsabilidad aprobada por la gerencia en cuanto al control, mantenimiento, uso y seguridad de dicho activo [4]. En el ámbito del Sistema de Gestión de Seguridad de la Información (SGSI), es necesario identificar de manera clara los activos importantes y posteriormente valorarlos para que así tengan un efecto significativo en la organización si sufren deterioro o fallos en los aspectos de seguridad [5].
Para la puntuación de los activos, se emplean criterios de evaluación basados en escalas de tres valores. A partir de esta valoración, se evalúa la magnitud de criticidad de cada activo, el cual se obtiene como un promedio de los criterios de C.I.A. [8]. Dependiendo de este nivel de criticidad, se clasifica el activo como alto, medio o bajo, lo que permite priorizar las acciones y medidas de protección necesarias para cada uno de ellos.

Nivel de Criticidad	
Alto	2 – 3
Medio	1 – 2
Bajo	0 – 1

Tabla 1. Nivel de Criticidad
Fuente: Propia a partir de apuntes de clases.

1.1. Confidencialidad (C.)

Se refiere a mantener la privacidad de la información solo a las personas autorizadas y negando su acceso a todos los demás.

Valor	Confidencialidad
0	Puede ser conocida y utilizada por cualquier persona, dentro o fuera de la institución.
1	Puede ser conocida y utilizada por cualquier persona, dentro de la institución.
2	Puede ser conocida y utilizada por un grupo de personas que la necesiten para realizar su trabajo.
3	Puede ser conocida y utilizada por un grupo muy reducido por personas, cuya divulgación podría ocasionar perjuicio a la institución o a terceros.

Figura 2. Criterio de Valoración – Confidencialidad
Fuente: Propia a partir de apuntes de clases.

1.2. Integridad (I.)

La veracidad, exactitud y exhaustividad de un activo.

Valor	Integridad
0	Cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la institución.
1	Cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio para la institución o terceros.
2	Cuya modificación no autorizada es de difícil reparación, y podría ocasionar un perjuicio significativo para la institución o terceros.
3	Cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades.

Figura 3. Criterio de Valoración – Integridad
Fuente: Propia a partir de apuntes de clases.

1.3. Disponibilidad (A.)

La temporalidad o frecuencia en la cual un activo debe estar disponible o preparado para su uso.

Valor	Disponibilidad
0	Cuya inaccesibilidad no afecta la actividad normal de la Institución.
1	Cuya inaccesibilidad durante una semana podría ocasionar un perjuicio significativo para la Institución.
2	Cuya inaccesibilidad durante la jornada laboral podría impedir la ejecución de las actividades de la Institución.
3	Cuya inaccesibilidad durante una hora podría impedir la ejecución de las actividades de la Institución.

Figura 4. Criterio de Valoración – Disponibilidad
Fuente: Propia a partir de apuntes de clases.

2. Amenazas y vulnerabilidades

2.1. Amenazas.

Los activos se enfrentan a diversas amenazas que pueden dar lugar a incidentes no deseados y causar daños a la organización y sus activos. Al identificar las amenazas que podrían afectar a una empresa, es útil clasificarlas según su naturaleza para poder gestionarlas de manera más eficiente [1]. A continuación, se presentan cuatro categorías en las que se pueden clasificar las amenazas:

Amenazas	
De origen natural	Fuego, Daños por agua y Desastres naturales
De origen industrial	Corte de suministro eléctrico, Condiciones inadecuadas de temperatura o humedad, Fallo de servicios de comunicaciones y Desastres industriales
Ataques intencionados	Denegación de servicio, Robo, Ataques destructivos, Extorsión, Ingeniería social, Manipulación de logs, Abuso de privilegios de acceso, Manipulación de equipos, Manipulación de configuración y Alteración de la información
Errores y fallos no intencionados	Fuga de información, Introducción de falsa información, Acceso no autorizado, Vulnerabilidad de programas (software), Corrupción de la información, Destrucción de información, Interceptación de información (escucha), Indisponibilidad del personal, Agotamiento de recursos, Errores de los usuarios, Errores del administrador, Errores de configuración, Degradación de los soportes de almacenamiento de la información, Difusión de software dañino, Errores de mantenimiento / actualización de programas (software), Errores de mantenimiento / actualización de equipos (hardware) y Caída del sistema por sobrecarga

Figura 5. Clasificación de amenazas
Fuente: Propia a partir de apuntes de clases.

2.2. Vulnerabilidades.

Las vulnerabilidades hacen referencia a aquellas debilidades de los activos de una empresa. Para comprender mejor estas vulnerabilidades, es útil pensar en ellas como deficiencias en el sistema de seguridad. Es importante tener en cuenta que las vulnerabilidades en sí mismas no causan daño, son factores que pueden permitir que una amenaza cause impacto en un activo [1]. A continuación, se presentan categorías en las que se pueden clasificar las vulnerabilidades:

- Recursos humanos: incluye la falta de capacitación en seguridad, la falta de conciencia sobre seguridad, la falta de eliminación de accesos al finalizar el contrato laboral y la falta de procedimientos que aseguren la entrega de activos al finalizar el contrato laboral, así como la desmotivación de los empleados.
- Control de acceso: se refiere a la segregación inadecuada de redes, la falta de políticas para

mantener limpios escritorios y pantallas, políticas incorrectas de control de acceso y contraseñas que no se modifican.

- Gestión de operaciones y comunicaciones: se relaciona con interfaces complicadas para usuarios, una gestión inadecuada de cambios, una deficiente gestión de la red, la falta de mecanismos que mejoren el envío y recepción de mensajes, la carencia de una política de clasificación de tareas, la ausencia de control y monitoreo de la impresora de la empresa, y la falta de protección adecuada en la conexión a redes públicas.

Después de analizar los riesgos, se han identificado y evaluado diversos elementos que se consideran como activos críticos para la empresa. Como los cuales:

Información: Es uno de los activos más valiosos para cualquier organización. En el contexto de la empresa en cuestión, la información puede incluir datos confidenciales de los clientes, registros financieros, estrategias comerciales, secretos comerciales y otra información confidencial. El acceso no autorizado, la pérdida o la divulgación indebida de esta información podrían tener consecuencias devastadoras, como la pérdida de confianza de los clientes, daños a la reputación y repercusiones legales.

Infraestructura: La infraestructura de la empresa abarca los sistemas informáticos, las redes, los dispositivos de almacenamiento y otros recursos tecnológicos utilizados para respaldar las operaciones comerciales. Estos componentes son fundamentales para el trabajo diario de la institución y su disponibilidad ininterrumpida es crucial. Un acceso no autorizado, un fallo de seguridad o una interrupción en la infraestructura podrían afectar negativamente la productividad, la continuidad del negocio y la capacidad de brindar servicios a los clientes.

Personal: El personal de la empresa, especialmente aquellos con roles clave en la toma de decisiones, el manejo de información confidencial y la ejecución de tareas críticas, se considera un activo crítico. Estas personas poseen conocimientos especializados, experiencia y habilidades que son fundamentales para el funcionamiento eficiente y efectivo de la organización. La pérdida de personal calificado o su involucramiento en acciones maliciosas podría impactar negativamente en la productividad, la calidad del trabajo y la seguridad de la información.

Respaldos: Los respaldos de datos y sistemas son esenciales para garantizar la continuidad del negocio. Estos respaldos pueden incluir copias de seguridad de datos, imágenes de sistemas, configuraciones y documentación relevante. La pérdida de los respaldos o la incapacidad para restaurarlos adecuadamente en caso de un incidente podría resultar en la pérdida irreversible de información crítica y una interrupción prolongada de las operaciones comerciales.

El análisis de riesgos ha revelado que la información, la infraestructura, parte del personal y los respaldos son los activos críticos de la empresa. La protección adecuada y la ejecución de medidas de seguridad sólidas para salvaguardar estos activos son fundamentales para mitigar los riesgos identificados y garantizar la continuidad del negocio.

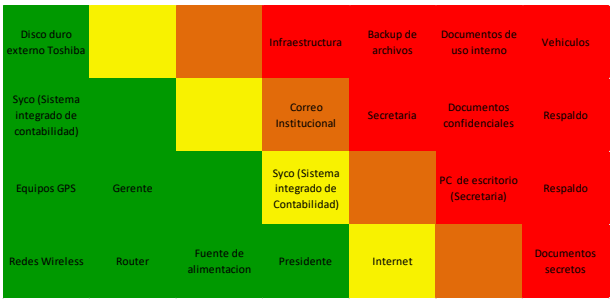


Figura 6. Mapa de calor
Fuente: Propia a partir de apuntes de clases.

Para mejorar la seguridad, se recomienda invertir en una serie de elementos. En términos de software de seguridad, es necesario adquirir un antivirus para protegerse contra virus y malware, un antispyware para detectar software espía y un firewall para salvaguardar la red contra accesos no autorizados. Además, se debe considerar el almacenamiento en la nube y un servicio de respaldo de datos para permitir la seguridad de la información. Es importante invertir en un sistema de control de acceso y autenticación confiable, como lectores biométricos, que garantizan una identificación precisa y segura de los empleados y visitantes. además, se puede considerar la instalación de cámaras de seguridad y sistemas de vigilancia en la oficina para mejorar la seguridad física. Considerando los precios actuales a julio del 2023, los costos asociados en promedio son $2000. Por último, es crucial brindar capacitación y concientización en seguridad a los empleados y contar con servicios de respuesta ante para abordar de manera efectiva cualquier eventualidad.

IV. RESULTADOS

1. Etapa previa al evento catastrófico

Engloban todas las acciones relacionadas con la planificación, preparación, entrenamiento y ejecución de las medidas de protección de la información, permitiendo así un proceso de recuperación eficiente y económico para las organizaciones. A continuación, se enumeran las actividades que se deben llevar a cabo:

1.1. Desarrollo de un plan estratégico

En esta fase de planificación, se establecen los protocolos y directrices para abordar diferentes aspectos relacionados con la seguridad de la empresa. Uno de los aspectos clave es la protección de la estructura física de la organización en casos de posibles incidentes, como robos, sismos o incendios. Se sugieren tomar las siguientes medidas de precaución [14]:

a) Protección de la estructura física

En el caso de posibles situaciones de robo, sismo o incendio, es crucial implementar precauciones efectivas que garanticen la seguridad de la organización.

Robos: en [13] el autor recomienda:

- Antes de acceder o abandonar las instalaciones, se sugiere que se realice una observación cuidadosa del entorno para detectar la presencia de personas sospechosas.
- Se recomienda contar con personal dedicado a la seguridad y vigilancia de las instalaciones, lo que contribuirá a una protección constante.
- La instalación de sistemas de alarma se considera una medida eficaz para detectar intrusiones o actividad sospechosa de manera oportuna.
- Además, es aconsejable evaluar la contratación de pólizas de seguro adecuadas para mitigar los posibles impactos financieros derivados de robos u otros incidentes.

Sismos: en [14] el autor recomienda:

- Mantener una verificación regular del estado de las instalaciones básicas de la oficina.
- Asegurar de manera adecuada las estanterías, armarios o algún mueble que pueda moverse, asegurar las lámparas al techo.
- Colocar de forma visible y accesible los números de emergencia, así como tener disponible un botiquín de primeros auxilios.

Incendios: en [14] el autor recomienda:

- Mantener una actitud vigilante y enfocada en la prevención para evitar incendios.
- Evitar el almacenamiento de productos inflamables en las instalaciones.
- Verificar regularmente la condición de los cables de los aparatos eléctricos y reemplazarlos si presentan daños.
- Evitar conexiones excesivas en los enchufes múltiples para prevenir sobrecargas en los circuitos eléctricos.
- Evitar el contacto de las instalaciones eléctricas con agua, ya que el agua es conductora de electricidad.
- Asegurarse de que todos los enchufes e interruptores estén correctamente protegidos con tapas aislantes.
- Establecer una prohibición de fumar en las instalaciones debido a los riesgos de incendio y la contaminación.
- Implementar un sistema de alarma contra incendios para detectar y alertar rápidamente sobre cualquier emergencia.
- Mantener un extintor contra incendios visible y accesible en caso de necesidad.
- Realizar simulacros periódicos para evaluar la respuesta y preparación ante situaciones de incendio.

b) Dispositivos informáticos

Se mantendrá un registro actualizado de los activos de TI que incluyan información detallada sobre su contenido, como el software utilizado, y su ubicación.

Como parte de las medidas de protección de los activos corporativos, las organizaciones pueden considerar la adquisición de una póliza de seguro comercial. Sin embargo, en el contrato se establecerá que, en caso de eventos adversos, la reposición de una computadora dañada se realizará mediante una actualización tecnológica que la reemplace por una de mayor capacidad, siempre y cuando esté dentro de los límites de cobertura establecidos por el seguro.

Estas medidas permitirán mantener un control y una identificación claros de los dispositivos de gestión de información, así como asegurar una protección adecuada de los activos corporativos en caso de eventos adversos. La inclusión de una actualización tecnológica como parte del reemplazo de equipos dañados proporcionará una mayor capacidad y eficiencia en el soporte de las operaciones de la organización. Además, la señalización o etiquetado de los equipos según su importancia contribuirá a una gestión más efectiva de la evacuación y la protección de la información sensible.

c) BACKUPS

Se implementarán procedimientos de copias de seguridad para mejorar la disponibilidad y el funcionamiento adecuado de los sistemas y aplicaciones de la organización.

La realización periódica de copias de seguridad de estos componentes de software aumentará la disponibilidad de los sistemas y aplicaciones, así como a minimizar los tiempos de recuperación en caso de incidentes o contingencias. La inclusión de copias de seguridad del hardware, a través de acuerdos con otras organizaciones, proporcionará un respaldo adicional en situaciones críticas, asegurando la continuidad de las

operaciones hasta que se resuelvan los problemas y se restaure la infraestructura necesaria.

d) Personal interno.

- Mantener un registro actualizado del personal y su disponibilidad.
- Identificar roles clave y asignar personal de respaldo para cada puesto.
- Establecer protocolos de comunicación claros para notificar ausencias o imprevistos.
- Realizar capacitaciones periódicas para asegurar que el personal conozca sus responsabilidades en caso de falta de personal.

2. Etapa durante el evento catastrófico

Mientras se presente la contingencia o siniestro, se deben llevar a cabo las siguientes acciones, que han sido previamente planificadas y programadas:

2.1. Plan de respuesta ante situaciones críticas

Este plan contempla las acciones a tomar en caso de eventos adversos, así como la difusión de estas medidas. Se recomienda considerar diversos escenarios posibles para la eventualidad de un evento desafortunado.

Asimismo, se deberá proporcionar información clara sobre la ubicación y señalización de los equipos de seguridad correspondientes a cada tipo de evento, como extintores u otros dispositivos pertinentes. Además, se establecerá una secuencia de llamadas en caso de emergencia, que incluirá los números de contacto de los servicios de bomberos, ambulancias, jefatura de seguridad y personal designado para hacer frente a situaciones de emergencia.

A continuación, se presentan algunas normas sugeridas en caso de que ocurra un evento como robo, sismo o incendio, las cuales deberán ser seguidas en beneficio de la seguridad y bienestar de todos los implicados.

Robos: en [13] el autor recomienda:

- Actuar con prudencia: Trate de recordar las palabras pronunciadas por el agresor y evite el contacto visual directo para evitar confrontaciones innecesarias.
- Utilizar la memoria: En el caso de que los atacantes tengan un medio de transporte para darse a la fuga, trate de memorizar el número de matrícula y las características del automóvil.
- Mantener un perfil bajo: Es esencial evitar llamar la atención y permanecer alerta ante cualquier situación sospechosa en el entorno.

Siguiendo estas recomendaciones, se contribuirá a preservar la seguridad personal en situaciones potencialmente peligrosas.

Sismo: en [14] el autor recomienda:

Ante la ocurrencia de un terremoto de gran magnitud, es fundamental mantener la calma y seguir las siguientes instrucciones de seguridad:

- Si se encuentra dentro de un edificio, es recomendable permanecer en su ubicación hasta que sea seguro salir. Si está en el exterior, busque un área despejada lejos de estructuras potencialmente peligrosas.
- En caso de incendio, utilice extintores para apagar las llamas. Evite el uso de llamas abiertas como cerillas, encendedores o velas durante o inmediatamente después del temblor.
- Si se encuentra en el exterior, mantenerse alejado de cables eléctricos, cornisas, cristales y barandillas que puedan representar un riesgo.
- Evite acercarse o ingresar a edificios dañados, ya que puede haber objetos peligrosos que puedan caer (vidrios, cornisas, etc.). Diríjase a espacios abiertos, camine con precaución y esté atento al tráfico.

Al seguir estas recomendaciones, se aumentará la seguridad personal durante un fuerte terremoto.

Incendios: en [14] el autor recomienda:

Ante la ocurrencia de un incendio, es importante seguir las siguientes pautas para cuidar la seguridad personal:

- Mantenga la calma y evite acciones que puedan generar pánico, como gritar, correr o empujar, ya que esto puede agravar la situación.
- Localice el extintor más cercano y, si tiene conocimiento sobre su uso, intente combatir el fuego. En caso de no saber cómo utilizarlo, solicite ayuda a alguien capacitado.
- Si el fuego es de origen eléctrico, evite intentar apagarlo con agua, ya que esto puede ocasionar descargas eléctricas. Utilice extintores apropiados para incendios eléctricos.
- Cierre puertas y ventanas para evitar la propagación del fuego, a menos que sea su única ruta de escape.
- Antes de abrir una puerta, verifique si está caliente al tacto. Si lo está, es probable que haya fuego al otro lado. En ese caso, absténgase de abrirla y busque otra salida.
- Si las salidas están bloqueadas por el fuego, mantenga la calma y busque un lugar seguro dentro del espacio. Espere a ser rescatado y

siga las indicaciones de los servicios de emergencia.
- En presencia de humo, desplácese lo más cerca posible del suelo, gateando si es necesario. Cubra su nariz y boca con un trapo, preferiblemente húmedo, para filtrar el humo y facilitar la respiración.
- Si su ropa se incendia, no corra. Tírese al suelo y ruede lentamente para apagar las llamas. Si es posible, cúbrase con una manta u otro material resistente para sofocar el fuego.
- Al seguir estas recomendaciones, se aumentarán las posibilidades de preservar la seguridad personal en caso de un incendio.

Personal Interno: en [14] el autor recomienda:

- Evaluar la situación y priorizar las tareas críticas y urgentes.
- Reasignar recursos disponibles para cubrir las funciones esenciales.
- Comunicar claramente los cambios en la distribución de tareas y responsabilidades.
- Mantener un registro de las acciones tomadas y los recursos utilizados.

Fallo de equipos informáticos: en [14] el autor recomienda:

- Notificar al personal de TI y al proveedor de soporte técnico sobre el fallo del equipo.
- Evaluar la gravedad del fallo y determinar las medidas correctivas necesarias.
- Reasignar temporalmente el trabajo en otros equipos o dispositivos disponibles.
- Establecer una comunicación clara sobre el progreso de la reparación y las acciones tomadas.

3. Etapa posterior al evento catastrófico

Una vez que ha tenido lugar el evento catastrófico o desastre, es crucial realizar las acciones descritas en el Plan de emergencias previamente establecido. A continuación, se presentan los aspectos que deben tenerse en consideración en este proceso.

3.1. Análisis de los impactos sufridos

Una vez que haya pasado el evento desafortunado, es esencial realizar una evaluación inmediata de los daños ocasionados. Esto implica determinar la extensión de los daños, identificar los sistemas afectados y los equipos que no están en funcionamiento, así como determinar qué elementos pueden ser recuperados y en qué plazo.

El encargado llevará a cabo esta evaluación a través de preguntas relevantes. Una vez obtenidos los resultados, se verificará qué medidas del plan de contingencias se ajustan al tipo de desastre ocurrido.

Al presentarse un desastre, se deben seguir las siguientes comprobaciones:

- Verificar la calidad e integridad de la información existente en la institución, realizando pruebas en los programas que funcionaban correctamente antes del desastre.
- Comprobar la integridad de los respaldos de la información.
- Restaurar la información al estado original anterior al desastre en la medida de lo posible.

Al realizar estas evaluaciones y tomar las medidas necesarias, se podrá iniciar el proceso de recuperación de manera adecuada y minimizar los efectos del desastre en la organización.

4. Clasificación de las actividades en el plan de estratégico

Es necesario analizar la disponibilidad del personal y aprovechar los recursos humanos de manera eficiente. Aquellos empleados que no estén directamente involucrados en las áreas afectadas pueden ser asignados temporalmente a tareas que no se hayan visto perjudicadas, para brindar apoyo al personal de los sistemas dañados. Esto ayuda a mantener la operatividad y minimizar los impactos del desastre.

Asimismo, es importante contar con un equipo de soporte técnico capacitado, que pueda brindar asistencia y soluciones en el restablecimiento de los sistemas afectados. Esta colaboración entre los diferentes departamentos y la asignación adecuada de recursos humanos contribuirán a la recuperación efectiva y a la continuidad de las operaciones en la empresa.

5. Retroalimentación del plan estratégico

Tras analizar los resultados, es necesario perfeccionar el plan inicial mediante la mejora que presentaron dificultades y fortalecer los aspectos que funcionaron de manera efectiva. Además, es importante evaluar cuál habría sido el costo de no contar con un plan de contingencias implementado en la institución.

6. Política de seguridad informática

6.1. Introducción

La Política de Seguridad de la Información de la empresa tiene como finalidad la implementación de un conjunto de acciones orientadas a salvaguardar la CIA.

Estos aspectos esenciales de la seguridad son prioritarios en nuestra organización, ya que respaldan de manera integral nuestros procesos de negocio. Mediante esta política, buscamos establecer requisitos claros y efectivos para proteger nuestra información, así como los equipos y servicios tecnológicos que sustentan nuestras operaciones diarias. Con ello, mantenemos la continuidad de nuestras actividades y fortalecemos la confianza en la empresa.

6.1.1. Objetivo

El propósito fundamental de la Política es establecer los principios y directrices fundamentales para controlar la seguridad en el contexto empresarial. Su finalidad última es asegurar la protección de la información y reducir al mínimo los riesgos no relacionados con aspectos financieros que puedan surgir una mala ejecución de esta misma.

6.1.2. Alcance

La política se emplea en toda la organización, englobando a todos los departamentos y niveles de jerarquía. Es fundamental que se cumplan los requisitos mínimos establecidos en esta política, sin descartar la posibilidad de mejorar continuamente la seguridad.

6.2. Roles y responsabilidades

Para llegar a los objetivos establecidos en la Política de Seguridad de la empresa, se han asignado los siguientes roles y responsabilidades como dice el autor [15]:

Secretaría:

- Encargada de coordinar y supervisar los trabajos de mantenimiento, tanto para reparaciones como para prevención, de los equipos informáticos utilizados por la entidad, incluyendo computadoras de escritorio, portátiles, impresoras y otros periféricos.
- Debe seguir las directrices y lineamientos proporcionados por la Oficina de Tecnologías.
- Asegurarse de que la seguridad de la información se gestione adecuadamente en todos los ámbitos de la organización.

Presidente:

- Responsable de coordinar la implementación de acciones con el propósito de garantizar el cumplimiento de la política establecida en el presente documento.
- Realizar la clasificación de la información según su nivel de sensibilidad y criticidad, así como mantener actualizada dicha clasificación.
- Definir los permisos de acceso a la información en base a las funciones y competencias de los usuarios correspondientes.
- Establecer objetivos y planes para controlar, monitorear y comprobar el cumplimiento de los procedimientos relacionados con la seguridad de la información, tanto como exigir la existencia de documentación física o digital actualizada asociada a dichos procedimientos.

Gerente:

- Es quien puede certificar la Política de Seguridad Institucional y sus eventuales modificaciones.
- Valorar el proceso de gestión de seguridad.
- Facilitar los recursos necesarios para el adecuado funcionamiento de la politica.

Socios y Clientes:

- Comprometidos a mantener la confidencialidad y a seguir las políticas y normas de seguridad en todas las actividades laborales.
- Notificar de forma inmediata cualquier incidente que pueda comprometer el cumplimiento de esta política al responsable designado de seguridad.

6.3. Gestión de activos

Es importante contar con un registro e inventario de los recursos de información esenciales para respaldar los procesos operativos de la empresa. Además, se requiere mantener dichos inventarios actualizados de forma periódica.

Es necesario clasificar cada recurso de acuerdo con el tipo de información que maneja, siguiendo las pautas establecidas en la sección correspondiente sobre la clasificación de la información.

Además, se asignará a cada recurso o elemento de información un responsable o propietario encargado de asegurar su inclusión en el inventario, su clasificación correcta y la implementación de las medidas de protección adecuadas.

Asimismo, se recomienda realizar ajustes regulares en la configuración de los recursos para facilitar su seguimiento y una actualización precisa de la información asociada [16].

6.3.1. Gestión de las copias de seguridad

Es crucial realizar regularmente backups de la información, el software y el sistema en la empresa, y llevar a cabo verificaciones periódicas para mejorar su integridad. Se recomienda programar copias de seguridad de aplicaciones, archivos y bases de datos al menos una vez por semana, a menos que no se haya

realizado ninguna actualización en ese periodo. En caso de que la información tenga un alto impacto para la empresa, se puede considerar aumentar la frecuencia de las copias de respaldo [16].

Siempre que sea posible, se debe buscar la encriptación de la información en las copias de respaldo como una medida general. Específicamente, se exigirá la encriptación para ciertos tipos de información confidencial, como requisito obligatorio de seguridad.

También es esencial llevar a cabo pruebas de restauración de las copias de respaldo disponibles y de los procedimientos de recuperación establecidos. Estas pruebas se realizarán periódicamente y se documentarán para asegurar la adecuada operación de los recursos y procesos de recuperación de datos.

6.4. Clasificación de la información

Es fundamental establecer en la empresa un método de categorización que permita implementar las medidas necesarias para preservar su seguridad. Este sistema de clasificación debe estar en consonancia con los lineamientos y directrices establecidos en la política correspondiente.

Asimismo, se designará a un responsable encargado de mantener actualizado el sistema de clasificación y de difundirlo entre todos los colaboradores de la empresa. Este responsable será responsable de realizar las actualizaciones pertinentes en el sistema de clasificación según sea necesario. De esta manera, se fomentará una comprensión clara y generalizada de las categorías de clasificación de la información en toda la organización [16].

6.4.1. Tipos de información

La empresa deberá realizar una categorización de la información en base al medio utilizado para su manejo [16]:

a) Medios digitales: se refiere a la información empleada a través de sistemas electrónicos, como aplicaciones de software, correo electrónico o sistemas de información personalizados o adquiridos a terceros.
b) Medios físicos: abarca la información almacenada en formatos físicos, como documentos impresos, dispositivos como: USB, DVD, entre otros.

6.4.2. Niveles de clasificación

La organización deberá categorizar la información en cinco niveles distintos, considerando su grado de sensibilidad [16]:

- Nivel de información de acceso público
- Nivel de información de acceso limitado
- Nivel de información confidencial
- Nivel de información reservada
- Nivel de información altamente confidencial

6.4.3. Gestión de información privilegiada

La empresa deberá implementar precauciones adicionales para salvaguardar la información como secreta. Serán necesarias medidas de seguridad extraordinarias, así como el uso de protocolos de comunicación seguros y técnicas de cifrado al transmitir este tipo de información, con el fin de garantizar su manejo adecuado y proteger su confidencialidad [16].

6.5. Prevención de fugas de información

La filtración de información implica la revelación no autorizada de datos, ya sea de forma intencional o accidental, resultando en la pérdida de control sobre quién accede a la información. Es crucial brindar capacitación a socios y clientes sobre buenas prácticas para prevenir la filtración de información. Algunos aspectos clave a considerar incluyen [17]:

- Gestión de dispositivos críticos: Implementar un proceso para manejar de manera adecuada los dispositivos de alta importancia.
- Uso seguro de dispositivos extraíbles: Promover pautas para utilizar de forma adecuada dispositivos como USB, CD/DVD u otros medios similares.
- Seguridad en el correo electrónico: Educar sobre prácticas seguras en el uso del correo electrónico para evitar la filtración de información sensible.
- Transmisión segura de información oral: Establecer medidas para proteger la privacidad durante la transmisión oral de información sensible.
- Impresión de documentos: Establecer directrices para la impresión segura de documentos confidenciales.
- Control en la salida de documentación: Implementar medidas para asegurar que la documentación confidencial se maneje de manera adecuada al salir de la organización.
- Dispositivos móviles: Fomentar el uso responsable y seguro de dispositivos móviles para prevenir la fuga de información.
- Seguridad en el uso de Internet: Promover pautas y precauciones para proteger la información mientras se utiliza Internet.
- Cuidado de equipos desatendidos: Adoptar medidas de seguridad para proteger la información en equipos que quedan desatendidos.

Es fundamental abordar estos aspectos a través de programas de capacitación para promover una cultura

de seguridad de la información en toda la organización.

6.6. Control de acceso

En la empresa, se debe implementar un sistema de gestión de acceso para todos los sistemas de información. El propósito es asegurar que únicamente los usuarios autorizados puedan acceder a dichos sistemas y prevenir cualquier acceso no autorizado. Se establecerán medidas de protección, como el uso de contraseñas seguras, para incrementar la seguridad de los sistemas.

El control de acceso se abordará tanto desde una perspectiva lógica, enfocada en los sistemas de información, como desde una perspectiva física. Esto implica la adopción de medidas de seguridad tanto a nivel digital como en el entorno físico de la empresa para mejorar la seguridad de la información y evitar intrusiones no deseadas [17].

6.6.1. Requisitos de negocio para el control de acceso

Se establecerán ciertos criterios de acción para regular el control de acceso, los cuales resultan esenciales para salvaguardar la seguridad. Estos criterios comprenden [17]:

- Usuarios individuales y privilegios mínimos: Se exigirá que cada usuario cuente con una identificación única y no se permitirá el uso compartido de cuentas. Además, los privilegios asignados a los usuarios se limitarán al mínimo necesario, según el principio de menor privilegio.
- Prohibición de cuentas genéricas: Se restringirá el uso de cuentas de usuario genéricas, promoviendo en su lugar el empleo de cuentas vinculadas a la identidad personal de cada individuo implicado.

Estos criterios se orientan a reforzar la seguridad y garantizar un control adecuado sobre el acceso a los sistemas empresariales, con el propósito de mitigar los riesgos inherentes a prácticas no autorizadas o potencialmente peligrosas.

6.6.2. Derechos de acceso

La empresa deberá implementar medidas de control de acceso que aseguren que los usuarios únicamente tengan los privilegios y derechos necesarios para llevar a cabo sus funciones específicas. Para ello, se considerarán los siguientes aspectos [17]:

- Control de acceso basado en roles: Se establecerán perfiles o roles de acceso para las aplicaciones y sistemas, de modo que puedan asignarse a los usuarios correspondientes de manera adecuada.
- Principio de necesidad de saber: Solo se permitirá el acceso a los recursos cuando exista una justificación legítima para el desarrollo de las actividades laborales.
- Privilegios mínimos: Los permisos otorgados a los usuarios serán limitados al mínimo requerido para llevar a cabo sus tareas de manera eficiente y segura.
- Segregación de funciones: Se debe realizar una adecuada separación de funciones para la asignación y gestión de los derechos de acceso, evitando posibles conflictos de interés y minimizando los riesgos asociados.

Adicionalmente, se establece que ningún usuario podrá acceder por sí mismo a un sistema de información controlado sin tener la autorización previa de la persona designada para tal fin. Esta medida refuerza el control y la responsabilidad en el manejo de la información sensible.

6.7. Seguridad física y del entorno

Los sistemas de información de la empresa deberán contar con medidas de seguridad en los espacios físicos donde se encuentran ubicados. Estas medidas incluirán control de acceso, cámaras de seguridad y precauciones para prevenir la inseguridad, como ingreso no permitido. [16].

Asimismo, se implementará un control de acceso físico a la información en formato físico, utilizando registros en papel para llevar un seguimiento de quién accede a dicha información. En el caso de información confidencial, se aplicarán medidas específicas, como el uso de armarios resistentes al fuego u otras medidas de seguridad adecuadas para su resguardo.

Estas acciones permitirán aumentar la seguridad de la información empresarial, evitando riesgos y asegurando un entorno seguro para los sistemas de información.

6.8. Seguridad en los proveedores

Es esencial realizar una exhaustiva evaluación de los servicios que puedan ser subcontratados por la empresa, con el fin de identificar aquellos que revistan una importancia crítica en términos de seguridad de la información. Estos servicios pueden variar en función de su naturaleza, la sensibilidad de los datos involucrados y su impacto en la continuidad de las operaciones [16].

Al seleccionar proveedores para dichos servicios, se deberá tener un cuidado especial en los procesos de selección, asegurándose de establecer requisitos contractuales adecuados.

Este enfoque permitirá garantizar que los servicios subcontratados cumplen con los estándares de seguridad requeridos por la empresa, salvaguardando la

información empresarial y asegurando la continuidad de las operaciones de manera adecuada.

6.9. Cumplimiento regulatorio

La organización se compromete a dedicar los recursos necesarios para hacer cumplir las leyes y regulaciones pertinentes en relación con la seguridad de la información. Además, se asignará los encargados de dar cumplimiento a los integrantes de la empresa según el rol que desempeñen [15].

En este sentido, se dará especial importancia a asegurar el cumplimiento de todas las leyes, normativas y regulaciones vigentes que afecten a la empresa. Será una prioridad para la organización mantenerse actualizada respecto a los requisitos legales y ejecutar su cumplimiento en todas las actividades relacionadas con la seguridad de la información.

6.10. Gestión de excepciones

Toda variación de la Política de Seguridad de la Información en la empresa será debidamente documentada y comunicada al responsable pertinente. Estas situaciones excepcionales serán evaluadas con detenimiento para determinar el nivel de riesgo que pueden implicar para la organización [15].

6.11. Sanciones disciplinarias

La empresa se reserva el derecho de tomar las medidas disciplinarias necesarias en caso de incumplimiento de la Política de Seguridad de la Información. Todos los empleados tienen la responsabilidad de informar encargado ante cualquier evento que pueda implicar una violación de las directrices establecidas en esta Política.

6.12. Revisión de la política

La implementación de esta Política cuenta con el total respaldo de la alta dirección de la empresa, quienes se comprometen a lograr todos los objetivos establecidos y cumplir con los requisitos establecidos. La Política de Seguridad será sometida a una revisión y aprobación anual por parte del órgano de gobierno correspondiente. En caso de producirse cambios relevantes en la organización o de identificarse modificaciones significativas en el entorno de amenazas y riesgos, tanto operativos como legales, regulatorios o contractuales, se llevará a cabo una revisión de la Política para asegurar su adecuación a la realidad de la empresa en todo momento [17].

7. Factibilidad

La factibilidad de implementar la política en la organización ha sido evaluada y analizada. Se ha llevado a cabo un estudio para determinar la viabilidad de aplicar los resultados de esta investigación en el entorno organizacional. es factible económicamente debido a su capacidad para prevenir incidentes costosos, proteger los activos de la empresa y mantener la continuidad de las operaciones comerciales. Si bien implica un gasto inicial, los beneficios a largo plazo y la reducción de riesgos compensan ampliamente la inversión realizada.

En términos de factibilidad técnica, se ha considerado la compatibilidad de los recursos tecnológicos y sistemas existentes en la organización. Se ha verificado que se cuenta con la infraestructura adecuada para llevar a cabo la implementación propuesta, y que no se requieren modificaciones significativas ni costosas inversiones en tecnología. Además, se ha evaluado la disponibilidad de personal capacitado o la posibilidad de capacitar al equipo existente para llevar a cabo la implementación de manera eficiente.

La factibilidad operativa también ha sido analizada. Se ha considerado la capacidad de la organización para gestionar y coordinar la implementación, permitiendo que se cuente con los recursos humanos necesarios, los roles y responsabilidades estén claramente definidos, y se establezcan mecanismos adecuados de seguimiento y control.

En términos de factibilidad económica, se ha realizado un análisis detallado de los costos asociados con la implementación. Se han evaluado los gastos de adquisición de equipos o tecnología adicional, la capacitación del personal, los posibles costos de mantenimiento y soporte, y otros gastos relevantes. Se ha comparado estos costos con los beneficios esperados y se ha evaluado la viabilidad económica del proyecto.

La inversión en seguridad es una decisión empresarial inteligente y factible desde el punto de vista económico. La empresa puede considerar la inversión en seguridad que debe realizar como algo favorable debido a los ingresos netos con los que esta cuenta y el beneficio es evitar los costosos incidentes que por fallos de seguridad pueden detener la operación de la empresa, por lo que el sistema protegerá su reputación y fortalecerá su presencia en el mercado.

V. DISCUSIÓN

La propuesta de una política de seguridad es fundamental en la gestión de cualquier organización en la era digital. En esta investigación, se ha desarrollado y presentado una política de seguridad basada en la metodología MAGERIT, con el objetivo de fortalecer el gobierno corporativo de TI y garantizar la protección adecuada de los activos de información.

La discusión se centra en la importancia de adaptar la política de seguridad de la información a las metas

estratégicas y necesidades específicas de cada empresa o proyecto. Si bien la metodología MAGERIT y la propuesta de plan que brindan un marco sólido, es necesario tener en cuenta que no existen reglas generales o resultados definitivos que sean aplicables de manera universal. Cada empresa tiene sus propias metas estratégicas y desafíos particulares, lo que requiere una adaptación y personalización de la política de seguridad.

El enfoque presentado en esta investigación destaca el uso de MAGERIT como una herramienta para potenciar proyectos estratégicos, centrándose en el análisis de riesgos y la protección adecuada de la información. A diferencia de enfoques anteriores, se ha puesto énfasis en la gobernanza de TI y se ha integrado el análisis y gestión de riesgos como parte integral del proceso. Esto proporciona una ventaja significativa al permitir que las organizaciones aborden de manera más efectiva los riesgos.

Es importante mencionar que la aceptación generalizada de la metodología MAGERIT en la industria de TI respalda la validez y aplicabilidad del enfoque propuesto. La existencia de estándares y marcos de referencia respaldados por la comunidad ayuda a que la metodología sea repetible y adaptable en diferentes entornos y empresas.

Sin embargo, es crucial que cada organización evalúe y adapte la política de seguridad de la información a sus propias necesidades y circunstancias. Cada empresa tiene su propio conjunto de requisitos y desafíos únicos, y la política de seguridad debe ser diseñada teniendo en cuenta estas consideraciones específicas.

En resumen, la propuesta de una política de seguridad de la información basada en la metodología MAGERIT representa un avance significativo en la protección de la información y el fortalecimiento del gobierno corporativo de TI. Sin embargo, es necesario reconocer la importancia de la adaptación y personalización de esta política para cumplir con los objetivos estratégicos y requisitos individuales de cada empresa. La aceptación generalizada de la metodología MAGERIT respalda su aplicabilidad en diferentes entornos, pero su implementación exitosa requiere una evaluación cuidadosa y una adaptación adecuada a cada contexto empresarial.

VI. Conclusión

A través de un minucioso análisis de los activos críticos de información de la empresa de transporte pesado, se logró identificar aquellos elementos de mayor relevancia y determinar su nivel de vulnerabilidad. Este proceso permitió comprender la importancia de proteger dichos activos y establecer medidas adecuadas para salvaguardar la CIA.

El análisis detallado de la normativa legal vigente en Ecuador, en particular la Ley Orgánica de Protección de Datos Personales, proporcionó una base sólida para el diseño de la política de seguridad. Se pudo comprender los requerimientos legales y las obligaciones que la empresa de transporte pesado debe cumplir en cuanto a la protección de los datos personales. Esto permite que la política propuesta se ajuste plenamente al marco legal establecido.

La elaboración de una política de seguridad sólida y completa para la protección de datos clasificados en la empresa de transporte pesado se realizó siguiendo las mejores prácticas y normativas nacionales e internacionales en materia de seguridad de la información. Esta política se adaptó específicamente a las necesidades y características de la organización.

Por último, se llevó a cabo una evaluación exhaustiva de la factibilidad de implementar la política de seguridad interna propuesta en la empresa de transporte pesado. Mediante un análisis detallado de los recursos disponibles, los aspectos operativos y las implicaciones prácticas, se pudo determinar que la implementación de la política de seguridad es viable y presenta beneficios significativos para la protección de los datos clasificados. Además, se formularon recomendaciones prácticas y realistas para facilitar la implementación efectiva y permitiendo la continuidad de las medidas de seguridad.

Referencias

[1] P. e. I. d. l. A. E. Dirección General de Modernización Administrativa, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[2] Maniah y S. Milwandhari, «Risk Analysis of Cloud Computing in the Logistics Process,» *2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE),* pp. 1-5, 2020.

[3] A. Teringl, J. Kůla, L. Kozubík y M. Osladil, «ASSET MANAGEMENT SYSTEM IN DSO USING BUSINESS INTELLIGENCE TOOLS AND ADVANCED ANALYTICS,» *CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution,* vol. 2021, 2021.

[4] M. Aleksandrov, V. Vasiliev y S. Aleksandrova, «Implementation of the Risk-based Approach Methodology in Information Security Management Systems,» *2021 International Conference on*

Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2021.

[5] S. Grishaeva y V. Borzov, «Information Security Risk Management,» *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS),* 2020.

[6] F. Y. Holguín García y L. M. Lema Moreta, «Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; focused on Shipping Companies,» *2018 7th International Conference On Software Process Improvement (CIMPS),* 2018.

[7] A. Fernandez y D. Garcia, «Complex vs. simple asset modeling approaches for information security risk assessment: Evaluation with MAGERIT methodology,» *2016 Sixth International Conference on Innovative Computing Technology (INTECH),* 2016.

[8] D. F. Carnero Garay y M. A. Carbajal Ramos, «Modelo de gestión de riesgos de seguridad de información para mitigar el impacto en las PYMEs en Perú,» *In CISTI (Iberian Conference on Information Systems & Technologies/Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings,* 2020.

[9] L. N. Brunet, «Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información,» *Revista de la Facultad de Derecho,* 2015.

[10] M. A. Ulloa-Enriquez, «Riesgos del Trabajo en el Sistema de Gestión de Calidad,» *Ingenieria Industrial,* vol. 33, nº 2.

[11] P. Guerrero Vivanco, «LEY ORGÁNICA DE PROTECCION DE DATOS PERSONALES,» *Asociacion Nacional de Asesores Productores de Seguros,* 2021.

[12] A. Nacional, «Ley Organica de Proteccion de Datos Personales,» 2021.

[13] F. B. Farro Zapata, «Elaboración de un plan de recuperación ante desastres para una empresa operadora satelital en el Perú y diseño de una estación terrena satelital,» *Pontifica Universidad Catolica del Peru,* 2015.

[14] D. G. Paredes Garces, «Plan de emergencia y contingencia para disminuir los factores de riesgo en incendios y desastres naturales en la Empresa "TEIMSA",» *Universidad Tecnica de Ambato,* 2012.

[15] A. Araujo, «Cómo hacer tu política de seguridad de la información,» *hackmetrix,* 2021.

[16] I. 27001, «FASE 3 ELABORACIÓN DE LA POLÍTICA,» *ISO 27001.*

[17] A. d. C. y. S. ACS, «Politica de Seguridad de la Informacion,» *Grupo ACS,* 2022.