ESCUELA DE POSTGRADO NEUMANN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

“Diseño de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001”

Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autore:
Bach. Jácome Sanchez, Alex Paul

Docente Guía:

Dra. Bahamondes Rosado, María Emilia
.

TACNA – PERÚ

2022

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) autor (es)”

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Los Sistemas de Gestión de Seguridad de la Información (SGSI) basados en la normativa ISO 27001, constituyen herramientas óptimas para resguardar los datos e información. Por lo que, esto consiente instaurar, efectuar, operar, monitorear, examinar, conservar y optimizar la seguridad informativa de una organización. En este sentido el presente trabajo tiene el objetivo de diseñar una propuesta sobre el SGSI, basado en la norma ISO 27001 para resguardar la privacidad, integridad y disponibilidad de la información que manipula la empresa de transporte la Ecuatoriana. Para lograr esto se implementó una metodología apoyada en el modelo MAGERIT (observación y diagnóstico para la GR ya que proporciona un método sistemático para analizar las amenazas derivadas de la implantación de tecnologías) y el enfoque PHVA (Planificar, hacer, comprobar y mejorar) con el propósito de gestionar los riesgos y en función de esto realizar modificaciones en los procedimientos para dar soluciones a situaciones problemáticas. Obteniendo como resultado en principio el diagnóstico sobre la información y datos y estableciendo que si la empresa de transporte la Ecuatoriana se acoge al diseño de propuesta, cumpliendo con los parámetros establecidos así como el presupuesto de inversión para la implantación del equipamiento preciso y adecuado para aplicar acorde a los requisitos de la normativa ISO 27001 y la incorporación del SGSI, ciertamente permitirá a sus proveedores, clientes y socios, confiabilidad al conocer que la empresa cumple con los estándares de seguridad en su proceso.

INTRODUCCIÓN

Actualmente muchas empresas latinoamericanas, manipulan información relevante y privada dentro de los formatos digitales, en relación al auge e impulso de la tecnología, especialmente la que está acopiada en el sistema informático (SI), para facilidad de organización. Por tal razón, es menester considerar que, la protección, privacidad, probidad y disponibilidad del SI que se pueda encontrar en riesgo o vulnerabilidad, ya sea a nivel de hardware o Software. Estos riesgos constituyen amenazas o detrimentos, basados en el hurto o manejo de la información en las empresas con fines no lícitos y sin autorización, vale destacar que los SI, junto a los métodos y procedimientos que se sirven de este, son activos valiosos de una organización.

En este sentido Andreu (2012) establece que “la privacidad, probidad y disponibilidad de información sensible, logran alcanzar la esencialidad para conservar los niveles de competencia, renta, aprobación legal e imagen corporativa obligatorios para alcanzar los objetivos de la organización y asegurar beneficios económicos” (p.45).

En alusión a esto, la empresa de transporte La Ecuatoriana, tiene como activo significativo su SI ya que a través de este, la empresa ejecuta diariamente en sus diversas acciones y operaciones, por lo que se hace necesario desarrollar una propuesta de implementación de SGSI sustentado en la Normativa ISO 27001, el cual le admitirá a la organización avalar que los riesgos de la SI puedan reconocer, asumirse, gestionarse y mitigarse a través de la información documentada, metódica, ordenada, eficientemente y adecuada a los cambios que se produzcan en los SI.

Respecto a este criterio, se aplicarán políticas y procedimientos en correlación a los objetivos de este estudio, con objeto de mantener el SI resguardado de cualquier tipo de riesgo.

Esta investigación, identifica un modelo de propuesta diseñado en las bases de un SGSI, el cual estipula ciertos estándares a cumplir que parten desde la normativa ISO 27001, como se mencionó en el párrafo anterior, estructurado a través de un enfoque metodológico como es el PHVA (Planificar, hacer, comprobar y mejorar), asentados en las políticas y objetivos de la empresa de transporte La Ecuatoriana. Por tanto, las directrices de esta propuesta responden al tratamiento conveniente y cumplimiento de todos lo parámetros para optimizar el SI y así comenzar la implantación de las medidas necesarias para asegurar la información sensible de la empresa.

Esta investigación se desarrolla por secciones y capítulos; el capítulo I; detallará todo lo relacionado a los Antecedentes del Estudio, desde el planteamiento, formulación, hipótesis, objetivos, metodología, definiciones, alcances y limitaciones.

Seguidamente, el capítulo II Marco Teórico; se estructura en base a las conceptualizaciones de los criterios relevante de autores consultados y la evidencia científica, seguido de la importancia de las variables, modelos, análisis comparativo y análisis crítico. Posteriormente el capítulo III permitirá establecer el marco referencial, es decir contendrá la reseña histórica de la empresa, presentación de actores y diagnóstico sectorial. El capítulo IV contiene los resultados y el diseño de planes de acción en esta modalidad la propuesta de mejora. Finalmente el capítulo V contiene sugerencia, llegando así a las conclusiones.

Capítulo I Antecedentes del Estudio

1.1. Título del Tema

Diseño de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la Norma ISO 27001

1.2. Planteamiento del Problema

La normativa ISO 27001 fundas buenas prácticas para implantar un SGSI. Por tanto, si las organizaciones reconocieran su importancia, entenderían que esta, permite proteger los datos e información que manejan, ya que constituyen un activo muy importante, ya que generan confiabilidad en los clientes, proveedores y empleados (DeloitteEcuador, 2020)

Hoy en día, en las muchas empresas, persisten falencias de culturización empresarial, específicamente en temas como la SI. En la cual predominan aspectos ambiguos que ponen en riesgo la integridad, recurso y privacidad de los datos de una organización. Un SGSI es unas herramientas que, en instantes críticos, permite el resguardo de datos. Siendo más resistentes a los ataques cibernéticos, conjuntamente consiente la mejora continua, el monitore, las auditorías internas, como herramientas que faciliten un control con constante actualización para un correcto funcionamiento (Cohen, 2015).

Hoy en día los nuevos procedimientos en los SGSI, permiten la implantación y utilización de herramientas que optimen los procesos y actividades internas con el fin de obtener un correcto desenvolvimiento en la empresa en la que se implementar o se desea aplicar. Por tal razón determina Guitierrez (2017) que; “el aumento actual de la SI, tales como; ataques cibernéticos a la información o a todo un sistema en

las organizaciones, constituye una violación de la seguridad de datos, generalmente porque no se cuenta con una gestión contra riesgos en el SI ” (p.98).

En Ecuador, es lamentable conocer que tanto grandes, medianas y pequeñas empresas, no aplican en sus procesos internos un SGI, o por lo menos políticas de SI y mucho menos aplican una normatividad que les permitan salvaguardar sus activos valiosos o la propiedad e información sensible de activos, clientes y proveedores o de los datos generales de la organización (Jimenez, 2017)

Bajo estos criterios, los principales problemas detectados de la empresa de transporte la Ecuatoriana residen en que poseen que se visualizan resultados negativos en sus políticas de seguridad, por lo que existen casos de inseguridad, Las causas se deben a la falta de planificación, así como protocolos de seguridad en sus sistemas informáticos y la no existencia de un instructivo o manual de seguridad. Por tanto, si no se implementa un SGSI la empresa corre el riesgos en cuanto al mantenimiento de la confidencialidad, integridad y disponibilidad de la información. Lo que afectaría su imagen corporativa y por ende la confiabilidad y credibilidad de sus clientes.

1.3. Objetivos

Objetivo General

Diseñar una propuesta sobre el Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001 para resguardar la confidencialidad, integridad y disponibilidad de la información que maneja la empresa de transporte la Ecuatoriana

Objetivos Específicos

1- Identificar los puntos críticos sobre los que se basará implementación del SGSI bajo la norma ISO 27001 para la empresa de transporte la Ecuatoriana

2- Formular un plan de acción sobre un SGSI bajo la norma ISO 27001 Establecer controles sobre los activos de la empresa de transporte la Ecuatoriana, basado en una propuesta de tratamiento de riesgo bajo la normativa ISO 27001
3- Establecer un mecanismo de control y el costo/beneficio de la propuesta formulada

1.4. Justificación

Por el planteamiento antes señalado, sobre el acceso a la propiedad informática y su gestiona miento sensible de activos, clientes y proveedores o de los datos generales de la empresa, ponen en peligro la reputación sobre las políticas de seguridad de las organizaciones.

Por tanto, se considera que, la propuesta de Implementar de un SGSI, sustentado en la normativa ISO 27001 constituye una estrategia viable para el resguardo y preservación la privacidad, probidad y recursos de la información que manipula la empresa de transporte la Ecuatoriana

Esta propuesta estará basada en resguardar los datos valiosos de la empresa de transporte la Ecuatoriana, considerándola como un mecanismo fundamental ya que se estaría tramitando todo el desenvolvimiento de activos informáticos de la empresa.

Por tal razón, esto reviste gran importancia ya que es primordial la planificación de un diseño de un SGSI, que asienta el resguardo de los datos confidenciales de la empresa, y a su vez contribuya con la adquisición de políticas de privacidad y confiabilidad para garantizar a los clientes que sus datos personales están seguros dentro de la compañía (Balaguer, 2014).

La planificación, para llevar a cabo la propuesta, estaría basada en los parámetros de la norma ISO 27001, siendo de gran aporte y adecuando se para la reducción de riesgos, sobre la perdida de información de cualquier índole dentro de la empresa.

Posteriormente a la planificación se establecerán, compendios que diferencien el desarrollo social, económico y político, la organización, de acuerdo al sector de su posicionamiento evitando tomar decisiones arriesgadas que afecten su reputación, para así, analizar la viabilidad en sus procesos. Con base en Jiménez (2017) “la tecnología actualmente rige políticas relacionadas al SGSI con el propósito de establecer una priorización de resguardo de activos informáticos o del SI de las empresas” (p.76).

Este criterio se unifica, con el de Villalonga (2019) quien argumenta que:

> “La norma ISO 27000 es una estrategia, que implementa un sistema de gestión basado en las normas internacionales, por tanto, permite el gestionar los riesgos que puedan estar presenten en los SI de las empresas y a partir de dicha gestión formular políticas de resguardo” (p.83).

Por tanto, estas consideraciones que justifican este diseño están basadas en la aplicación de un SGSI, con el cual, se resguardará los activos más sensibles y valiosos de la empresa para fortalecer la confianza de las partes interesadas y el cumplimiento legal y contractual (Romero et al., 2018).

Entendiendo que estas intervenciones, permitirán preservar la seguridad de la información en cuanto a la confiabilidad, privacidad, recursos, considerando las cuestiones internas y externas así como los requisitos de las partes interesadas.

1.5. Metodología

El enfoque metodológico a aplicar para el diseño de la propuesta sobre el SGSI, sustentado en la normativa ISO 27001 para salvaguardar la confiabilidad, integridad y recursos activos (información) que manipula la empresa de transporte la Ecuatoriana, y para la consecución de los objetivos serán; en principio para realizar el análisis de riesgo; como lo es MAGERIT y la aplicación del enfoque PHVA. Cada uno de estos métodos, tiene sus propias peculiaridades, beneficios y desventajas; por lo que se seleccionan las que más se adaptan conforme a la realidad de la empresa y de la forma de examinar las debilidades presentes en la empresa.

Por tanto, también se aplicó el método analítico ya que admitió la clasificación y examinación sobre el SI, obteniendo resultados con base en las aportaciones de la empresa de transporte la Ecuatoriana

En lo que respecta a la metodología Magerit, corresponde a un enfoque metodológico basado en una examinación para gestionar los riesgos. Con base en las estipulaciones de Hernández (2016) que refiere, “este método suministra un procedimiento sistemático para estudiar los riesgos procedentes del uso de tecnologías de la información y comunicaciones para así poder efectuar la aplicación de medidas de control que disminuyan las amenazas y mitiguen los riesgos” (p.29).

Como bien se mencionó, este método está sustentado en el análisis de impactos, posibles amenazas o vulnerabilidades en cuanto a una posible violación a los SI y así poder identificarlos y gestionarlos de manera precisa e implantar en función de esto medidas preventivas y correctivas acorde a las necesidades (DeloitteEcuador, 2020).

La fase de aplicación de este método Magerit, se basó en establecer los conceptos informalmente. Enmarcando acciones para gestionar procedimiento que

puedan mitigar tales amenazas. Así mismo se concretaron y establecieron los pasos para formalizar las acciones para examinar y valorar los riesgos. Posteriormente se describieron las elecciones y criterios para tratar los riesgos. Así mismo se establecieron las medidas a tomar (estrategia PHVA) en conjunto con un análisis de riesgos del sistema y eventualmente, incorporando cambios sustanciales. Se permitió determinar los planes de seguridad o también conocidos como planes estratégicos. Y finalmente permitió realizar un estudio de costo/beneficio para planificar la implementación del SGSI.

Seguidamente se empleó un metodología apoyada en una propuesta; como una estrategia de planeación y actuación que consiente la implementación, de ejercer controles sobre sus propias práctica , a través de un proceso de examinar-controlar(Hernández, 2016).

El ciclo PHVA implica 4 pasos: planear, hacer, verificar y actuar. En cuanto a las fases de aplicación de la PHVA, consistió en la aplicación de un proceso estructurado en 4 fases:

La primera fase planear: se establecieron los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente y las políticas de la organización. La segunda fase, hacer; se realizó todo lo que se ha planeado, donde se implementó la mejora. La tercera fase se basó en verificar, es decir realizar el seguimiento y medir los procesos y los productos contra las políticas, los objetivos y los requisitos del producto. Y finalmente la fase cuatro, actuar; en esta se toman acciones para mejorar continuamente el desempeño de los procesos. Institucionalizar la mejora, sino se deberá volver al paso hacer.

1.6. Definiciones

1.8.1 Gestión tecnológica en una organización

La Gestión Tecnológica definida en sus siglas GT, ciertamente constituye una herramienta de control en las empresas, instituciones y organizaciones con el propósito de valorar la situación interna de una empresa, esto a través de la implantación de procedimientos de innovación y equipamiento que puedan anteponerse a través de la detección a cualquier riesgo (Jimenez, 2017). Por su parte Sánchez (2011) ha establecido que:

> "cuando se estudia la situación interna de una empresa, y se toman decisiones asertivas sobre adoptar e implementar tecnologías que mejoren los procesos internos de una corporación, se está actuando de forma responsable con los clientes, proveedores y empleados que forman parte de tal entidad" (p.13)

1.8.2 Sistemas de Información (SI)

Los SI constituyen un conglomerado de procesos que se integran a ciertos entornos, y en una correlación activa entre el usuario y el sistema (computador/programas). Tal correlación se estructura sobre datos, información, registros, documentaciones con contenido sensible, necesaria para la operatividad de una empresa (Andreu, 2012, p.17). En cuanto a su función principal dentro de las empresas, reside en la suministración de datos internos y entre las diversas asociaciones para la operatividad de la empresa y sus actividades diarias (Smith, 2018)

1.8.3 Estrategia tecnológica de una organización.

En relación con la estrategia tecnológica Smith (2018) ha definido que “constituye un conjunto de técnicas inclinadas a los procesos de gestionamiento para poder examinar, estudiar, diagnosticar, y regular de forma eficiente todas las acciones con base en la tecnología de una organización” (p.34).

A estos lineamientos, argumenta Sánchez (2011) que, debido a “la falta de un SGSI las empresas están latentes a correr riesgos constantes ya que ni si quieran pueden identificar sus amenazas, por lo que sino pueden conocerle mucho menos identificarle” (p.23). Esto con el propósito de ser asumidos con base en una planificación y a través de una documentación sistemáticamente estructurada adecuada a los riesgos que se desean mitigar. En este sentido es menester la aplicación de estrategias que determinen cambios efectivos para la empresa

1.8.4 Planificación Estratégica

La planificación estratégica de acuerdo con Ortiz (2019) “es la acción de estimación metodología de un determinado entorno, parte de un diagnóstico y para llevarse a cabo se deben establecer objetivos y metas dirigidos a establecer cambios, sobre la solución de problemas de largo plazo” (p.5) Si bien es cierto la planificación estratégica es el camino para alcanzar determinadas metas. Esta constituye una herramienta que hace posible la organización y el orden dentro de los procesos de cada empresa (James, 2015)

1.8.5 Norma ISO 27001

La normativa ISO permite a la organización establecer un orden en sus actividades y procesos con el fin de hacerlas certificables. Específicamente la ISO 27001 establece tal orden y organización, pero directamente en los sistemas informáticos de una empresa determinada para certificarla como una organización

que implanta sistemas y gestiona la seguridad de sus documentos digitales y principales activos informáticos (Balaguer, 2014).

La normativa además de ser aplicable a todo tipo de empresas en cuanto a sus políticas, actividades de planificación, y responsabilidades, según Ortiz (2019) “se caracteriza por asegurar la privacidad e integridad de los datos y de la información, así como de los sistemas que la procesan creando una relacion de confianza del cliente y la empresa” (p.7).

1.9. Alcances y Limitaciones

El alcance de este estudio, el propio establecimiento de una propuesta a desarrollar de manera más amplia, basada en el diseño sobre el SGSI para la empresa de transporte la Ecuatoriana, bajo la norma ISO 27001. Esta propuesta, representa un enfoque de innovación, que aporta gran confiabilidad en el servicio prestado por la organización (Beynon, 2015).

En cuanto a las limitaciones del desarrollo de este proceso, es la falta de culturización empresarial, un SGSI, debe ser constantemente actualizado ya que los riesgos siempre están latentes y nunca dejan de aparecer, por lo que la primera acción será la documentación, en principio diagnosticar y plasmar las falencias, en base a estas, se deberá comenzar con una planificación estratégica, estableciendo los objetivos a corto y largo plazo, para contrarrestar las fallas determinas en el diagnóstico (AudiSec., 2012).

Esto forma parte de la primera etapa de una propuesta para la implantación de un SGSI específicamente a la empresa de transporte la Ecuatoriana, para esto se implementarán y ejecutara una planificación sustentada en 3 pilares claves: el primero las personas, el segundo; los procesos y finalmente la tecnología; si uno de estos pilares, entorpece los requerimientos organizacionales, claramente se verá

afectada la planificación de actividades y procedimientos del diseño (Lara y Corella, 2019)

Capítulo II Marco Teórico

2.1. Conceptualización de la(s) variable(s) o tópico(s) clave

Este capítulo contiene la descripción de la fundamentación teórica y argumentos sobre el SGSI sustentado en los criterios de diversos autores especialistas en el tema con el propósito de sentar las líneas de investigación para el cumplimiento de los objetivos propuestos.

2.1.1 Gestión tecnológica en una organización.

La Gestión tecnológica en una organización es entendida según Jiménez (2017) como “un proceso a través del cual se aplican un conjunto de herramientas que permiten identificar diversas situaciones e implementar cambios dentro de los sistemas informáticos de una empresa” (p.56)

En este sentido refiere Sánchez (2011) que; “la implementación de planes inclinados a gestionar los sistemas informáticos de una empresa, con el propósito de mejorar e innovar los procedimientos internos de tal empresa” (p.34).

En este sentido, determina Castro (2018) “las instituciones y empresas deben implementar gestiones tecnológicas en sus procesos basada en SGSI para proporcionar una alta productividad dentro de sus actividades básicas” (p.87).

Finalmente se considera que, una adecuada gestión tecnológica se considera una estrategia de protección y resguardo de la privacidad de datos e información, de una empresa.

2.1.2 Sistemas de Información (SI)

En cuanto al SI, el autor Andreu (2012), indica que: “El SI comprende una serie de complementos que integran procedimiento, desarrollados en un

determinado entorno en el cual interviene dos elementos correlacionados el usuario y el sistema (computador/programas)" (p.90). Por su parte acota Castro (2018) que estos dos elementos "operan sobre un conjunto de datos de forma estructurada, para la recopilación y distribución de información selectiva indispensable para el funcionamiento de la empresa y su dirección" (p.17).

Actualmente existen diversos sistemas de información, que persiguen el propósito de establecer acciones correctivas dentro de las operaciones de una empresa, a través de una gestión tecnológica adecuada (Beynon, 2015).

Por su parte, Cohen (2015) define que "un SI lo comprenden una indeterminada cantidad de elementos que interactúan entre sí" (p.21). El autor determina que esto, tiene el fin de apoyar las actividades de una empresa o negocio.

Castro (2018) argumenta que para apoyar tales actividades "se requieren para el funcionamiento del SI un determinado conjunto de componentes físicos (computadoras y sus complementos), programas (software), el recurso humano (quien se encarga manualmente del procesamiento de información)" (p.17).

Respecto a estos criterios se concluye que la funcionalidad de los SI, reside en el suministro de datos que poseen las organizaciones para su operatividad (Smith, 2018)

2.1.2.1 Software

El software es definido por Sánchez (2013) como "uno de los mecanismos primordiales para los SI, su importancia es trascendental ya que el ordenador no realizaría ninguna tarea o acción sin su presencia" (p.12) Por tanto se considera que existe diversos softwares, desde programas específicos hasta complejos que son el complemento de los sistemas operativos tecnológicos (AudiSec., 2012)

Por su parte refiere García (2018) que, los profesionales que diseñan distintos softwares “se designan como programadores y hacen usos de lenguajes determinados de programación, por lo que tales lenguajes específicamente para la comunicación entre el usuario y el ordenador” (p.4)

2.1.2.2 Software de seguridad

Respecto a la contextualización del software de seguridad Montecé (2017) primeramente resalta que la seguridad de la información a través del tiempo ha ido evolucionando, debido a las potentes amenazas y riesgos existentes en la actualidad, algunas entidades que utilizan sistemas informáticos aún no han tomado conciencia de lo importante que es para su funcionamiento el cuidado y la seguridad de la información considerada como el bien fundamental. Por tanto (Romero, Figueroa, Vera, & Álava, 2018) define que un programa de seguridad a la información se basa en codificar y proteger archivos electrónicos en un sistema informático (p.19)

Con base en los criterios de Beynon-Davies (2015), cuando se hace referencia al software o programa, se determina que este contiende una cantidad de códigos para ser entendidos y leídos por la máquina a través de diferentes lenguajes como el ensamblador y el de alto nivel” (p,9). Si bien es cierto existen diversos software, sin embargo determina Castro (2018) “al mencionar los que se utilizan para implantar un SGSI, generalmente son los de seguridad tales como codificaciones, password o protección de virus informáticos” (p.13).

2.1.2.3 Virus informáticos

Para López (2018) define que, “el virus se considera un compendio de códigos informáticos programados intencionalmente para instalarse y desplegarse en un sistema operativo (computador) de forma incógnita o sin permiso” (p.11). Otra

definición reside en los criterios de García (2018) el autor determina que virus informático es considerado “un parásito que ataca los archivos o al sector de arranque de un sistema computarizado y que puede multiplicarse causando graves daños” (p.11)

Tal como indica García (2018) estos virus “pueden llegar a afectar considerablemente a los sistemas computarizados mediante su duplicación” (p.29). Ciertamente tienes diversos propósitos determina Castro (2018) estos son; infectar, alteraciones o eliminación de datos, destrucción de sistemas, extracción, migración y robo de información , algunos solo muestran mensajes, pero todos persiguen un propósito en común “propagarse” (p.34)

2.1.3 La estrategia de TI de una organización.

En cuanto a la estrategia de TI de una organización especifica Smith (2018) que esta, “involucra la planificación de un compendio de procesos, gestionados con el fin especifico de adaptarlo a la tecnología de una determinada empresa con el fin de evaluar, clasificar y tomar acciones para establecer una mejora continua” (p.76)

En este sentido determina Ortiz (2019) que la falta de un SGSI, “promueven amenazas latentes a las seguridad de la información de la empresa, y por tanto a no ser conocidos, no se pueden asumir, ni gestionarse y mucho menos ser minimizados a través de una sistematización” (p.45).

2.1.4 Las Tecnologías de Información en la Organización

En relación a las tecnologías de información en la organización Pérez (2018) determina que: “el levantamiento de la tecnología de información (TI) representa un impacto para la organización” (p.34). Respecto a esto considera Pérez (2018) que “hoy en día las organizaciones hacen uso de las TI con una herramienta estratégica

como solución a las falencias y la estructuración de ejes para la competitividad" (p.51).

Argumenta Castro (2018) que: "Al realizar un cambio dentro de una organización y que claramente represente una optimización de sus procesos constituye una decisión estratégica y asertiva para la sostenibilidad de tal organización (p.7).

2.1.5 Planificación Estratégica

Para contextualizar la Planificación Estratégica conocida por sus siglas (PE) Ortiz (2019) define que : "constituye un compendio de acciones con fines evaluativos de forma sistemática en una empresa con el propósito de fijar metas, redireccionar objetivos para mitigar las falencias o puntos débiles en la actividades de una empresa de forma rápida y eficaz"(p.5).

Si bien es cierto dentro de la PE despliegan estrategias para obtener dichos objetivos y delimitando los recursos. Ciertamente en palabras de Terán (2019) "la PE, permite definir lo que se requiere hacer en la organización, en este caso específico de estudio es SGSI como medio de esparcimiento que permitirá evaluar riesgos y oportunidades" (p.29).

2.1.6 El proceso de decisión estratégica y las necesidades de información

En cuanto al proceso de la decisión estratégica, comprende un complemento a la planificación, para planificar se debe decidir. Para Pérez (2018) considera que ""constituye la primera línea de planificación, pues los directivos de una organización deben reunirse para diseñar las estrategias empresariales, y por ende iniciar el proceso de la toma de decisiones estratégica y asertivas" (p.54)

2.1.7 Norma ISO 27000

La normativa ISO 27000 contextualizada por el autor Gutiérrez (2017) determina que, “no es más que un compendio de modelos internacionales basado en la SI, por lo que esta familia sujeta una cantidad determinada de buenas prácticas para la implantación, control y mantenimiento y sobre todo mejora continua del SGSI” (p.29).

“Las empresas hoy en día buscan regir sus procesos basados en la SI con el propósito de preservar sus activos críticos; gestionar los riesgos de manera eficaz, y así contribuir a la mejora y establecimiento de una relacion de confianza con los clientes” (Pérez, 2018)

La normativa ISO permite a la organización establecer un orden en sus actividades y procesos con el fin de hacerlas certificables. Específicamente la ISO 27001 establece tal orden y organización, pero directamente en los sistemas informáticos de una empresa determinada para certificarla como una organización que implanta sistemas y gestiona la seguridad de sus documentos digitales y principales activos informáticos (Balaguer, 2014).

La normativa además de ser aplicable a todo tipo de empresas en cuanto a sus políticas, actividades de planificación, y responsabilidades, según Ortiz (2019) “se caracteriza por asegurar la privacidad e integridad de los datos y de la información, así como de los sistemas que la procesan creando una relacion de confianza del cliente y la empresa” (p.7).

2.1.8 Contextualización

En toda empresa, es evidente que sus activos son valiosos y que su resguardo, depende de las políticas de seguridad que tal organización implemente (Cohen, 2015).

Respecto a la importancia de implementar políticas de SI, refiere Castro (2018) que; “es importante que las empresas planifiquen estrategias basadas en la SI pues hoy en día la tecnología permite evaluar amenazas, definir estrategias y objetivos y mitigar impactos” (p.23)

Si bien es cierto el desarrollo de nuevas tecnologías en un aspecto positivo, ha permitido diagnosticar amenazas y vulnerabilidades y crear estrategias en función de estas, para disminuir el impacto, también ha aumentado los riesgos debido al acceso de información (Pérez, 2018)

Por otra parte, partiendo de las estipulaciones de Pérez (2018):

> “debido al desarrollo de nuevas tecnologías, muchas personas también disponen de aplicaciones las cuales han vulnerado las políticas de seguridad informativa en muchas organizaciones, por tanto, es trascendental que las empresas no solo apliquen políticas de seguridad informática, sino que se mantengan en constante actualización y realizando planificaciones estratégicas” (p.10)

2.2. Importancia de la(s) variable(s) o tópico(s) clave

En este apartado se detalla la importancia de las variables y tópicos establecidos en el marco teórico se definieron criterios respecto al SGSI.

En cuanto a la gestión tecnológica en una organización se considera un pilar fundamental ya que adopta tecnologías a través de procedimientos innovadores para resguardar el sistema informativo de una empresa.

Por tanto, la importancia de la gestión tecnológica, se debe a que constituye “un conjunto de acciones que hacen posible la identificación de falencias dentro de una empresa, y a partir de estas implementar innovaciones tecnológicas, es decir; se implementa para crear valor en la empresa” (Terán, 2019)

En este sentido, la importancia de la gestión tecnológica reside en que es un “instrumento estratégico que permite el gestionamiento efectivo para el resguardo de datos e información, ante riesgo o vulnerabilidades de la empresa” (Beynon, 2015)

Así mismo, el SI forma parte de la gestión tecnológica, pues la importancia del sistema es que este opera sobre un compendio de datos de una empresa, , para la recopilación, proceso y distribución selectiva de la información que maneje los procesos habituales de una empresa.

Estos elementos intervienen entre sí, con el propósito de ayudar a los procedimientos de una empresa o negocio. Por tanto Smith (2018) define que “constituyen los componentes; para poner en marcha políticas de seguridad, se puede determinar que estos son; el componente físico (equipos de cómputo y sus complementos), programaciones (Manejo y control de datos), el recurso humano (quienes ejecutan tales programaciones)”(p.44)

En síntesis, la importancia y principal función de los Sistemas de Información, es proveer datos que precisan las diferentes sociedades para su desarrollo por lo que esta información debe estar protegida (Smith, 2018)

En este mismo orden, una vez identificado la relevancia y relacion entre la gestión financiera y los sistemas de información es necesario destacar la importancia de lo que representa un software de seguridad para ello, por tanto Montecé (2017) resalta que, la seguridad de la información está expuesta a amenazas y riesgos existentes en la actualidad, algunas entidades que utilizan

sistemas informáticos aún no han tomado conciencia de lo importante que es para su funcionamiento el cuidado y la seguridad de la información considerada como el bien fundamental.

Por tanto, Romero, Figueroa, Vera, y Álava (2018) determina que toda empresa debe contar con un software de seguridad pues este les permite detectar las amenazas o riesgos en los sistemas de información, por tanto, es importante ya que es el encargado de proteger la información acopiada en los SI (Andreu, 2012).

Para entender la importancia del software de seguridad es menester contextualizar que una de las amenazas a los sistemas de información de una empresa es el virus informático entendido como un programa escrito que con un determinado propósito irrumpen en un sistema para acceder a información u ocasionar daños. (SOPHOS, 2019)

Por tanto, esta amenaza es la que mayormente interfiere con los sistemas de información. Entendido este concepto se puede apreciar la importancia de que las organizaciones cuente con un programa de seguridad que no solo resguarde la información, sino que elimine la amenaza, lo que se conoce como software de seguridad. (López, 2019)

Otra variable clave a resaltar es la estrategia tecnológica implica los procesos de gestión que con base en Sánchez (2011) esto se caracteriza por “la implementación de planes inclinados a gestionar los sistemas informáticos de una empresa, con el propósito de mejorar e innovar los procedimientos internos de tal empresa” (p.34).

Respecto a la revolución de la tecnología de información (TI) tiene gran importancia por su impacto en las empresas que se acogen a estas políticas pues constituyen elementos fundamentales para establecer lineamientos para la

competitividad y de esta manera garantizarle al publico interno y externo la seguridad en las documentaciones que maneja (Beynon, 2015)

Por tal motivo la tecnología de información se relaciona con la Planificación Estratégica conocida como PE donde su importancia reside en el despliegue de estrategias para gestionar la seguridad de la información como medio de expansión, en donde se valoren y evalúen los riesgos u oportunidades.

Acota Pérez (2018) que parte de la importancia de las planificación estratégica se debe a que se considera “un valioso instrumento de diagnóstico, estudio, valoración de tipo reflexivo para tomar decisiones efectivas de forma colectivas, en torno a las situaciones que se presenta y en pro de ello implantar medidas correctivas y así lograr el máximo de eficiencia y calidad de sus servicios”(p.33).

Ahora bien en lo que respecta a la importancia del proceso de decisión estratégica y las necesidades de información vale destacar que, según Castro (2018) “se considera como un elemento importante más que debe estar presente al momento de diseñar tales estrategias, en primer lugar debido a lo relevante de la información a resguardar así como los registros a medida de que la organización y la TI evolucionen ” (p.45).

Parte de su relevancia reside en cambiar la información disponible en acciones, para que junto a la planificación y la toma de decisiones se puedan determinar politices de resguardo para la empresa en donde se establece el proceso” (Ortiz, 2019).

En otro orden, ya identificada la importancia de la gestión de la información así como los sistemas y planificaciones estratégicas, se puede enunciar la relevancia que tiene la certificación de todos estos elementos, una vez que la

organización implemente y gestione todos estos procesos, podrá optar por la certificación de la norma ISO 27000 es una norma aplicable a todo tipo de organizaciones y a su estructura organizativa, basada en las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos (ISO27001, 2009).

Es importante porque permite establecer buenas prácticas para la implantación de SGS en las empresas y que estas puedan regir sus procesos en la normativa, asegurándose de establecer políticas de seguridad sobre sus activos (documentaciones y registros) (Beynon, 2015).

Hasta ahora se ha destacado que la gestión de la información es necesaria para el establecimiento y certificación de la norma ISO27001 en una organización, “por tanto se considera que la documentación y registros personales y privados que maneja una empresa se considera un activo muy valorado, más sino se gestionan estrategias para mantener la integridad y privacidad en sus sistemas informáticos “ (Cohen, 2015).

Por tal razón el perfeccionamiento de las tecnologías permite crear estrategias de resguardo de la información, determina Pérez (2018) que: “Se exponen a nuevas amenazas cada día” (p.67). “Lamentablemente sin el correcto establecimiento de líneas, políticas y medidas de seguridad se hace muy fácil tener acceso a las herramientas que permiten a personas no autorizadas llegar hasta la información protegida con el propósito de causar daños a la empresa que contiene tales documentos” (Esguerra y Ortiz, 2018)

“La implantación de un SGSI, basado en la norma permite establecer políticas, procedimientos y controles con objeto de disminuir los riesgos de su organización” (ISO27001, 2009).

2.3. Modelos de la(s) variable(s)

En cuanto al modelo de las variables empleado en este estudio, es de tipo cualitativo. Las variables cualitativas expresan cualidades o atributos de los agentes, objeto y sujetos de estudio. (Parra, 2019)

“En este estudio particular, se implementó las variables proxy o cualitativas que, normalmente recogen aspectos de la presencia o no de determinado atributo” (Hernández, 2016).

De acuerdo con Parra (2019), “las variables cualitativas se agrupan en la naturaleza de tales realidades y su dinámica, mientras que las variables cuantitativas se implementan para determinar la fuerza que tienen las variables”. (p.9)

En este sentido las variables dependientes establecidas para este estudio se basan en :

Tabla 1. *Operacionalización de variables*

Varaible Independiente	**SGSI** **Definición conceptual:** permite a las empresas evaluar los riesgos y definir las aplicaciones de control necesarias para poder eliminarlos o minimizar sus consecuencias negativas **Definición Operacional:** enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio **Indicadores**: - Analisis de riesgo - Plan de acción . Gestión tecnologica **Norma ISO 27001** **Definicion conceptual**: norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan **Definición operacional:** indica que la organización se encuentra en el deber de planificar, implementar y controlar los procesos que sean necesarios para cumplir cada uno de los requisitos de seguridad de la información e implementar las acciones **Indicadores:** - Control de los procesos y sistemas informaticos - Certificación de las organizaciones

Información Digital

Definición concpetual: Son medios de comunicación y utilización de aplicaciones de forma electronica

Variable Dependiente

Definición operacional: Se refiere a la interacción o intercambio que se realiza entre usuarios con los datos digitales y se medirá por los ingresos a los sistemas informáticos

Indicadores:

- Promedio de ingreso de documentos digitales.
- Conectividad de unarios a los aplicativos.

Nota: Variables utilizadas en la investigación. Jácome (2021)

2.4. Análisis comparativo

Las organizaciones, empresas o compañías, actualmente deben estar preparadas ante cualquier amenaza informática en sus sistemas. Por tanto es trascendental que manejen políticas para el resguardo de información así como sistema de detección ante cualquier amenaza o vulnerabilidad a su integridad y privacidad (Beynon, 2015)

En este sentido es fundamental que las empresas cuenten con sistemas aleatorios que les posibiliten la identificación, valoración de posibles riesgos y amenazas, y que de este modo puedan realizar planificaciones estrategicas para mitigar los impactos (ISO27001, 2009)

De acuerdo con Sánchez (2011); para que una empresa sea totalmente competitiva “debe contar con politicas y certificaciones en cuanto a la normativas legales, siendo unas de estas la implementacion de un SGSI para resguardar los activos vitalesy así establecer controles pertinentes para la prevención de riesgo y gestión de impactos” (p.225)

Este estudio comparativo se basa en el análisis de las herramientas que utiliza y demanda el SGSI para hacer una empresa certificable en sus politicas de sistemas informáticos. Por tal razón se destaca que la normativa ISO 27001, representa un marco de referencia para la planificación estrategica de la seguridad informática de una emporesa, en ella se define los objetivos y metas, políticas y actividades responsables, prácticas, recursos y procedimientos para determinar las políticas del SI de una empresa (Esguerra y Ortiz, 2018)

En este sentido se puede especificar que esta normativa internacional empleada para la GR de las empresas, detalla los principales requerimientos para la implantación de controles de seguridad, adecuados a las necesidades de la organización (ISO27001, 2009)

Por otra parte en lo que respecta a los modelos de los SGSI, es menester determinar que “estos no solo ayudan a identificar amenazas, sino que a partir de estos permiten implementar politicas y acciones dirigidas a establecer la seguridad en los registros y documentos de una empresa” (Sánchez, 2011)

Si bien es cierto y de acuerdo con ICONTEC (2013), “la normativa ISO 27001 suministra los requerimientos para el diseño, implantación, ,mantenimiento y mejora continua de los sistemas de seguridad de una empresa” (p.73) Estos estándares precisamente se basan en auditorias, gestiones y controles internos y externos así

como la valoración de recursos y presupuestos para que una empresa pueda llegar a certificarse y alcanzar sus metas de confiabilidad ante su público objetivo.

La gestión de la SI claramente se debe llevar a cabo, a través de un proceso sistemático, de acuerdo con Sánchez (2011):

> “debe ser documentado y conocido por todo el público interno de la empresa, debe poseer un enfoque sustentado en sus procesos y de acuerdo a los requerimientos de la normativa ISO, con el propósito de destacar cuales serían los controles y mecanismos adecuadas para el desempeño y efectividad de tal implementación” (p.39)

Establecido todo respecto a los elementos de la implementación de un SGSI en una determinada empresa u organización así como los requerimeintos que deben cumplirse y los alcances de la normativa ISO, se hace evidente determinar las acciones y métodos dentro de este estudio, para llevar a cabo la implementación. Como primer aspecto se destaca el modelo PHVA que de acuerdo con Esguerra y Ortíz (2018), “es un ciclo que consta de cuatro etapas; la primera planear, seguidamente hacer y finalmente verificar y actuar” (p.108)

Así mismo el SGSI determina una serie de procedimeintos, que de acuerdo con Sánchez (2011):

> “se nivelan en cuatro etapas; la primera en el diseño de un manual de seguridad, la segunda elestablecimeinto de procedimimientos de gestión, la tercera las acciones operativas y la última en donde se visualizan los registros y documentos como principales activos a resguardar” (p.95)

Por lo que se concluye que estos enfoques que sustentan el SGSI comprenden un conjunto de acciones positivas que le permiten a la empresa una

ventaja competitiva. Por tal motivo se realiza este análisis comparativo, con el propósito de elegir un modelo en particular, referencial para establecer los procedimientos óptimos que debe implementar la empresa de transporte la Ecuatoriana para la aplicación de políticas de seguridad.

2.5. Análisis crítico.

Con base en el análisis comparativo y partiendo de este es menester considerar la relación existente en establecer el SGSI para la certificación de la normativa ISO 27001, por ello, para establecer esta propuesta se considera fundamental emplear el modelo PHVA, como se ha indicado anteriormente, Urbina (2017) “constituye un ciclo de cuatro fases; planificar, hacer, verificar y actuar, esto permite realizar un diagnóstico para determinar las necesidades a cubrir, con el propósito de establecer un plan de acción sobre estas” (p.87)

Así mismo cabe destacar que Romero et al. (2018) determina; “es necesario establecer un esquema sobre las amenazas de los activos diagnosticados y de este modo realizar una planificación dirigida a contrarrestar el impacto de los diferentes activos” (p.54)

Este análisis permite visualizar la importancia de establecer, las amenazas y riesgos que existen sobre los activos de la empresa de transporte la Ecuatoriana con el propósito de diagnosticar y medir las falencias internas y que tipo de políticas implementan. Permitiéndole a la empresa estar alerta ante cualquier circunstancia apoyándose en los mecanismos de los SGSI y de la normativa ISO 27001 como una guía fundamental para el análisis de riesgo y en base a esto establecer el plan de acción.

Por tal motivo, hoy en día cualquier organización debe estar en presta y estar al corriente de las estrategias para preservar sus activos informáticos y electrónicos,

tal como la implantación de SS que permitan una valoración y gestión de riesgos que hagan posible la identificación de amenazas a la que puedan estar expuesta tales activos de la organización. Dentro de las acciones de valoración, se debe tener en cuenta la frecuencia de ocurrencia de tales amenazas y determinar el impacto que tendría en la organización en caso de la ejecución las amenazas previamente diagnosticadas, reduciendo los riesgos; y por el contrario, considerar que, el análisis de riesgo es un procesamiento analítico donde interceden una cantidad indeterminada de variables por lo que una sola metodología no es aplicable a todas las organizaciones.

Bajo esto criterios se recomienda que la organización se pueda apoyaren las normas ISO/IEC 27005:2008, ISO/IEC 27001, ISO/IEC Guía 73:2002 que se utilizan como guía para que la organización establezca su propia metodología de análisis de riesgos y finalmente pueda implantar su propio SGSI para el análisis de riesgo y establecer el plan de acción.

Capítulo III Marco Referencial

3.1. Reseña histórica

La empresa de transporte la Ecuatoriana dio paso su constitución legal el 7 del mes de Julio del año 2007 en el DMQ- Ecuador, su domicilio legal reside en el Sector Centro Norte de la ciudad, con dos sucursales ubicadas en la provincia de Santo Domingo y Guayaquil. Opera jurídicamente bajo la figura de persona natural con un capital inicial de ($35.000).

En cuanto a su trayectoria, la empresa de transporte la Ecuatoriana ha implementado dentro de su eje competitivo estrategias de marketing referencial con el fin de potenciar su mercado.

La empresa de transporte coloca a disponibilidad de todos sus clientes los siguientes servicios:

Tabla 2 *Servicios de la empresa de transporte la Ecuatoriana*

Servicios Empresa de transporte la Ecuatoriana	Seguro de Carga
	Servicio de Puerta a Puerta
	Vehículos nuevos que garantizan Eficiencia y Rapidez
	Vehículos equipados con RASTREO Satelital
	Furgones Cerrados
	Viajes en Convoy
	Entrega de su Mercadería en 24 horas
	Precios Negociables
	Logística

Nota: Manual de procesos de la empresa de transporte la Ecuatoriana. (2020)

En cuanto al personal que labora para la empresa de transporte la Ecuatoriana se conforma por 28 empleados incluyendo el área operativa y administrativa. Así mismo la misión y visión de a empresa se enuncia a continuación:

Misión

> Prestar un servicio de calidad en el transporte de carga cumpliendo con los estándares de seguridad, garantía y tiempo de entrega acordado con nuestros clientes.

Visión

> Llegar hacer una empresa de transporte de carga reconocida a nivel nacional, con una sólida estructura organizacional, políticas de seguridad acorde a las exigencias y expectativas en nuestros empleados, clientes y proveedores.

3.2. Presentación de actores

En cuanto a la presentación de actores, según la normativa ISO 27001 y los criterios de Balaguer (2014) " los responsables de realizar las acciones para la implementación del SGSI, deben profesionales y calificados, sobre todo capacitados y con experiencias previas para un logro exitoso del proyecto" (p.98)

En este sentido se puede identificar que, los actores y sus funciones son los descritos en la siguiente tabla:

Tabla 3*. Presentación de actores*

Actor/cargo	***Función***
Proveedor del servicio	Determina todas las aptitudes necesarias para cada rol durante la gestión de la Seguridad de la Información. Asegura que los trabajadores son conscientes de la relevancia y la importancia que tienen sus actividades en el más amplio contexto del negocio y además, de cómo contribuyen al cumplimiento de los objetivos establecidos por el Sistema de Gestión de Seguridad de la Información. Mantiene actualizados los registros en los que se incluya la educación, la formación, las habilidades y la experiencia de los trabajadores. Provee de capacitación a los empleados para satisfacer las necesidades de la organización. Realiza una evaluación de efectividad de todas las actuaciones que se han realizado.
Director del proyecto	Es el mayor responsable del proyecto. Hace de enlace entre el cliente y la organización. Es el encargado de planificar los costes y los plazos que se fijan para ejecutar y controlar el SGSI.

Jefe de equipo	Responsable de desarrollar las tareas que han sido asignadas al equipo, dirige a los empleados, asigna tareas, etc.
Analista	Encargado de realizar el análisis de todos los requisitos exigidos por los clientes, además de minimizar la dificultad, conocer el resultado del análisis, etc.
Diseñador	Encargado de realizar el diseño del proyecto que se quiere realizar. tendrán como base los análisis que se realizan por los analistas, además intentan ajustarse lo máximo posible a todas la funcionalidad y requisitos que se exigen.
Programadores	Encargados de implantar el código fuente y el objetivo mediante el análisis y el diseño que ha sido realizado por parte del diseñador, además debe recopilar toda la información que resulte útil, manejable y sencilla para el Sistema de Gestión de Seguridad de la Información.
Probadores de software	Encargados de recopilar las pruebas sobre el Sistema de Gestión de Seguridad de la Información una vez se han finalizados los procesos anteriores, se deben encontrar los fallos que no hayan sido solventados y las futuras incidencias que se pueden producir durante la utilización del SGSI, además tiene que verificar que todas las funciones que se han requerido hayan sido implementadas.

Instaladores	Encargado de instalar los softwares necesarios para que la implementación del Sistema de Gestión de Seguridad de la Información ISO 27001 se realice de forma correcta.
Auditor interno	Realiza la auditoría final del proyecto, con lo que se podrá comprobar si se ha realizado de forma correcta la implementación del SGSI ISO 27001. Se emite un informe que aporte fiabilidad y seguridad.

Nota: Cuadro de los actore y sus funciones. (Esguerra y Ortiz, 2018)

La estructura de los actores en la organización será la siguiente:

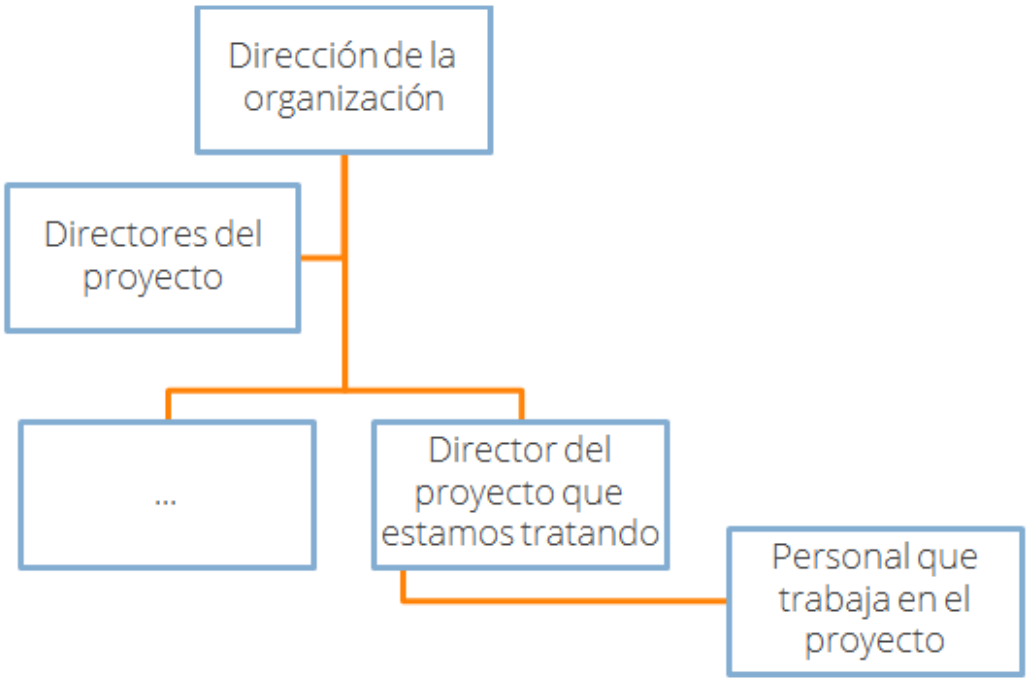
Figura 1. *Organigrama de los actores de la organización*

Nota: Estructura organizativa de los responsables de la organización

En este sentido y bajo la estructura de los actores de la organización el jefe del proyecto es el responsable de planificar y ejecutar, así como de establecer controles en todo el proyecto.

En el siguiente gráfico se puede identificar cómo se organiza la empresa:

Figura 2*. Estructura funciona de los actores de la organización*



Nota: Esquema de la estructura funcional de la organización y la responsabilidad de los actores. (Esguerra y Ortiz, 2018)

Como se observa en organigrama, la dirección de la organización es la responsable de establecer controles durante la duración del proyecto. Cada departamento de actividades del proyecto contará con un director que le permita encargarse de la operatividad del mismo.

3.3. Diagnóstico sectorial

En la fase de diagnóstico sectorial, se implementan objetivos, estrategias y el alcance de la empresa con el fin de definir los parámetros, lineamientos para dar inicio a la planificación del SGSI.

Si una empresa conoce totalmente su funcionamiento, actividades y operaciones y ha fijado su misión, visión y políticas con el propósito de implementar planificaciones estratégicas, está aplicando un diagnóstico sectorial. Si bien es cierto, en palabra de Andreu (2012) “este tipo de diagnóstico se basa en el estudio personalizado de cada

sector operativo de la empresa y permitirá valorarla internamente para a partir de los resultados poder establecer directrices que permita hacer frente a las falencias encontradas” (p.67)

Por tal motivo en el inicio de este capítulo se visualizan todos los aspectos relevantes de la empresa de transporte la Ecuatoriana, teles como su figura jurídica, numero de empleados, organigramas de las secciones y sectores activos de la empresa, presentación de sus actores principales, así como su misión y visión, con el fin de poder obtener un análisis preliminar de la situación actual de la empresa. En función de esto a continuación se evidencian sus políticas, directrices estratégicas e identificación de sus procesos.

- ***Políticas de gestión:***

La empresa la Ecuatoriana se caracteriza por prestar servicios de transporte de carga con los más altos estándares de calidad y seguridad, un personal competente y una estructura adecuada lo que ha permitido establecer un arduo compromiso con sus clientes a través de las siguientes políticas de gestión

Figura 3. Políticas de gestión

- Cumplir con las necesidades y exigencias de sus clientes y partes interesadas.
- Aplicar controles para eliminar o minimizar los riesgos presentes en los sitios de trabajo, procurando con ello prevenir lesiones, incidentes y enfermedades laborales en sus trabajadores, contratistas y visitantes.
- El fomento de la adopción de estilos de vida y trabajo saludables.
- Prevenir o minimizar los impactos ambientales asociados a la generación de residuos sólidos reciclables y peligrosos, consumo de recursos naturales y derrames de sustancias químicas.
- Cumplir con los requisitos legales vigentes y requisitos de otra índole aplicables a las actividades desarrolladas por la organización.
- Mejorar continuamente la eficacia del desempeño del sistema de gestión en Seguridad, Salud Ocupacional, Ambiente y calidad.

Nota: Políticas de gestión de la empresa de transporte la Ecuatoriana. (2021)

Para el éxito de estas políticas, la empresa de transporte la Ecuatoriana posee recursos humanos competentes así como tecnológicos, físicos y económicos para el desarrollo de esta gestión y el diseño de un SGSI.

En cuanto a sus técnicas, cabe destacar que al establecer la misión, visión y políticas, permite la extracción de las ideas principales y factores claves para focalizar las directrices estratégicas que a continuación se mencionan: :

Tabla 4. *Directrices estratégicas*

No.	DIRECTRICES ESTRATEGICAS
1	Líder a nivel regional en la prestación del servicio de transporte terrestre especial de pasajeros.
2	Personal competente en la prestación del servicio de transporte terrestre especial de pasajeros.
3	Satisfacción de los clientes.
4	Cumplimiento de los requisitos legales aplicables al sector transportador en Colombia.
5	Mejoramiento continuo de los procesos.
6	Empresa segura y confiable para los trabajadores y los clientes.
7	Cumplimiento de los requisitos ambientales.

Nota: Directrices estratégicas de la empresa de transporte la Ecuatoriana. (2021)

En cuanto a la vinculación por perspectiva, referidas dentro de la directriz estratégica responde a los métodos del BSC, incluyendo el recurso humano, proceso, clientes y recursos económicos. A continuación, se evidencia la relación de tales perspectivas:

La vinculación por perspectivas se relaciona a continuación:

Tabla 5. Vinculación por perspectiva

No.	DIRECTRICES ESTRATEGICAS	PERSPECTIVAS
1	Líder a nivel regional en la prestación del servicio de transporte en la ciudad	**Financiera**
2	Empresa segura y confiable para los trabajadores y los clientes	**Financiera**
3	Satisfacción de los clientes	**Clientes**
4	Cumplimiento de los requisitos legales aplicables al sector transportador en Ecuador	**Procesos**
5	Mejoramiento continuo de los procesos	**Procesos**
6	Cumplimiento de los requisitos Ambientales	**Procesos**
7	Personal competente en la prestación del servicio de transporte terrestre especial de pasajeros	**Talento Humano**

Nota: Vinculación por perspectiva de la empresa de transporte la Ecuatoriana. (2021)

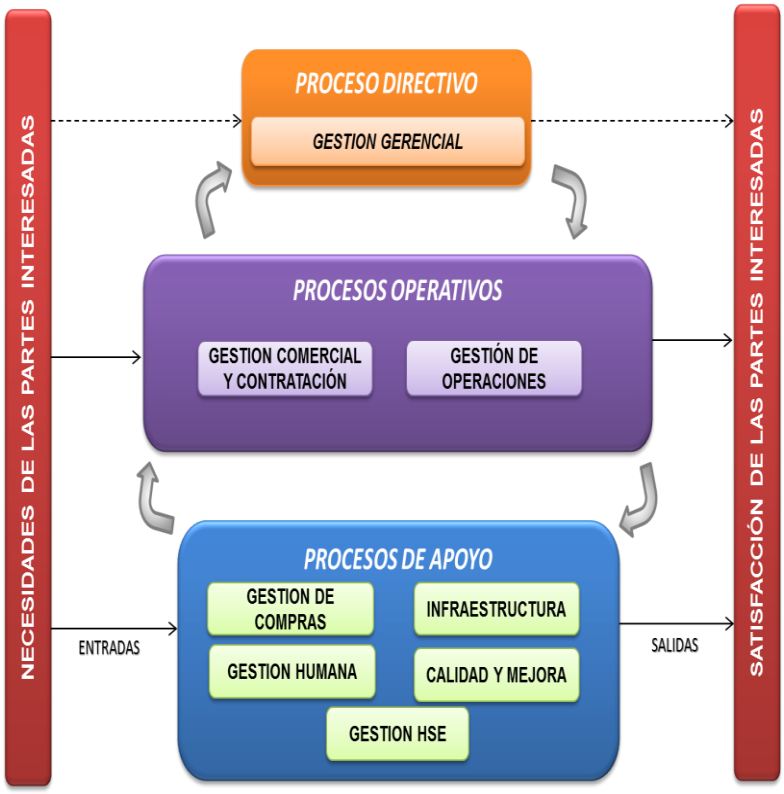
Estas líneas estratégicas consideran Sánchez (2011) “es la etapa donde se planifica la responsabilidad del personal en concordancia a los productos, procedimientos, sistemas de apoyo y metas de la organización, delimitada por el establecimiento de objetivos estratégicos y la identificación de procesos (p.7)

- ***Identificación de procesos:***

Con base en Ortiz (2019), “se considera un proceso al compendio de actividades interrelacionadas hacia determinados elementos con el fin de obtener resultados” (p.59)

Por tal razón al hablar de identificación de procesos se determina como las estrategias de apoyo que permiten el análisis de todos los sectores de la empresa para desarrollar planificaciones que contrarresten las falencias encontradas, este proceso consta de:

Tabla 6. Identificación de procesos



Nota: Identificación de procesos. Sánchez (2011)

Capítulo IV Resultados

4.1. Diagnóstico

Este diagnóstico se sustenta conforme a los requerimientos de la normativa ISO 27001 con el propósito de establecer un conjunto de mecanismos dentro de la empresa para prepararla para la implementación del SGSI y su futura certificación.

En este sentido en la figura 3 se evidencian los bienes a proteger en la empresa de transporte la Ecuatoriana

Figura 4. Identificación de los bienes a proteger

Nota: Identificación de los viene de la empresa de transporte la Ecuatoriana a proteger. Jácome (2021)

Respecto a estas estipulaciones en la siguiente tabla se establece el diagnostico sustentado en la ISO 27001 de la empresa de transporte la Ecuatoriana.

Tabla 6. Requisito normativo- diagnóstico actual ponderado

REQUISITO NORMATIVO	PORCENTAJE DE CUMPLIMIENTO
4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**26%**
4.1 Requisitos generales	20
4.2 Establecimiento y gestión del SGSI	21
4.3 Requisitos de la documentación	37
5. RESPONSABILIDAD DE LA DIRECCIÓN	**59%**
5.1 Compromiso de la dirección	60
5.2 Gestión de los recursos	58
6 AUDITORÍAS INTERNAS DEL SGSI	**10%**
7 REVISIÓN POR LA DIRECCIÓN DEL SGSI	**7%**
7.1 Generalidades	10
7.2 Elementos de entrada para la revisión	0
7.3 Resultados de la revisión	10
8 MEJORA DEL SGSI	**10%**
8.1 Mejora continua	10
8.2 Acción correctiva	10
8.3 Acción preventiva	10
PORCENTAJE DE CUMPLIMIENTO GENERAL	**22,40%**

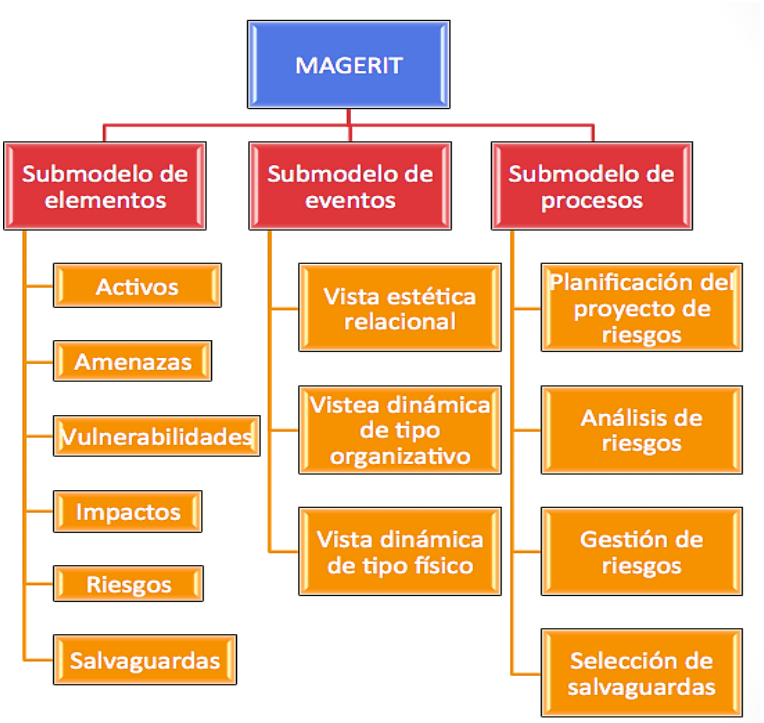
Nota: Diagnóstico realizado en base a la norma ISO 27001. Jácome (2021)

El método seleccionado para esta evaluación y análisis de riesgo fue el MAGERIT con el fin de mejorar los aspectos internos de la organización La metodología seleccionada para la evaluación de riesgos es MAGERIT. Sin embargo, con base al porcentaje de cumplimiento expresado en la tabla 6 como requisitos normativos, se visualiza que la empresa de transporte la Ecuatoriana solo cumple un 22,40% para la implementación de un SGSI y certificación de la normativa ISO 27001.

Determinando que su cumplimiento es muy bajo lo que apoya el desarrollo de esta propuesta.

A continuación, la figura 4 se establece el esquema de valoración de riesgo en base a la metodología MAGERIT:

Figura 5. Metodología MAGERIT



Nota: Esquema de implementación de metodología Magerit. (Marquina, 2012)

- Sub Modelo de Elementos: activos, amenazas, vulnerabilidades, impacto, riesgo, salvaguarda.
- Sub Modelo de Eventos: dinámico físico, dinámico organizativo y estático.

- Sub Modelo de Procesos. análisis de riesgo, planificación, gestión de riesgo y selección de salvaguardas.

Las fases para la implementación de la Metodología MAGERIT, según Marquina (2012) son las siguientes (ver matriz – tabla):

Tabla 7. Fases para la implementación del método MAGERIT

FASES PARA LA IMPLEMENTACION	
FASE 1	Toma de datos y procesos de información: va de la mano con el alcance definido para el SGSI, y se deben tener en cuenta los procesos que lleva a cabo la organización y analizar los riesgos que puedan interferir en los procesos críticos; también se debe precisar a qué nivel de detalle se debe llegar.
FASE 2	Establecimiento de parámetros: se deben identificar los parámetros que se utilizarán durante todo el proceso de análisis de riesgos, los cuales son: Valor de los activos: se asigna una valoración económica a todos los activos de la Entidad
FASE 3	Análisis de activos: identificar cuáles son los activos que posee la empresa y que necesita para llevar a cabo sus actividades; debe ir acorde con el alcance definido. Los activos se pueden clasificar en: físicos, lógicos, de personal, de entorno e infraestructura, intangibles.
FASE 4	Análisis de amenazas: amenazas son

	aquellas situaciones que podrían llegar a darse en una organización y que resultarían en un problema de seguridad. Se clasifican en: Accidentes: situaciones no provocadas voluntariamente y que generalmente no pueden evitarse. Errores: situaciones cometidas de forma involuntaria, por el desarrollo de las actividades propias de la empresa, ya sea por desconocimiento o descuido del personal o terceros
FASE 5	Establecimiento de vulnerabilidades: vulnerabilidades son aquellos agujeros que se tienen en la seguridad de una empresa y que permiten que una amenaza pueda dañar un activo. Se debe tener claro que, sin vulnerabilidad, la amenaza no puede dañar un activo y que las vulnerabilidades por sí mismas no provocan daños, sino que estos son siempre provocados por las amenazas
FASE 6	Establecimiento de impactos: los impactos son las consecuencias que provoca en la empresa el hecho de que cierta amenaza, aprovechando una vulnerabilidad, afecte un activo. Al analizar los impactos, se deben tener en cuenta los siguientes aspectos: el resultado de la agresión de una amenaza sobre un activo, el efecto sobre cada activo, el valor económico de las pérdidas

	producidas en cada activo, las pérdidas cuantitativas o cualitativas
FASE 7	Análisis de riesgo intrínseco: el riesgo intrínseco en la metodología utilizada, se toma como el riesgo en la situación actual de la empresa que se analiza. De acuerdo a esto, con los valores analizados en los puntos descritos anteriormente, sólo es necesario multiplicar los valores así: *Riesgo* = Valor del activo × Vulnerabilidad × Impacto
FASE 8	Influencia de salvaguardas: las salvaguardas son los controles de seguridad, para este análisis se clasifican en dos tipos: preventivas (reducen las vulnerabilidades) y correctivas (reducen el impacto de las amenazas). En esta fase se trata de encontrar las soluciones de seguridad que existan en el mercado de ambos tipos.
FASE 9	**Fase 9**. Análisis de riesgos efectivo: se estudia cómo se reducen los riesgos con cada una de las salvaguardas identificadas en la fase anterior, es decir, se calcula el riesgo efectivo que tendría la empresa para cada una de las amenazas identificadas. Este cálculo se realiza de la siguiente manera: Riesgo efectivo = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad

	x Porcentaje de disminución de impacto
FASE 10	**Fase 10.** Evaluación de riesgos: consiste en la toma de decisiones por parte de la empresa sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permiten reducir los riesgos en aquella. Las organizaciones deben pretender disminuir todos los riesgos que han detectado hasta situarlos por debajo del denominado "umbral de riesgos" y que represente un menor costo.

Nota: Aplicación del método MAGERIT a los procesos de la empresa de transporte la Ecuatoriana. Jácome (2021)

Respecto al desarrollo de un SGSI, se el enfoque metodológico MAGERIT para la gestión de los riesgos, conformada por diez (10) fases:

Fase 1. Establecer el alcance del SGSI para el manejo de riesgos de la empresa de transporte la Ecuatoriana:

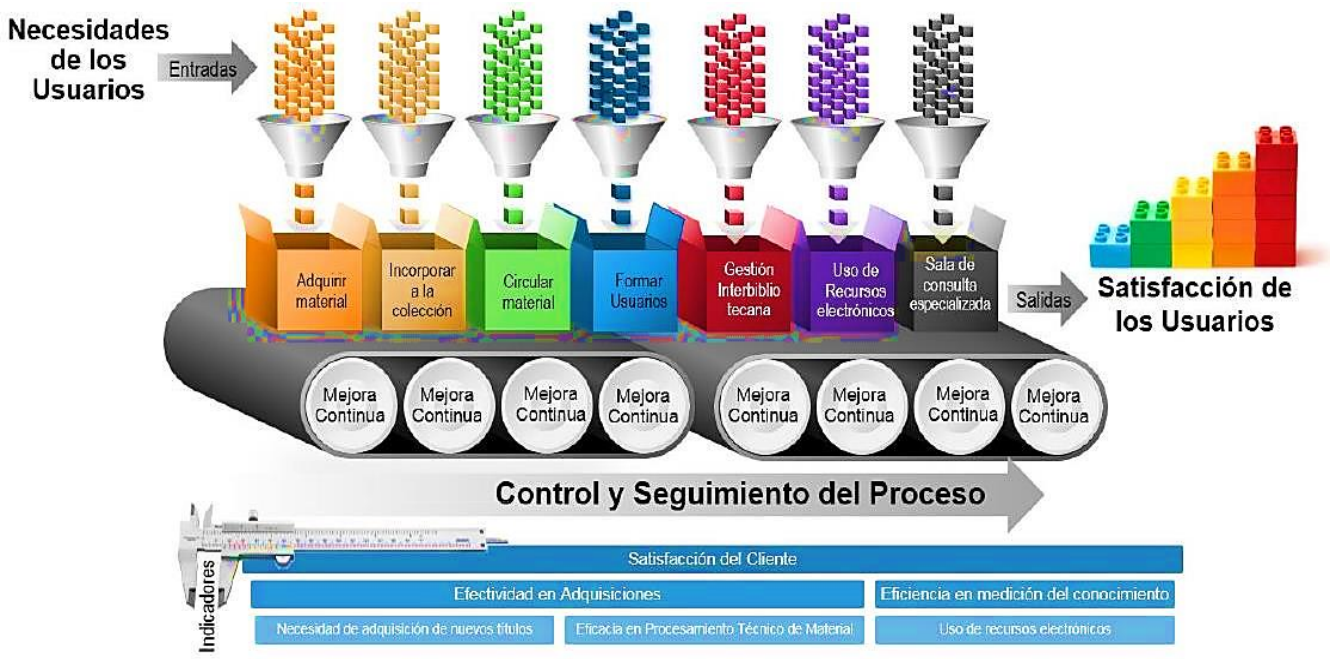
Tabla 8. Procesos de la empresa de transporte la Ecuatoriana

Proceso de Calidad	Sub procesos
1. Selección y adquisición de material físico y electrónico.	Adquisición de Material físico, formularios y fichas de llenado Recepción y Procesamiento información de proveedores Recepción de Material electrónico
2. Análisis, Procesamiento técnico y ubicación del material físico y electrónico	Recepción y Procesamiento de material físico y electrónico Validación de Criterio de Catalogación de Material (confidencial – no confidencial)
3. Registro de usuarios	Solicitud de información de Usuarios de Biblioteca
4. Circulación de material físico y electrónico	Renovación y actualización de información
6. Uso de recursos físico externo	No presenta sub procesos
5. Base de Datos.	No presenta sub procesos

Nota: Procesos de la empresa de transporte la Ecuatoriana. Jácome (2021)

En cuanto a la caracterización y evaluación de los procedimientos que lleva a cabo la empresa de transporte la Ecuatoriana se hallan establecidos en su Manual de procesos, en donde expone que existen siete (7) procesos entre ellos:

Figura 6. Procesos de la empresa



Nota: Necesidad de los usuarios de la empresa de transporte la Ecuatoriana. Jácome (2021)

Con base en los lineamientos establecidos en la norma ISO, cada procedimiento muestra sus entradas, funciones y salidas, con el fin de aseverar la calidad:

Tabla 9. Procesos (entradas y salidas)

Procesos (entradas, funciones y salidas)	Paso 1: Recibe material físico y electrónico, envía a las partes interesadas y/o solicitantes (Directores de Departamento, identificadores de programa, entre otros)
	Paso 2: Recibe las solicitudes y verifica que el formato este diligenciado correctamente: No, se devuelve. Si, informa al solicitante que la solicitud está recibida, y realiza verificación en acervo.
	Paso 3: Verificación en acervo: Si el material se encuentra en el acervo con la cantidad apropiada de ejemplares y actualizado, informa al solicitante que su solicitud no fue admitida y que el material se encuentra disponible en el sistema. No se encuentra en el acervo: Se envía correo al solicitante informando que su solicitud fue admitida y solicita cotización del servicio.
	Paso 4: Recibe y verifica: las cotizaciones de los proveedores que cumplan con las especificaciones de la solicitud y acuerdos comerciales, Se envía la información pertinente y se solicita aprobación para adquisición.
	Paso 5: Recibe las cotizaciones de material solicitado, valida y/o modifica las propuestas y envía la información a Secretaría
	Paso 6: Recibe: de la dirección, la validación de las cotizaciones con aprobación o solicitud de modificaciones.
	Paso 7: Evalúa las cotizaciones y devuelve la aprobación a la secretaría para la adquisición del servicio
	Paso 8: Tramita la solicitud a través del aplicativo ágil.
	Paso 9: Recibe y registra la llegada del material en el formato de Recepción del servicio, completando la información de orden de compra y factura.
	Paso 10: Completa la información del material recibido, en el formato de Recepción de servicio y registra la información en el Formato de Control del servicio.

Nota: Aplicación de procesos (entrada y salidas) de la empresa de transporte la Ecuatoriana. Jácome (2021)

4.2. Diseño de la Mejora

En cuanto al diseño de la mejora es clave considera que, la información puede llegar a ser considerada como uno de los mayores activos de una organización ya que se visualiza como un componente elemental para el desenvolvimiento y documentación de todos sus procedimientos, actividades y registro. Por lo que es fundamental que la empresa sea del sector público o privada implante un SGSI como medida de preservación que garantice estos activos y la continuación de las actividades de esta de forma perdurable.

Con base a los riegos identificados en el planteamiento del problema, se evidencia que la empresa de transporte la Ecuatoriana arroja en sus actividades y procesos internos resultados negativos, a causa de la no implementación de políticas de seguridad, por lo que existen casos de inseguridad. Las causas se deben a la falta de planificación, así como protocolos de seguridad en sus sistemas informáticos y la no existencia de un instructivo o manual de seguridad.

En este sentido, y atendiendo a estos factores este diseño de mejora trata de la creación de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001.

Por tanto si no se implementa un SGSI la empresa corre el riesgos en cuanto al mantenimiento de la confidencialidad, integridad y disponibilidad de la información. Lo que afectaría su imagen corporativa y por ende la confiabilidad y credibilidad de sus clientes.

Propuesta

Objetivo general

- Plantear un modelo SGSI para la empresa de transporte la Ecuatoriana basado en la Noma ISO 27001

Objetivo especifico

- Examinar la gestión y valoración de los riesgos laborales permita medir las amenazas a la información, así como dar seguimiento y monitorización de las operaciones del sistema de la empresa de transporte la Ecuatoriana
- Diseñar un plan de continuidad del negocio, con base en los requerimientos de la Normativa ISO 27001, con el fin de dar inicio al proceso de certificación de la empresa de transporte la Ecuatoriana

Destinatarios

- Empresa de transporte la Ecuatoriana (Directiva- empleados- proveedores- usuarios)

Contenido

- Gestión, valoración y seguimiento de riesgo sobre la disponible de la empresa de transporte la Ecuatoriana
- Plan de continuidad y mejora aplicado a la empresa de transporte la Ecuatoriana para su proceso de certificación basado en la Norma ISO 27001

El método a aplicar para la implementación de la propuesta está basado en una medición sistemática en medir y evaluar los resultados, y establecer un ciclo que permita la mejora continua, en tal sentido se desea aplicar el modelo PHVA cuyo significado se basa en 4 factores; Planear, Hacer, Verificar, Actuar.

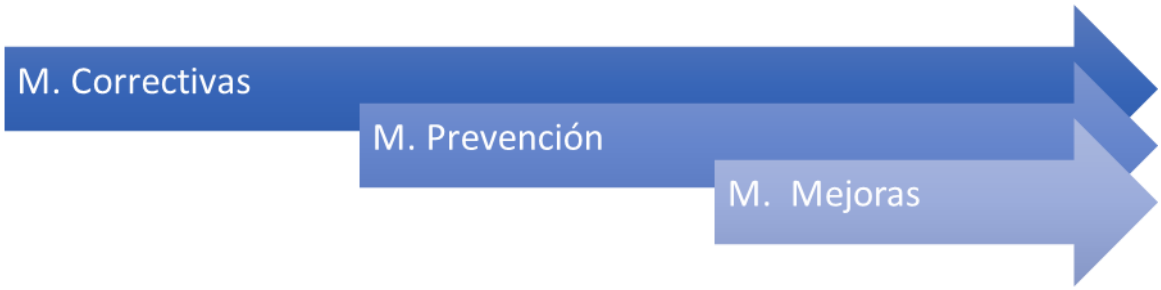
La primera etapa de este Modelo PHVA corresponde a la fase de planeación, para esto se establece un estudio para conocer la cuales son las políticas de seguridad o si existen en la expresa y a partir de ello estimar las medidas correctivas que satisfagan las necesidades de la empresa.

La siguiente fase corresponde a la Ejecución del Modelo PHVA en esta se ejecuta la implantación de controles (técnicos de seguridad seleccionados en la fase anterior.

La tercera fase del Modelo PHVA corresponde al Seguimiento. Esta permite la evaluación de la eficacia de la implantación de los controles establecidos en la fase anterior, por lo que tal efectividad dependerá de los indicadores impuestos para la valoración de tales controles, así como la determinación de las estrategias de mejoramiento continuo

Para esto se emplean 3 tipos de medidas:

Figura 7. Medidas a aplicar a la empresa de transporte la Ecuatoriana



Nota: Medidas aplicar en la empresa de transporte la Ecuatoriana. Jácome (2021)

Estas medidas permiten: Establecer los procedimientos que deben cumplir y de esta forma determinar lo que se desea resguardar como hacerlo, así como los procedimientos a seguir para implantar el SGSI

Para esto es importante establecer una valoración de los recursos económicos y de personal a necesitar en esta etapa ya que esto permitirá tener una idea del importe de diagnostica y aplicar un SGSI

En este sentido la política de seguridad debe basar en estos 5 aspectos:

Figura 8 Políticas de seguridad a considerar para la empresa de transporte la Ecuatoriana

Política de Seguridad	1. Definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo de control que permite compartir la información
	2. Declaración por parte de la Dirección apoyando los objetivos y principios de la seguridad de la información. 3. Breve explicación de las políticas
	4. Definición de responsabilidades generales y específicas, en las que se incluirán los roles pero nunca a personas concretas dentro de la organización. 5. Referencias a documentación que pueda sustentar la política. La Política de Seguridad debe ser un documento completamente actualizado, por lo que debe ser revisado y modificado anualmente.

Nota Políticas de seguridad a aplicar a la empresa de transporte la Ecuatoriana. (AudiSec., 2012)

Estas políticas permitirán que el personal desarrolle nuevas actividades de acuerdo a la normativa y a los términos establecidos.

4.4. Mecanismos de Control

A continuación se detallan los mecanismos de control aplicados para el SGSI de la empresa de transporte la Ecuatoriana bajo la Norma ISO 27001, destacando que estos controles se estructuran con base en los objetivos de la propuesta, de modo que se diseñaron dos por objetivos.

Objetivo específico 1: Analizar la gestión y tratamiento de los riesgos laborales permita medir las amenazas a la información, así como dar seguimiento y

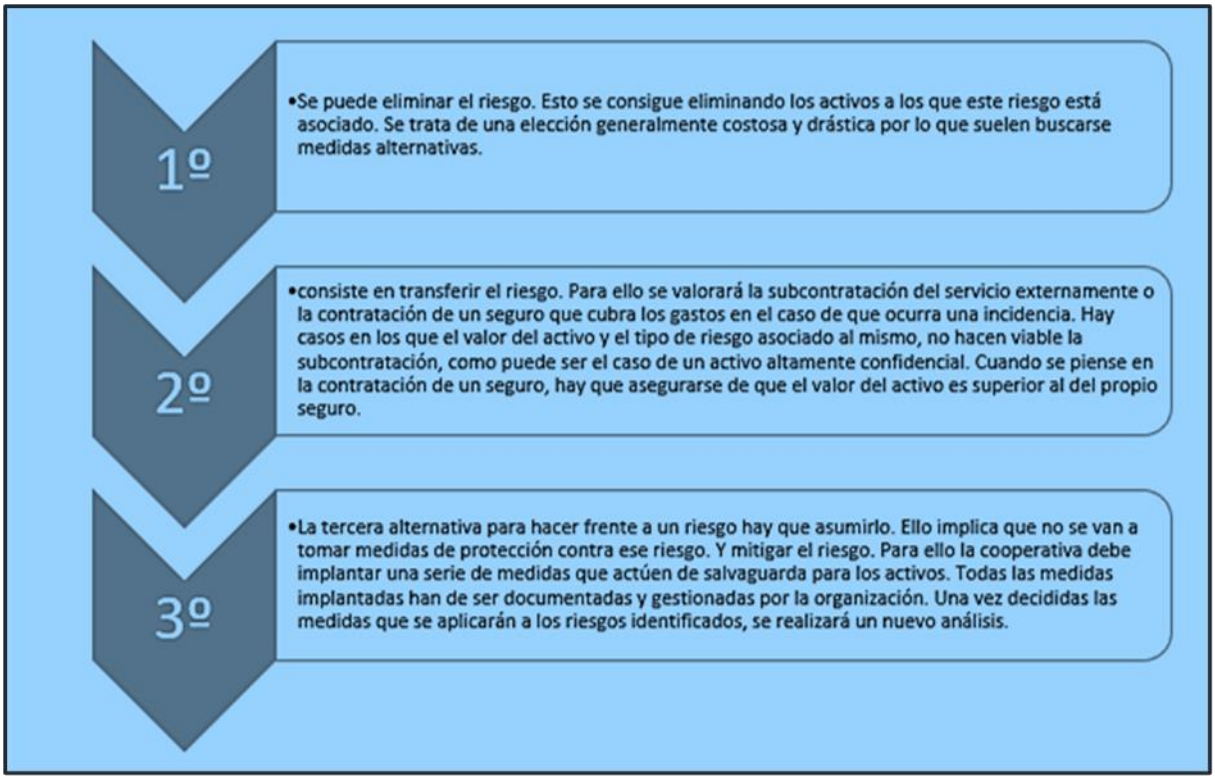
monitorización de las operaciones del sistema de la empresa de transporte la Ecuatoriana.

- **Control 1: Gestión y Tratamiento de los Riesgos. Selección de los Controles.**

Para este control, es necesario gestionar los riesgos, se aplica al determinar cuáles de esas amenazas son riesgos latentes en la empresa de transporte, para esto es elemental considerar cuales deben ser las medidas a tomar de forma oportuna para solventar cualquier situación que se pueda presentar.

Claramente se entiende que tal gestionamiento es parte de los procedimientos que permiten establecer los controles necesarios para la minimización y eliminación de dichas amenazas que puedan afectar en un futuro parte o la totalidad de los activos de información de la organización. Por lo que a continuación se disponen varias iniciativas para afrontar estos riesgos:

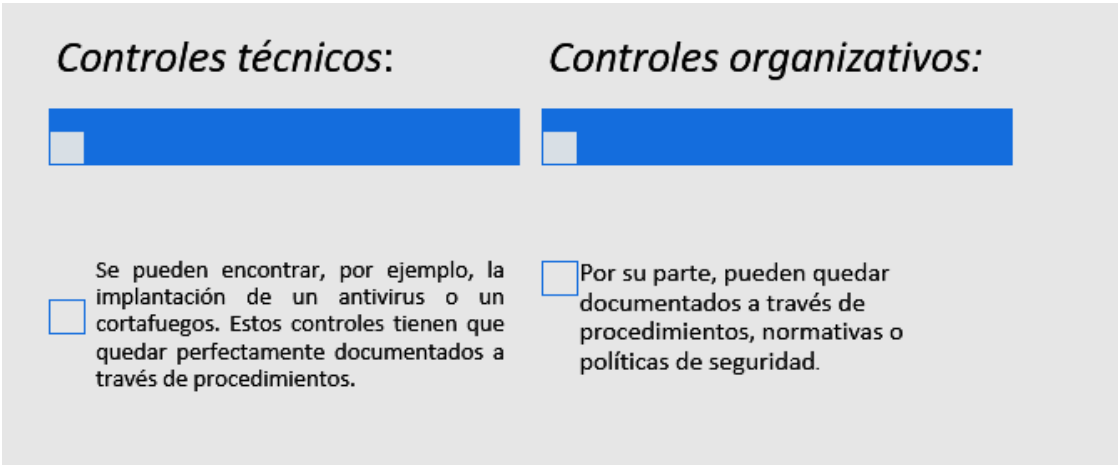
Figura 9. Iniciativas para afrontar los riesgos de la empresa



Nota: Enfoques para contrarrestar los riesgos la empresa de transporte la Ecuatoriana. Jácome (2021)

Existen dos tipos de controles que se complementan: técnicos y organizativos, y que a continuación se determinan en el siguiente cuadro:

Tabla 10. Controles



Nota: Controles técnicos y organizativos en los procesos de la empresa de transporte la Ecuatoriana. Jácome (2021)

Posteriormente se aplicará el diseño de documentaciones y registros que permitan describir las medidas de control a implantar, que detallen los objetivos, indicadores y justificaciones. Con la complementación de un informe de costos de los recursos utilizados para evitar o disminuir el impacto en caso de materializarse tal riesgo.

- **Control 2: Seguimiento, Monitorización y Registro de las Operaciones del Sistema.**

El SGSI debe ser examinado habitualmente para aseverar el cumplimiento de los objetivos establecidos por la empresa de transporte. Para este seguimiento se hace necesario establecer lo siguiente:

- Informe de las auditorías internas que recoge el estado del sistema y de las incidencias detectadas
- Informe de operaciones ejecutadas por parte de los responsables
- Resumen de estado de incidencias reportadas y soluciones otorgadas
- Resumen del estado de cambio de la organización trimestralmente

Objetivo específico 2: Diseñar un plan de continuidad del negocio, acorde a los requerimientos de la Norma ISO 27001, para iniciar el proceso de certificación

- **Control 1: Plan de Continuidad del Negocio.**

Constituye una eficaz respuesta a las situaciones críticas que afectan a la empresa de transporte la Ecuatoriana. Por lo que es necesario aplicar lo siguiente:

- Mantener los niveles de seguridad establecidos para la información manejada por la empresa

- Establecimiento del tiempo de recuperación que garantice el ejercicio continuo de las actividades de la empresa
- Examinar los resultados de la ejecución del plan y consideraciones de futuras mejoras
- Definición de las situaciones criticas
- Establecimiento del comité de emergencias quienes defina las soluciones

El Plan de Continuidad del Negocio se estructura por las siguientes fases

Tabla 11. Fases del plan de continuidad

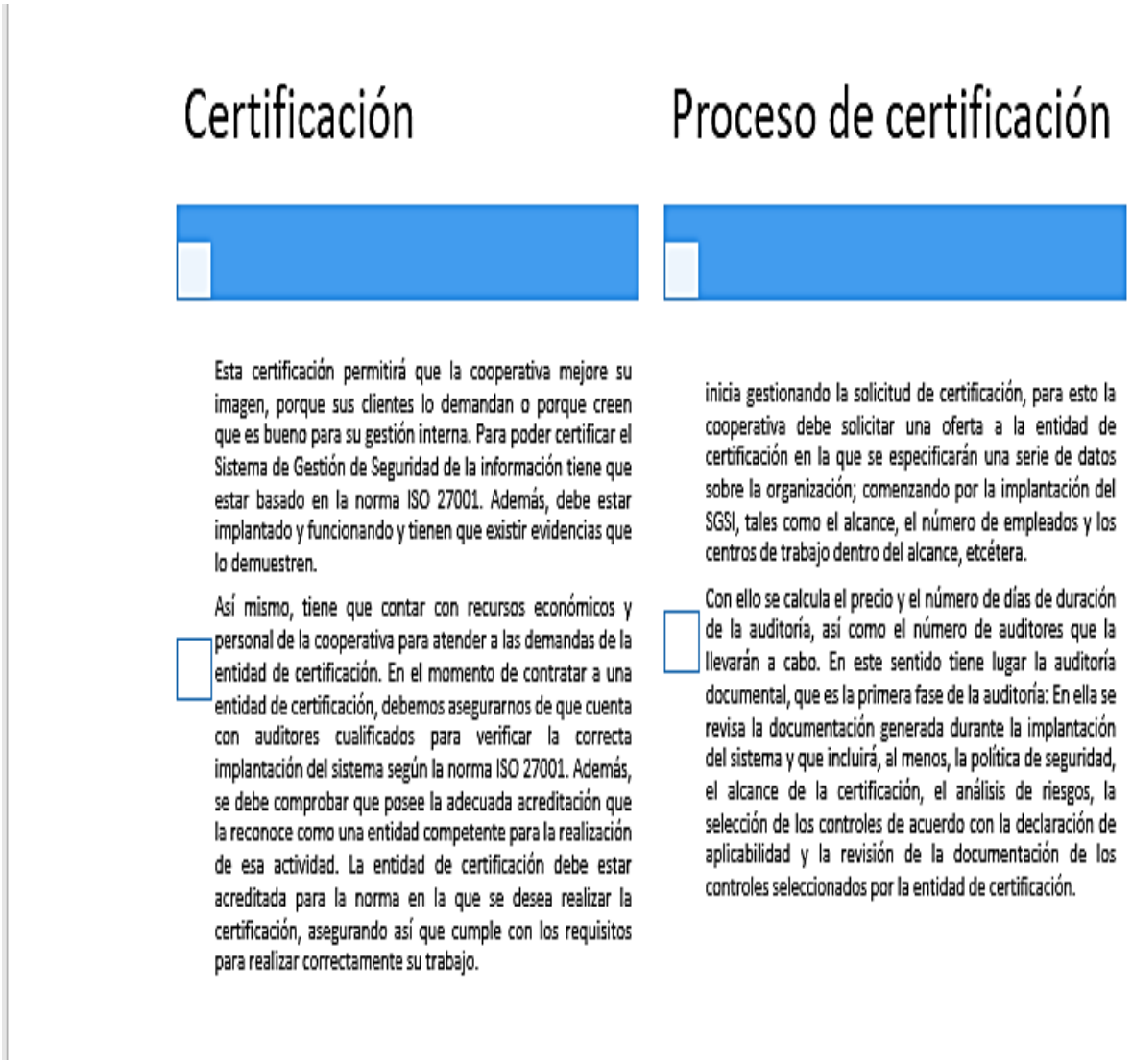
FASES	
	1. Definición del proyecto: Es necesario establecer los objetivos, el alcance y el peor de los escenarios.
	2. . *Análisis de impacto en el negocio:* Se debe realizar un análisis de riesgos, evaluar el impacto del incidente tanto económico como de cualquier otro tipo, identificar los procesos y activos críticos, asignar el tiempo objetivo de recuperación y evaluar las coberturas de los seguros y contratos
	3. *Selección de estrategias:* Se debe identificar los recursos disponibles, evaluar las salvaguardas y estimar si conviene más aportar una solución a nivel interno o a nivel externo. Con toda la información hay que valorar las ventajas y desventajas de cada una de las estrategias posibles y escoger la más conveniente para la cooperativa
	4. . *Desarrollo de planes:* En esta fase se debe implementar diferentes procedimientos para afrontar las diversas incidencias.
	5. Pruebas y mantenimiento del plan de continuidad: Es necesario probar el plan para garantizar que cuando haya que usarlo todo funcione como está previsto. El plan debe ser probado periódicamente para identificar y corregir posibles deficiencias e incluir actualizaciones del sistema. Estas pruebas deben incluir, al menos, la restauración de las copias de seguridad, la coordinación del personal y departamentos involucrados, la verificación de la conectividad de los datos y del rendimiento de los sistemas alternativos, y la verificación del procedimiento para la notificación de las incidencias y la vuelta a la situación inicial de normalidad.

Nota: Fases del plan de continuidad de la empresa de transporte la Ecuatoriana. Jácome (2021)

- **Control 2: Proceso de Certificación.**

En cuanto al proceso de certificación, es necesario que una vez aplicado todas las pautas determinadas y relacionadas a la implantación del SGSI, en donde la empresa de transporte la Ecuatoriana pues si cumple con los estándares requeridos y se verifica su correcta implantación puede llegar acetificarse, siguiendo el proceso a continuación:

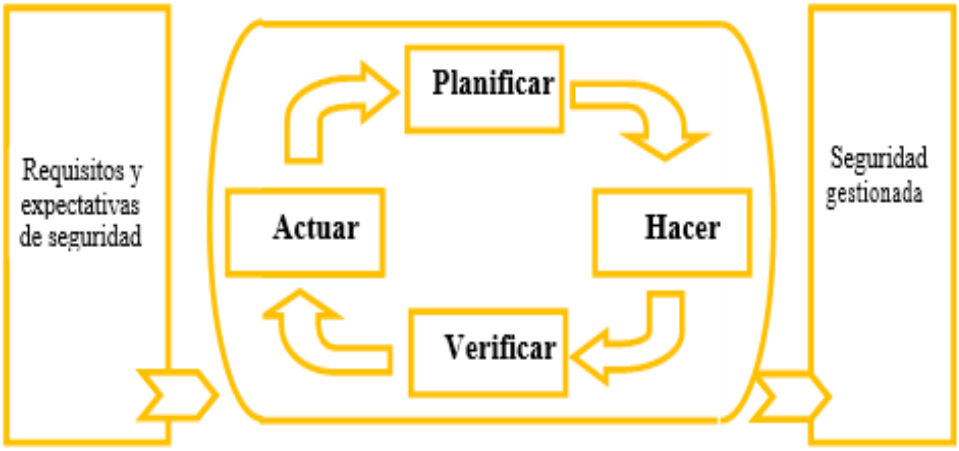
Tabla 12. Proceso de certificación de la norma ISO 27001



Nota: Proceso de certificación que debe cumplir la empresa de transporte la Ecuatoriana. Jácome (2021)

En este sentido, confirmado los controles para optar por el proceso de certificación se llevará a cabo una auditoria in situ por parte del órgano certificador, esta tendrá lugar en la empresa de transporte la Ecuatoriana donde se desplazarán los auditores para verificar la documentación revisada en la fase anterior, así como los registros del sistema. En esta fase los auditores confirman que la organización cumple con sus políticas y procedimientos, comprueban que el sistema desarrollado está conforme con las especificaciones de la norma. Para esto se debe verificar si los objetivos determinados están siendo alcanzados.

Figura 10 Modelo PHVA aplicado a los procesos del SGSI



Nota: Aplicación del método PHVA a los procesos de la empresa de transporte la Ecuatoriana. Jácome (2021)

El proceso de actuación se detalla en la figura 11, en donde aleatoriamente se evidencia el mecanismo de control basado en la planificación, acción (hacer), de acuerdo a los requerimientos que imponen la norma para establecer el SGSI.

Tabla 13. Proceso de actuación

Actuación	**Planificar (Establecer el SGSI)** Establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática, con el fin de entregar resultados acordes con las políticas y objetivos globales de la cooperativa.
	Hacer (Implementar y operar el SGSI) Tiene como objetivo fundamental garantizar una adecuada implementación de los controles seleccionados y la correcta aplicación de los mismos.
	Verificar (Revisar y dar seguimiento al SGSI) Evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
	Actuar (Mantener y mejorar el SGSI) Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua del SGSI.

Nota: Proceso de actuación en la empresa de transporte la Ecuatoriana. Jácome (2021)

La actuación bajo el objetivo del mecanismo de control representa una buena caracterización del sistema informático, lo cual permite conocerlo a plenitud y evita pérdida de tiempo e imprecisiones. Tal como se mencionó en el diagnóstico de este apartado los bienes identificados a proteger son el software, hardware y documentos como los bienes informativos vulnerables y que pueden están en situación crítica, son los objetivos donde se inclina los mecanismos de control.

Una vez que se identifican los activos informáticos que ameritar protección, se debe establecer un orden de importancia y proceder a la implementación de estrategias con base en tal jerarquización.

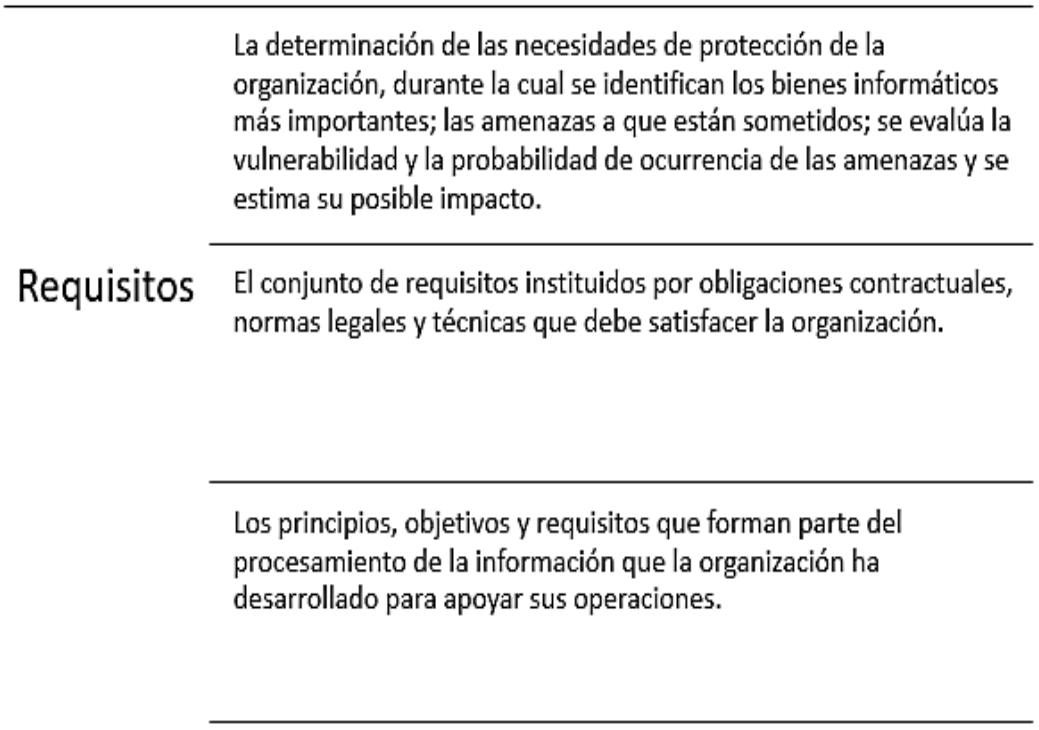
Tal valoración permite que dichos activos puedan ser categorizados por un orden de atención determinando en qué medida uno es más importante que otro,

considerando aspectos fundamentales como: su función, costo, repercusión, valoración de daños y pérdida, y determinación de la recuperación.

Respecto a esto, una evaluación critica, permite medir la efectividad de los controles implementados. Por tal razón los resultados de esta evaluación contribuyen a orientar y a determinar una apropiada acción gerencial y las prioridades para gestionar los riesgos de la SI.

Para el establecimiento de los requisitos de la seguridad, se debe cumplir con 3 requerimientos fundamentales:

Figura 11 Requisitos de seguridad



Nota: Determinación de los requisitos de seguridad de la empresa de transporte la Ecuatoriana. Jácome (2021)

Los requerimientos permiten identificar a través de una evaluación critica, los riesgos de los activos de la empresa de transporte la Ecuatoriana. En lo que respecta al gasto de los controles implementados, por lo que debe existir parámetros de equilibrio en concordancia al perjuicio latente para la empresa, tales son el resultado de los fallos de seguridad (costo - beneficio).

En este sentido, los mecanismos de control de seguridad que se seleccionen para la empresa de transporte la Ecuatoriana, deben reducir los riesgos a un nivel aceptable, para que cubran todas las necesidades específicas de esta.

En lo que corresponde a la selección de los controles de seguridad, claramente dependerá de la decisión estratégica organizacional sustentada en los criterios para la aceptación del riesgo.

En este sentido, los objetivos de control responderán a las necesidades de la empresa, sin embargo, deben estar planteado con base a resultados inmediatos o por lo menos a mediano plazo según corresponda, esto en cumplimiento de los requisitos legales, o reglamentarios; en las obligaciones contractuales y en las necesidades orgánicas de la empresa de transporte la Ecuatoriana, en materia de seguridad informática. Ahora bien, un aspecto trascendental a considerar es que en caso de su no aplicación es decir sino se establecen tales controles puede llegar a ocasionar grandes costos adicionales.

Finalmente la dirección instaurará políticas de seguridad en relación a los objetivos de la entidad y demostrando su apoyo y compromiso a la seguridad informática, haciendo pública y notoria todas estas políticas en la organización

Estas políticas promoverán elementos estratégicos para el mantenimiento de medidas y procedimientos requeridos para salvaguardar el SI.

En este sentido en cuanto a tales políticas de seguridad deben estar estructuradas con bases en reglamentos y regulaciones, así como normativas de obligatorio cumplimiento.

Entre los componentes que deben formar parte de las políticas de seguridad de termina Cohen (2015) se incluyen:

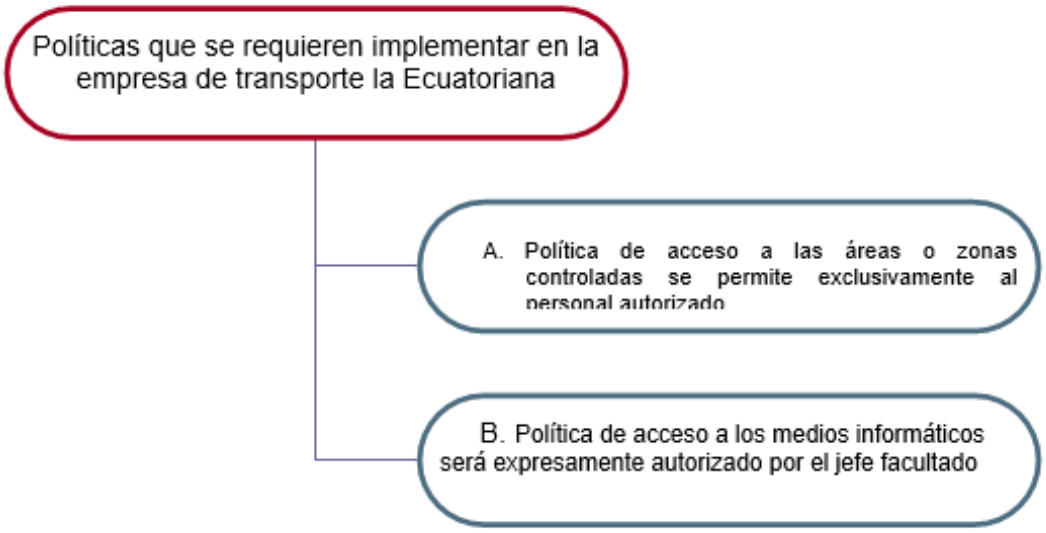
> “en principio el tratamiento que requiere la información oficial que procese intercambie o reproduzca la tecnología de información de acuerdo con su categoría; en segundo lugar, el empleo conveniente de las tecnologías instaladas y cada uno de los servicios que estas puedan ofrecer” (p.8).

En conclusión, con base en la contextualización de los accesos a los bienes informáticos, se deben fijar pautas, basada en controles autorizados para garantizar su protección, contra modificaciones no autorizadas, perdidas o revelación de datos.

Por al razón se muestran 2 ejemplos de políticas que se requieren implementar en la empresa de transporte la Ecuatoriana:

Figura 12. Políticas de implementación en la empresa de transporte la Ecuatoriana

Nota: Aplicación del método MAGERIT a los procesos de la empresa de transporte la Ecuatoriana. Jácome (2021)



Nota: Políticas de la empresa de transporte la Ecuatoriana. Jácome (2021)

Establecidos los mecanismos de control, se procede a determinar los recursos necesarios para llevar a cabo lo relacionado a la propuesta y en cumplimiento al objetivo de investigación dirigido a: “Determinar en costo/beneficio para establecer la rentabilidad de la propuesta” se evidencia lo siguiente:

- Inversión económica:

Tabla 14. Inversión inicial

Inversión inicial			
I Inversión inicial fija			**12.750,5**
		$ 8.797,50	
	8.797,50		
		3.953,00	
	2.400,00		
Recursos Materiales			
Recursos humano	220,00		
Equipos			
Instalación	1.333,00		
Total inversión			**$ 12.750,5**

Nota: Inversión inicial para implementar un SGSI en la empresa de transporte la Ecuatoriana. Jácome (2021)

Se requerirá de una inversión económica de 12.750,5 dólares conforme con la valoración de riesgos y los razonamientos para asumir o minimizar los distintos niveles de riesgo

Tabla 15. Presupuesto de inversión para la implementación del SGSI (Recurso)

Recursos	Presupuesto	Total
Personas	$ 5.850	$ 5.850
Instalación	$ 2.369	$ 2.369
Equipo	$ 4.531,5	$ 4.531,5
	Total	**$ 12.750,5**

Nota: Presupuesto de inversión para implementar un SGSI en la empresa de transporte la Ecuatoriana. Jácome (2021)

- Personas:

En la empresa de transporte la Ecuatoriana, deben precisar los roles y responsables de acuerdo al establecimiento del SGSI determinando el desempeño de sus funciones.

Tabla 16 Presupuesto para el recurso humano

Nombre del recurso (Humano)	Tipo	Iniciales	Grupo	Capacidad máxima	Salario
Gerente de Proyecto	Trabajo	GP	Personal	100%	$ 1400
Ingeniero líder	Trabajo	IL	Personal	100%	$ 1.400
Ingeniero Asistente	Trabajo	IA	Personal	100%	$ 950
Técnico	Trabajo	TEC	Personal	100%	$ 425
Asesor TI	Trabajo	ATI	Personal	100%	$ 837,5
Asesor GP	Trabajo	AGP	Personal	100%	$ 837,5
Total					**$ 5.850**

Nota: Presupuesto de recursos humanos para implementar un SGSI en la empresa de transporte la Ecuatoriana. Jácome (2021)

- Equipos de seguridad e Instalaciones:

Por tanto todas las instalaciones de la empresa de transporte debe estar preparada para brindar estrategias de seguridad que afronte las amenazas de riesgos a lo que se puedan estar expuestos una organización. Siendo esto esencial para el cálculo del proyecto de implementación del SGSI

Tabla 17 Presupuesto para las instalaciones

Nombre del recurso (Instalación)	Tipo	Iniciales	Capacidad máxima	Costo
Firewall	Material	FW	100%	$ 250
NAS	Material	NAS	100%	$ 480
Antivirus	Material	AV	100%	$ 220
TeamViewer	Material	TV	100%	$ 400
SQL Server	Material	SQ	100%	$ 570
Energía de respaldo	Material	UPS	100%	
Cámaras de vigilancia (3 Cámaras)	Material	CCTV	100%	$ 149,6(C/U) **Total $2.369**

Nota: Presupuesto de recursos para implementar un SGSI en la empresa de transporte la Ecuatoriana. Jácome (2021)

- Equipos de oficina y administrativos:

Así mismo se debe incorporar los equipos necesarios que permitan establecer los SS para el resguardo de la información

Tabla 18 Presupuesto de los equipos de oficina

Nombre del recurso (Equipo)	Tipo	Iniciales	Capacidad máxima	Costo
Computador (4)Desktop	Equipo	COMP	100%	$ 350
Computador (4) Laptop	Equipo	CLP	100%	$ 550
Impresora (2)	Equipo	I	100%	$ 220
Video (2)Proyector	Equipo	VP	100%	$420
Presupuesto excedente				$201,5
Total				**4.531,5**

Nota: Presupuesto de los equipos para implementar un SGSI en la empresa de transporte la Ecuatoriana. Jácome (2021)

Fuente: elaboración propia

- Estimación del tiempo requerido para su realización.

Tabla 19 Estimación del periodo de implementación de SGSI

Proceso	Periodo de tiempo
Selección de personal	6 meses y 20 días
Compra de equipos	2 meses y 7 días
Instalaciones de equipo	1 mes y 15 días
Proceso de validación de SGSI y certificación de la norma ISO 27001	De acuerdo a los procedimientos instaurados por las autoridades de validación del SGSI. Para la posterior certificación
Estimación del proceso	**10 meses y 12 días**

Nota: Estimación y duración de tiempo para implementar un SGSI en la empresa de transporte la Ecuatoriana. Jácome (2021)

El periodo estimado se cumplimiento con los requisitos para la certificación de la empresa la Ecuatoriana es de 10 meses y 12 días. En este sentido a continuación en base a los costos se realiza una proyección en caso de que sea propuesto a 3 años la implementación de los requisitos con dos años adicionales estimados

Tabla 20 Costos

DESCRIPCION	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
COSTOS	12.750,5	12.760,00	12.880,00	12.880,00	12.900,00
MANO DE OBRA DIRECTA	5. 850	5.860	5.880	5.880	5.900
GASTOS DE SERVICIOS DE INSTALACIÓN	2.369	2370	2.380	2.380	2.390
EQUIPOS	4.531,5	4.540,5	4.550,5	4.550,5	4.600

Nota: Proyección de costos para implementar un SGSI en la empresa de transporte la Ecuatoriana. Jácome (2021)

Capítulo V Sugerencias

En cuanto a las sugerencias aportadas a este estudio, se detallan en tres fases la fase voluntaria, regulatoria y complementaria:

Fase voluntaria:

Se sugiere en primer lugar acoger la propuesta, ya que esta establece las estipulaciones necesarias para iniciar un proceso de gestión de información acorde a la normativa ISO 27001, bajo el propósito de la certificación, entendiendo que sus requisitos optimizan la seguridad y los datos informativos que maneja la empresa, obteniendo beneficios que permiten proteger y salvaguardar los bienes de la empresa de transporte la ecuatoriana. Así mismo se sugiere educar y culturizar a las empresas a tomar acciones en base a seguridad en los miembros de la empresa.

Se sugiere la implementación de la propuesta para la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001, como una estrategia de innovación que aporta gran confiabilidad en el servicio prestado por la empresa, la cual ciertamente permitirá el desarrollo de este proceso para un alcance definido.

Posteriormente se recomienda la constante actualización y planificación de estrategias y políticas que permitan mantener un sistema óptimo para el mantenimiento de la certificación, pues cada vez surgen nuevas amenazas o riesgos que pueden llegar a cierto tiempo reducir el alcance.

Fase regulatoria

Soporte a nivel de placa de ganancia: un SG de la información sólo será eficaz con la unión de la directiva y trabajo en conjunto. En esta fase se preparan las acciones y actividades para sustentar los costes, rendimiento de la inversión, los riesgos, amenazas y oportunidades. (Inversión económica descrita en la propuesta).

Estimar legislación aplicable: Es necesario instituir y organizar el SGSI a las normativas y controles, que permita ejecutar a las políticas de regulación interna y reglamentos

Análisis de carencias: reconocimiento de las capacidades efectivas para la ejecución y cumplimento. Por tal razón se necesita instaurar una orientación definida hacia acciones que permitan mantener la concentración.

Trabajar en base plazos realistas: El establecimiento de programaciones en base al tiempo de forma real y en lapsos alcanzables. La asignación de tareas con fechas de vencimiento ayudará a facilitar las actividades y la administración del proyecto con éxito.

Fase complementaria

Establecidas las fases voluntaria y regulatoria se sugiere de forma complementaria la unificación de un SG, pues estos sistemas consienten a las empresas constituir sus sistematizaciones para optimar su control.

Así mismo se puede complementar con un análisis y gestión de los riesgos de la información continuamente, es necesario tener en cuenta que, lo riesgos cambian con la evolución de la empresa al surgir nuevas modalidades de amenazas y aparición de vulnerabilidades. Finalmente se sugiere que se complemente una

implementación de escenarios de prueba: El inventario de activos es la herramienta que se utiliza como punto de partida para el ejercicio de análisis y gestión de los riesgos de la información.

Conclusiones

El presente trabajo se estructuró bajo un diseño de propuesta para la aplicación y gestión de un SGSI en la empresa de transporte la Ecuatoriana bajo la normativa ISO 27001, en base al resguardo de información y registro que maneja la empresa.

Respecto al diagnóstico sobre los punto críticos de la empresa de transporte la Ecuatoriana se evidenció que no implementa políticas de seguridad en sus sistemas informático por lo que sus datos y documentación confidencial es vulnerable a cualquier riesgo. Así mismo no cuenta con un instructivo, planificación estrategias o protocolos de emergencia lo que ocasiona un grave problema en cuanto a su imagen y seguridad de sus clientes.

Por tanto al análisis crítico manejado durante el desarrollo de este estudio se estableció que, claramente la información es un activo esencial para la operación de una empresa, por tanto deben implementar mecanismos de control que salvaguarden de forma óptima ante alguna amenaza que ocasione daños muy relevantes a tal empresa

Posteriormente en cuanto a la formulación de una propuesta como plan de acción basado en el diagnóstico inicial, se estableció desde un enfoque de protección, en cuanto a los registros de usuario, financieros, datos, y no solo la información que maneja la organización sino de la infraestructura. Su objetivo principal fue el de diseñar una propuesta sobre el Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001 para preservar la confidencialidad, integridad y disponibilidad de la información que maneja la empresa de transporte la Ecuatoriana, para ello se analizó el alcance, objetivos y políticas del SGSI. Posteriormente se definieron los riesgos sobre los activos en el alcance del SGSI bajo la normativa ISO 27001, así como la examinación de las probabilidades e impactos de los riesgos sobre los activos identificados bajo el alcance, calculando los niveles de riesgo, aplicando la metodología MAGERIT. Por lo que se describieron controles sobre los activos, basado en un plan de tratamiento de riesgo bajo la normativa ISO 27001 y finalmente se estableció un mecanismo de control de la propuesta efectuada complementado con el costo/beneficio que permitió planificar las estrategias, recursos y presupuestos para su implementación.

En este sentido, y para cumplir con los objetivos de la propuesta se efectuó el diagnostico para el análisis preliminar de la situación actual de la empresa en cuanto a su SI determinando que, en primer lugar se requiere una gestión integral por

procesos, así como establecer responsabilidades y regulaciones en cuanto a los recursos humanos, tecnológicos, inversión en equipos e instalaciones.

En cuanto a los lineamientos y requerimientos legales, se deben emplear la auditoria para dar cumplimiento a las leyes y reglamentos, en concordancia con las metas de la organización.

Se concluye que, se implementa la normativa ISO27001, porque es un instrumento eficaz para manejar un SGSI en cualquier organización, sin importar a que se dedique esta. En este sentido, si la empresa de transporte la Ecuatoriana se acoge al diseño de propuesta, cumpliendo con los parámetros establecidos así como el presupuesto de inversión para la instalación de los equipos necesarios para realizar conforme a los requisitos de la normativa ISO 27001 la incorporación del SGSI, ciertamente permitirá a sus clientes, proveedores y demás asociados de negocio, confiabilidad al saber que la empresa cumple con los estándares de seguridad en su proceso.

Bibliografía

Andreu. (2012). Sistem de informacion: Manejo en las entidades. 17.

AudiSec. (2012). *GUÍA DE IMPLANTACIÓN DE UN SISITEMA*. Obtenido de www.audisec.es

Balaguer. (2014). La nueva version ISO 27001:2013: un cambio en la. *Colegio de ingenieros de Perú*.

Beynon. (2015). *Sistemas de información: introducción a la informática en las organizaciones. .* Barcelona, España: Reverté.

Castro. (2018). Diseño organizacional de los SI. 7.

Cohen. (2015). Definición de sistema de información. *TecnologíaOnline*, 17.

DeloitteEcuador. (2020). Seguridad de la información (SGSI). *DELOITTE*, 12.

Esguerra, & Ortiz. (2018). *PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013* . Obtenido de https://repository.udistrital.edu.co/bitstream/handle/11349/13419/Geraldine%20Alejandra%20Ortiz%20C%E1rdenas%202018.pdf;jsessionid=5C6A2A25F62B8FA55321391C3076EB75?sequence=4

García. (2018). *Ingeniería del Software*. Obtenido de https://repositorio.grial.eu/bitstream/grial/1228/1/07-rep.pdf

Guitiérrez. (2017). Analisis sobre la normativa ISO 27001. 29.

Hernández. (2016). Metodología de Intervención.

ICONTEC. (2006). NORMA TÉCNICA NTC-ISO/IEC. En Instituto. Bogotá.

ISO27001. (2009). *A Project to Build an ISMS. SANS Institute InfoSec Reading*. Obtenido de https://www.sans.org/reading-room/whitepapers/leadership/tackling-iso-27001-project-build-isms-33169

James. (2015). Programaciones y sistemas. 34.

Jimenez. (2017). GESTIONES TECNOLOGICAS: ENTIDADES. *ECOMERCE*, 16.

Lara, & Corella. (2019). *COMPARACIÓN DE MODELOS TRADICIONALES DE SEGURIDAD DE LA INFORMACIÓN PARA CENTROS DE EDUCACIÓN*. Obtenido de file:///C:/Users/Usuario1/Downloads/742-Texto%20del%20art%C3%ADculo-2380-1-10-20190109.pdf

López. (2019). *Los virus informáticos: una amenaza para la sociedad.* https://interpolados.files.wordpress.com/2018/06/los-virus-informaticos_-una-ame-yansenis-lopez-matachana.pdf.

Management, A. G. (2014). *Project Management Institute (PMI) .* Philadelphia: PMI.

Montecé. (2017). *Software de seguridad que permita la confidencialidad de los datos del sistema*. Obtenido de file:///C:/Users/Usuario1/Downloads/Dialnet-SoftwareDeSeguridadQuePermitaLaConfidencialidadDeL-6326645.pdf

Moral. (2014). *Modelos de regresión: lineal simple y regresión logística*. Obtenido de https://revistaseden.org/files/14-CAP%2014.pdf

Ortiz. (2019). Planificación estrategicas de las organizaciones. *ECONIN*, 5.

Parra. (2019). *Modelo cualitativo*. Obtenido de https://bookdown.org/content/2274/portada.html

Pérez. (2018). SI: Información y seguridad empresarial. *LIDERLIVE*.

Romero, Figueroa, Vera, & Álava. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Sánchez. (2011). *Análisis y Gestión de Riesgos en los Sistemas de Información .* Departamento de Publicaciones, EUI-UPM.

Sánchez. (2013). *SOFTWARE* . Obtenido de https://proyectocirculos.files.wordpress.com/2013/11/software.pdf

Smith. (2018). Funciones de los sistemas de información. *SegurityEnterprise*.

Smith. (2018). Funciones de los sitemas de información. *SegurityEnterprise*.

SOPHOS. (2019). *INFORME DE AMENAZAS 2019 DE SOPHOSLABS*. Obtenido de https://www.sophos.com/es-es/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

Terán. (2019). *Gestión de la tecnología e innovación: un Modelo de Redes Bayesianas*. Obtenido de

http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-33802019000100063

Urbina. (2017). Método de PHVA.

Villalonga. (2019). Gestión tecnológica para las empresas. *GIE*, 9.