UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

ANÁLISIS DE VULNERABILIDADES DEL SISTEMA DE INFORMACIÓN DEL ÁREA DE LOGÍSTICA DE LA EMPRESA TRANSCARGA S.A.

AUTORES:

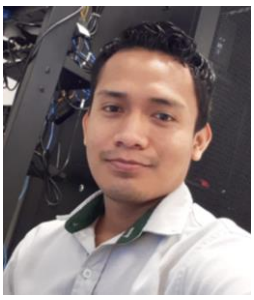
JHONNY JOFFRE CHOEZ BURGOS
ABRAHAM JOSUE QUISPE PALACIOS

DIRECTORA:

MÓNICA DANIELA GÓMEZ RIOS

CUENCA – ECUADOR
2023

Autores:



Jhonny Joffre Choez Burgos
Ingeniero en Computación e Informática.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
jhonnyjcb@gmail.com

Abraham Josue Quispe Palacios
Ingeniero en Computación e Informática.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
Tauren_91@hotmail.com

Dirigido por:

Mónica Daniela Gómez Ríos
Ingeniero de Sistemas.
Magister en Ciencias de la Computación mención Networking.
Magister en Ciencias de la Computación mención Aplicaciones Distribuidas.
mgomezr@ups.edu.ec

Análisis de vulnerabilidades del sistema de información del área de logística de la empresa Transcarga S.A.

DEDICATORIA

Dedico este gran paso profesional a Dios sobre todas las cosas a mis padres, quienes han sido mi principal apoyo y fuente de motivación durante toda esta trayectoria. Valoro profundamente su constante aliento, paciencia y comprensión durante el proceso académico y los momentos de estrés. Sin su inquebrantable amor y respaldo, este trabajo no habría sido posible.

Asimismo, quiero expresar mi gratitud hacia mis dos grandes amigas, quienes me acompañaron en los procesos más difícil de esta carrera. Agradezco su disposición para escuchar mis ideas, brindarme ánimo cuando las dudas me embargaban y celebrar mis éxitos. Su amistad ha sido un clave en los momentos difíciles y una fuente de alegría en los momentos triunfales.

Jhonny Joffre Choez Burgos

Dedico este trabajo a mi familia, a mi esposa quien me ha sido el pilar de motivación para continuar mejorando profesionalmente. Quiero agradecer a todos aquellos que, de una forma u otra, contribuyeron a la realización de esta tesis. Sus ideas, sugerencias y comentarios han enriquecido mi trabajo y me han impulsado a crecer como profesional.

Abraham Josue Quispe Palacios

AGRADECIMIENTO

Agradecimiento a la Universidad Politécnica Salesiana de Ecuador por brindar a sus alumnos la oportunidad de crecer profesionalmente. El respaldo y los recursos proporcionados por la institución han sido fundamentales para el éxito de este proyecto. Agradezco sinceramente a la institución por su compromiso con la excelencia académica y por fomentar un entorno propicio para el aprendizaje, desarrollo y la investigación.

También queremos extender mi más sincero agradecimiento a la tutora Monica Gómez Ríos por su orientación invaluable a lo largo de todo el proceso de esta tesis. Su experiencia, conocimientos y dedicación han sido pilares fundamentales para el desarrollo y la finalización de este trabajo. Aprecio profundamente su disposición para brindarme orientación, su apoyo constante y su capacidad para motivar a alcanzar esta meta académica. Sus comentarios y sugerencias han sido invaluables para mejorar la calidad y el rigor de este trabajo.

Espero que este trabajo sea un testimonio de nuestra gratitud y un tributo a la generosidad de la Universidad Politécnica Salesiana de Ecuador y sus ilustres docentes. ¡Gracias!"

Tabla de Contenido

Índice de Tablas

Índice de Figuras

Análisis de vulnerabilidades del sistema de información del área de logística de la empresa Transcarga S.A.

Autores:

Jhonny Joffre Choez Burgos

Abraham Josue Quispe Palacios

Resumen

El presente trabajo de investigación tiene por objetivo principal identificar las vulnerabilidades de seguridad de la información en el área de logística de la empresa Transcarga S.A. para presentar un plan de acción apoyado en la normativa ISO/IEC 27001. Como metodología de la investigación se trató de una investigación descriptiva con enfoque mixto y un diseño no experimental; como principales técnicas de recolección de información se efectuó entrevista y encuesta a personal de la empresa objeto de estudio, además de la investigación documental.

Dentro de los principales resultados obtenidos se pudo conocer que la empresa no cuenta con un sistema de seguridad de la información que garantice su resguardo colocándola en una posición vulnerable ante el acceso de intrusos a la información de la empresa, pérdida de datos, exposición a virus, daño de equipos tecnológicos, alteración de fuentes de datos y otros escenarios que impiden la garantía de seguridad.

Se concluye que la empresa requiere emplear de forma inmediata las acciones necesarias para diseñar las políticas de seguridad de la información, que le ayuden a establecer las estrategias ante posibles riesgos con el manejo de los datos, así como precisar responsables y capacitar al personal en todas las áreas. Finalmente se propone un plan de acción que permita mejorar los niveles de seguridad de la información, tomando como referencia la normativa ISO 27001.

Palabras clave: Seguridad de la Información, Vulnerabilidad de datos, Resguardo, Plan de Acción, Norma ISO 27001.

ABSTRACT

The main objective of this research work is to identify information security vulnerabilities in the logistics area of the company Transcarga S.A. to present an action plan supported by the ISO/IEC 27001 standard. As research methodology, it was a descriptive investigation with a mixed approach and a non-experimental design; As the main data collection techniques, an interview and survey of the personnel of the company under study was carried out, in addition to documentary research.

Among the main results obtained, it was possible to know that the company does not have an information security system that guarantees its protection, placing it in a vulnerable position before the access of intruders to the company's information, loss of data, exposure to viruses, damage to technological equipment, alteration of data sources and other scenarios that prevent the guarantee of security.

It is concluded that the company needs to immediately use the necessary actions to design information security policies, which help it to establish strategies in the face of possible risks with data handling, as well as to specify those responsible and train personnel in all the areas. Finally, an action plan is proposed to improve the levels of information security, taking the ISO 27001 standard as a reference.

Keywords: Information Security, Data Vulnerability, Protection, Action Plan, ISO 27001 Standard.

1 Introducción

Las tecnologías de la información, cumplen una labor fundamental en las empresas, debido a lo que significa para los modelos de negocios, la administración de la infraestructura, la seguridad en general y en diversos componentes organizacionales. A su vez, y a la par de los avances tecnológicos, las amenazas han venido en aumento exponencialmente; por lo tanto, representa una preocupación constante y fundamental en el manejo de la organización que busca resguardar el principal de los activos, los datos.

Los análisis de la vulnerabilidad, son esenciales para la identificación de todas aquellas amenazas que se aprovechan de puntos débiles para atacar e invadir los sistemas informáticos. Por lo tanto, es de suma importancia que las organizaciones de manera recurrente analicen la gestión de los riesgos de manera eficiente, para poder garantizar el óptimo funcionamiento de los sistemas de información, el resguardo de los datos y de esta manera, tener una toma de decisiones asertivas y basadas en la realidad existente.

En base a esta problemática, se han desarrollado diversas normas como es el caso de la ISO/IEC 27001 que trata de un estándar internacional que busca el establecimiento de los requisitos para la implementación, mantenimiento y mejoras continuas de los Sistemas de Gestión de la Seguridad de la Información (SGSI); como un mecanismo para la protección de la confidencialidad, la integridad y la disponibilidad de la información dentro de las organizaciones [1].

Este tema trata acerca de la identificación de las vulnerabilidades de seguridad de la información en el área de logística de la empresa Transcarga S.A., y se busca presentar un plan de acción apoyado en la normativa ISO/IEC 27001, con el fin de asegurar el activo fundamental de los sistemas, como lo es la información.

La presente investigación, se realiza con el fin ofrecerle a la empresa que es cuestión de estudio un plan destinado en ofrecer políticas de seguridad informática bien sea a los usuarios en general y a los equipos informáticos con los que cuenta la organización, mismos que están expuestos a las amenazas informáticas, pudiendo ser un blanco fácil

en la indisponibilidad de la información y el funcionamiento general de la empresa, por tanto, el trabajo se estructura en siete apartados; el primero corresponde a la introducción, desarrollando los antecedentes, la formulación del problema la justificación y los objetivos de estudio. En segundo lugar, el estado del arte y el marco teórico, mismo en el que se incluyen todos los términos relacionados al trabajo de investigación, citando los autores según la norma correspondiente y las bases teóricas. Por otro lado, la metodología, seguida de los resultados, las conclusiones y recomendaciones. El final, las referencias bibliográficas citadas a lo largo de la investigación y los anexos correspondientes.

1.1 ANTECEDENTES

El avance y el desarrollo tecnológico dentro de los sistemas computacionales, el internet y las comunicaciones; conllevan a que: pequeñas, medianas y grandes empresas, incorporen nuevas tecnologías y métodos de seguridad dentro de sus negocios, con el propósito de mejorar el rendimiento y desempeño de sus distintas áreas laborales [2]. Además, el alto uso que tienen las TIC (Tecnologías de la información y la Comunicación) dentro de organizaciones públicas y privadas, son parte del conjunto de herramientas para la transmisión, procesamiento y almacenamiento de la información de una empresa. Por otro lado, el manejo de los sistemas de información empresariales es propenso a condiciones de riesgos [3]. En la actualidad existen diversas modalidades que ponen al descubierto la información que podrían intentar perjudicar o apropiarse de la misma; ante estas situaciones los miembros de la empresa y sobre todo el personal informático debe estar sobre aviso y en constante preparación.

En cualquier organización sea pública o privada, la seguridad de la información es fundamental, por el alto valor que representa para la empresa y en algunos casos dicha información, infraestructuras y procesos son confidenciales. Es por ello que, se deben identificar las amenazas y vulnerabilidades presentes para mantener esta información de manera íntegra, disponible y absolutamente reservada, aplicando medidas de seguridad como lo exigen las normativas internacionales [4] [5]., con el propósito de evitar que las amenazas comprometan los activos de información.

Para proteger a los sistemas de información ante cualquier ataque informático, las empresas tienen la necesidad de llevar a cabo capacitaciones, programas o proyectos de seguridad informática; esto se debe a que las políticas de seguridad de información son la base necesaria en los programas de seguridad organizacional [6] [7]. Dentro de los lineamientos de un sistema de Gestión para la seguridad de la información debe contener políticas, procedimientos o directrices específicas para cada actividad, proceso o sistema de información para cumplir con el objetivo de protección de los activos de información en una organización [8].

La normativa ISO 27001 propone la aplicación de buenas prácticas para implementar un correcto SGSI. Por tanto, si las organizaciones reconocieran su importancia, entenderían que esta, permite proteger los datos e información que manejan, que son el activo muy importante de las organizaciones, cabe recalcar que la ISO 27001 mantiene los principios de la seguridad de información en cuanto a su integridad, confidencialidad y disponibilidad, generando así confianza en los clientes, proveedores y empleados [9] [10].

La empresa Transcarga S.A. se ubica en la ciudad de Guayaquil la misma que se dedica a la transportación de carga pesada. La empresa entre sus sistemas de información cuenta con aplicativos propios y de terceros con los cuales realiza procesos de facturación electrónica, cobros, pago a proveedores, manejos de inventarios, entre otros. De la misma forma poseen otros componentes que intervienen en un sistema de información como lo son la infraestructura de red, equipos informáticos, infraestructura de video vigilancia y el personal.

A pesar de contar con protecciones de seguridad a nivel de redes, navegación y roles de usuarios en los sistemas; la empresa se ha visto vulnerada por el desconocimiento de los usuarios y la exposición de la información dentro del área de logística; lo cual se convierte en un riesgo, expuesto a delitos informáticos que pueden ocasionar daños a los activos, servidores, redes e información de la empresa.

Mediante las consideraciones antes analizadas, es de alta importancia llevar a cabo un análisis de vulnerabilidad del sistema de información del área de logística, ya que por

medio de esta se podrán detectar las posibles amenazas o ataques informáticos que atentan con poner en riesgo los principios de seguridad de la información y equipos tecnológicos de la empresa, debido que en esta área se manejan grandes volúmenes de información sensible como lo son contactos de clientes, costos de operación, valores de servicios ofrecidos.

Para el desarrollo de la presente investigación se realizará una encuesta dirigida al personal de la empresa Transcarga S.A, con el fin de conocer las razones por las cuales la gestión actual de la seguridad de la información necesita ser mejorada. En tal sentido, se considera la norma ISO/IEC 27001, debido a su utilidad en la estandarización de la seguridad de la información, ayudando a la presente empresa en la mejora de la gestión de los riesgos de la seguridad de la información en el área logística.

1.2 Formulación del Problema

La falta de controles de seguridad de la información podría ocasionar que los sistemas informáticos queden comprometidos con eventuales interrupciones de servicio incluso pudiendo llegar a la pérdida de información. Además, el rápido desarrollo en el campo de la informática demanda que las empresas implementen estrategias de seguridad que permitan preservar sus sistemas de información. Debido a esto, la empresa Transcarga S.A. considera a la tecnología el eje principal para alcanzar sus objetivos, por lo que se apoya en la Dirección de Tecnologías para la gestión de aplicativos con los que realiza sus procesos internos, para lo cual requiere estandarizar sus mecanismos de control en base a estándares.

La Norma ISO/IEC 27001 define las buenas prácticas para la implementación de los sistemas de gestión de seguridad de la información dentro de las organizaciones. Cuando las mismas cumple con esta norma, cuentan no solo con la protección de sus datos, que representan el activo más importante, sino que también generan una confianza mayor a los clientes, proveedores y colaboradores [11].

En este sentido, la certificación de esta norma internacional permite la demostración de la buena funcionalidad de los servicios ofrecidos y las buenas prácticas ejecutas. Por ende, las empresas deben de contar con un Plan de Acción basado en esta Norma a fin

de preservar la confidencialidad e integridad de la información empresarial y garantizar la disponibilidad de los datos. De acuerdo con ello, la finalidad de realizar este trabajo plantea las siguientes preguntas para dar cumplimiento a los objetivos:

¿Cuáles son las razones que afectan la seguridad de la información en el área de logística de la empresa Transcarga S.A.?

¿Qué consecuencias que se pueden generar ante la falta de mecanismos de seguridad y resguardo de la información y datos, en la empresa Transcarga S.A.?

¿Qué plan de acción se puede proponer basado en la normativa ISO/IEC 27001 que contribuya a la seguridad de la información en la empresa Transcarga S.A.?

Mediante el análisis basado en la norma ISO/IEC 27001, se procura brindar lineamientos de seguridad para prevenir la explotación de vulnerabilidades, proporcionando mecanismos de control que puedan ser aplicados en la empresa Transcarga S.A.

Por tanto, la norma ISO/IEC 27001, aplicada en la organización que es cuestión de estudio, permitirá mitigar las amenazas que afectan la seguridad de la información de la empresa. Dicha información representa un insumo considerablemente importante en la toma de decisiones estrategias, por lo que la protección de ella debe de ser garantizada.

1.3 JUSTIFICACIÓN

La falta de políticas de seguridad de información apoyado por el desconocimiento de los usuarios en el uso de medios digitales, la exposición de la información del sistema dentro del área de logística de una empresa, además de las amenazas que trae el uso de las tecnologías (virus, fuga de información, espionaje, instrucciones o delitos informáticos) [12] [13]; afectan el nivel de seguridad informática; siendo este el caso de la empresa Transcarga S.A, la cual, no cuenta con políticas de seguridad informática y tanto los usuarios como los equipos informáticos se encuentran expuestos, lo cual puede ocasionar indisponibilidad de información funcionamiento de la empresa. Al mismo tiempo, la empresa cuenta con información sensible tanto de los clientes como de las operaciones que esta lleva a cabo, por lo que representa un blanco para los ataques informáticos; pero la custodia, operación y almacenamiento de esta no se

encuentra gestionado según las políticas de las Normas ISO/IEC 27001, viéndose de esta forma expuesta la integridad, seguridad y disponibilidad de los datos.

Para ello, se considera oportuno aprovechar al máximo los recursos tecnológicos de la empresa para la administración, control y manejo de datos, siendo fundamental la implementación de políticas que aporten a la reducción de posibles ataques por amenazas precautelando la seguridad del sistema.

La aplicación de la norma ISO sería una solución viable para gestionar los riesgos y controlar la seguridad de la información. Esta solución, destinada a la disminución de los riesgos en el sistema puede ser estudiada mediante un análisis de vulnerabilidad y un desarrollo de políticas conjuntas, mismas que deben de ser cumplidas por los involucrados de la organización.

El propósito de esta iniciativa es crear un plan de acción basado en el reporte de la vulnerabilidad de la información obtenida, al igual que elaboración de políticas de seguridad y mitigar los posibles riesgos que se presenten. Por lo tanto, su desarrollo es factible debido a que está orientado al uso de las buenas prácticas señaladas en la norma, permitiendo la mejora de los sistemas de seguridad utilizados para gestionar la información.

1.4 Objetivos

1.4.1 Objetivo general

Identificar las vulnerabilidades de seguridad de la información en el área de logística de la empresa Transcarga S.A. para presentar un plan de acción apoyado en la normativa ISO/IEC 27001.

1.4.2 Objetivos específicos

OE1: Inspeccionar las razones por las cuales la gestión actual de la seguridad necesita estandarizar sus mecanismos de control, mediante entrevistas y encuestas al personal.

OE2: Determinar las causas por las cuales los actuales mecanismos de control de seguridad pudieran provocar fallos en el SGSI mediante ataques controlados al sistema.

OE3: Proponer un plan de acción acorde a las causas detectadas en base a la normativa ISO/IEC 27001.

2 Marco teórico referencial

La revisión de literatura dentro de esta tesis acoge términos y definiciones de análisis de vulnerabilidades relacionadas a tecnologías de información, así como los elementos de seguridad informática. También se mencionan características de la Norma ISO/IEC 27001 relacionadas al análisis de vulnerabilidades.

2.1 Seguridad de la Información

La información es un conjunto de datos que en conjunto tienen un significado especifico, bien para reducir ciertas dudas o para aumentar el conocimiento respecto a algo. En medidas generales. La información es un mensaje que tiene un significado específico según sea el contexto en el que descifre; la misma, está disponible para el uso inmediato y puede también proporcional orientación acerca de acciones pertinentes en la toma de decisiones [14].

En base a esta definición, se puede entender que dentro de las organizaciones, la información representa un activo importante, valioso y sensible que da un valor significativo en la toma de las decisiones y en la planificación o ejecución de planes de acción destinados a las mejoras, posicionamiento en el mercado, en el talento humano, en las proyecciones de crecimiento, en los estados contables, entre otros aspectos significativos empresariales [15].

Por lo tanto, la seguridad de la información es una de las tareas más importantes, pero también desafiantes que enfrentan las organizaciones en la actualidad. De acuerdo al Comité Nacional de Sistemas de Seguridad (CNSS) señala que la seguridad de la información está encargada de la protección de la información y sus elementos clave, sean estos los sistemas y el hardware que emplean, almacenan y transmiten información. Además, se recalca que la seguridad de la información incluye una amplia

gama de áreas, como la gestión de la seguridad de la información, los datos seguridad y seguridad de la red [16].

Para la Normas ISO/IEC, la seguridad de la información representa todos aquellos conceptos asociados a las buenas prácticas y metodologías que tengan el fin de proteger la información y los sistemas de información del uso, acceso, interrupción, divulgación, modificación o destrucción [1].

La seguridad, de manera general, representa la protección de los activos; bien sea, para evitar la invasión de atacantes, la perdida por desastres naturales o por condiciones ambientales, robos, vandalismo, intento de extorsión, entre otros. Por lo tanto, la seguridad de la información se ha vuelto en la actualidad una necesidad debido a la digitalización de la información, el internet y los cambios evolutivos que han tenido las tecnologías de la información que a su vez generan cambios importantes, aparición de amenazas y muchas veces pérdidas significativas para las organizaciones.

Un punto a considerar, es que el termino seguridad de la información y el termino seguridad informática, no son los mismos, el primero engloba al segundo, pero no se trata de sinónimos. La seguridad informática es referente a la seguridad de los sistemas de información por lo que está asociada a la automatización de la información. Mientras que la seguridad de la información, es más bien la encargada de la información en sí, considerando todas las formas (orales, escritas, electrónicas, entre otras) y cualquier ciclo de vida de esta (creación, adecuación, distribución, uso, mantenimiento, almacenamiento, destrucción, entre otros) con el fin de protegerla de las amenazas que suponen una merma o una depreciación del valor de ella [17].

Tabla 1. Diferencias entre Seguridad de la Información y la Seguridad Informática

Seguridad de la Información	Seguridad Informática
Está orientado a la protección de los activos de la información sin considerar la forma o el estado, basados en metodologías, normas, técnicas, herramientas, estructuras empresariales, entro otros, para aplicar y gestionar las medidas de seguridad necesarias para	Está limitado a la protección de activos de información en un formato digital y también a los sistemas informáticos que son procesados y almacenados, sin considerar si se encuentran o no interconectados

cada caso. Por lo que abarca a la seguridad de la informática.	

Fuente: Figueroa et al., [18].

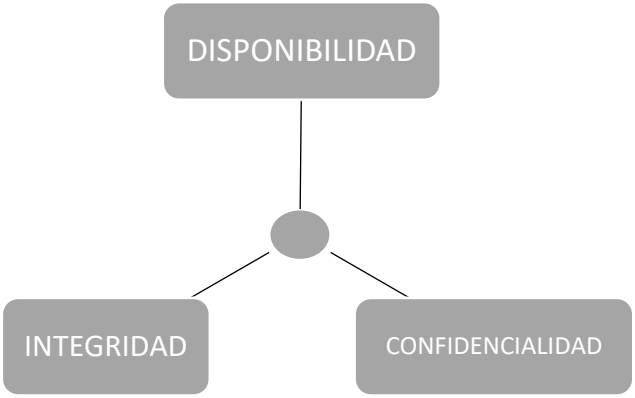
La seguridad de la información no solo representa una cuestión técnica, sino que también es un proceso de responsabilidad de la dirección empresarial, al igual que de sus directivos. Es considerada de la misma forma como una disciplina que se encarga de garantizar la confidencialidad, la integridad y la disponibilidad de la información [18].

Dentro de las empresas, organizaciones o sociedades jurídicas, existe un porcentaje de vulnerabilidad en la información, por lo que siempre se deben de tener en cuentas los motivos para estar prevenidos ante ataques inminentes y en el caso de que ocurran, tener las protecciones adecuadas, considerando puntos estratégicos para dichos procesos, como lo son: el derecho a la privacidad, el derecho a la información, la protección de los activos, la protección de la información (bases de datos, documentos digitales), la protección de los equipos (sistemas de control, redes , entre otros); y, el refuerzo de leyes, políticas y procedimientos [19].

2.2 Pilares de la Seguridad de la Información

Ciertos puntos a considerar en la seguridad de la información son precisamente el conocimiento de los pilares por los que se fundamenta: la confidencialidad, la integridad y la disponibilidad, como se aprecia en la Figura 1; estos en conjunto son comúnmente conocidos como la triada de la seguridad de la información [20].

Figura 1. Pilares en la seguridad de la información



Fuente: Elaboración propia

Esta triada, asegura de manera precisa que se apliquen correctamente las barreras y los procedimientos necesarios para resguardar el acceso, la originalidad y la seguridad de los datos; y, de esta manera, permitir el acceso a las personas autorizadas para esto [21]. A continuación, en la Tabla 2 se definen de forma diferenciada los tres pilares de la seguridad de la información:

Tabla 2. Pilares de la seguridad de la información

Pilares de la Seguridad de la Información		
Integridad	**Disponibilidad**	**Confidencialidad**
Es referente a que la información que se resguarda sea la correcta y esté libre de errores y modificaciones no autorizadas	Es referente a que la información se encuentre accesible cuando requiera ser utilizada	Implica la accesibilidad a la información solamente por parte del personal autorizado. Es el referente al término need-to-know, que considera que la información solo debe estar en manos de personas, entidades o sistemas que se encuentren previamente autorizados.

Fuente*:* Tejada, [21].

La confidencialidad comúnmente es confundida con la privacidad, pero en realidad se refiere a la capacidad de protección sobre los datos y las barreras que se implementan para evitar que las personas no autorizadas los vean o manipulen. Por lo tanto, la confidencialidad tiene la finalidad de permitir que la información solo sea accesible a las

personas autorizadas para esto, considerando las medidas de control y autorización. Es más bien una necesidad de mantener bajo un secreto la forma de acceder a la información o los recursos que llevan a esta [20].

Un ejemplo de vulneración en la confidencialidad es el caso de que una persona observe sin autorización mientras se escribe una contraseña, se pierda el computador portátil y en este se encuentre almacenada información importante, un envío equivocado de archivos adjuntos, un robo de los portátiles con los datos de acceso; o, cuando un atacante ingresa al sistema utilizando aplicaciones Man in the Middel, perpetrando así un tipo de ciber ataque [23].

La integridad de la información hace referencia a que la información que se tiene bajo resguardo sea la correcta y no sufra modificaciones no autorizadas o indeseables. El aspecto más importante de este pilar es que si la información está alterada y se piensa tomar decisiones a partir de estas, se predispone un error garrafal en desarrollo de las actividades empresariales [24].

En el mismo orden de ideas, la integridad supone que las modificaciones en la información solo se ejecutaron por una autorización previa, y en caso de que no sea así, predispone la medida para que no ocurra dicho evento [21].

Por último, la disponibilidad, es la capacidad que se tiene en el sistema de gestión de acceder a la información siempre que se necesite. Una pérdida de la disponibilidad, supone la caída o interferencia en cualquier eslabón de la cadena de comunicación o servidores web que permiten el acceso a los datos. Esta problemática puede ser el resultado de la suspensión o fallas en el servicio eléctrico, problemas en el sistema operativo, ataques a la red u otros problemas que imposibiliten el acceso a la información, generalmente, dichos ataques son el resultado de la negación del servicio (DoS) [25].

La seguridad de la información, tiene un sentido estricto cuando se es consciente del motivo por el cual se deben de preservar las características de la información; por esto, es imprescindible que dentro de dicho proceso se asuman los cuatro pasos o etapas de los procesos administrativos: la planeación, la dirección, la organización y el control [26]. De esta manera, la cadena de suministros informáticos funcionará de manera óptima y organizada, teniendo la organización mayores probabilidades de mantenerse,

posicionarse y sobrevivir dentro de un mercado con competencias, pero también con amenazas latentes a los sistemas de gestión de la información.

2.3 Vulnerabilidad de la Seguridad de la Información

La vulnerabilidad es una debilidad dentro de un sistema informático, misma que puede ser utilizada para causar daños internos. Los sistemas pueden presentar vulnerabilidades en el hardware, en el software e inclusive en el sistema operativo interno [27].

Dentro de los sistemas informáticos lo que se pretende proteger son los activos, mismos que se agrupan en tres partes: 1. El hardware: son todos los elementos físicos que conforman los sistemas informáticos, tales como los procesadores, el cableado red, los medios de almacenamiento [28]. 2. El software: conjunto de elementos lógicos o programas que se ejecutan a partir del hardware, siendo los propios del sistema operativo. Como es el caso de las aplicaciones [28]. 3. Los datos: son un conjunto de informaciones lógicas procesadas por el software por medio del uso del hardware. De manera generalizada, son las informaciones estructuradas en la base de datos o paquetes informáticos que se trasladas por la red [28].

Tabla 3. Agrupación de las vulnerabilidades de los sistemas de información

AGRUPACION DE LAS VULNERACIONES DE LOS SISTEMAS INFORMATICOS	
Vulnerabilidad por diseño	Debilidad en el diseño de protocolos utilizados en las redes Políticas de seguridad deficiente e inexistente
Vulnerabilidad por implementación	Errores de programación Existencia de “puertas traseras” en los sistemas informático Descuido de los fabricantes
Vulnerabilidad por uso	Mala configuración de los sistemas informáticos Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática Disponibilidad de herramientas que facilitan los ataques Limitaciones gubernamentales de tecnologías de seguridad

Vulnerabilidad del día cero	Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución "conocida", pero se sabe cómo explotarla.
Vulnerabilidades conocidas	Vulnerabilidad de condición de carrera

Fuente: Calderón, [28].

Un aspecto importante que debe de ser tratado es en cuales situaciones son de las que realmente se busca proteger los sistemas informáticos, entendiendo en primera instancia que las amenazas son lo desarrollado en un suceso o acción, bien sea deliberado o no, pero que compromete la seguridad de alguno elemento informático.

Cuando dentro de un sistema de información, se detecta una vulnerabilidad, se debe de considerar en primera instancia que está asociada a una amenaza, y que en cualquier momento el suceso o evento se va a producir y que el sistema se encontrará en inminente riesgo. Si dicho evento se perpetua, el sistema informático sufrirá las fallas por este, por lo que debe de ser analizado cualitativa y cuantitativamente para determinar lo denominado como "impacto" [29].

Por lo tanto, y tras la unificación de los conceptos, se puede determinar que un evento producido en un sistema informático es asumido como una amenaza, con asociación a una vulnerabilidad del sistema, que produce un impacto sobre el mismo. El riesgo, siempre debe de ser considerado como una probabilidad de amenaza concreta que aprovecha la vulnerabilidad para el ataque, por lo que es preciso aplicar una fórmula de representación básica [29]:

Figura 2. Forma de medir el riesgo

Fuente: Elaboración propia

Con la figura presentada, queda claro que el riesgo es la suma del impacto producido por el factor amenazante con la probabilidad de que dicha amenaza tenga un éxito en perpetrarse. De la misma forma se denota que, para evaluar la vulnerabilidad de los

sistemas de información, las empresas deben de considerar los factores que la demuestran, estos son:

- Los recursos posibles
- Las amenazas
- Las vulnerabilidades
- Los riesgos

2.4 Norma ISO 27000

Las ISO, son normativas que permiten a las organizaciones poder establecer un orden ya sea en sus actividades y o procesos con el propósito de hacer a la organización certificable. Las ISO en su gran mayoría son aplicadas por organizaciones que por su entorno son emprendedoras, innovadoras y buscan siempre mantener los estándares de calidad, competitividad y productividad elevados [9] [30].

La norma ISO 27000, fue publicada en mayo del año 2009, revisada posteriormente en diciembre de 2014 para la publicación de su segunda edición, la tercera en enero de 2014; y, la última es febrero de 2016. Esta norma, es la visión global de lo que respectan todas las normas que conforman esta serie 27000, misma que dentro de sus líneas especifica el alcance y el propósito de cada uno de ellas. Dentro de esta serie, se determina un cumulo de definiciones enfocadas en la importancia de la implementación de un SGSI, al igual que la introducción a los Sistemas de Gestión de Seguridad de la Información, una corta descripción de los pasos en el establecimiento, monitorización, mantenimiento y mejora de SGSI [31].

Se ha realizado una revisión de diversas investigaciones referentes a la aplicación de la Normas ISO/IEC 27001 en diversas organizaciones empresariales, como es el caso de la realizada por el autor Alvarado [32], buscando garantizar la disponibilidad, confidencialidad e integridad de la información de una empresa en la ciudad de Guayaquil, encuentra y reúne información necesario para implementar un SGSI, basado en la norma internacional de estandarización ISO 27001. En primer lugar, se efectuó un análisis completo de la gestión de los riesgos, permitiendo de esta manera estimar el impacto de los riesgos que se presenten en amenazas y vulnerabilidades detectadas en

todo el sistema, consiguiendo con ella, conocer los activos más críticos de la información. Luego de tener dicha información, identificaron y analizaron el nivel de cumplimiento de los requisitos básicos de la norma. Durante este proceso, lograron identificar de manera correcta la identificación de los activos, siendo el principal de estos la información almacenada en la base de datos de la compañía, misma que resguarda información de los clientes, cuantas bancarias y gestión diaria de la telefonía.

Señalando otra investigación al respecto, se menciona la realizada por Alomoto [33], que al igual que el anterior busca diseñar e implementar un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2023 dentro de una Unidad Educativa de la ciudad de Quito, realizando en primera instancia un inventario general, al igual que valorar el nivel de cumplimiento de los requisitos establecidos por las normas, basados en todo lo obtenido por medio de estos generaron propuestas basadas en un plan de acción y correctivos mostrado a lo largo de la investigación. Por medio del análisis, observaron un incumplimiento de la norma en un 79,89% de los procesos que se realizan dentro de la organización educativa según la norma ISO, por lo que implementar un SGSI era de primera necesidad debido a que la institución era altamente vulnerable en termino de Seguridad de la Información a todas las amenazas y riesgos asociados.

Por otro lado, al igual que en los casos anteriores, visibilizando la importancia de la Norma ISO IEC 27001:2013, para la seguridad de la información dentro de las empresas u organizaciones, el autor Crespo [34], señala primeramente que la evolución de las tecnologías y los medios de comunicación es exponencial y vertiginosa, llegando a incrementar de esta forma la inseguridad de un activo que resulta de vital importancia para el desempeño de las organizaciones siendo el caso de la información, esto se puede deber bien sea a la negligencia en el uso o de manera intencional, sea cual fuere el motivo es imperante que se direccionen esfuerzos en la gestión de la seguridad de la información, para así evitar pérdidas o alteraciones que involucren de datos de la empresa.

2.5 Norma ISO/IEC 27001

En la presente investigación se considera el uso de la Norma ISO/IEC 27001, como una guía y referencia para los requisitos en la implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Informática, de la empresa Transcarga S.A, buscando con ella, proteger la confidencialidad, la integridad y la disponibilidad de la información.

Según lo establecido en la Norma ISO/IEC 27001, el eje central para la implantación de un SGSI es la evaluación de los riesgos. Con esta, la empresa puede tener una visión ampliada y específica a lo que respectan los alcances y los ámbitos de la aplicación de la norma, al igual que todas las políticas y medidas que integran el sistema metodológico común para todas las normas ISO [11].

La implementación de la norma ISO/IEC27001, representa beneficiosa en el ámbito de los riesgos de la seguridad de la información dentro de las organizaciones, mismos que son asumidos como amenazas considerables por las posibles pérdidas económicas o daños generales, pérdidas en los servicios esenciales de la red, la reputación y la confianza de los clientes. Dentro de la norma, la gestión de los riesgos es un elemento fundamental en la prevención de los fraudes online, el robo de la identidad, los datos al web, la perdida de información y datos. por lo que cuando las empresas no cuentan con un marco de gestión, están susceptiblemente expuestas a las amenazas informáticas [33].

La implementación de la norma ISO, es una tarea de suma importancia dentro de las organizaciones, y cuando se es implementada de manera efectiva, los beneficios son altamente significativos, sobre todo en aquellas organizaciones que tienen a su poder información valiosa o sensible. Existen tres áreas en las que se dividen los beneficios obtenidos por la ISO/IEC 27001: Beneficios comerciales, operacionales y tranquilidad [11]

2.6 Área de Logística Empresarial

Logística empresarial, según Servera [34] es un término generalizado para denominar a toda la logística necesaria para el funcionamiento de una empresa. Esta abarca los

aspectos internos y corporativos de la logística, señalando entre estos las compras, el envío y distribución de la mercancía, y la logística de la producción.

La logística representa una piza clave en el sistema de producción y suministro de las organizaciones. Con ella, las empresas logran poner a despensa de los clientes los productos o servicios que ofrecen y que estos a su vez, lleguen a los lugares y en el tiempo adecuado. Por lo tanto, supone una serie de pasos para su correcto funcionamiento: la ejecución, la planificación, y el control de las actividades. Según lo que define Nuño [35], entre las funciones y actividades de la logística empresarial, se pueden destacar cinco principales:

- El servicio al cliente: ya que el departamento por medio de la gestión de los productos y servicios es organizado según las necesidades de los clientes. Aunado a que los tiempos en la respuesta van asociados con la calidad percibida por ellos [35].
- Diseño y planificación de rutas de transporte: según las necesidades estas deben de ser planificadas de manera óptima y adecuada, al igual que los medios y las formas precisas en las que debe de ser distribuida la mercancía o el servicio [35].
- Gestión de inventarios: es tener el control de las materias primas al igual que de los productos ya terminados. Para este apartado, son muchos los elementos que se deben de considerar en el óptimo manejo de la mercancía: el tipo, tamaño, espacio y lugar correcto de almacenamiento de los productos, entre otros tipos de consideraciones. Además, es importante tener un control exhaustivo del stock [35].
- Procesamiento de pedidos: cuando las empresas tienen una buena gestión del stock, este es fácilmente procesado, satisfaciendo de esta manera la demanda [35].
- Gestión de datos: refiere al conocimiento profundo de los productos y servicios ofrecidos, almacenados y distribuidos. Pero también de toda la información que respecta dicho proceso [35].

3 Materiales y metodología

3.1 Tipo de investigación

Como metodología se realiza una investigación de tipo descriptivo, con enfoque mixto porque se realizan análisis de datos en forma cualitativa y cuantitativa; señaló Campos [36] que, en el método mixto de investigación, el investigador combina los elementos que caracterizan el estudio cuantitativo y el estudio cualitativo, recopilando, analizando e integrando la investigación, con las bondades de ambos métodos.

3.2 Diseño de la investigación

La investigación es descriptiva con un diseño no experimental. Señalaron Hernández et al. [37] que, por medio del diseño no experimental, el problema solo se observa sin pretender intervenir en el desarrollo, es decir, no se manipulan las variables de estudio. Por tanto, esta investigación busca poner en contexto la importancia de estandarizar los mecanismos de control de seguridad que se requieren en la empresa objeto de estudio.

3.3 Técnicas de investigación

Para llevar a cabo la investigación, se utilizaron las siguientes técnicas de recolección de información:

3.3.1 Revisión y análisis documental

Capote [38] mencionó que el análisis documental tiene por finalidad fundamentar el proceso investigativo que se desarrolla, utilizando la literatura, documentos, investigaciones, leyes, reglamentos y otros similares. Siguiendo lo que señaló el autor, para llevar a cabo la investigación se hizo inicialmente una revisión a la literatura para conocer los fundamentos teóricos que permiten comprender la importancia de disponer de mecanismos de seguridad que ayuden al resguardo de la información en todas las áreas de la empresa. De igual forma, se indagó lo que señala la Norma ISO/IEC 27001 en ocasión al resguardo de la información y los controles de seguridad. Todo esto permitió conocer de qué manera la empresa está cumpliendo con la seguridad de la información y el acceso a la misma, tomando en cuenta lo que señala la norma y demás documentos indagados.

3.3.2 Técnica de encuesta

Seguidamente, se utilizó la técnica de la encuesta con la finalidad de validar el problema de estudio y recabar la información necesaria que permite conocer la situación actual de la empresa, con relación a los mecanismos de control y seguridad de la información. El autor Hurtado, explicó que la técnica de encuesta corresponde a un ejercicio de búsqueda de información acerca del evento de estudio, mediante preguntas directas, a varias unidades, o fuentes [39]. Partiendo de lo que explicó Hurtado, esta técnica requiere de la utilización de un cuestionario que se conforma de distintos planteamientos o interrogantes estrechamente vinculadas al tema principal de investigación.

Niño [40] explicó que un cuestionario es un conjunto de preguntas técnicamente estructuradas y ordenadas que se presentan de manera escrita y comúnmente impresas, las cuales deben ser respondidas por las personas encuestadas. Se trata de una herramienta que permite obtener información para el desarrollo de una investigación siendo una de las más utilizadas y que requiere una estructura y riguroso orden en la elaboración de la información.

En el presente estudio se realizó una encuesta dirigida al personal que labora en el departamento de sistemas y logística de la empresa objeto de estudio. Para el cuestionario utilizado se tomó como referencia el Test propuesto por la ISO 27001 el cual está estructurado por 7 apartados con interrogantes en cada uno de estos, que permiten conocer aspectos relacionados con la protección de los datos y el resguardo de la información considerando lo siguiente: La organización y su contexto, el liderazgo, la planificación, el soporte, la operación, la Evaluación del desempeño, la mejora. Estos elementos se detallan en el apartado 7.5. El cuestionario se muestra en el Anexo 1.

3.3.3 Técnica de entrevista

Según Lebet [41] la entrevista se corresponde con una conversación dirigida, con un propósito específico y que usa un formato de preguntas y respuestas. Por tanto, por medio de la entrevista se llevó a cabo una conversación donde una de las partes buscó recoger información y la otra se mostró como fuente de esa información. Dada la importancia de la entrevista, en el presente estudio se optó por esta técnica realizando

una entrevista al jefe del departamento de sistema. Para la estructura del cuestionario utilizado en la entrevista, se tomó como referencia preguntas propuestas por la página https://iso27001.mx/cuestionario-iso-27001/ las cuales permiten determinar la necesidad de proteger la información empresarial. Del cuestionario referido, se tomaron las siguientes interrogantes para la entrevista:

1. ¿La Organización cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI)?
2. ¿Se cuenta con un comité interno para Establecer las políticas de Seguridad?
3. ¿Existen políticas de Seguridad documentadas y Gestionadas?
4. ¿Se cuenta con Gestión de dispositivos móviles y el teletrabajo?
5. ¿Se cuenta con Tecnología para evitar y responder a amenazas Cibernéticas?

3.4 Población y muestra

Para llevar a cabo la recolección de la información a través de la encuesta, se determinó la población de estudio la cual estuvo representada por la cantidad de 30 empleados que ejercen funciones en distintas áreas y departamentos de la empresa.

Hurtado [39] define la población como “un conjunto de elementos o seres concordantes entre sí en cuanto a una serie de características, de los cuales se desea obtener alguna información, puede decirse que la población es el conjunto de unidades de estudio de una investigación” (p. 268). De igual manera, la muestra representa una parte de la población, no obstante, en la presente investigación no se realizó cálculo muestral en virtud de que la población es pequeña y puede ser manejada en su totalidad.

3.5 Procesamiento de la información

Para el procesamiento de la información, se realizó la encuesta al personal de los departamentos de sistemas y logística. Los resultados obtenidos fueron tabulados en el software estadístico SPSS para conocer las tablas de frecuencia y la totalidad de las respuestas obtenidas. El cuestionario está estructurado en siete apartados con 53 interrogantes, que ofrecen datos diversos sobre la seguridad de la información en la

empresa. Los datos obtenidos en la encuesta realizada se han agrupado en respuestas de acuerdo a los siete apartados del Cuestionario ISO 27001, atendiendo a:

La organización y su contexto: Por medio de este competente se busca conocer si la empresa dispone de la integración entre los procesos, es decir, si la empresa cuenta con objetivos relacionados al sistema de gestión de seguridad de la información, si se han identificado cuestiones internas o externas de seguridad, otros similares.

El liderazgo: Se busca revelar el compromiso que tiene cada uno de los miembros de la organización, hacia el cumplimiento de metas y objetivos del Sistema. Además del liderazgo en la dirección de las actividades a desarrollar.

La planificación: Conocer de que forma la empresa maneja el proceso de reflexión estratégica y de gestión de riesgos, es decir, las acciones para abordar los riesgos y oportunidades.

El soporte: Ayuda a revelar los recursos de los que dispone la empresa o que son necesarios para implementar el sistema.

La operación: Permite conocer sobre la planificación y el control operacional, lo cual requiere a su vez la interacción con los clientes, controlar los procesos, así como la implementación y ejecución del sistema.

La Evaluación del desempeño: Se busca conocer las principales herramientas de evaluación gestión por procesos, se conocen si cumplieron o no los objetivos propuestos con el sistema.

La mejora: Conocer si los resultados conllevan al fortalecimiento de los procesos, mejora, cambio o eliminación, previo seguimiento a las no conformidades detectadas.

4 Resultados y discusión

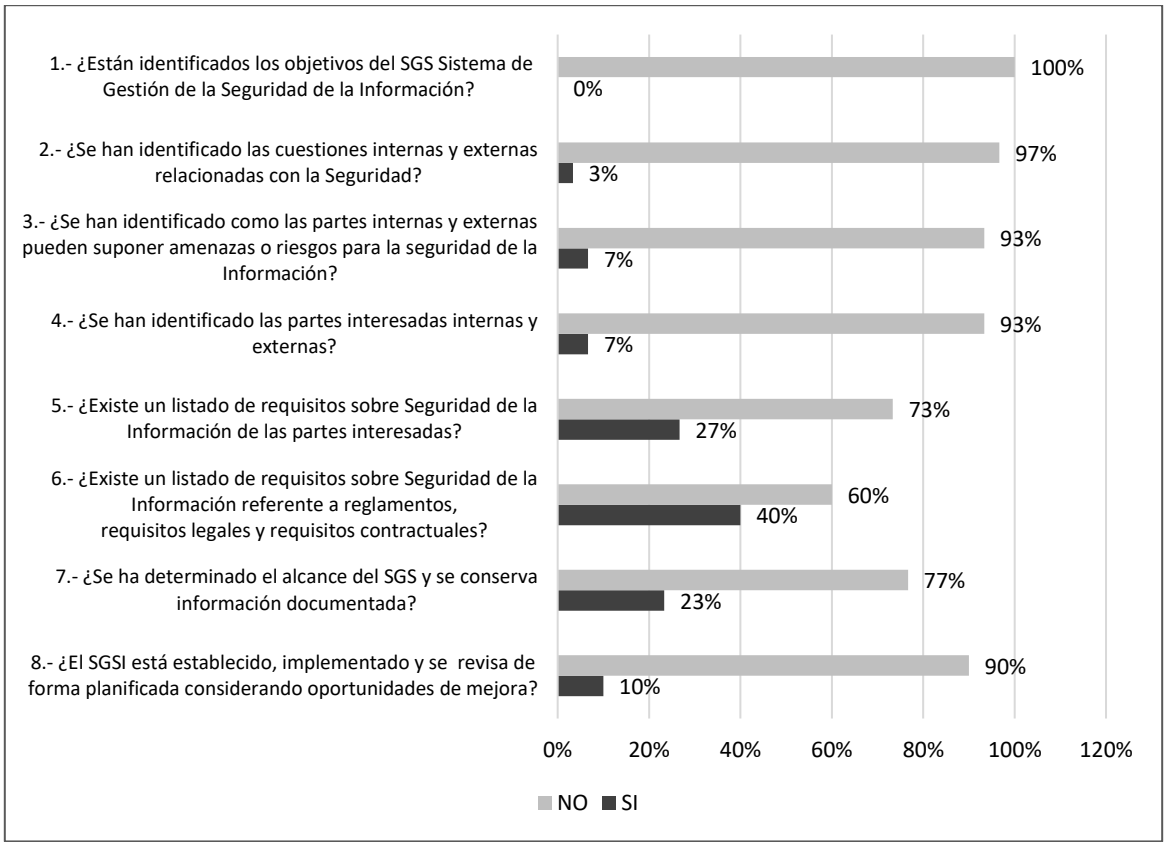
4.1 Resultados de encuesta

Se presentan resultados de encuesta en función de los apartados del Cuestionario.

4.1.1 Resultados encuesta: Apartado Organización y su contexto

La organización y su contexto permite conocer las expectativas de las partes interesadas y el alcance del Sistema de Gestión de la Seguridad de la Información. En la Figura 3 de aprecian los resultados en este apartado.

Figura 3. Resultados: La Organización y su Contexto



Nota. Se detallan los resultados de la organización y su contexto.
Obtenido de encuesta realizada a personal de la empresa Transcarga S.A.

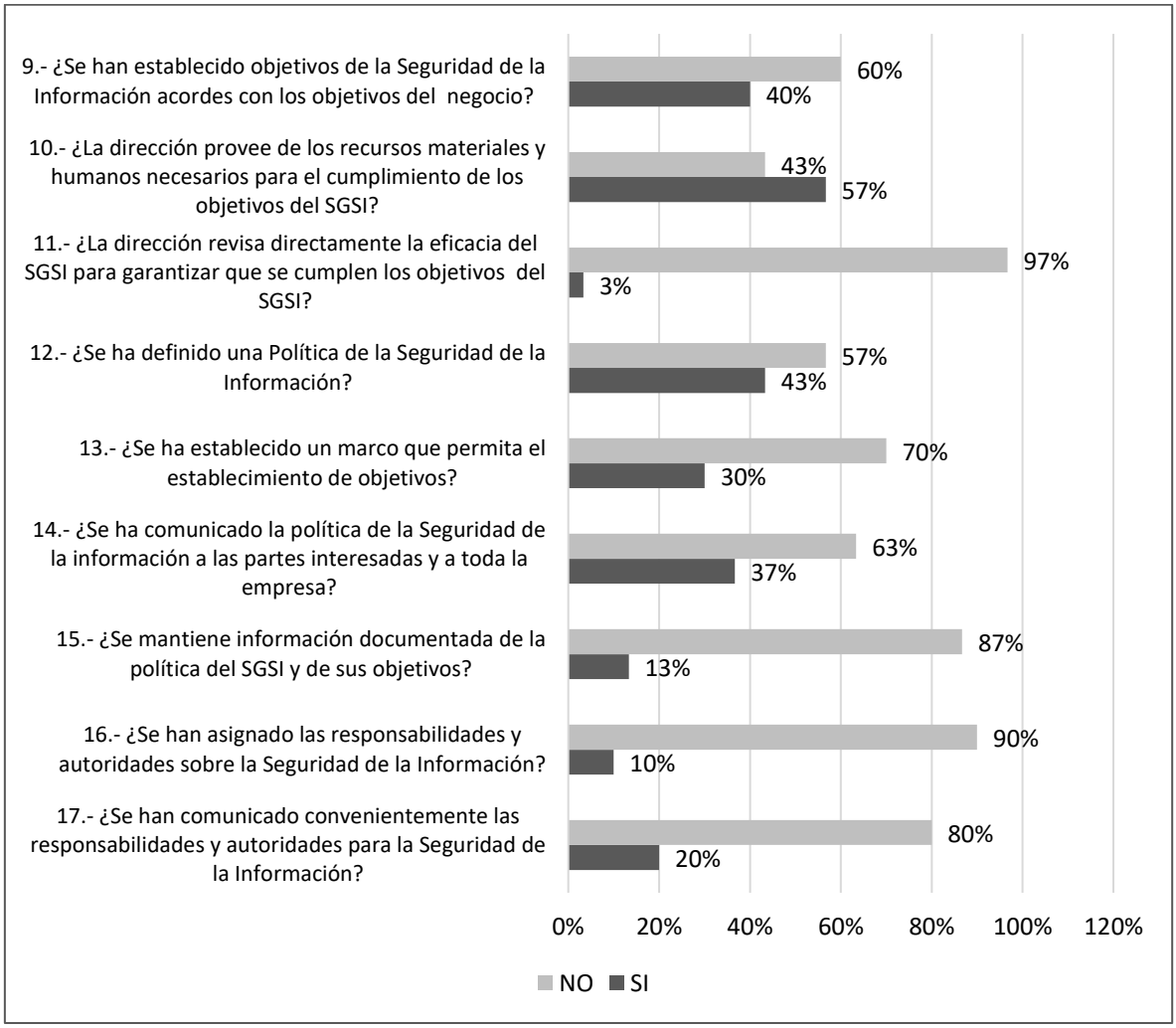
Se aprecia en la Figura 3 que la empresa no cuenta con objetivos relacionados al sistema de gestión de seguridad de la información, tampoco se han identificado cuestiones internas o externas de seguridad. Más del 90% de las respuestas coinciden en que la empresa no tiene un listado de requisitos sobre la seguridad, tampoco se conserva la

información documentada y un 100% de las respuestas dieron a conocer que no existe un SG establecido que garantice la seguridad de la información que se maneja en las distintas áreas y departamentos de la empresa.

4.1.2 Resultados encuesta: Apartado Liderazgo

A través del liderazgo se puede tener conocimiento sobre el compromiso, las políticas de seguridad en la información, los roles y las responsabilidades. En la Figura 4 de aprecian los resultados en este apartado.

Figura 4. Resultados: Liderazgo



Nota. Se detallan los resultados dl liderazgo.
Obtenido de encuesta realizada a personal de la empresa Transcarga S.A

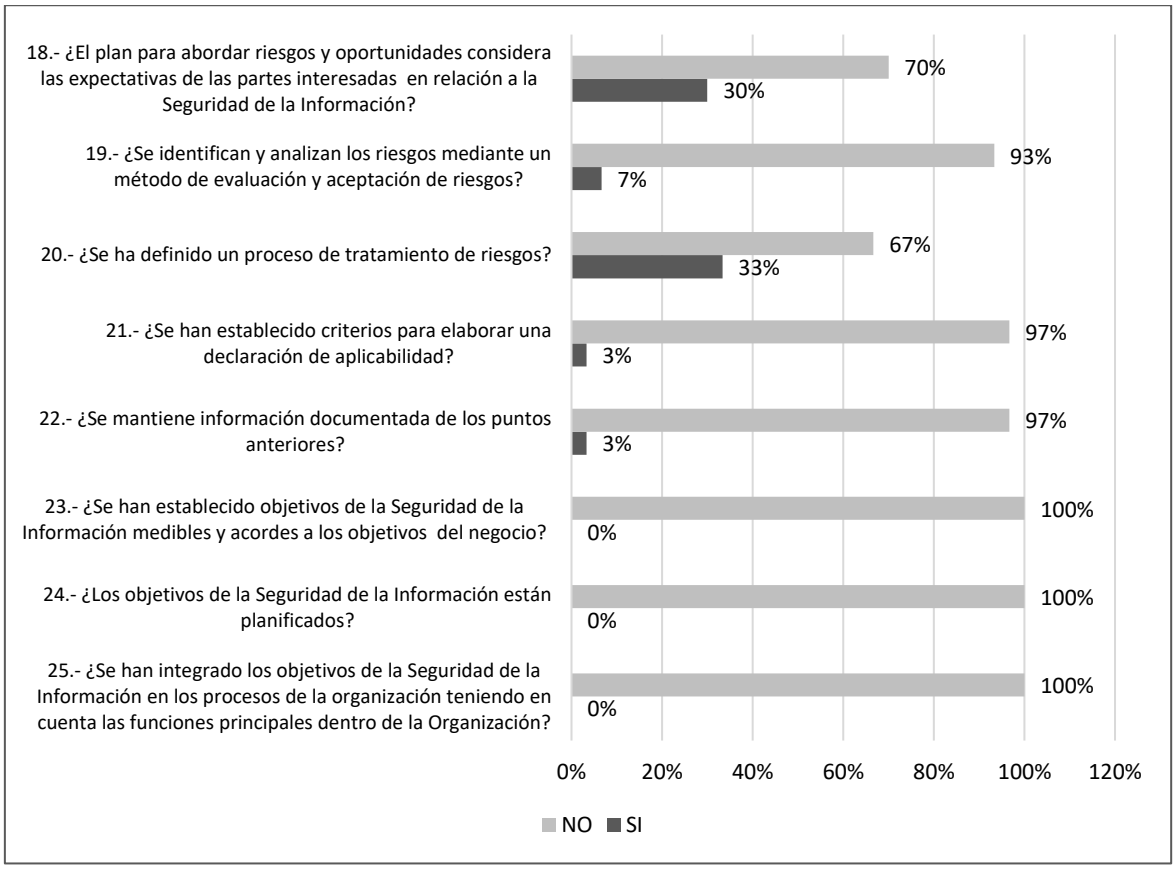
Con relación al apartado de liderazgo, el 80% de los encuestados opinó que no se han establecido objetivos de seguridad de la información; el 87% coincide en que no existe una revisión de la dirección en asuntos del resguardo de la información; un 57% opinó

que si se han asignados responsabilidades sobre el resguardo de la información, lo cual se describe en las funciones de cada puesto de trabajo, pero no trasciende a mantener políticas de seguridad ni el establecimiento de objetivos relacionados.

4.1.3 Resultados encuesta: Apartado Planificación

Por medio de la planificación se conoce sobre el tratamiento del riesgo y las oportunidades en el manejo de la información, así como la planificación en la consecución de los objetivos. En la Figura 5 de aprecian los resultados en este apartado.

Figura 5. Resultados: Planificación



Nota. Se detallan los resultados de la planificación.
Obtenido de encuesta realizada a personal de la empresa Transcarga S.A

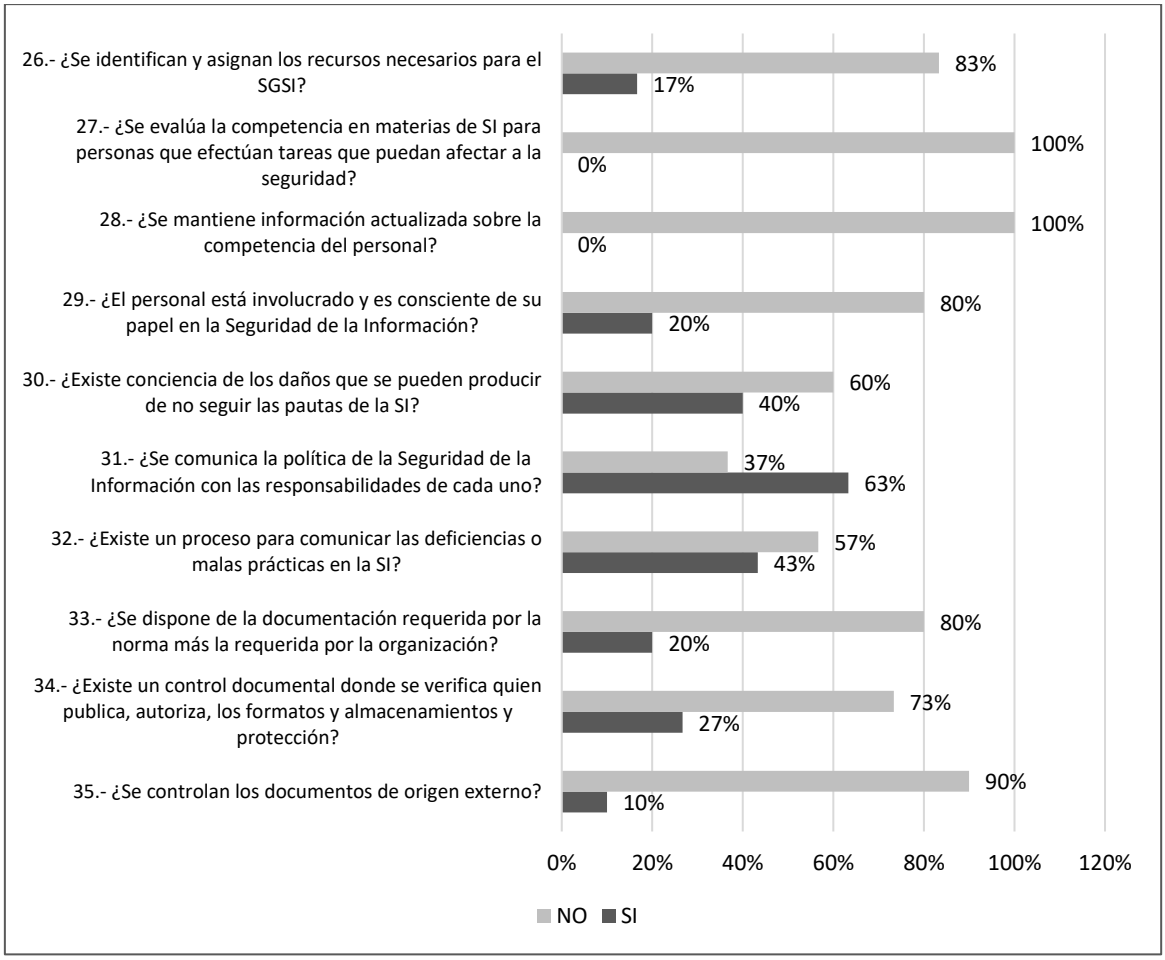
Respecto a la planificación, las respuestas de los encuestados coincidieron en un 100% al indicar que no existe un plan para determinar riesgos y oportunidades en el manejo y resguardo de la información; no existe un proceso de tratamiento ante posibles riesgos, no se mantiene información documentada de riesgos u oportunidades. Un 67% señaló que se han establecidos objetivos de seguridad de la información manejada pero solo a

un grupo reducido del personal, especialmente los que laboran en el área de sistemas e informática, pero no cuentan con objetivos de seguridad planificados.

4.1.4 Resultados encuesta: Apartado Soporte

Por medio del soporte, se conoce sobre los recursos, la competencia, la concienciación y la comunicación sobre las políticas de seguridad de la información y la información documentada. En la Figura 6 de aprecian los resultados en este apartado.

Figura 6. Resultados: Soporte



Nota. Se detallan los resultados del soporte.
Obtenido de encuesta realizada a personal de la empresa Transcarga S.A

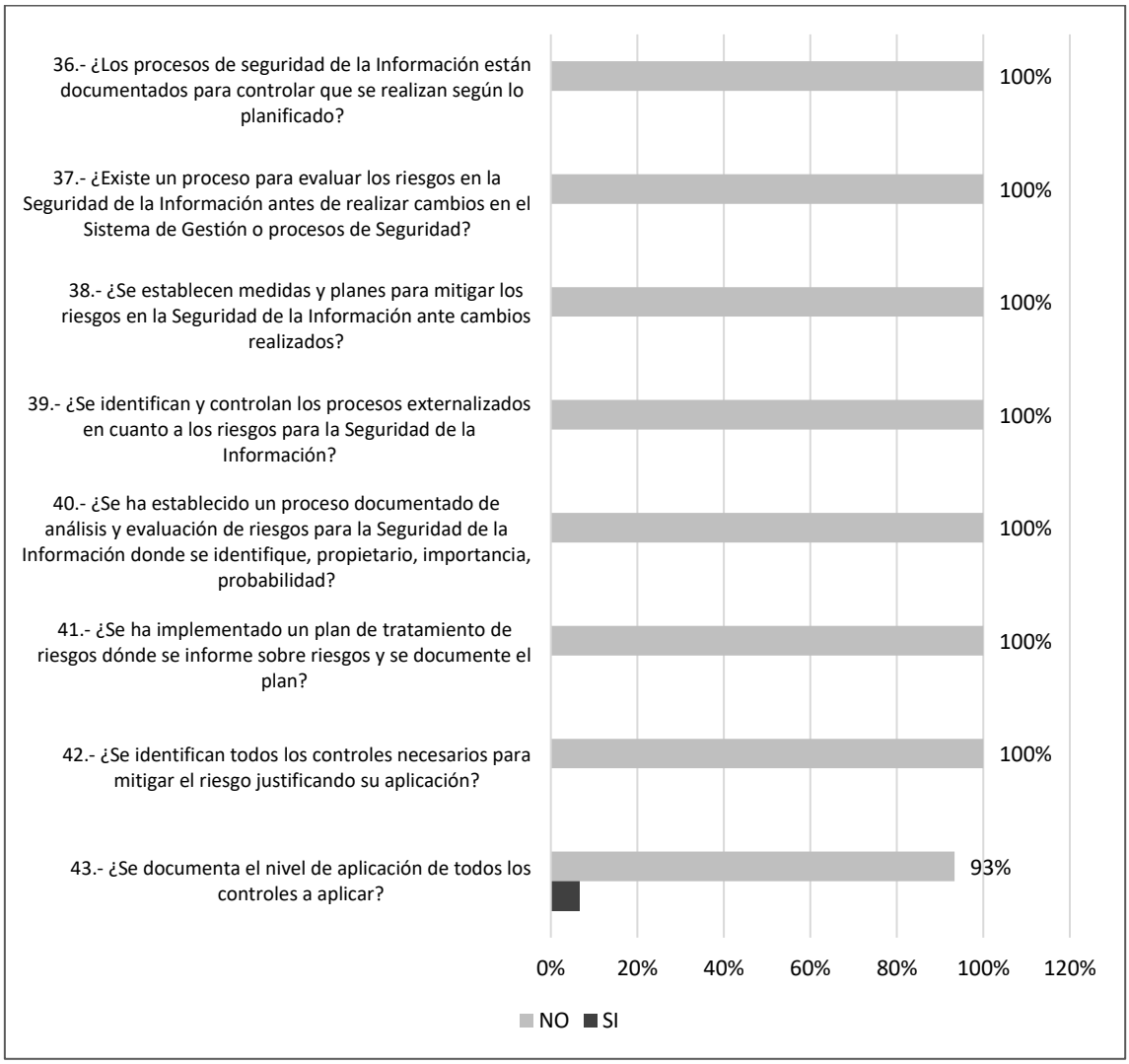
De acuerdo con las respuestas relacionadas con el soporte de la seguridad y la información, un 90% opinó que no se identifican ni asignan recursos para establecer un SGSI; el 73% indicó que se toman en cuenta las competencias en seguridad de la información, que tengan las personas que manejan datos de la empresa. Un 63% de los encuestados manifestó que si tienen conciencia de los daños que puedan generarse

ante un mal manejo de la información. Del mismo modo, el 100% señaló que no existe un control documental ni se dispone de la información requerida por la norma y la organización.

4.1.5 Resultados encuesta: Apartado Operación

A través de la operación se tiene conocimiento del control operacional y los análisis de riesgo sobre la seguridad de la información y su tratamiento. En la Figura 7 de aprecian los resultados en este apartado.

Figura 7. Resultados: Operación



Nota. Se detallan los resultados de operación.
Obtenido de encuesta realizada a personal de la empresa Transcarga S.A

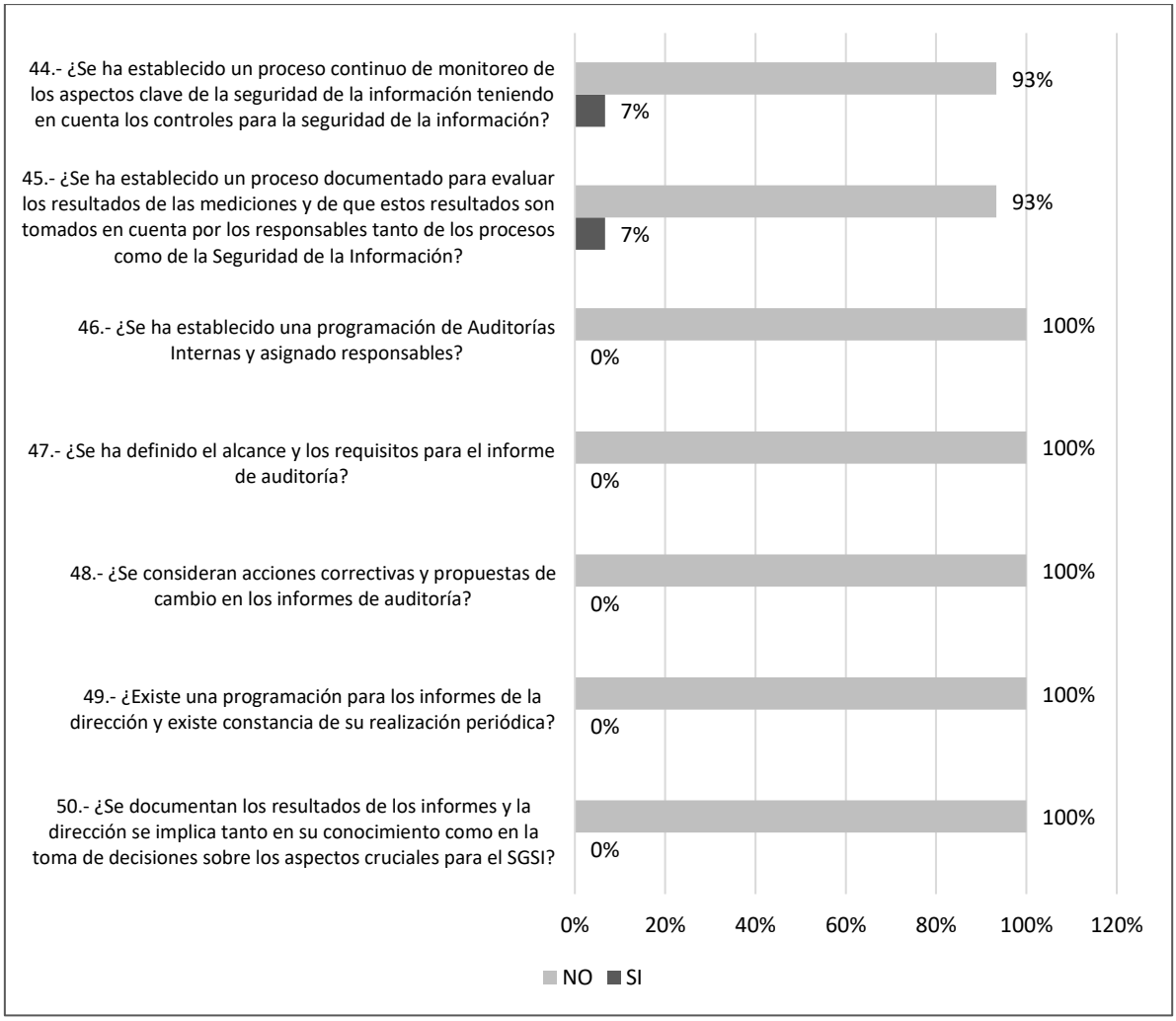
El 100% de los encuestados indicó que la empresa no cuenta con procesos para evaluar riesgos, tampoco hay planes para mitigarlos. De igual forma se pudo conocer que no se

identifican y controlan procesos externalizados ni procesos documentados. El apartado de operación presenta alta deficiencia en la empresa, pues no se cuenta con políticas que ayuden a minimizar la exposición a la pérdida de información y datos manejados en la empresa.

4.1.6 Resultados encuesta: Apartado Evaluación de desempeño

Este apartado permite conocer si se llevan seguimiento y revisión, auditorías internas, si se presentan informes a la gerencia, relacionados con la seguridad de la información. En la Figura 8 de aprecian los resultados en este apartado.

Figura 8. Resultados: Evaluación del desempeño



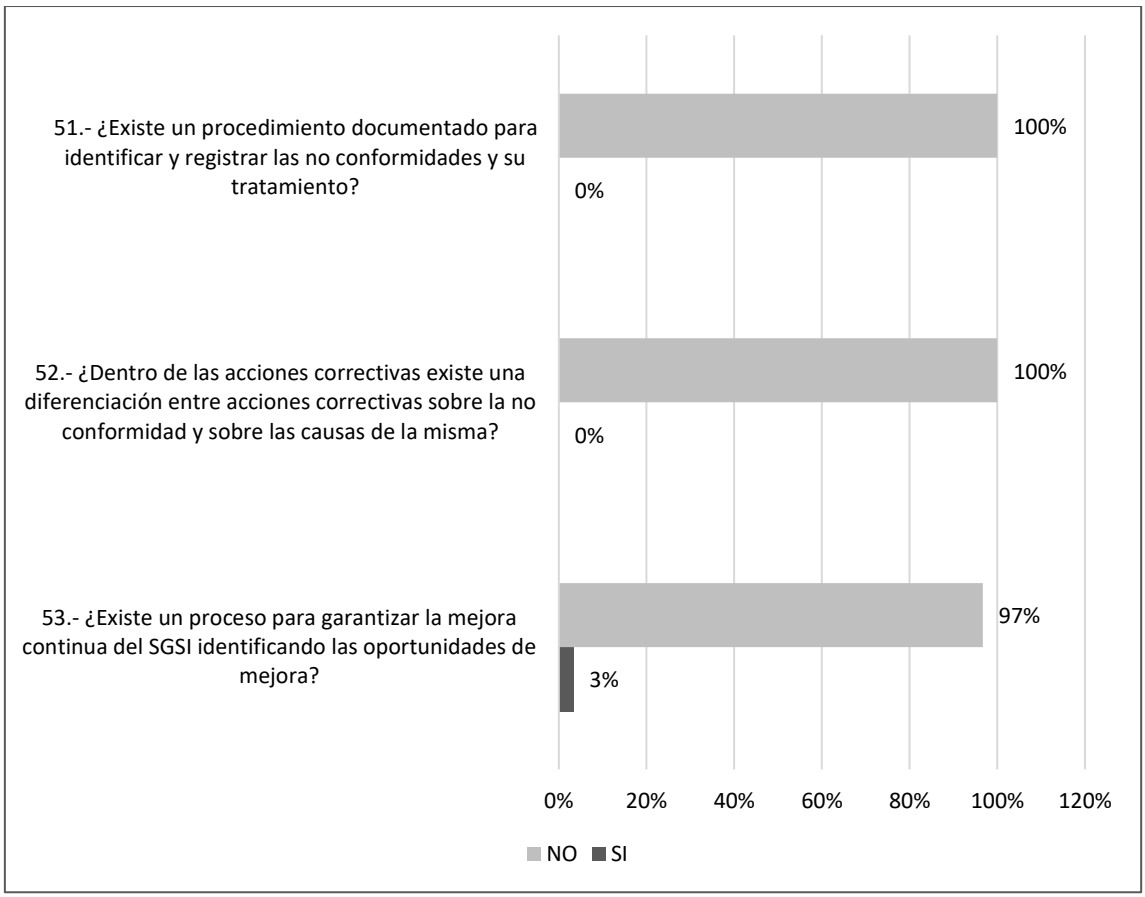
Nota. Se detallan los resultados de evaluación del desempeño.
Obtenido de encuesta realizada a personal de la empresa Transcarga S.A

Con relación a la evaluación del desempeño, un 100% de las respuestas coinciden en que la empresa no tiene establecido un proceso continuo de monitoreo en temas de seguridad de la información, tampoco se evalúan resultados, ni se llevan a cabo auditorías internas. Todo esto conlleva a la falta de acciones correctivas y no se cuenta con una programación para el control de la seguridad.

4.1.7 Resultados encuesta: Apartado Mejora

Con relación al apartado de mejora, este ayuda a conocer si se llevan controles de las no conformidades y las acciones correctivas, así como la mejora continua. En la Figura 9 de aprecian los resultados en este apartado.

Figura 9. Resultados: Mejora



Nota. Se detallan los resultados de mejora.
Obtenido de encuesta realizada a personal de la empresa Transcarga S.A

Respecto a la mejora, el 97% de los empleados encuestados señalaron que no existe un procedimiento documentado que permita identificar y hacer un registro de las no

conformidades; el 100% opina que no existen acciones correctivas que ayuden a identificar las causas de los riesgos en la vulnerabilidad de la información ni las causas que la provocan. De igual forma, se conoció que no existe un proceso que garantice la mejora continua, porque no se ha establecido un SGSI.

4.1.8 Resultados entrevista realizada al jefe de departamento de Sistema

Se realizó encuesta al jefe del departamento de sistemas obteniéndose las siguientes respuestas:

1. ¿La Organización cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI)?

No, actualmente la empresa no cuenta con un sistema de gestión de la seguridad de la información. Se han realizado algunas conversaciones a nivel de la gerencia para establecer controles más estrictos en el resguardo de datos, pero no se ha avanzado al respecto.

2. ¿Se cuenta con un comité interno para Establecer las políticas de Seguridad?

No, lastimosamente en la empresa no se ha gestionado coordinar un comité o equipo de trabajo que se encargue de elaborar políticas de seguridad en los datos, documentos y la información que se maneja en todas las unidades o áreas de la organización. Si es muy importante tomar las medidas necesarias.

3. ¿Existen políticas de Seguridad documentadas y Gestionadas?

Se han realizado algunos controles a los archivos que se manejan en la empresa, en cada departamento y entre departamentos, pero no se dispone de políticas exclusivas que puntualicen la seguridad de la documentación.

4. ¿Se cuenta con Gestión de dispositivos móviles y el teletrabajo?

Si, se han llevado a cabo algunos controles con el uso de dispositivos en todas las áreas y departamentos, con la finalidad de evitar que esto influya en el trabajo que cada una realiza, a su vez se ha prohibido el pase de laptops personales a las oficinas.

5. ¿Se cuenta con Tecnología para evitar y responder a amenazas Cibernéticas?

Se han instalado algunos programas que disminuyen el riesgo para contraer virus en la información que se encuentra en los ordenadores de las distintas oficinas. Las amenazas

de contraer virus se buscan contrarrestar con programas que ayudan a identificar este tipo de malware.

4.2 Razones que afectan la seguridad de la información en el área de logística de la empresa Transcarga S.A.

Para el logro del objetivo específico 2, se tomó como base fundamental los resultados obtenidos en las técnicas de recolección de información utilizadas en el presente estudio, como la encuesta y la entrevista. Se pudo conocer que la empresa no cuenta con mecanismos de control que garanticen una seguridad de la información que se maneja en las distintas áreas y departamentos. Un mínimo porcentaje de los encuestados opinó que se llevan algunos controles donde se responsabilizan a algunos trabajadores para que realicen resguardo de datos de manera empírica, es decir, sin la utilización de un sistema que contribuya a fortalecer la garantía de los datos.

Como resultado general de la información obtenida, la empresa no cuenta con mecanismos de control, no tiene establecido políticas de resguardo de la información ni se dan acciones que ayuden a la minimización de riesgos a que los datos sean vulnerados o perdidos. La organización requiere canalizar los esfuerzos para que las directrices de seguridad y resguardo de la información alcancen el éxito. Para esto es necesario que la gerencia o directivos de la empresa reconozcan la importancia de la implementación de mecanismos de control que ayuden a establecer buenas políticas de seguridad informática.

Tomando en cuenta las necesidades que presenta la empresa ante la falta de controles en la seguridad de la información, se considera importante que la empresa estandarice mecanismos que le ayuden a minimizar los riesgos de pérdida de datos e información propia de la actividad de la empresa. Estandarizar un proceso se corresponde con la unificación de procedimientos, estos deben estar vinculados a las actividades de la empresa. El proceso está relacionado con el procedimiento, el cual se corresponde con una serie de pasos o tareas que deben cumplirse o llevarse a cabo para lograr la solución de un problema o el logro de un objetivo o meta.

En este contexto, dentro de las principales razones por las cuales la empresa necesita estandarizar los mecanismos de control en el resguardo de la información, se mencionan los siguientes:

Tabla 4. Razones por las cuales la gestión actual necesita emplear mecanismos de control en la seguridad de la información

Razones	Descripción
Falta de un sistema de gestión de resguardo de la información	La empresa no cuenta con un sistema de gestión de la seguridad que garantice el resguardo de la información. En algunas ocasiones se ha canalizado esfuerzos para lograr un control en el manejo de datos y de información, pero esto no se ha logrado con éxito, es decir, solo se ha fomentado guardar los archivos, clasificados por carpetas en los ordenadores, dependiendo del área o departamento, pero no pasa más allá en términos de garantía de seguridad de la información
Falta de objetivos de políticas de seguridad de la información	La empresa no cuenta con políticas exclusivamente destinadas a controlar y resguardar la información y los datos que se manejan en los distintos departamentos y áreas. Todo esto debe partir de una evaluación de los riesgos a los que se expone la empresa, siendo necesario emplear acciones y estrategias que ayuden a detectar los posibles eventos donde la información se muestra vulnerable a la pérdida o mal uso de los datos.
Falta de designación de las responsabilidades	La empresa no ha designado responsables que se encarguen de evaluar todo el sistema de seguridad de la información y lo que esto involucra. Las áreas o departamentos no cuentan con un delegado o responsable que tome decisiones relacionadas con el resguardo de la información, sin que cada miembro

	de la empresa deje de comprender el nivel de responsabilidad que tiene para que se garantice el cumplimiento de las políticas y la seguridad informática.
Poco valor agregado a los procesos	Una de las principales razones por las cuales se debe estandarizar los mecanismos de control es el valor que suma a la calidad de la información manejada. La empresa no está garantizando el resguardo de los datos que maneja, lo cual mengua la calidad en el producto final de los procesos administrativos, por ende, la gerencia afecta su gestión.
Falta al cumplimiento en la seguridad de los datos	Se requiere que la dirección de la empresa conozca el alto nivel de responsabilidad en el manejo de información y datos que pueden estar vulnerables ante hechos delictivos de robo o mal uso de los datos.
Pocos equipos tecnológicos y ordenadores actualizados	La empresa en la actualidad dispone de equipos de computación ya un poco obsoletos, lo cual debe ser revisados por la gerencia para evaluar la necesidad de adquirir software más actualizados que garanticen un mejor manejo y resguardo de la información.
Falta de planes de capacitación	La empresa no realiza planes de capacitación que garantice a los empleados conocimiento y habilidades en el manejo de la información, la importancia de su resguardo y las responsabilidades que puede tener cada puesto de trabajo en el buen uso de la información y resguardo de esta.
Falta de integración en las estrategias del negocio	La empresa no ha involucrado a todo el personal en asuntos concernientes con el buen manejo y resguardo de la información. Todo esto puede conllevar a que los trabajadores, sin saberlo, estén comprometiendo información sensitiva de la

	empresa lo que finalmente afectará la imagen corporativa. No todos los miembros de la empresa sienten el compromiso y la responsabilidad de manejar adecuadamente la información y los datos.
Desligamiento entre la misión, visión y las decisiones de seguridad de la información	La empresa no proyecta a través de la planificación estratégica, la importancia de la seguridad de la información, lo cual requiere ser atendido para minimizar los riesgos de vulnerabilidad de la seguridad de los datos.
Desconocimiento en el manejo de sistemas de gestión de seguridad de la información	La empresa no ha llevado a cabo procesos de capacitación para que el personal de las distintas áreas y departamentos conozcan todo lo concerniente a la importancia del resguardo y seguridad de la información que se maneja en todas las áreas de la empresa. La falta de conocimiento genera falta de compromiso y responsabilidad, pues no se ha fomentado la divulgación de los beneficios y los riesgos que se derivan de controlar o no la información y los datos de la empresa. Puntualmente, la empresa no ha capacitado al personal en el manejo de la Norma ISO 27001 como una de las más importantes que debe ser del conocimiento de los trabajadores, en sus distintos niveles de dirección, operativos o técnicos, para fomentar la responsabilidad y el manejo de los riesgos.

Nota. Se detallan las razones por las cuales la empresa debe estandarizar mecanismos de control en la seguridad de la información y datos.

De esta manera, de acuerdo a lo que se expone en la Tabla 4, es necesario que la empresa tenga clara las razones que conllevan a emplear medidas de seguridad de la información.

4.3 Consecuencias que se pueden generar ante la falta de mecanismos de seguridad y resguardo de la información y datos, en la empresa Transcarga S.A.

Siguiendo la información obtenida en la encuesta y entrevista realizadas al personal de la empresa, se detectaron diversas consecuencias que conllevan a la vulneración de la información que se maneja en la empresa Transcarga S.A. En la siguiente Tabla 5 se muestra el Test de Cumplimiento como herramienta que permitió realizar una evaluación inicial a la empresa mediante una auditoría de seguridad. Este Test de Cumplimiento está sugerido en la Norma ISO 27001.

Tabla 5

Test de cumplimiento para conocer la situación inicial de la empresa

Ítems	SI	NO	Total
4. La Organización y su Contexto			
4.1 Entendiendo la Organización y su contexto de la Información			
1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	3	27	30
2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad?	7	23	30
3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	12	18	30
4.2 Expectativas de las partes interesadas			
4.- ¿Se han identificado las partes interesadas?	8	22	30
5.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	2	28	30
6.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	2	28	30
4.3 Alcance del SGSI			
7.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	1	29	30
4.4 SGS Sistema de Gestión de la Seguridad de la información			
8.- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	0	30	30
5. Liderazgo			
5.1 Liderazgo y compromiso			
9.- ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	6	24	30
10.- ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	3	27	30
11.- ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	4	26	30
5.2 Política de la Seguridad de la Información			
1.- ¿Se ha definido una Política de la Seguridad de la Información?	11	19	30
2.- ¿Se ha establecido un marco que permita el establecimiento de objetivos?	9	21	30

3.- ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?	13	17	30
4.- ¿Se mantiene información documentada de la política del SGSI y de sus objetivos?	1	29	30
5.3 Roles y Responsabilidades			
1.- ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	17	13	30
2.- ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	12	18	30
6. Planificación			
6.1 Tratamiento de Riesgos y Oportunidades			
1.- ¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?	0	30	30
2.- ¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?	0	30	30
3.- ¿Se ha definido un proceso de tratamiento de riesgos?	0	30	30
4.- ¿Se han establecido criterios para elaborar una declaración de aplicabilidad?	1	29	30
5.- ¿Se mantiene información documentada de los puntos anteriores?	1	29	30
6.2 Planificación para consecución de objetivos			
1.- ¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?	10	20	30
2.- ¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación	2	28	30
3.- ¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?	9	21	30
7. Soporte			
7.1 Recursos			
1.- ¿Se identifican y asignan los recursos necesarios para el SGSI?	3	27	30
7.2 Competencia			
1.- ¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?	8	22	30
2.- ¿Se mantiene información actualizada sobre la competencia del personal?	6	24	30
7.3 Concienciación			
1.- ¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?	13	17	30
2.- ¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?	19	11	30
7.4 Comunicación			
1.- ¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?	12	18	30
2.- ¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?	6	24	30
7.5. Información Documentada			
1.- ¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)	0	30	30

2.- ¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección	0	30	30
3.- ¿Se controlan los documentos de origen externo?			
8. Operación **8.1 Control Operacional**			
1.- ¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?	2	28	30
2.- ¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?	0	30	30
3.- ¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados?	0	30	30
4.- ¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?	0	30	30
8.2 Análisis de riesgos de la Seguridad de la Información			
1.- ¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia	0	30	30
8.3 Tratamiento de riesgos de la Seguridad de la Información			
1.- ¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados	0	30	30
2.- ¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?	0	30	30
3.- ¿Se documenta el nivel de aplicación de todos los controles a aplicar?	0	30	30
9. Evaluación del desempeño **9.1 Seguimiento y medición**			
1.- ¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?	0	30	30
2.- ¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?	0	30	30
9.2 Auditorías Internas			
1.- ¿Se ha establecido una programación de Auditorías Internas y asignado responsables?	0	30	30
2.- ¿Se ha definido el alcance y los requisitos para el informe de auditoría?	0	30	30
3.- ¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?	0	30	30
9.3 Informe de Revisión por la Dirección			
1.- ¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?	2	28	30
2.- ¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?	2	28	30
10. Mejora **10.1 No Conformidades y acciones correctivas**			
1.- ¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?	1	29	30
2.- ¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?	0	30	30
10.2 Mejora continua			
1.- ¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?	0	30	30

Elaborado por el autor.

4.3.1 Falta de valoración de los activos a través de un análisis de los riesgos

La empresa no ha empleado las acciones y medidas necesarias que ayuden al resguardo de los activos que posee la empresa. Esta valoración debe darse en todos los bienes que posee la entidad, con el propósito de que las políticas sean adecuadas a las necesidades de la organización. Esto quiere decir, que no se trata solo de valorar los activos y determinar los riesgos para luego diseñar políticas que garanticen su resguardo, sino que también tales políticas deben responder a las necesidades de la empresa.

4.3.2 Posible acceso de intrusos a redes y sistemas de la empresa

En la actualidad la empresa se ve expuesta a la vulnerabilidad de sus datos ante los ataques cibernéticos que buscan el robo de información de distintas índoles para fines delincuenciales. La empresa, no cuenta con un sistema de seguridad que garantice el adecuado resguardo de la información, tampoco existen claves de accesos en todas las áreas y departamento que restrinjan el uso de los datos a terceros.

El uso de dispositivos tecnológicos, equipos inalámbricos y dispositivos de red, se utilizan sin mayor control sobre los ataques que día a día surgen a nivel de las redes de internet, por tanto, la empresa se coloca en una posición arriesgada al no disponer de políticas y acciones que ayuden a minimizar la exposición a los riesgos de robo de información o mal uso de los datos. Si la gerencia no socializa políticas de seguridad de la información, se expone a que intrusos, partes internas o externas, accedan a datos que solo compete a la empresa y sus principales actividades. Esto puede ocurrir en situaciones inesperadas, por ejemplo, trabajadores que se ausentan de sus puestos de trabajo por tiempos cortos, dejando los ordenadores sin contraseña de acceso, esto puede propiciar el uso indebido de terceros.

4.3.3 Posible instalación de virus en sistemas de la empresa

La falta de acciones de seguridad en la información que se maneja en los ordenadores de la empresa, puede exponerla a los virus o programas que infectan la información. Existen diversos virus entre los que se pueden mencionar: virus de macros o códigos fuente, que afectan el sistema central de información de una empresa u organización; virus mutantes, gusanos que son programas que se cargan en la memoria del ordenador y borran información; los caballos de troya, que suelen conocerse como archivos de basura que al cabo de cierto tiempo se activan y dañan la información de los equipos, entre otros virus peligrosos que pueden dañar la memoria del ordenador, así como eliminar información.

4.3.4 Exposición a la interceptación de las comunicaciones en la empresa

Ante la falta de controles de seguridad en la información, la empresa se expone a que terceros ajenos a la empresa intercepten las comunicaciones y esta pueda ser copiada o modificada para intereses distintos. Es necesario que la gerencia capacite al personal en este tipo de penas con el propósito de que el personal conozca que la intercepción puede realizarse a través de acceso físico a las redes de comunicación de la empresa, a las líneas telefónicas o controladores de transmisión.

4.3.5 Accidentes naturales que afectan la seguridad de la información

Se refiere a los riesgos que puede enfrentar la empresa ante problemas o accidentes generados por situaciones naturales como fuertes tormentas, inundaciones, terremotos, otros similares que pueden interferir en el procesamiento de la información y la seguridad de esta.

La empresa no cuenta con políticas de seguridad que tomen en cuenta las afectaciones en caso de situaciones provenientes de la naturaleza, lo cual es esencial considerar con la finalidad de que no se pierda información o se dañen equipos y ordenadores.

4.4 Proponer un plan de acción basado en sugerencias de la normativa ISO/IEC 27001 para lograr una mayor seguridad de la información en la empresa

4.4.1 Alcance del plan de acción de seguridad de la información

El plan de acción para controlar la exposición a los riesgos en la vulnerabilidad de la información, podrá ser aplicada sobre cualquiera de los procesos que se desarrollan en las distintas áreas y departamentos de la empresa. Utilizando por principios básicos y metodológicos que amerita la administración de los riesgos de seguridad de la información.

Para cumplir con el alcance se requiere utilizar la Tabla 6 la cual contiene información que contribuye a conocer los conceptos técnicos, de calidad y administrativos, así como los criterios de aceptación. Del mismo modo, permitirá conocer los componentes y el producto entregado por cada uno de estos.

Tabla 6. Formato para conocer Alcance del Plan de Acción de seguridad de la información

Descripción del Alcance	
El alcance del sistema de gestión es el siguiente: “Gestión de la Seguridad de la información”. Las instalaciones donde se desarrollan los procesos y servicios dentro del alcance del del Plan de Acción están ubicadas en: Samanes 4 Manz 413 V20 V. 19 Guayaquil - Guayas.	
Requisitos	**Características**
Lograr la adecuación de los procesos al estándar ISO 27001:2013	Cumplimiento de la Norma
Criterios de Aceptación	
Conceptos	**Criterios de aceptación**
Técnicos	Se debe cumplir 100% las responsabilidades asignadas

De calidad	Se debe cumplir el Plan de Acción
Administrativos	Se debe cumplir todas las medidas de seguridad de la información requeridas
Entregables del Plan de Acción	
Componentes	**Producto entregado**
Organización y su contexto	Identificar partes interesadas
Liderazgo	Políticas del Sistema de Seguridad de la Información
Planificación	Metodología de gestión de riesgo
Soporte	Estrategia de comunicación del plan de acción
Operación	Evaluación de los riesgos y tratamiento
Evaluación de desempeño	Plan de auditoría interna
Mejora	Solicitud de acción de mejora o correctivas

Fuente: Elaboración propia

En la Tabla 7 se identifican las partes interesadas internas y externas

Tabla 7. Partes interesadas internas y externas

Grupo	Partes interesadas	Expectativas	Necesidad	Influencia en el SGSI
Personas con influencia para impulsar o impedir el funcionamiento de la organización	Propietarios, administradores, supervisores, otros similares	Llevar a cabo un plan de acción que garantice la seguridad de la información	Contar con información y medios seguros	Cumplimiento de la legislación vigente en materia de Seguridad de la información
Partes que tienen relación con la organización (Internos)	Trabajadores	La seguridad de la información ayuda a un mejor desempeño de las funciones.	Se requiere conocer las políticas que conllevan a la seguridad de la información	Formación y compromiso de los trabajadores
Grupos con los que se trabaja frecuentemente (Externos)	Clientes	Que no surjan inconvenientes con datos de sus empresas.	Seguridad de la información.	Dotar de información confiable
	Proveedores	Que no surjan inconvenientes con datos de sus empresas.	Seguridad de la información.	Dotar de información confiable
	Estado	Cumplimiento de la seguridad de datos y de información, de la empresa y terceros.	Que se cumpla con el resguardo de la información y las normas que regulan la seguridad	Cumplimiento de la Norma de Seguridad de la información

Fuente: Elaboración propia

A continuación, se presentan en la Tabla 8, las políticas del Sistema de Seguridad de la Información, propuestas a través del Plan de Acción:

Tabla 8. Política de Seguridad de la Información

Objetivo de la Política: El objetivo principal de la presente Política es definir los principios y las reglas básicas para la gestión de la seguridad de la información
Alcance de la política: La Política es aplicable para todo el personal que labora en la empresa Transcarga S.A. el cual deberá dar cumplimiento a lo establecido.
Políticas de Seguridad de la información
Bloquear sesión de los equipos cuando el empleado no esté en su puesto de trabajo. Cada empleado dejará recogido el entorno de trabajo al finalizar cada jornada laboral. Cualquier documento o soporte de información debe quedar fuera de la vista de, es decir, debe quedar resguardado bajo llave. Mantener ordenado el puesto de trabajo, sin documentos que revelen operaciones de la empresa o que necesiten estar debidamente archivados. Los empleados no pueden entregar sus contraseñas de acceso a los equipos de trabajo, a terceros a la empresa. Cada usuario de los dispositivos será responsable de la información manejada. Se restringe el acceso de equipos tecnológicos personales (Computadoras, portátil, otros) a las oficinas de la empresa. Los empleados utilizarán sus equipos de trabajo como ordenadores y similares, bajo supervisión y autorización del jefe inmediato. Cualquier eventualidad que pueda afectar a la confidencialidad, integridad o disponibilidad de estos dispositivos debe ser reportada al departamento de sistemas.

Fuente: Elaboración propia

4.4.2 Recursos requeridos para ejecutar el plan de acción

Se requiere talento humano que maneje información relacionadas con las normas se seguridad y control de los riesgos, en base a resguardo de los datos, identificación de virus, elementos perjudiciales para el procesamiento de datos, entre otras habilidades y competencias necesarias para un buen establecimiento de las políticas de control y seguridad.

También es necesario el recurso material, conformado por los equipos tecnológicos que se encuentran en las áreas y departamentos de la empresa, en las oficinas de logística de información, así como centros de control de la información, dispositivos, componentes requeridos para el resguardo de la información. Dentro de los recursos materiales se consideran los siguientes:

Infraestructura: Siendo necesario que se asegure un espacio en el área de sistemas donde se garantice el monitoreo para detectar cambios no autorizados en los Accesos establecidos, tanto para administradores como para operarios.

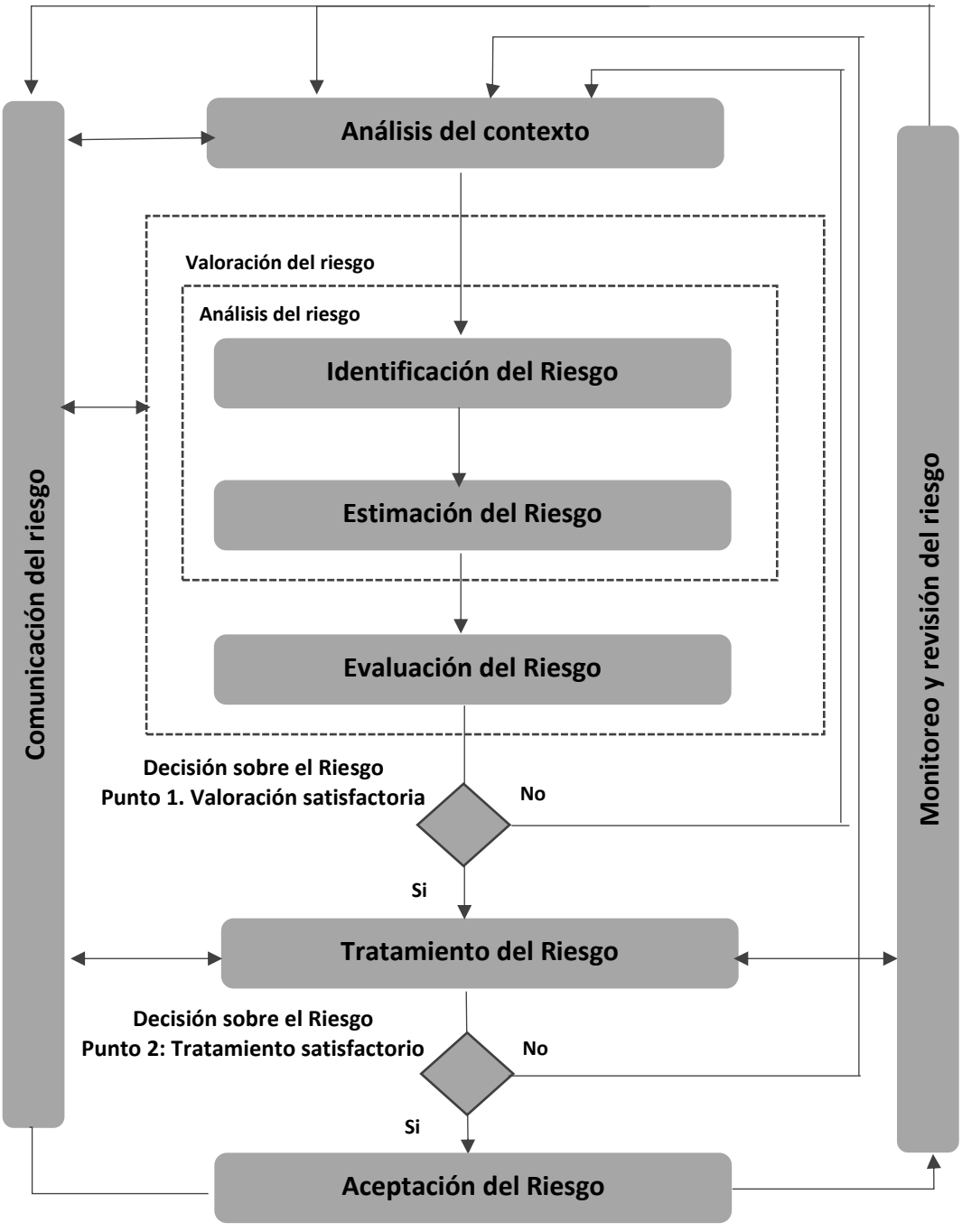
Plataforma: Se debe proporcionar mecanismos de seguridad que se correspondan, garantizando el buen desenvolvimiento del sistema de seguridad.

El recurso financiero también se requiere para ejecutar el plan de acción, siendo necesario que la gerencia apruebe los recursos para adquirir los equipos que ayudarán a fortalecer la seguridad de la información en la empresa.

4.4.3 Socialización del mapa de proceso de riesgo y seguridad de la información

Se requiere que la gerencia socialice con todo el personal, el mapa de proceso donde se identificará el modelo de gestión de riesgo diseñado, tomando como base lo que propone la Norma ISO 27001. En la Figura 10 se detalla el mapa de proceso indicado:

Figura 10. Mapa de proceso de riesgo y seguridad



Nota. Se detalla el mapa de proceso de riesgo y seguridad.

Fuente: Adaptado de ISO 27001

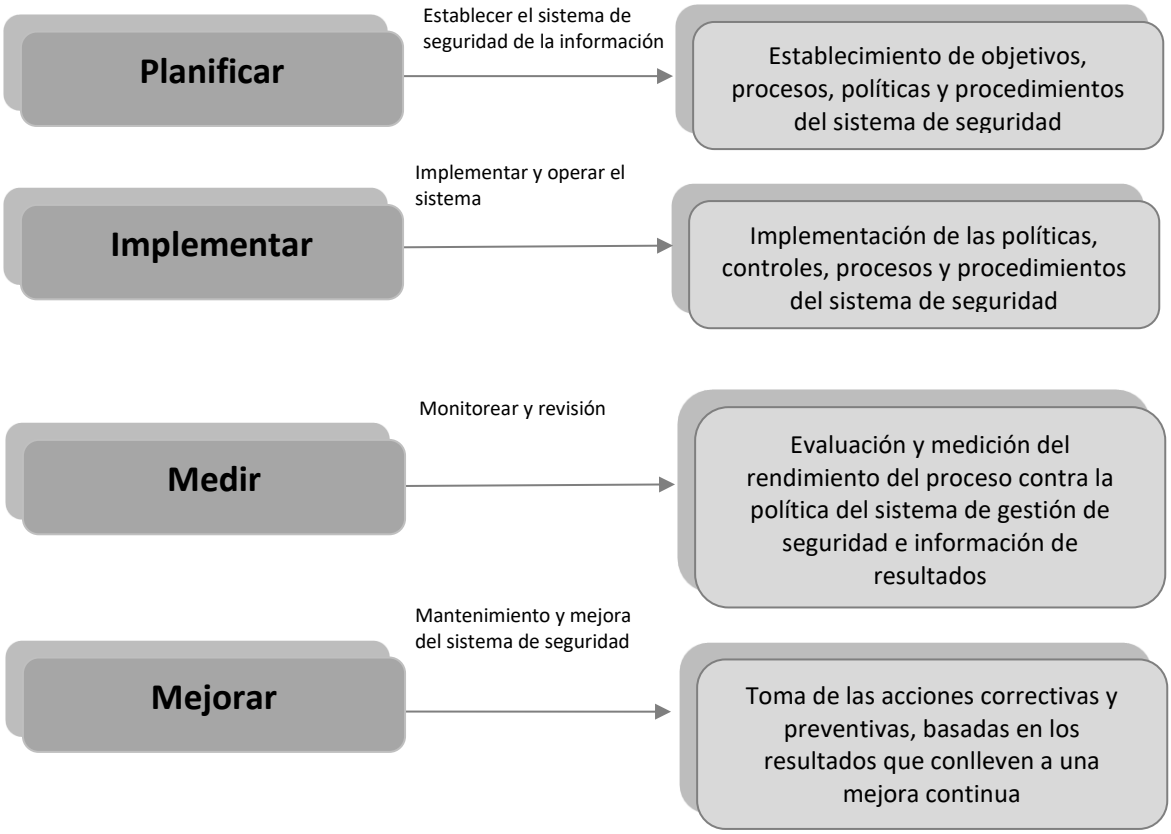
En la Figura 10 se detalla el proceso de riesgo y seguridad el cual inicia con un análisis del contexto, lo cual le permitirá a la empresa conocer que factores del entorno interno y externo están afectando la seguridad de la información. Este análisis debe conllevar a

la identificación de los riesgos a los que se expone la empresa, para lo cual es importante que quien o quienes realicen la identificación conozcan ampliamente los procesos que se llevan en cada uno de los departamentos y áreas de la empresa. Después de identificado es necesario estimar el riesgo para conocer cual es el grado al que se está exponiendo la empresa. Todo esto permitirá realizar una evaluación correcta sobre la cual la gerencia o el equipo encargado de valorar el riesgo decidirá efectuar o no el tratamiento de riesgo. Es importante que durante todo el proceso se haga monitoreo y revisión de los riesgos para conocer si se cumplen los objetivos de seguridad.

4.4.4 Procesos generales del plan de acción

Siguiendo las sugerencias que propone la Norma ISO/IEC, se toma del mismo la adopción de un enfoque basado en procesos con el propósito de que la empresa pueda identificar actividades de funcionamiento y la interacción entre estas, todo esto conlleva a resaltar la importancia de la gestión de la seguridad de la información. En la figura 11 se detalla el enfoque basado en procesos:

Figura 11. Enfoque de la seguridad de la información basada en procesos



Nota. Se detalla el enfoque basado en procesos para resguardo y seguridad de la información.

Fuente: Elaboración propia

La Figura 11 muestra los cuatro pasos que se relacionan con el enfoque basado en procesos para resguardar la información, iniciando con la planificación donde es necesario establecer los objetivos, procesos, políticas y procedimientos que se requieren para la seguridad de la información. La planificación debe ser clara, con objetivos alcanzables y medibles, que conlleven a minimizar la exposición a los riesgos y garantizar la seguridad de la información. A través de la implementación de las políticas, controles, procesos y procedimientos se busca que todas las áreas y departamentos conozcan sobre las actividades planificadas, de manera que se logre un trabajo en equipo donde los miembros de la empresa unan esfuerzos para lograr los objetivos de seguridad. La medición, conlleva a conocer los resultados del proceso, así como el rendimiento de las acciones que se han llevado a cabo y se hará la medición de caraca las políticas que se hayan establecido.

Finalmente, la mejora es una de las etapas más importantes porque permitirá tomar las acciones correctivas y preventivas necesarias de acuerdo a los resultados que se hayan alcanzado tras la implementación de los controles de seguridad.

4.4.5 Establecimiento de los riesgos en la seguridad de la información

Se propone la definición de criterios básicos que ayudarán a la empresa a enfocar las acciones para obtener los resultados esperados. Para esto se necesitan fuentes que permitan conocer los orígenes de los riesgos y oportunidades y el valor de los riesgos en términos de consecuencias y probabilidad. Se consideran los siguientes criterios:

4.4.5.1 Criterios de evaluación del riesgo de seguridad de la información

- Esta evaluación se enfocará en la desglose y valoración de los activos de información que están inmiscuidos en las áreas de la empresa.
- El cumplimiento de los requisitos legales y las obligaciones contractuales.

- Relevancia en la disposición, transparencia y confidencialidad de la información manejada
- Conocimiento de las expectativas y percepciones que tengan las partes interesadas tanto internas como externas, en el sistema de seguridad de la información.

4.4.5.2 Criterios de impacto y relevancia

- Estos dependerán del grado del daño o costo que represente para la empresa, que se deriven de un evento de seguridad de la información manejada en la que se involucren activos impactados, brechas de seguridad de la información, cuando se pierdan datos; operaciones deterioradas, es decir, deterioro o daño de partes internas o externas de los componentes de la información, pérdida del valor financiero del negocio, entre otros similares.
- El impacto también lo determinará el incumplimiento de los requisitos legales a los que deba atender la empresa, en ocasión al resguardo de la información.

4.4.5.3 Valoración de los riesgos

Es importante que antes de valorar los riesgos, la empresa identifique claramente los activos de la información de los procesos que se llevan a cabo en las áreas y departamentos, lo cual servirá de fundamento para dicha valoración. Esta fase consta de dos etapas:

1. Análisis de riesgos

- Identificación de los riesgos
- Estimación del riesgo

2. Evaluación del riesgo

4.4.5.4 Identificación de los riesgos

Se sugiere evaluar en primer lugar identificar los activos de información por proceso en evaluación. Estos activos comúnmente se clasifican en dos tipos: Los primarios y los de soporte.

Los primarios se relacionan con:

a) Procesos

- Procesos y subprocesos cuya degradación imposibilitan alcanzar la misión y visión de la empresa.
- Procesos que si sufren alguna modificación afectarán de forma relevante los objetivos empresariales.
- Procesos que se requieren realizar para cumplir con las normativas, reglamentos y obligaciones de la empresa.

b) Información

- Aquella que se requiere para ejecutar la visión y misión de la empresa.
- Información personal que debe definirse así atendiendo a los derechos de privacidad.
- Información relacionada con las estrategias que ayudan a cumplir los objetivos empresariales.
- Información del alto costo, en virtud de que el resguardo, recolección, almacenamiento, proceso y transmisión, exige un periodo largo de tiempo.

c) Procesos y actividades relacionadas con el negocio

Está relacionado con la propiedad intelectual; este tipo de activos no deben degradarse, de ocurrir imposibilita la ejecución de las tareas de la empresa en sus distintas áreas y departamentos, incidiendo en el cumplimiento de leyes o acuerdos contractuales, entre otros.

4.4.5.5 Estimación de los riesgos

Por medio de la estimación de los riesgos se busca determinar la probabilidad de que ocurra algún evento o incidente y el impacto que puede ocasionar, calificando las consecuencias y evaluándolas con el propósito de establecer el nivel de riesgo que se corresponda. En esta etapa se toma en consideración:

- **La probabilidad de ocurrencia:** relacionada con la cantidad de veces que el riesgo se ha presentado en un periodo de tiempo (Ver Tabla 9).

Tabla 9. Escala de probabilidad de ocurrencia

Escala de probabilidad	
Nivel	**Descripción**
1. Raro	Evento que puede ocurrir sólo en circunstancias excepcionales, 0 y 1 vez en un semestre
2. Improbable	Evento que puede darse en pocas circunstancias, entre 2 y 5 veces en un semestre
3. Posible	Evento que puede ocurrir en algunas de las circunstancias entre 6 y 10 veces en un semestre
4. Probable	Evento que puede ocurrir entre 11 y 15 veces en un semestre
5. Casi seguro	Evento que puede ocurrir más de 15 veces en un semestre

- **El impacto:** relacionado con las consecuencias que puede generar a la empresa que el riesgo ocurriese, está vinculado a la magnitud del efecto (Ver Tabla 10).

Tabla 10. Escala de probabilidad de ocurrencia

Valor de Impacto		
Nivel	**Descripción**	**Escala**
1. Insignificante	Impacta negativamente de forma leve. No tiene impacto financiero para la empresa ni sus procesos.	>=1 y <=4
2. Menor	Impacta negativamente de manera importante. Se pueden presentar sobre costos para la empresa y sus procesos	>=5 y <=8
3. Moderado	Impacta negativamente la imagen de la empresa por retraso en sus servicios y/o producción. Se presentan sobre costos por reprocesos.	>=9 y <=12
4. Mayor	Impacta negativamente la imagen de la empresa a nivel nacional, al igual que las operaciones por incumplimiento de objetivos estratégicos empresariales	>=13 y <=16

5. Catastrófico	Impacta negativamente de forma significativa. Puede recibir sanción por incumplimiento de seguridad.	>=17 y <= 20

Es importante que este análisis sea del conocimiento de todos los involucrados, con la finalidad de socializar la importancia de evaluar los riesgos y sus consecuencias, lo cual fomentará la responsabilidad y la disposición de cumplir con las políticas que se establezcan y las medidas de prevención.

4.4.5.6 Determinación de los riesgos

Se presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad determinados, así como las zonas de riesgo mostrando las posibles conveniencias de tratamiento que se puede dar a ese riesgo, tal como se muestra en la Tabla 11:

Tabla 11. Matriz Impacto & Probabilidad

Impacto	**Valor**	**Evaluación**				
Catastrófico	5	5	10	15	20	25
Mayor	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Menor	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
	Valor	1	2	3	4	5
	Probabilidad	**Raro**	**Improbable**	**Posible**	**Probable**	**Casi seguro**

Al analizar el riesgo, su probabilidad e impacto, se puede determinar el grado de exposición al riesgo que tiene la empresa. Las zonas de riesgos se pueden apreciar en la Tabla 7, cuyos colores facilitan la comprensión del gráfico. Esto contribuirá a priorizar los riesgos que deben atenderse dependiendo de la magnitud del efecto o impacto que tenga en el desenvolvimiento de las actividades de la empresa. Las zonas de riesgo se diferencian por colores y por número de zona, como se muestra en la Tabla 12:

Tabla 12. Zona de riesgo

Zona de Riesgo
B: Zona de riesgo baja (color verde) 5 zonas siendo la Z-5 la de mayor riesgo
M: Zona de riesgo moderada (color amarillo) 4 zonas siendo la Z-9 la de mayor riesgo
A: Zona de riesgo alta (color rojo) 8 zonas siendo la Z-17 la de mayor riesgo
E: Zona de riesgo extrema (color vino tinto) 8 zonas siendo la Z-25 la de más alto riesgo

Nota. Se detalla en la tabla las posibles zonas de riesgo en las que se encuentre la empresa

Después de conocer los riesgos a los que se expone la empresa y evaluarlos, es importante y necesario identificar la zona de riesgo en la cual se encuentra la empresa, lo cual permitirá que se tomen las medidas necesarias para enfrentar las debilidades en loa procesos de seguridad de la información. Para ello, a través de la Tabla 12, se puede disponer de información para precisar la zona de riesgo como baja, moderada, alta o extrema.

4.4.6 Monitoreo y seguimiento

Como parte de las buenas prácticas principales de seguridad de la información, es necesario que la empresa designe un equipo de personas responsables de la gestión de la seguridad de la información, de manera que se analicen y planifiquen los tiempos de implementación de los controles de seguridad, lo cual contribuirá a mitigar los riesgos que existen. La designación de un equipo encargado de revisar los procesos de control, contribuirá a resultados más efectivos, basados en los siguientes criterios:

- Monitorear la gestión de seguridad de la información y comprobar su eficacia.
- Monitorear para prevenir incidentes de seguridad.

- Diseñar y ejecutar los indicadores de gestión de monitoreo.
- Velar por el correcto uso de las redes y comunicación.
- Monitorear y vigilar el servicio ofrecido por terceros.

5 Conclusiones

Se hizo una investigación de las razones que afectan la seguridad de la información en el área de logística de la empresa Transcarga S.A. utilizando técnicas como la entrevista y encuesta dirigidos a personal de la empresa, lo cual permitió dar cumplimiento a, primer objetivo específico. La entrevista fue realizada al jefe del departamento de sistema pudiéndose validar el problema de estudio. La empresa no cuenta con un sistema de seguridad de la información y el uso de los datos, lo cual la coloca en una posición vulnerable.

A través de la encuesta realizada al personal de la empresa, se pudo determinar que el personal desconoce sobre las responsabilidades que pueden acarrear en un mal uso o manejo de los datos y la información de la empresa. Los encuestados coincidieron en que no existen políticas de seguridad de la información que ayuden a garantizar el correcto manejo de acceso a la información, publicación de esta o manipulación de datos.

Dando cumplimiento al segundo objetivo específico, se pudo conocer las consecuencias que se generan ante la falta de mecanismos de seguridad y resguardo de la información y datos, en la empresa Transcarga S.A. El estado de vulnerabilidad en el que se encuentra la empresa conlleva a la falta de valoración de los activos de información de los que se dispone, también se expone a posibles riesgos de instalación de virus o acceso de intrusos a la información de la empresa, porque no se cuentan con niveles de seguridad para ingresar a los equipos tecnológicos de la empresa.

Se prone un plan de acción basado en sugerencias de la normativa ISO/IEC 27001 para lograr una mayor seguridad de la información en la empresa. Este plan resume el

alcance, los recursos requeridos, los procesos generales del plan de acción y los pasos para determinar los niveles de riesgo a los que se expone la empresa.

Durante el desarrollo de la investigación se presentaron algunos inconvenientes relacionados con la facilidad de poder acceder con mayor detalle a las actividades que se realizan en cada una de las áreas de la empresa, pues lo empleados deben desarrollar sus actividades cotidianas laborables y ha sido un poco difícil interrumpir sus jornadas. No obstante, el personal entrevistado brindó información que fue de gran valor para el desarrollo del tema.

De igual forma, cabe señalar que la investigación realizada ha sido de gran valor porque ha permitido destacar que la seguridad de la información es una de las principales garantías que debe dar la gerencia en el uso y manejo de datos. La ISO 27001 brinda una solución muy válida además de pertenecer al conjunto de Normas que a nivel internacional contribuyen a una mayor calidad de los procesos internos en las organizaciones, siendo este el caso, en el resguardo de la información. Se puede disponer de otros sistemas de seguridad que ofrece el mercado empresarial, no obstante, la implementación de una alternativa basada en la ISO 27001, no solo puede garantizar la seguridad de la información, sino que conllevar a una futura Certificación que ayuda a colocar a la empresa en una posición competitiva en el mercado.

5.1 Recomendaciones

Se recomienda que la empresa realice los trámites y acciones necesarias para implementar el sistema ISO/IEC 27001:2013 con la finalidad de obtener la certificación que le permitirá ser competitivo y garantizar el resguardo de la información que se maneja en la empresa.

Se recomienda involucrar a todo el personal de la empresa, es decir, independientemente del área en el que desempeñen funciones, se sugiere que todos

los miembros conozcan sobre el sistema de seguridad de la información y la responsabilidad que tienen en dicho sistema. Esto puede hacerse a través de reuniones mensuales con los miembros de cada área o departamento, para precisar sus funciones y asignarles por escrito la responsabilidad que tienen en el resguardo y uso correcto de los datos de la empresa, es decir, que todos los empleados aportes a la seguridad.

Se recomienda realizar revisión periódica de los procesos de seguridad de la información, con el propósito de precisar si existen algún fallo que deba ser corregido o mejorado, con el propósito de lograr los objetivos que se persiguen con el sistema.

Es recomendable que la empresa también haga una revisión anual de los activos de la información, para garantizar que se estén tomando en cuenta las medidas de protección de la información establecidas. Para esta revisión anual la empresa debe preparar información básica que precise características del activo utilizando un identificador del mismo, proceso en el cual se utiliza el activo, el nombre del activo, la descripción general del mismo, descripción de las áreas y personas que manejan el activo, tipo de activo, ubicación física, clasificación de la información que se maneja en el activo, valoración del impacto en caso de pérdida de información contenida en el activo, entre otros aspectos que ayudarán a conocer la situación del activo en la empresa.

6 Referencias

[1] ISO/IEC 27000:2018, «. Information technology–Security techniques–Information security management systems — Overview and vocabulary,» ISO, 2018.

[2] A. Heredia, «Políticas de fomento para la incorporación de las tecnologías digitales en las micro, pequeñas y medianas empresas de América Latina: revisión de experiencias y oportunidades.,» *CEPAL,* 2020.

[3] J. Berruz Gordillo, «Vulnerabilidades en el sistema de información en el soporte de inventario del distribuidor mayorista de productos de ferretería ¨ferrequim sa¨,» *UTB-FAFI,* 2022.

[4] J. Cuellar Castrillón, «Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Institución Edutec de los Andes Pitalito, argumentada en la norma ISO/IEC 27001.,» *UNAD,* 2020.

[5] C. Benussi Díaz, «Obligaciones de seguridad en el tratamiento de datos personales en Chile: escenario actual y desafíos regulatorios pendientes.,» *Revista chilena de derecho y tecnología,* vol. 9, nº 1, 2020.

[6] F. Arévalo Moscoso, «Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos.,» *Universidad de Cuenca,* 2017.

[7] J. Asurza Caceres, «Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa Bafing SAC en 2021,» *Universidad Cientifica del sur,* 2022.

[8] A. Garcia Vega y D. Morales Baren, «Seguridad informática mediante hacking ético en la aplicación de pentesting para el análisis de vulnerabilidades en las redes de datos de la Cooperativa,» *Universidad Técnica de Cotopaxi ,* 2022.

[9] A. Jacome Sanchez, «Diseño de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001,» *ESCUELA DE POSTGRADO NEUMANN,* 2022.

[10] L. Lucano Cordones, «Diagnóstico y diseño de un sistema de gestión de seguridad de la información (SGSI), basado en la norma ISO/IEC 27001: 2013, en un banco público,» *Universidad Central del Ecuador,* 2019.

[11] J. Russell, «ISO 27001,» nqa., Reino Unido , 2013.

[12] J. Zambrano Loor, «Diseño de modelo de seguridad y plan de mejoras para la seguridad de la red, en función de las vulnerabilidades y amenazas detectadas en la empresa CENFORSP. CIA LTDA,» *Ubiversidad Ecotec,* 2021.

[13] C. García Wirton, «Ciberseguridad en el Sector Financiero¿ Cómo transformar una amenaza en una oportunidad?,» *Comillas,* 2021.

[14] J. Ríos, «El concepto de información: dimensiones bibliotecológica, sociológica y cognoscitiva,» *Investigación Bibliotecológica,* vol. 28, nº 62, 2014.

[15] A. Colina y J. Túa, «Activos informáticos: un referente en la caracterización de procesos de la gestión riesgos de TI,» *INNOVA Research Journal,* vol. 5, nº 3.2, pp. 196-213, 2020.

[16] M. E. Whitman y . H. J. Mattord, Principles of Information Security, 7 ed., C. Learning, Ed., 2021, p. 752.

[17] S. Garre, «Introducción a la seguridad de la información,» UOC Universitat Oberta de Catalunya, Cataluña, España, 2018.

[18] J. Figueroa, R. Rodríguez, C. Bone y J. Saltos, «La seguridad informática y la seguridad de la información,» *Polo del Conocimiento,* vol. 2, nº 12, pp. 145-155, 2017.

[19] G. Arias, N. Merizalde y N. Noriega, «Anaálisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audio-visual,» Repoitorio Universidad Politécnica Salesiana, Guayaquil, Ecuador, 2013.

[20] E. Vega, Seguridad de la información, 3ciencias, 2021.

[21] PMG-SSI , «Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad,» Blog especializado en Seguridad de la información y ciberseguridad, Alemania, 2018.

[22] J. Tejada, «Datos personales y pilares de la seguridad de la información,» Universidad Pontificia Bolivariana, Medellín, Colombia, 2021.

[23] A. S. U. T. E. G. y. B. M. Tchernykh, «Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability.,» *Journal of Computational Science,* vol. 36, nº 100581, 2019.

[24] INCIBE, «Protección de la Información,» INCIBE. Gobierno de España, España, 2014.

[25] Q. D. T. C. Y. y. Q. G. Wang, «DoS attacks and countermeasures on network devices,» 2017 26th Wireless and Optical Communication Conference (WOCC), 2017.

[26] G. Baca, Introducción a la seguridad informática, México: Grupo Editorial Patria, 2016.

[27] C. Avenía, «Fundamentos de seguridad informática,» *Fundación Universitaria del Área Andina,* pp. 1-98, 2017.

[28] L. Calderón, «Seguridad informática y seguridad de la información,» Universidad Piloto de Colombia, 2015.

[29] M. Romero, G. Figueroa, D. Vera, J. Álava, G. Parrales, C. Álava, L. Murillo y M. Castillo, «Introducción a la seguridad informática y el análisis de vulnerabilidades,» 3ciencias, Alicante, 2018.

[30] J. Altamirano Grijalva, «Herramientas estadísticas y certificación ISO 9001: 2015 en la empresa Productos Lácteos Píllaro.,» *Universidad Técnica de Ambato. Facultad de Ciencias Administrativas. Carrera de Organización de Empresas,* 2021.

[31] G. Pedraza, «Plan de implementación de un sistema de gestión de seguridad de la información en una entidad del sector público basado en la NTC ISO 27001:2013,» Fundación Universidad de América, Bogotá D.C., Colombia, 2017.

[32] ISO 27000 ES, «ISO 27000 ES,» Integrar normas y sistemas, [En línea]. Available: http://www.iso27000.es/iso27000.html. [Último acceso: 2 mayo 2023].

[33] Normas-iso, «asesoría y formación en sistemas de gestión,» 2021. [En línea]. Available: https://www.normas-iso.com/iso-27001/. [Último acceso: 2 mayo 2023].

[34] D. Servera, «Conceptos y evolución de la función logística,» *INNOVAR. Revista de Ciencias Administrativas y Sociales,* vol. 20, nº 38, pp. 217-234, 2010.

[35] P. Nuño, «Emprende Pyme,» Fleebe.AI, 23 marzo 2023. [En línea]. Available: https://emprendepyme.net/la-logistica-empresarial.html. [Último acceso: 2 mayo 2023].

[36] A. Campos, Métodos mixtos de investigación, Editorial Magisterio, 2021.

[37] A. Hernández, M. Ramos y B. Placencia, Metodología de la investigación cientifica, Editorial Área de Innovación y Desarrollo SL, 2019.

[38] M. Capote, Trabajo con documentos: en Ciencias de la Educación, Editorial Eduin Educación Universitaria, 2018.

[39] J. Hurtado, Metodología de la investigación Guía para la comprensión holística de la ciencia, Cuarta ed., Caracas: Libreria Virtual Ozal, 2012.

[40] V. Niño, Metodología de la Investigación, Bogotá: Ediciones de la U, 2019.

[41] G. Lebet, «https://gabriellebet.files.wordpress.com/2013/01/tecnicas-de-recoleccic3b3n4.pdf,» Enero 2013. [En línea]. Available: https://gabriellebet.files.wordpress.com/2013/01/tecnicas-de-recoleccic3b3n4.pdf. [Último acceso: 11 Septiembre 2018].

7 Anexos

Anexo 1. Cuestionario sugerido ISO 27001

ISO 27001

4	**La Organización y su Contexto**
4.1	**Entendiendo la Organización y su contexto**
1.-	¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?
2.-	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?
3.-	¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?
4.2	**Expectativas de las partes interesadas**
1.-	¿Se han identificado las partes interesadas?
2.-	¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?
3.-	¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?
4.3	**Alcance del SGSI**
1.-	¿Se ha determinado el alcance del SGS y se conserva información documentada?
4.4	**SGS Sistema de Gestión de la Seguridad de la información**
1.-	¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?
5	**Liderazgo**
5.1	**Liderazgo y compromiso**
1.-	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?
2.-	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?
3.-	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?
5.2	**Política de la Seguridad de la Información**
1.-	¿Se ha definido una Política de la Seguridad de la Información?
2.-	¿Se ha establecido un marco que permita el establecimiento de objetivos?
3.-	¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?
4.-	¿Se mantiene información documentada de la política del SGSI y de sus objetivos?
5.3	**Roles y Responsabilidades**

1.-	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?
2.-	¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?
6	**Planificación**
6.1	**Tratamiento de Riesgos y Oportunidades**
1.-	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?
2.-	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?
3.-	¿Se ha definido un proceso de tratamiento de riesgos?
4.-	¿Se han establecido criterios para elaborar una declaración de aplicabilidad?
5.-	¿Se mantiene información documentada de los puntos anteriores?
6.2	**Planificación para consecución de objetivos**
1.-	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?
2.-	¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación
3.-	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?
7	**Soporte**
7.1	**Recursos**
1.-	¿Se identifican y asignan los recursos necesarios para el SGSI?
7.2	**Competencia**
1.-	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?
2.-	¿Se mantiene información actualizada sobre la competencia del personal?
7.3	**Concienciación**
1.-	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?
2.-	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?
7.4	**Comunicación**
1.-	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?

2.-	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?
7.5	**Información Documentada**
1.-	¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)
2.-	¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección
3.-	¿Se controlan los documentos de origen externo?
8	**Operación**
8.1	**Control Operacional**
1.-	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?
2.-	¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?
3.-	¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados?
4.-	¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?
8.2	**Análisis de riesgos de la Seguridad de la Información**
1.-	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia
8.3	**Tratamiento de riesgos de la Seguridad de la Información**
1.-	¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados
2.-	¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?
3.-	¿Se documenta el nivel de aplicación de todos los controles a aplicar?

ISO 27001

9	**Evaluación del desempeño**
9.1	**Seguimiento y medición**
1.-	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?
2.-	¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?
9.2	**Auditorías Internas**
1.-	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?
2.-	¿Se ha definido el alcance y los requisitos para el informe de auditoría?
3.-	¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?
9.3	**Informe de Revisión por la Dirección**
1.-	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?
2.-	¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?
10	**Mejora**
10.1	**No Conformidades y acciones correctivas**
1.-	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?
2.-	¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?
10.2	**Mejora continua**
1.-	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?