Maestría en

GESTION DE RIESGOS

Trabajo de investigación previo a la obtención del título de

Magíster en Gestión en Riesgos

AUTORES:

Enrique Santiago Almagor Farinango

Moisés Francisco Calderón Morejón

René Esteban Cedillo Pinos

Nicolás Alejandro Coto Rodas

Joffre Raphael Rivas Cevallos

Michael Abdón Villarreal Fuertes

TUTORES:

Paloma Manzano Martínez

Wilson Fabián Goyes Arroyo

Enrique Molina Suárez

David Genaro Benavides Gutiérrez

Diseño del manual de gestión en riesgos de la norma ISO 31000 en la Empresa SYTSA

Quito, (Marzo-2026)

Certificación de autoría

Nosotros, Enrique Santiago Almagor Farinango, Moisés Francisco Calderón Morejón, René Esteban Cedillo Pinos, Nicolás Alejandro Coto Rodas, Joffre Raphael Rivas Cevallos, Michael Abdón Villarreal Fuertes**,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ENRIQUE SANTIAGO ALMAGOR FARINANGO

Firma del graduando
(Enrique Santiago Almagor Farinango)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MOISES FRANCISCO CALDERON MOREJON

Firma del graduando
(Moisés Francisco Calderón Morejón)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
RENE ESTEBAN CEDILLO PINOS

Firma del graduando
(René Esteban Cedillo Pinos)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
NICOLAS ALEJANDRO COTO RODAS

Firma del graduando
(Nicolás Alejandro Coto Rodas)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JOFFRE RAPHAEL RIVAS CEVALLOS

Firma del graduando
(Joffre Raphael Rivas Cevallos)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MICHAEL ABDON VILLARREAL FUERTES

Firma del graduando
(Michael Abdón Villarreal Fuertes)

Autorización de Derechos de Propiedad Intelectual

Nosotros, Enrique Santiago Almagor Farinango, Moisés Francisco Calderón Morejón, René Esteban Cedillo Pinos, Nicolás Alejandro Coto Rodas, Joffre Raphael Rivas Cevallos, Michael Abdón Villarreal Fuertes, en calidad de autores del trabajo de investigación titulado **Diseño del manual de gestión en riesgos para la implementación de la norma ISO 31000 en la Empresa SYTSA**, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, (mes año)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ENRIQUE SANTIAGO ALMAGOR FARINANGO

Firma del graduando
(Enrique Santiago Almagor Farinango)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MOISES FRANCISCO CALDERON MOREJON

Firma del graduando
(Moisés Francisco Calderón Morejón)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
RENE ESTEBAN CEDILLO PINOS

Firma del graduando
(René Esteban Cedillo Pinos)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
NICOLAS ALEJANDRO COTO RODAS

Firma del graduando
(Nicolás Alejandro Coto Rodas)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JOFFRE RAPHAEL RIVAS CEVALLOS

Firma del graduando
(Joffre Raphael Rivas Cevallos)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MICHAEL ABDON VILLARREAL FUERTES

Firma del graduando
(Michael Abdón Villarreal Fuertes)

Aprobación de dirección y coordinación del programa

Nosotros, **Paloma Manzano Martínez Director/a EIG y David Genaro Benavides Gutiérrez Coordinador/a UIDE,** declaramos que los graduandos: Enrique Santiago Almagor Farinango, Moisés Francisco Calderón Morejón, René Esteban Cedillo Pinos, Nicolás Alejandro Coto Rodas, Joffre Raphael Rivas Cevallos, Michael Abdón Villarreal Fuertes son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DAVID GENARO BENAVIDES GUTIERREZ

MANZANO MARTINEZ PALOMA - 24244436K
Firmado digitalmente por MANZANO MARTINEZ PALOMA - 24244436K
Fecha: 2026.08.03 18:28:33 +02'00'

Paloma Manzano Martínez
Director/a de la
Maestría en Gestión de Riesgos

David Genaro Benavides Gutiérrez
Coordinador/a de la
Maestría en Gestión de Riesgos

DEDICATORIA

A Dios, por darme la sabiduría, la fortaleza y la perseverancia para llegar hasta aquí, y por guiar cada uno de mis pasos en este camino académico y personal.

A mis padres, por ser el pilar más sólido de mi vida. Su ejemplo de esfuerzo, honestidad y dedicación ha sido mi mayor inspiración. Todo lo que soy y lo que he logrado se lo debo a ustedes.

A mis hermanos y familiares, por su cariño y por estar siempre presentes, recordándome que los grandes logros se disfrutan mejor cuando se comparten.

Finalmente, a mis mentores y colegas, quienes con su experiencia y apoyo contribuyeron a mi formación profesional y personal.

- Enrique Santiago Almagor Farinango

A mí padre celestial Dios todo poderoso, que me ha amado y mirado con misericordia. A mi padre Juan Francisco, mi ejemplo a seguir y motivación constante por quien llevo con orgullo mi apellido Calderón. A mi primer y eterno amor, Maribel, mi madre, a quien dedico mis logros después de a Dios. A mi hermano Danielito quién me motiva para ser su ejemplo a seguir e inspiración. A toda mi familia que siempre ha estado conmigo ayer, hoy y siempre, de manera especial a mi abuelito Galo Hernán que hoy me espera al otro lado de la vida con su incondicional cariño. Finalmente, a

mis mentores profesionales quienes confiaron en mi para dar mis primeros pasos profesionales. Gracias a cada uno de ustedes por ser parte de este logró.

- Moisés Francisco Calderón Morejón

Dedico este trabajo, en primer lugar, a mis padres, quienes con su esfuerzo, valores y ejemplo han sido el pilar fundamental de mi formación personal y profesional. Su apoyo incondicional ha sido la base que me ha permitido avanzar y alcanzar cada una de mis metas.

A mi esposa, por su comprensión, paciencia y constante motivación durante este proceso. Su compañía y apoyo han sido esenciales en los momentos de mayor exigencia, brindándome fortaleza para continuar.

A mis hijos, quienes son mi mayor inspiración y la razón principal de mi superación. Este logro también les pertenece, con la esperanza de que en el futuro vean en él un ejemplo de esfuerzo, perseverancia y compromiso.

- René Esteban Cedillo Pinos

Dedico este proyecto de grado, fruto de esfuerzo, constancia y dedicación, en primer lugar, a mi familia, quienes han sido mi pilar fundamental a lo largo de este camino. Gracias por su amor

incondicional, por su paciencia, por creer en mí incluso en los momentos más difíciles y por impulsarme a seguir adelante cuando las fuerzas parecían faltar.

A mis docentes, quienes con su conocimiento, guía y compromiso contribuyeron significativamente a mi formación académica. Gracias por inspirarme a dar siempre lo mejor y por cada enseñanza que quedará conmigo para toda la vida.

Finalmente, dedico este logro a todas aquellas personas que, de una u otra manera, formaron parte de este proceso y confiaron en mis capacidades. Este proyecto representa no solo la culminación de una etapa, sino también el inicio de nuevos desafíos y sueños por cumplir.

- Nicolás Alejandro Coto Rodas

El presente proyecto de titulación va dedicado a mi amada familia, pilar fundamental en cada paso de este camino.

A mis padres, por enseñarme con su ejemplo que el esfuerzo, la humildad y la perseverancia son las verdaderas llaves del éxito. Su amor incondicional y sus consejos han sido la guía que me ha sostenido en los momentos más difíciles.

A mis hermanos, compañeros de vida, por su apoyo sincero, sus palabras de aliento y por recordarme siempre que los logros se disfrutan más cuando se comparten.
Y a mis hijos, mi mayor inspiración, por dar sentido a cada sacrificio y motivarme a ser mejor cada

día. Este logro es también son suyos, porque en cada meta alcanzada está reflejado su amor y la fuerza que me impulsa a seguir adelante.

- Joffre Raphael Rivas Cevallos

Este esfuerzo quiero dedicarlo a mi compañera de vida, Dome, quien gracias a su paciencia, su tiempo y su guía me ayudó a poder culminar esta nueva etapa que alimenta mi crecimiento personal y profesional.

A mi madre, que con su ejemplo de superación y su enseñanza de siempre buscar algo más para fortalecer el crecimiento mediante la educación, me inspira a valorar el aprendizaje como una herramienta para poder seguir adelante. Mi padre y su apoyo incondicional desde el momento que tuvo conocimiento de esta nueva etapa que estoy por culminar.

Mis hermanas, que gracias a sus deseos y el amor que nos caracteriza me han demostrado que a pesar de la distancia siempre nos tenemos el uno al otro. Y a mis sobrinos, que espero poder ser una guía y una inspiración para que puedan cumplir todas las metas que se propongan.

-Michael Abdón Villarreal Fuertes

AGRADECIMIENTOS

Expresamos nuestro más sincero agradecimiento a todas las personas e instituciones que hicieron posible la culminación de este trabajo de investigación.

A la Universidad Internacional del Ecuador (UIDE) y a la EIG, por esclarecer los conocimientos, proveer las herramientas y el espacio académico para desarrollar esta tesis de maestría. Su compromiso con la excelencia educativa ha sido fundamental en nuestra formación profesional en gestión de riesgos. Nuestros tutores, la Msc. Paloma Manzano Martínez, el Mgtr. Wilson Fabián Goyes Arroyo, el Mgtr. Enrique Molina Suárez y el Dr. David Genaro Benavides Gutiérrez, por su invaluable orientación, paciencia y rigor académico. Sus acertados consejos y su dedicación fueron esenciales para dar forma y profundidad a este proyecto.

A todo el equipo de trabajo integrado por Moisés Francisco Calderón Morejón, René Esteban Cedillo Pinos, Nicolás Alejandro Coto Rodas, Joffre Raphael Rivas Cevallos y Michael Abdón Villarreal Fuertes, su colaboración, compañerismo y esfuerzo conjunto sumaron talentos y compromiso.

A la empresa Transportes y Servicios Asociados SYTSA Cía. Ltda., y en especial a su Gerencia General, por abrirnos las puertas de su organización y permitirnos realizar este estudio. Su confianza y disposición fueron clave para el desarrollo de una propuesta aplicada y relevante para el sector logístico y de transporte.

RESUMEN

El presente trabajo de análisis, diseño e implementación tuvo como objetivo principal el planteamiento de un Manual de Gestión de Riesgos sustentado en la norma internacional ISO 31000:18 para la empresa de Transportes y Servicios Asociados SYTSA Cía. Ltda. Entidad corporativa que se especializa en la provisión de soluciones logísticas integrales. Ante la carencia de un sistema formal y estructurado enfocado en la seguridad, surgió la necesidad de crear un instrumento que proteja la continuidad operativa en base al mapeo integral de procesos, la categorización de riesgos asociados a la seguridad de información y las políticas de confidencialidad y consentimiento impuestas por la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP), con el fin de implementar una Gestión del Riesgo integrada, estructurada, inclusiva y dinámica orientada a la mejora continua. Por lo que, el resultado final proporcionó un manual que sirve como herramienta y que permitió facilitar la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar el desarrollo de sus actividades. Este enfoque buscó contribuir al fortalecimiento de la gestión organizacional mediante la incorporación de buenas prácticas alineadas a estándares internacionales.

Palabras Claves: gestión del riesgo, gestión organizacional, mejora continua, LOPDP, norma internacional.

ABSTRACT

The primary objective of this analysis, design, and implementation project was to develop a Risk Management Manual based on the international standard ISO 31000:18 for SYTSA Cía. Ltda., a transportation and related services company that specializes in providing comprehensive logistics solutions. Given the lack of a formal, structured system focused on security, the need arose to create a tool that would safeguard operational continuity based on comprehensive process mapping, the categorization of risks associated with information security, and the confidentiality and consent policies mandated by Ecuador's Organic Law on the Protection of Personal Data (LOPDP), with the aim of implementing an integrated, structured, inclusive, and dynamic risk management system geared toward continuous improvement. Consequently, the final result was a manual that serves as a tool to facilitate the identification, analysis, assessment, and mitigation of risks that could affect the company's operations. This approach sought to strengthen organizational management by incorporating best practices aligned with international standards.

Keywords: Risk management, Organizational management, Continuous improvement, LOPDP, International standard

TABLA DE CONTENIDOS (Índice)

Contenido

LISTA DE TABLAS (INDICE DE TABLAS)

LISTA DE FIGURAS (Índice de figuras)

CAPITULO 1:
INTRODUCCION

En el contexto actual, caracterizado por la globalización, la transformación digital y la creciente complejidad de los entornos empresariales, las organizaciones enfrentan múltiples factores de incertidumbre que pueden afectar el cumplimiento de sus objetivos estratégicos. En este escenario, la gestión de riesgos se consolida como un componente esencial para la sostenibilidad, competitividad y continuidad del negocio, permitiendo anticipar, evaluar y mitigar eventos adversos de manera estructurada (Hopkin, 2018)

Particularmente, en sectores como el logístico y tecnológico, donde los procesos operativos involucran flujos constantes de información, recursos y servicios, la exposición a riesgos operativos, financieros, tecnológicos y reputacionales es significativamente elevada (Castellanos, 2015). En este sentido, la adopción de enfoques sistemáticos de gestión del riesgo permite a las organizaciones no solo reducir pérdidas potenciales, sino también mejorar la eficiencia de sus procesos y fortalecer la toma de decisiones (Christopher, 2016).

En respuesta a esta necesidad, la norma ISO 31000:2018 establece principios, directrices y un marco de referencia internacional para la gestión del riesgo, aplicable a cualquier tipo de organización independientemente de su tamaño o sector. Este estándar promueve la integración del riesgo en todos los niveles organizacionales, fomentando una cultura preventiva y orientada a la mejora continua (International Organization for Standardization [ISO (Standardization, s.f)].

En este contexto, el presente trabajo tiene como objetivo general diseñar un manual de gestión de riesgos basado en la norma ISO 31000 para la empresa SYTSA, con el fin de proporcionar una herramienta estructurada que facilite la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar el desarrollo de sus actividades. Este enfoque busca contribuir al fortalecimiento de la gestión organizacional mediante la incorporación de buenas prácticas alineadas a estándares internacionales.

El principal reto de la investigación radica en la adaptación de un modelo teórico de carácter global a la realidad específica de la organización, considerando sus características operativas, su entorno empresarial y sus limitaciones estructurales. Esto implica no solo comprender los fundamentos conceptuales de la gestión de riesgos, sino también traducirlos en una herramienta práctica, aplicable y coherente con las necesidades de la empresa.

La realización de este trabajo se justifica en la necesidad de fortalecer la capacidad de respuesta de la organización frente a escenarios de incertidumbre, así como en la importancia de promover una cultura organizacional orientada a la prevención y gestión eficiente de riesgos. Además, el diseño del manual representa un aporte significativo para mejorar la toma de decisiones, optimizar los procesos internos y proteger los activos estratégicos de la empresa, generando valor sostenible a largo plazo (Aven, 2015).

En consecuencia, el desarrollo de esta investigación no solo constituye un ejercicio académico, sino también una propuesta aplicada que busca aportar soluciones concretas a problemáticas reales dentro del ámbito empresarial, alineando la teoría con la práctica en el campo de la gestión de riesgos.

1. PLANTEAMIENTO DEL PROBLEMA E IMPORTANCIA DEL ESTUDIO

1.1 Definición del proyecto

El presente proyecto se desarrolla en la empresa SYTSA, organización ecuatoriana dedicada a la provisión de soluciones logísticas integrales, cuyas operaciones se encuentran expuestas a diversos riesgos de carácter operativo, tecnológico, financiero y estratégico, propios de su actividad y del entorno empresarial en el que se desenvuelve.

A partir del diagnóstico realizado, se ha identificado como problemática principal la ausencia de un sistema formal de gestión de riesgos basado en estándares internacionales, lo que limita la capacidad de la organización para identificar, analizar y tratar de manera estructurada los eventos que pueden afectar el cumplimiento de sus objetivos. Actualmente, la gestión del riesgo en la empresa se realiza de manera empírica y reactiva, sin lineamientos claros ni herramientas metodológicas que permitan una adecuada toma de decisiones.

En este contexto, el proyecto consiste en el diseño de un Manual de Gestión de Riesgos basado en la norma ISO 31000:2018, con el propósito de dotar a la empresa de una herramienta técnica que permita gestionar la incertidumbre de manera sistemática, fortaleciendo sus procesos internos y su capacidad de respuesta frente a eventos adversos.

1.2 Naturaleza o tipo de proyecto

Desde el punto de vista metodológico, el proyecto corresponde a un diseño de propuesta, ya que no busca mejorar un sistema previamente existente, sino desarrollar una herramienta nueva que permita establecer las bases para la implementación de un modelo formal de gestión de riesgos dentro de la empresa.

1.3 Objetivos

1.3.1 Objetivo general

Desarrollar un manual de gestión para la implementación de la Norma Internacional ISO 31000-2018 en la empresa de SOLUCIONES LOGISTICAS INTEGRALES DEL GRUPO SYTSA con el fin de precautelar la seguridad de la calidad y eficiencia de la cadena de suministro bajo estándares internacionales fortaleciendo la toma de decisiones y asegurar la continuidad del negocio mediante una gestión eficaz de la incertidumbre.

1.3.2 Objetivo especifico

- Identificar y categorizar los principales riesgos internos y externos que impactan los objetivos estratégicos del grupo SYTSA.
- Realizar un análisis de la situación actual de la empresa SYTSA para obtener una línea base en la cual podamos medir el progreso del Manual de la Gestión del Riesgo.
- Identificar los procesos necesarios para la generación de un Manual de Gestión del Riesgo

teniendo como base la Norma Internacional ISO 31000-2018.

- Establecer los lineamientos y metodologías para la valoración y tratamiento de riesgos dentro del manual.

1.4 Justificación e importancia del trabajo de investigación

La presente investigación se desarrolla en un contexto empresarial caracterizado por altos niveles de incertidumbre, cambios constantes en el entorno y crecientes exigencias regulatorias, lo que hace indispensable la adopción de enfoques estructurados para la gestión del riesgo. En este sentido, el estudio se justifica, en primer lugar, por la necesidad de que las organizaciones cuenten con herramientas metodológicas que les permitan identificar, analizar y gestionar los riesgos de manera sistemática, contribuyendo a la toma de decisiones informadas y a la continuidad del negocio (Hopkin, 2018).

Desde el punto de vista normativo, la norma ISO 31000:2018 establece principios y directrices reconocidos internacionalmente para la gestión del riesgo, promoviendo un enfoque integral que puede ser aplicado en cualquier tipo de organización (International Organization for Standardization (Standardization, s.f). Sin embargo, diversos estudios evidencian que muchas empresas, especialmente en contextos latinoamericanos, presentan limitaciones en la implementación de estos modelos debido a la falta de herramientas prácticas adaptadas a su

realidad organizacional (Aven, 2015). En este contexto, surge la necesidad de desarrollar instrumentos aplicados que faciliten la adopción de estos estándares en entornos específicos.

En el caso de la empresa SYTSA, la ausencia de un manual formal de gestión de riesgos limita la capacidad de anticipar eventos adversos y gestionar adecuadamente amenazas operativas, tecnológicas y estratégicas. Por ello, este estudio se realiza con el propósito de diseñar un manual basado en la norma ISO 31000 que permita estructurar el proceso de gestión del riesgo dentro de la organización, fortaleciendo sus procesos internos y mejorando su capacidad de respuesta ante escenarios de incertidumbre.

En cuanto a su relevancia, el presente trabajo tiene un aporte significativo en el ámbito profesional y organizacional, ya que proporciona una herramienta práctica que puede ser implementada en la empresa, contribuyendo a la mejora de la eficiencia operativa, la protección de activos y la generación de valor sostenible. Asimismo, desde una perspectiva académica, la investigación aporta al desarrollo de estudios aplicados en gestión de riesgos, evidenciando la importancia de adaptar modelos teóricos a contextos reales.

Finalmente, el estudio resulta necesario porque no solo busca resolver una problemática específica dentro de la organización, sino también servir como referencia para otras empresas del sector que enfrentan desafíos similares. De esta manera, se contribuye a la difusión de buenas

prácticas en gestión de riesgos, promoviendo una cultura organizacional orientada a la prevención, la mejora continua y la resiliencia empresarial (Castellanos, 2015) (Christopher, 2016)

CAPITULO 2:

LA ORGANIZACIÓN

2. PERFIL DE LA ORGANIZACIÓN.

2.1. NOMBRE, ACTIVIDADES, MERCADOS SERVIDOS Y PRINCIPALES CIFRAS

2.1.1 Nombre de la empresa

SYTSA S.A. es una empresa ecuatoriana dedicada a la provisión de soluciones logísticas integrales en el sector del transporte terrestre de carga y servicios logísticos en la Comunidad Andina de Naciones.

2.1.3 Misión, visión, valores

Contribuir al éxito empresarial de nuestros clientes proporcionando excelencia operativa con soluciones logísticas integrales, inteligentes y sostenibles.

Su visión está enfocada en ser un referente en soluciones logísticas integrales a nivel nacional e internacional, respaldado por innovación, tecnología, seguridad, sostenibilidad y excelencia operativa para generar valor con sus clientes.

Entre sus valores corporativos destacan la ética, innovación, compromiso, responsabilidad social y orientación al cliente.

2.1.3 Actividades, marcas, productos y servicios

La empresa desarrolla actividades relacionadas con:

- Prestación de servicios de transporte pesado mensualizado.
- Prestación de servicios de transporte pesado por proyectos.
- Almacenaje temporal de carga en frontera con Colombia en Tulcán.
- Almacenaje y transporte de materiales químicos peligrosos.
- Alquiler de grúa y manejo de control de izaje de carga pesada.

Marca

La marca SYTSA® se orienta al fortalecimiento de la competitividad de sus clientes en el mercado mediante la provisión de soluciones logísticas integrales, eficientes y estratégicamente diseñadas. Su propuesta de valor se fundamenta en la optimización de la cadena de suministro a través de infraestructura de alta calidad y sistemas de movilidad de carga que garantizan cobertura en diversas regiones geográficas.

En este sentido, la organización se posiciona como un actor clave dentro del sector logístico, al facilitar la articulación entre productores y consumidores finales, reduciendo las barreras asociadas al tiempo y la distancia. Asimismo, su experiencia en el sector le permite ofrecer

un servicio confiable, caracterizado por la puntualidad en las entregas y la adaptación a las dinámicas del mercado contemporáneo.

Figura 1

Logotipo de la empresa SYTS S.A.

Nota: Elaborado por: SYTSA S.A

Productos

- Comunidad Andina (CAN) y MERCOSUR

SYTSA® desarrolla operaciones en los mercados de la Comunidad Andina (CAN) y el Mercado Común del Sur (MERCOSUR), participando en un entorno de integración regional que promueve la libre circulación de bienes, servicios y factores productivos. Este marco contempla

además la coordinación de políticas macroeconómicas y sectoriales, así como la armonización normativa entre los Estados miembros.

- Sector petróleo y energía

La empresa brinda servicios logísticos especializados al sector petrolero y energético, abarcando el diseño integral de la cadena logística, la gestión documental, la coordinación de transporte multimodal y el despacho aduanero, hasta la entrega final en sitio.

- Sector minero

En el ámbito minero, SYTSA® garantiza altos estándares de seguridad en la manipulación de cargas sobredimensionadas y de gran volumen, priorizando la eficiencia operativa, la puntualidad y la optimización de costos.

- Sector químico

La organización ofrece soluciones logísticas adaptadas al sector químico, cumpliendo estrictamente con normativas de seguridad y control ambiental, mediante procesos diseñados bajo estándares internacionales de calidad.

- Izaje de carga pesada

La empresa dispone de equipamiento hidráulico especializado para el montaje y desmontaje de infraestructura industrial, así como para operaciones de carga y descarga de contenedores y equipos de gran tamaño.

- Productos perecibles

SYTSA® garantiza la integridad y frescura de productos perecibles, mediante soluciones logísticas que optimizan tiempos de entrega, reducen desperdicios y aseguran la calidad del producto final.

Servicios

- Transporte aéreo y marítimo

La empresa ofrece servicios de transporte de carga a nivel nacional e internacional, incluyendo mercancías especiales como productos químicos y graneles, asegurando tiempos de entrega eficientes.

- Transporte terrestre

SYTSA® gestiona el transporte terrestre mediante una red logística que garantiza cobertura, seguridad y eficiencia en la distribución de mercancías.

- Aduanas y almacenamiento

La organización proporciona servicios de gestión aduanera y almacenamiento, facilitando el cumplimiento normativo y la optimización de inventarios.

- Proyectos logísticos

La empresa cuenta con un equipo especializado en logística de proyectos, orientado a la planificación, diseño y ejecución de operaciones complejas en entornos desafiantes, bajo criterios de sostenibilidad.

- Ingeniería del transporte

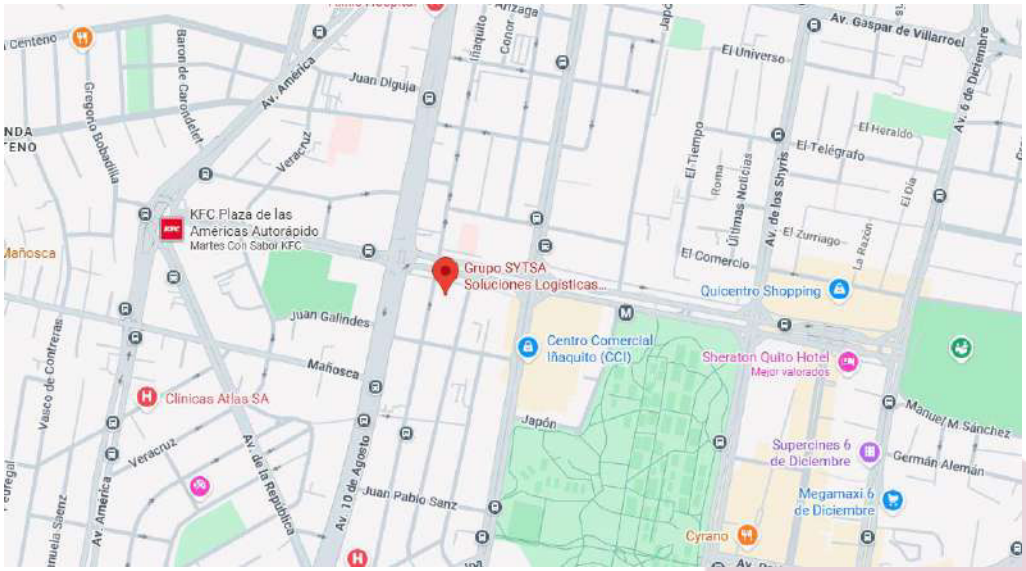
SYTSA® desarrolla soluciones de ingeniería aplicadas al transporte, enfocadas en la seguridad, la eficiencia operativa y la mejora continua de la productividad.

2.1.4 Ubicación de la sede

La empresa opera en Ecuador y se encuentra registrada legalmente en el país bajo la normativa de la Superintendencia de Compañías, Valores y Seguros.

Figura 2

Ubicación sede matriz de la empresa SYTSA S.A.



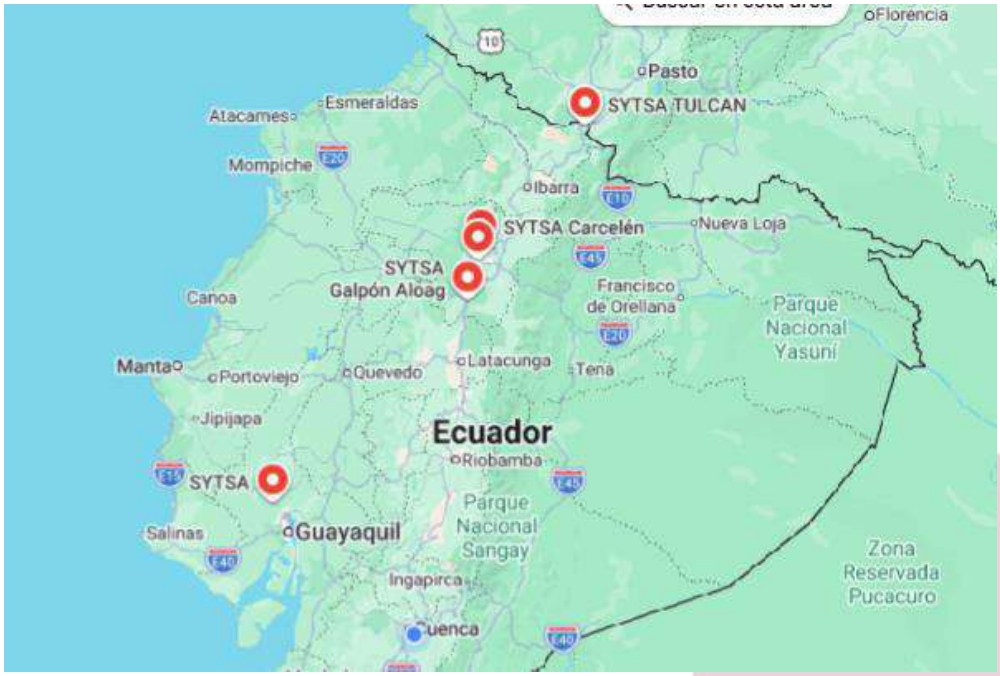
Nota: Fuente (SYTSA, 2023)

2.1.5 Ubicación de las operaciones

Las operaciones comerciales y técnicas se desarrollan dentro del territorio ecuatoriano, atendiendo tanto al sector público como privado.

Figura 3

Ubicación de las sedes y sucursales de la empresa SYTSA S.A en Ecuador



Nota: Fuente (SYTSA, 2023)

2.1.6 Propiedad y forma jurídica

SYTSA está constituida como sociedad anónima (S.A.), conforme a la Ley de Compañías del Ecuador.

- Denominación de la compañía: Transportes y Servicios Asociados SYTSA CIA. LTDA
- Sector: Societario

- Número de expediente: 90657
- Domicilio: Quito
- RUC: 1791770358001
- Representante(s) legal(es): Chávez Ortiz Luis Arturo
- La compañía tiene actual existencia jurídica y su plazo social concluye el: 20-03-2051
- Disposición judicial que afecta a la compañía: Ninguna
- Capital social: $ 3,000,000
- Situación actual: Activa

Figura 4

Suscripción legal de la empresa SYTSA S.A.

SOCIOS O ACCIONISTAS DE LA COMPAÑIA

No. de Expediente: 90657

No. de RUC de la Compañía: 1791770358001

Nombre de la Compañía: TRANSPORTES Y SERVICIOS ASOCIADOS SYTSA CIA. LTDA

Situación Legal: ACTIVA

Disposición judicial que afecta a la compañía: NINGUNA

No.	IDENTIFICACIÓN	NOMBRE	NACIONALIDAD	TIPO DE INVERSIÓN	CAPITAL	RESTRICCIÓN
1	1710548643	CHAVEZ LASCANO IGOR PAUL	ECUADOR	NACIONAL	$ 300,000 .0000	N
2	1712905353	CHAVEZ LASCANO LUIS GUILLERMO	ECUADOR	NACIONAL	$ 300,000 .0000	N
3	1713382354	CHAVEZ ORTIZ CHRISTIAN OLMEDO	ECUADOR	NACIONAL	$ 300,000 .0000	N
4	1711413748	CHAVEZ ORTIZ JORGE RENATO	ECUADOR	NACIONAL	$ 300,000 .0000	N
5	1710119288	CHAVEZ ORTIZ LUIS ARTURO	ECUADOR	NACIONAL	$ 600,000 .0000	N
6	1702393271	CHAVEZ VALLEJO LUIS ARTURO	ECUADOR	NACIONAL	$ 1,200,000 .0000	N

CAPITAL SUSCRITO DE LA COMPAÑIA (USD)$: 3,000,000.0000

Nota: Extraído de la Superintendencia de Seguros y Compañías

2.1.7 Mercados servidos o ubicación de sus actividades de negocio

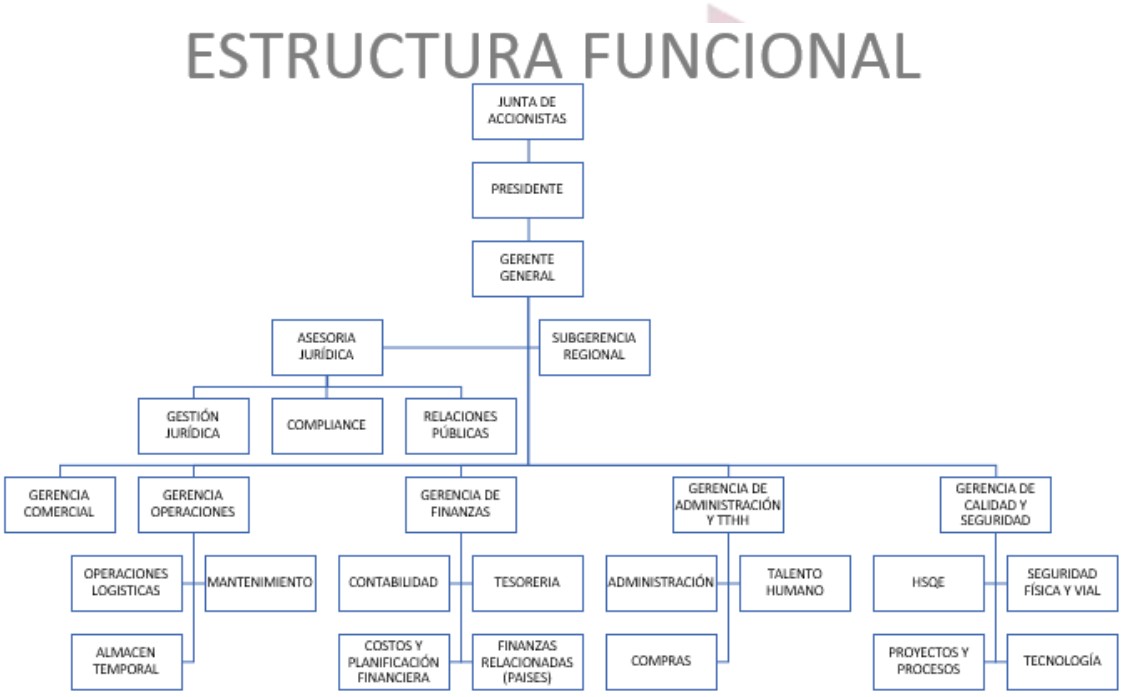
La empresa atiende a mercados diversificados entre los que destacan: industriales, comerciales y tecnológicos en Ecuador con la prestación de servicios logísticos integrales

2.1.8 Tamaño de la organización

Corresponde a una empresa del sector privado con estructura organizacional formal, personal técnico especializado y enfoque empresarial orientado a la eficiencia operativa.

Figura 5

Organigrama de la empresa SYTSA S.A.



Nota: Elaborado por SYTSA

2.1.9 Información sobre empleados y otros trabajadores

En el marco del análisis organizacional, se realizó la caracterización del talento humano de la empresa SYTSA®, a partir de la información correspondiente a la planilla del Instituto Ecuatoriano de Seguridad Social (IESS), con el propósito de identificar la distribución del personal según variables demográficas básicas.

En este contexto, la organización cuenta con un total de 410 colaboradores, lo que evidencia una estructura organizacional de tamaño mediano con una alta capacidad operativa. En cuanto a la distribución por género, se identificó que 340 colaboradores corresponden al género masculino, mientras que 70 pertenecen al género femenino.

Desde una perspectiva porcentual, la composición del talento humano refleja una marcada predominancia del personal masculino, representando el 82,93 % del total de empleados, en contraste con el 17,07 % correspondiente al personal femenino. Esta distribución puede asociarse a la naturaleza del sector logístico y de transporte, el cual históricamente ha presentado una mayor participación masculina, especialmente en áreas operativas.

Tabla 1

Distribución del personal por género en SYTSA®

Indicador	Valor	Porcentaje %
Número total de empleados	410	100
Número de hombres	340	82,93
Número de mujeres	70	17,07

Nota. Los valores fueron estimados mediante análisis nominal de los nombres registrados en la planilla del IESS, por lo que pueden presentar un margen de error.

Análisis e implicaciones

La distribución del talento humano evidencia una brecha de género significativa, lo cual constituye un elemento relevante para el análisis organizacional y la formulación de estrategias de gestión del talento humano. En este sentido, la empresa podría considerar la implementación de políticas orientadas a la equidad de género, especialmente en áreas donde tradicionalmente la participación femenina ha sido limitada.

Asimismo, este análisis se complementa con el levantamiento de información adicional relacionada con variables como los puestos de trabajo desempeñados, los rangos de edad del personal y la estructura directiva de la organización, lo cual permitirá una comprensión integral de la dinámica organizacional.

2.1.10 Procesos claves relacionados con el objetivo propuesto

Procesos Estratégicos

- Proceso: Planificación Estratégica

Objetivo: Proporcionar una guía clara y concisa, para el desarrollo y la dirección de la organización.

Inicia: Desde la definición del plan

Termina: Evaluación del plan

- Proceso: Gestión de SIG

Objetivo: Velar por el óptimo funcionamiento de los sistemas de Gestión de Calidad, Seguridad, Salud y medio ambiente implementados por la compañía

Alcance: Todos los procesos de SYTSA

Procesos de Valor

- Proceso: Gestión de Operaciones

Objetivo: Cumplir y operativizar los servicios de transporte, almacenamiento, alquiler de equipos especiales asignando recursos y registrando en los sistemas de SYTSA.

Inicia: Desde la recepción del pedido

Termina: Hasta el servicio ejecutado y facturado

Procesos de Apoyo

- Proceso: Gestión Comercial

Objetivo: Planificar, implementar y seguir las estrategias y acciones que permitan aumentar las ventas, mejorar la rentabilidad y fortalecer la posición competitiva de la empresa en el mercado.

Empieza: Requerimiento de servicio

Termina: Cotización, venta

- Proceso: Gestión Jurídica

Objetivos: Gestionar la administración de seguros y sistema documental para la flota vehicular.

Brindar un asesoramiento jurídico para la toma de decisiones por parte de la administración de la empresa.

Empieza:

- Necesidad de obtener/renovar un contrato de seguro

- Necesidad de obtener y/o mantener al día los documentos habilitantes

- Necesidad de brindar asesoramiento jurídico

Termina:

- Entrega física/virtual de pólizas

- Documento entregado a operaciones

- Inquietud jurídica solventada

- Proceso: Gestión de Mantenimiento

Objetivo: Mantener la disponibilidad de los equipos conforme la planificación de mantenimiento en términos de costos y servicios.

Empieza: Necesidad de mantenimiento

Termina: Mantenimiento ejecutado

- Proceso: Gestión de Seguridad Física y Vial

Objetivo: Identificar evaluar y controlar los riesgos asociados a la mercadería en el proceso de transporte y almacenamiento de distribución primaria.

Empieza: Solicitudes de inspección, registros, requerimientos

Termina: Inspecciones, trazabilidad, informes

- Proceso: Gestión de Talento Humano

Objetivo: Implementar un modelo de gestión de talento humanos que permita atraer, retener y desarrollar a las personas.

Inicia: Requerimiento de personal calificado

Termina: Personal calificado

- Proceso: Gestión de Tecnologías de da Información

Objetivo: Ofrecer seguridad, disponibilidad y escalabilidad.

Inicia: Recepción de novedades en sistemas y equipos

Termina: Solución de novedades

- Proceso: Gestión de Compras

Objetivo: Cubrir las necesidades de adquisición de insumos y servicios.

Empieza: Requerimiento de compra

Termina: Compra de bienes y servicios

- Proceso: Gestión Administrativa

Objetivo: Administrar los recursos materiales y activos.

Inicia: Requerimientos administrativos

Termina: Documentación actualizada

- Proceso: Gestión de Proyectos y Procesos

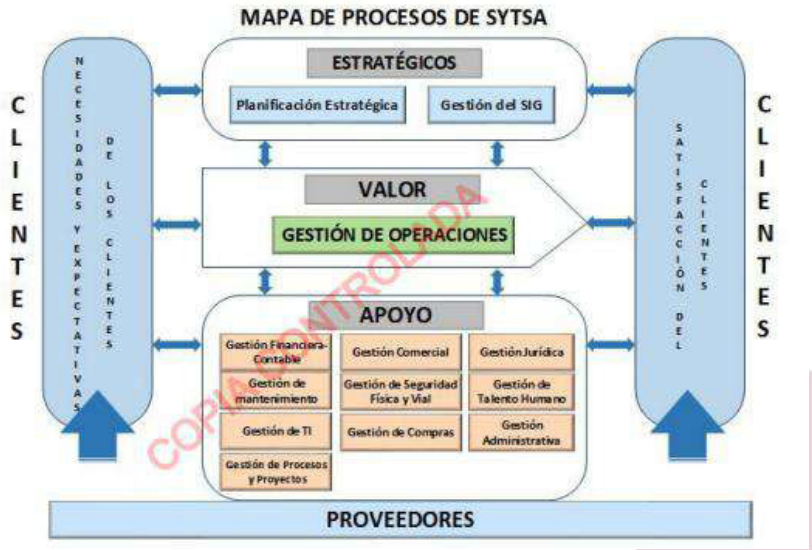
Objetivo: Identificar, evaluar y controlar las necesidades de levantamiento de procesos y proyectos.

Empieza: Necesidad de levantamiento

Termina: Procesos actualizados y proyectos implementados

Figura 6

Mapa del proceso de la gestión de proyectos y procesos



Nota: Fuente SYTSA S.A.

2.1.11 Principales cifras, ratios y números que definen a la empresa

Como empresa privada, sus indicadores financieros incluyen ingresos operacionales, margen de rentabilidad, liquidez y capacidad operativa, conforme a los estados financieros reportados ante organismos de control.

Capital Social: Tres millones de dólares (USD 3.000.000,00)

Capital Suscrito de La Compañía: Tres millones de dólares (USD 3.000.000,00)

Este es la información disponible de la empresa, el resto de información financiera es de carácter reservado.

2.1.12 Modelo de negocio

SYTSA opera bajo un modelo de proveedor integral de soluciones logísticas, en el que no solo ofrece transporte de carga, sino que diseña, coordina y administra toda la cadena logística de sus clientes mediante soluciones personalizadas, tecnología especializada y sistemas internacionales de gestión

2.1.13 Grupos de interés internos y externos

- Proveedores.
- Contratistas.
- Empleados.
- Médico ocupacional.
- Accionistas.
- Gerente General.
- Visitantes.

Tabla 2

Matriz de grupos de interés interno y externo

MATRIZ DE PARTES INTERESADAS

1. Identificación		2. Interacción		3.Requerimientos		4. Responsables
Parte interesada	Grupos de Interés	Proceso con el que interacciona	Necesidades	Expectativas	Seguimiento	
Proveedores, Contratistas, Visitantes	Externo	Compras	Pronto pago	La empresa legalmente constituida Frecuencia de compras	Establecer procedimientos de control y actualización de cumplimiento legal	Jefe de compras, Asistente de compras
		Adquisiciones	Adelanto de pagos	Contar con el SIG Estabilidad o liquidez	Implementar el SID, BASC y contar con otras certificaciones	
		Administrativo	Firma de contrato	Seguridad y confianza Contrato corto o largo plazo	Evaluar a proveedores continuamente con la matriz de proveedores y nivel de criticidad	

MATRIZ DE PARTES INTERESADAS

1. Identificación		2. Interacción	3.Requerimientos			4. Responsables
Parte interesada	Grupos de Interés	Proceso con el que interacciona	Necesidades	Expectativas	Seguimiento	
Empleados	Interno	Talento Humano	Pago a tiempo de salarios, bienestar social, exámenes médicos, salario acorde al mercado laboral, cumplimiento con la seguridad social	Mejorar el clima laboral de acuerdo a las competencias	Establecer procedimientos de control, cumplimiento y capacitación Encuesta de clima laboral Programa de vigilancia médica Evaluación anual de desempeño	Jefe de RR HH
Médico Ocupacional	Interno	Talento Humano	Exámenes médicos preocupacionales Dispensario médico, infraestructura e insumos	Mantener y mejorar el estado de salud de los trabajadores de la organización	Plan de vigilancia de salud	Medico Ocupacional y RR HH

MATRIZ DE PARTES INTERESADAS

1. Identificación		2. Interacción	3.Requerimientos			4. Responsables
Parte interesada	Grupos de Interés	Proceso con el que interacciona	Necesidades	Expectativas	Seguimiento	
Accionistas	Interno	Gerente General	Utilidades positivas de la empresa	Crecimiento de la empresa. Mejorar el estándar de calidad del servicio	Reunión de Kapex	Junta de Accionistas
Gerente General	Interno	Accionistas	Estructura organizacional eficaz Liquidez financiera continua Personal capacitado en jefaturas Flota operativa	Crecimiento de la empresa con reconocimiento nacional e internacional	Reunión de Kapex, reunión bianual de accionistas para la evaluación de la empresa	Junta de Accionistas

Nota: Fuente SYTSA S.A.

2.1.14 Otros datos de interés

La empresa se encuentra sujeta a regulación ecuatoriana en materia societaria, tributaria y laboral.

CAPITULO 3. SEGURIDAD DE LA INFORMACIÓN

3.1 Análisis de riesgos

3.1.1 Identificación de la organización y sus centros de trabajo

Nombre de la organización:

Transportes Y Servicios Asociados Sytsa Cia. Ltda

Sede principal

- Pichincha / Quito / Iñaquito / Av. Naciones Unidas E2-30 Y Núñez De Vela

Sucursales

- Carchi / Tulcán / Urbina (Taya) / Panamericana Norte S/N
- Pichincha / Mejía / Machachi / Panamericana Norte 2 Y Sn
- Guayas / Nobol / Narcisa De Jesús (Nobol) / Vía a Nobol Guayaquil - Petrillo
- Guayas / Guayaquil / Guayaquil / Alfa S/N Y Mangos

3.1.2 Representante legal y responsable de seguridad

Representante legal

Chávez Ortiz Luis Arturo

Analista de procesos

Toapanta Sandoval Nicole Germania

3.1.3 Actividades de la organización

Todas las actividades de transporte de carga por carretera, incluido en camionetas de: troncos, ganado, transporte refrigerado, carga pesada, carga a granel, incluido el transporte en camiones cisterna, automóviles, desperdicios y materiales de desecho, sin recogida ni eliminación.

3.1.4 Tratamientos de la organización y sus riesgos

La empresa SYTSA S.A. se desarrolla en el mercado logístico dónde existen varias amenazas a la seguridad empresarial las cuales pueden afectar a la confiabilidad y la imagen de la organización lo que puede detener la detención de flotas de transporte y provocar retrasos y pérdidas significativas

Algunos de los principales riesgos a los que enfrenta la empresa son:

Clientes

- *Phishing:* Al enviar correos falsos o con virus pueden obtener información confidencial como credenciales de acceso al software de la empresa o descargar portales de rastreo de la mercadería que se transporta.
- *Filtración de datos:* Al existir una filtración de datos pueden obtener información personal

de la base de datos de la empresa como por ejemplo direcciones, números de teléfono e información financiera.

- *Suplantación de identidad:* Con información extraviada se pueden generar fraudes financieros en contra al titular de los datos.

Proveedores

- *Ataques a la cadena de suministro:* En caso de una infiltración al software de proveedores del dominio del departamento de TI.
- *Suplantación de proveedores:* Contratan el servicio con cuentas bancarias falsas para desviar los pagos de las facturas
- *Malware en documentos compartidos:* Infección de virus a los archivos enviados por correo

Colaboradores

- *Ransomware:* Apertura de archivos con virus enviados por correo.
- *Pérdida o robo de dispositivos móviles.*
- *Shadow IT:* Uso de herramientas, aplicaciones o nubes no autorizadas por la empresa.

VIDEOVIGILANCIA

- *Hacking:* Los ciberdelincuentes pueden tomar el control de cámaras de seguridad debido a

accesos débiles.

- *Ataques de denegación de servicio:* Sobrecargan las cámaras con tráfico falso que provoca la inhabilitación de sistema de vigilancia.
- *Vulnerabilidad en dispositivos IoT:* Al no estar actualizados o tener una mala configuración pueden usarse como entrada para afectar a la red corporativa de la empresa.
- *Espionaje industrial:* El acceso a las cámaras pueden permitir robar información comercial sensible.

3.1.5 Consentimientos y notas informativas

Consentimiento para el tratamiento de datos personales

Yo, [NOMBRE DEL CLIENTE], portador de la cédula de ciudadanía No. [XXXXXX], por medio del presente documento, manifiesto de forma libre, previa, específica, informada e inequívoca mi consentimiento a favor de la empresa SYTSA S.A que en adelante se lo dominara como LA EMPRESA para el tratamiento de mis datos personales, incluyendo pero no limitándose a: nombres, apellidos, número de cédula, dirección, fecha de nacimiento, datos de contacto (teléfono fijo, celular, correo electrónico) y demás datos contemplados en la normativa vigente, bajo los siguientes términos:

1. Finalidad del tratamiento de datos personales

Declaro conocer que mis datos personales serán tratados con las siguientes finalidades:

- Proveer los productos y servicios ofrecidos por LA EMPRESA.
- Gestionar la relación contractual y comercial con el cliente.

- Realizar procesos de facturación, cobro y gestión administrativa.
- Cumplir obligaciones legales y regulatorias.
- Ejecutar actividades de atención al cliente y soporte técnico.
- Realizar encuestas de satisfacción y evaluación de calidad del servicio.
- Desarrollar actividades de promoción, publicidad y marketing de servicios actuales y futuros.
- Elaborar estudios de mercado y mejora continua de los servicios.

2. Naturaleza de los datos recolectados

Reconozco que los datos proporcionados:

- Serán almacenados en bases de datos físicas y/o digitales.
- Serán tratados únicamente por personal autorizado o encargados debidamente contratados.
- Estarán protegidos bajo medidas de seguridad y confidencialidad conforme a la LOPDP.

3. Base legal del tratamiento

El tratamiento de mis datos personales se realiza con base en mi consentimiento, conforme a lo dispuesto en la Ley Orgánica de Protección de Datos Personales del Ecuador.

4. Consentimiento informado

Declaro haber sido informado de manera clara, precisa y suficiente sobre:

- La finalidad del tratamiento de mis datos personales.
- El uso y destino de los mismos.
- Los derechos que me asisten como titular.

Otorgo mi consentimiento de manera libre y voluntaria.

5. Derechos del titular

Conozco que puedo ejercer en cualquier momento los siguientes derechos sobre el tratamiento de mis datos:

- Acceso
- Rectificación y actualización
- Eliminación
- Oposición
- Portabilidad
- Suspensión del tratamiento

6. Mecanismos para ejercer derechos

Podré ejercer mis derechos mediante solicitud dirigida a:

SYTSA S.A.

Correo electrónico: _____

Dirección: _____

La empresa atenderá la solicitud dentro de los plazos establecidos en la normativa vigente.

7. Revocatoria del consentimiento

Podré revocar este consentimiento en cualquier momento, sin efectos retroactivos, conforme a la LOPDP.

8. Seguridad y confidencialidad

LA EMPRESA garantiza la implementación de medidas técnicas, organizativas y legales necesarias para proteger mis datos personales contra:

- Acceso no autorizado
- Pérdida
- Alteración

- Uso indebido

9. Transferencia o comunicación de datos

Mis datos personales podrán ser compartidos con:

- Autoridades competentes, cuando sea requerido por ley.
- Proveedores o terceros encargados del tratamiento, bajo contratos que garanticen la protección de datos.

10. Duración del tratamiento de los datos

Mis datos serán conservados:

- Durante la vigencia de la relación comercial o contractual.
- Durante el tiempo necesario para cumplir obligaciones legales.
- Posteriormente, serán eliminados o anonimizados de forma segura.

11. Videovigilancia

Declaro conocer que LA EMPRESA podrá contar con sistemas de videovigilancia, por lo que:

- Se podrán recolectar imágenes y/o videos en sus instalaciones.
- La finalidad será garantizar la seguridad de personas, bienes e infraestructura.

- Las grabaciones serán almacenadas por un período de [X días].
- El acceso a dichas grabaciones estará restringido.

Podré ejercer mis derechos respecto a estos datos mediante los canales indicados.

12. Ley aplicable

Este documento se rige por la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP) y su normativa complementaria.

13. Declaración final

Declaro que:

- He leído y comprendido íntegramente este documento.
- He sido informado de manera clara sobre el tratamiento de mis datos personales.
- Otorgo mi consentimiento de manera libre, expresa e informada.

14. Firmas

Firma del cliente

Nombre: _____

Cédula: _____

Fecha: //__

Firma del responsable

Nombre: _____

Cargo: _____

Fecha: //__

3.2 Registro de Actividades de Tratamiento

3.2.1 Grupos de información

La empresa SYTSA Cía. Ltda. gestiona información personal de sus colaboradores como parte de la administración laboral, operativa y de seguridad organizacional.

Tipos de datos tratados del personal:

- Datos identificativos (nombre, cédula)
- Datos laborales (cargo, área, funciones)
- Datos de contacto (correo corporativo)
- Datos de acceso a sistemas (credenciales)
- Datos biométricos (si aplica: huella, reconocimiento)
- Datos de geolocalización (uso de GPS en vehículos)

Información de los clientes

SYTSA trata datos de clientes en el desarrollo de sus actividades comerciales, logísticas y tecnológicas, por ejemplo:

- Datos identificativos (Nombre, Cédula o RUC)
- Datos de contacto (teléfono, correo)

- Información contractual
- Información logística (rutas, carga, operaciones)
- Datos comerciales

Información de los proveedores

La organización resguarda los datos de sus proveedores como son los datos identificativos donde en su mayoría se clasifican en:

- Datos identificativos (Nombre, Cédula, RUC, Razón Social)
- Datos de contacto (Contacto, Correo, Ubicación)
- Información financiera (Cuentas bancarias, Condiciones y términos de pagos)
- Información comercial (Historial de ventas, Especificaciones de productos o servicios)
- Información operativa (Credenciales de los operarios)
- Datos de desempeño y cumplimiento (Certificaciones nacionales e internacionales)

Videovigilancia

Existen cámaras de seguridad distribuidos en la empresa SYTSA S.A. ubicadas estratégicamente en áreas comunes y lugares de trabajo con la finalidad de salvaguardar la seguridad de las personas (internas y externas), los bienes de la institución y las instalaciones.

Los datos que se recopilan mediante el sistema de videovigilancia son:

- Imagen y video
- Audio
- Datos técnicos (ubicación, hora y fecha)

3.2.2 Sistemas de tratamiento y niveles de seguridad

La organización maneja información mediante sistemas electrónicos y, en menor medida, mediante documentación física. Los sistemas tecnológicos son administrados por el Departamento de Tecnologías de la Información, mientras que la documentación física es gestionada por las áreas administrativas correspondientes.

El tratamiento de la información puede realizarse en soporte físico, electrónico o mixto, dependiendo del tipo de proceso o sistema utilizado dentro de la organización.

En el caso de la información de los colaboradores, proveedores y de los clientes se tiene un soporte mixto y un nivel de seguridad alto debido a que se trata información confidencial que no debe ser divulgado, por ejemplo:

Soporte físico

- *Trabajador: E*xperiencia laboral, evaluaciones de desempeño, registro de asistencia a capacitaciones, actas de entrega de equipo y uniformes.

- *Cliente:* Información contractual, consentimientos, acuerdos de confidencialidad
- *Proveedor:* Ingreso y salida de proveedores, facturas, guías de remisión.

Soporte digital

- *Trabajador:* Sueldos, información bancaria, registro de asistencia, cronograma de reuniones, planificación mensual, correos, etc.
- *Cliente:* Información identificativa, de contacto, historial de compras, información crediticia, información financiera
- *Proveedor:* Información identificativa, de contacto, historial de ventas, información crediticia, información financiera

La videovigilancia a su vez se utiliza un soporte digital con un nivel de seguridad alto con monitoreos contantes ante cualquier amenaza de ataques de ciberdelincuentes que puedan hurtar información sensible mediante la infiltración al dominio de la organización. Los sistemas de videovigilancia capturan datos personales como los rasgos físicos de las personas que se monitorean en un área específica en tiempo real.

Procedimientos de resguardo de la información

Información física

- Se almacena en archivos físicos dentro de las oficinas administrativas.

- El acceso está limitado al personal autorizado de cada área.
- Los documentos se conservan según las políticas internas y necesidades operativas.

Información electrónica

- Se almacena en plataformas tecnológicas utilizadas por la empresa.
- El acceso se realiza mediante credenciales de usuario.
- La administración de usuarios y permisos es realizada por el Departamento de TI.

Niveles de seguridad aplicados

- Control de acceso a sistemas mediante usuarios y contraseñas
- Supervisión del Departamento de TI sobre plataformas tecnológicas
- Restricción de acceso a documentación física
- Uso de plataformas tecnológicas especializadas para cada proceso

El acceso a los sistemas y plataformas es limitado únicamente al personal autorizado y a los proveedores tecnológicos cuando se requiere soporte técnico, siempre bajo la supervisión del Departamento de Tecnologías de la Información.

3.2.3 Finalidades, categorías de datos, interesados y destinatarios

La organización maneja diferentes categorías de datos en el desarrollo de sus actividades administrativas, operativas y tecnológicas. Dichos datos se almacenan y gestionan a través de diferentes sistemas informáticos y procesos internos, con la finalidad de cumplir con las operaciones empresariales, obligaciones legales y gestión administrativa de la organización.

Tabla 3

Categoría de datos y finalidades

Categoría de datos	Finalidades del tratamiento	Datos incluidos	Interesados	Destinatarios
Colaboradores	Gestión interna, comunicación corporativa, control de procesos y cumplimiento de la normativa vigente de la empresa	Documentos administrativos y de procesos, registros internos, correo corporativo,	Personal interno	Jefaturas, Coordinadores, Áreas responsables
Clientes	Gestión de operaciones y logística	Información de rutas, vehículos, operaciones	Clientes	Área operativa, comercial y logística

Proveedores	Gestión empresarial	Registros de operaciones, gestión administrativa	Proveedores	Área comercial y logística
Videovigilancia	Seguridad física y de bienes de la empresa	Imagen, video, audio y datos técnicos	Departamento de seguridad, personal interno	Jefaturas, coordinadores,

Nota: Sytsa Cia. Ltda (2025)

3.2.4 Encargados de los tratamientos

Las siguientes empresas brindan servicios tecnológicos relacionados exclusivamente con la infraestructura, sistemas y plataformas administradas por el Departamento de TI.

Tabla 4

Empresas relacionadas a brindar servicios o soporte al departamento de TI

Empresa	Tipo de soporte	Sistemas / Servicios
Intelworks	Soporte TI	Nigisu, UniFi, cámaras de seguridad e infraestructura tecnológica
Augusto Pesantes	Soporte Técnico	Soporte del Sistema Nigisu

Killka	Soporte, desarrollo y configuración ERP	ERP Odoo
Cloudfleet	Plataforma tecnológica	Sistema de gestión de flotas
Silogtran	Plataforma tecnológica	Sistema logístico de transportes
ISOLUCION	Plataforma de gestión	Sistema de gestión ISO
Correo web Roundcube	Servicio de correo	Plataforma de correo electrónico

Nota: Sytsa Cia. Ltda. (2025)

3.3 Registro de dispositivos

La empresa SYTSA S.A mantiene 271 celulares corporativos para uso exclusivo de trabajo en el cual se divide en las áreas de logística, comercial (compras y vetas), administrativas, jefaturas y gerencias con el fin de mantener una clara comunicación entre departamentos y para el desempeño de sus diferentes funciones. De igual manera, la empresa cuenta con un despliegue total de 98 cámaras distribuidas en las diferentes sucursales de la organización a nivel nacional.

Adicional se mantiene un registro de dispositivos de computación que se detalla a continuación.

Tabla 5

Registro de dispositivos de computación

SEDE	UBICACIÓN	ÁREA	MARCA	MODELO
NNUU	Oficina 1605	Operaciones	Dell	Inspiron 15 3520 (escritorio)
Machachi	Camper Ambiental	Operaciones	Dell	Inspiron 14-3467 (escritorio)
Petrillo	Camper Operaciones	Operaciones	Dell	Inspiron 3501(escritorio)
NNUU	Oficina 1605	Comercial	Dell	Latitude 3440(escritorio)
NNUU	Oficina 1605	Operaciones	HP	HP Laptop 14-em0026la
NNUU	Oficina 1402	Jurídico	Dell	Inspiron 3501(escritorio)
NNUU	Oficina 1204	Administrativo y TTHH	Toshiba	Dynabook Portege X40-J
NNUU	Oficina 1203	Calidad y Seguridad	Dell	Inspiron 15 3511(escritorio)
Petrillo	Teletrabajo	Operaciones	HP	HP ProBook 450 G4

NNUU	Oficina 1203	Calidad y Seguridad	HP	HP 255 15.6 inch G10 Notebook PC
Machachi	Camper Operaciones	Operaciones	Dell	Inspiron 15 3511(escritorio)
NNUU	Oficina 1204	Financiero	Dell	Inspiron 15 3525(escritorio)
Tulcán	Oficina Almacén Temporal	Almacén Temporal	Dell	Inspirion 15 3511(escritorio)
NNUU	Oficina 1204	Administrativo y TTHH	HP	HP 250 15.6 inch G10 Notebook PC
NNUU	Oficina 1204	Administrativo y TTHH	HP	ProBook 440 G8 Notebook PC
Machachi	Camper Oil Services	Operaciones	HP	HP Laptop 14-cf2523la
Machachi	Camper Operaciones	Operaciones	Dell	Vostro 3400
Machachi	Oficina 1204	Operaciones	Dell	Inspiron 15 3511(escritorio)
NNUU	Oficina 1204	Financiero	HP	HP ProBook 440 G8 Notebook PC
NNUU	Oficina 1204	Financiero	Dell	Inspiron 15 3520(escritorio)
NNUU	Oficina 1402	Jurídico	HP	HP 250 15,6 inch G10 Notebook PC

Machachi	Campero Mantenimiento	Mantenimiento	Dell	Inspiron 15 3520(escritorio)
Guayaquil	Linde Bulk	Calidad y Seguridad	Lenovo	IdeaPad 3 15ITL6 82H8 (Tablet)
Machachi	Camper Seguridad	Calidad y Seguridad	Dell	Inspiron 15 3520(escritorio)
NNUU	Oficina 1204	Administrativo y TTHH	HP	HP 250 15.6 inch G10 Notebook PC
NNUU	Oficina 1203	Calidad y Seguridad	Apple	MacBook Air (laptop)
Machachi	Teletrabajo	Calidad y Seguridad	HP	HP 250 15,6 inch G10 Notebook PC
NNUU	Oficina 1203	Calidad y Seguridad	Asus	VivoBook X1605VA (laptop)
Machachi	Bodega	Compras	Lenovo	Ideapad 110 -15ISK
Tulcán	Operaciones	Calidad y Seguridad	Dell	Vostro 3490
Machachi	Camper Compras	Administrativo y TTHH	HP	HP Laptop 15-ef109la
Petrillo	Bodega	Operaciones	Toshiba	Dynabook Portege X40 -J
Machachi	Bodega	Compras	Dell	Inspiron 15 3511(escritorio)

Petrillo	Camper Operaciones Puerto	Operaciones	HP	HP 250 15.6 inch G10 Notebook PC
Machachi	Campero Mantenimiento	Mantenimiento	Dell	Vostro 14 3420
NNUU	Oficina 1203	Calidad y Seguridad	Dell	Latitude 5540
NNUU	Oficina 1605	Comercial	HP	HP 250 15.6 inch G10 Notebook PC
NNUU	Oficina 1605	Comercial	HP	HP 250 15.6 inch G9 Notebook PC
Guayaquil	Indura	Operaciones	HP	HP 250 G8 Notebook PC
Petrillo	Tenaris	Externo	Dell	Latitude 5440
NNUU	Oficina 1605	Operaciones	HP	HP Laptop 15-fd0053la
Tulcán	Oficina Almacén temporal	Operaciones	Asus	X555QA
Machachi	Camper Compras	Administrativo y TTHH	HP	HP Laptop 15-fd0053la
Tulcán	Bodega Almacén temporal	Almacén Temporal	Dell	Inspiron 15 3511(laptop)
Tulcán	Oficina Almacén Temporal	Almacén Temporal	Dell	Inspirion 15 3520 (laptop)

Tulcán	Oficina de Transporte	Operaciones	HP	348 G7(laptop)
Tulcán	Oficina Almacén Temporal	Calidad y Seguridad	HP	HP 14-cf2523la (laptop)
Tulcán	Oficinas Generales	Operaciones	HP	HP 255 15.6 inch G10 Notebook PC
NNUU	Oficina 1204	Financiero	Dell	Inspiron 15 3520 (laptop)
Machachi	BODEGA SLB	Operaciones	HP	HP 348 G7(laptop)
Guayaquil	Indura	Calidad y Seguridad	Dell	Inspiron 15 3520 (laptop)
Petrillo	Patio Petrillo	Operaciones	Dell	Inspiron 15 3520 (laptop)
NNUU	Oficina 1204	Compras	HP	HP 250 15,6 inch G10 Notebook PC
Machachi	Camper Seguridad	Calidad y Seguridad	Dell	Latitude 3440
Machachi	Camper Seguridad	Calidad y Seguridad	HP	Hp Laptop 14-dq2159la
Machachi	Camper Seguridad	Calidad y Seguridad	Dell	Inspiron 15 3511 (laptop)
Machachi	Camper Seguridad	Calidad y Seguridad	Dell	Latitude 3440

Guayaquil	Linde Cilindros	Operaciones	Dell	Inspiron 15 3520 (laptop)
Machachi	Camper Ambiental	Calidad y Seguridad	Dell	Latitude 3410
NNUU	Oficina 1605	Operaciones	HP	HP 250 15,6 inch G10 Notebook PC
Guayaquil	Agencia de aduana Sytsa	Aduana	HP	HP 250 15,6 inch G10 Notebook PC
Guayaquil	Agencia de aduana Sytsa	Aduana	HP	HP 250 15,6 inch G10 Notebook PC
Machachi	Camper Seguridad	Calidad y Seguridad	Dell	Latitude 3440
Machachi	Linde Cilindros	Operaciones	HP	HP 250 15,6 inch G10 Notebook PC
Machachi	Camper Mantenimiento	Operaciones	Dell	Inspiron 15-3567 (laptop)
NNUU	Oficina 1605	Operaciones	HP	HP Laptop 14-cf2523la
Machachi	Camper Mantenimiento	Operaciones	HP	HP Laptop 14-cf2523la
Machachi	Monitoreo	Calidad y Seguridad	Dell	Inspiron 3458 (laptop)
Machachi	Camper Mantenimiento	Operaciones	Dell	Latitude 3510

Machachi	Camper Mantenimiento	Operaciones	HP	HP 348 G5
Machachi	Camper Mantenimiento	Mantenimiento	HP	HP Laptop 14-cf2523la
Machachi	Camper Operaciones	Financiero	Toshiba	Dynabook Satellite Pro C40-J
Machachi	Camper Oil Services	Operaciones	Dell	Latitude 3410
NNUU	Oficina 1204	Financiero	Dell	Inspiron 15 3520 (laptop)
NNUU	Oficina 1203	Calidad y Seguridad	Lenovo	Legion 5 16IRX9
Machachi	Camper TTHH	Administrativo y TTHH	Dell	Inspiron 15 3511 (laptop)
NNUU	Oficina 1203	NNUU	HP	HP ENVY x360 Convert 15m-es0013dx
Petrillo	Camper Operaciones	Operaciones	Dell	Inspiron 3511 (laptop)
Machachi	Camper TTHH	Administrativo y TTHH	Dell	Inspiron 15 3511 (laptop)
Machachi	Camper Seguridad	Monitoreo	Panasonic	CF-VEK33 (monitor)

NNUU	Oficina 1402	Jurídico	HP	ProBook 440 G7
NNUU	Oficina 1605	Operaciones	Dell	Vostro 14 5410
Petrillo	Bodega SLB	Compras	Panasonic	CF-53
Machachi	Oficinas Oil Services	Operaciones	Dell	Vostro 3420
NNUU	Oficina 1204	Administrativo y TTHH	Dell	Inspiron 15 3520 (laptop)
Guayaquil	Linde Bulk	Operaciones	Dell	Latitude 5420
Machachi	Camper Mantenimiento	Mantenimiento	Panasonic	CF-VEK33
Machachi	Camper Compras	Administrativo y TTHH	HP	HP Laptop 15-fd0053la
Guayaquil	Linde Cilindros SUR	Operaciones	HP	HP Laptop 17-by4xxx
Machachi	Bodega Repuestos SYTSA	Administrativo y TTHH	Dell	Vostro 3420
Machachi	Bodega Repuestos SYTSA	Administrativo y TTHH	Dell	Inspiron 15 3511 (laptop)
NNUU	Oficina 1204	Administrativo y TTHH	HP	HP 250 15.6 inch G10 Notebook PC

Machachi	Garita Machachi		Guardiania	HP	Laptop 14-bs0xxx
Machachi	Camper Operaciones		Operaciones	HP	Laptop 14-dq2519la
Tulcán	Operaciones		Operaciones	HP	HP Laptop 15-fd0053la
NNUU	Oficina 1605		Operaciones	HP	HP Laptop 15-fd0053la
NNUU		1204	Administrativo y TTHH	Dell	15 DC15250
Guayaquil	Linde Cilindros/Bulk		Operaciones	HP	HP 255 G10
NNUU	Oficina 1605		Operaciones	HP	HP 250 15,6 inch G10
Tulcán	Oficina de Transporte		Operaciones	Dell	Inspiron 15 3511 (laptop)
NNUU	Oficina 1204		Financiero	Dell	15 DC15250
NNUU	Oficina 1204		Financiero	Dell	Inspiron 15 3520 (laptop)
NNUU	Oficina 1204		Financiero	Dell	Inspiron 15 3520 (laptop)
NNUU	Oficina 1402		Financiero	Dell	Inspiron 15 3520 (laptop)

NNUU	Oficina 1203	Calidad y Seguridad	Dell	Inspiron 15 3520 (laptop)
Petrillo	Camper Operaciones	Operaciones	HP	HP 250 15.6 inch G10 Notebook PC
NNUU	Oficina 1203	Calidad y Seguridad	HP	HP Laptop 15-fd0053la
Petrillo	Camper Operaciones Puerto	Operaciones	Toshiba	Dynabook Portege X40-J
Petrillo	Garita Petrillo	Guardiania	Lenovo	IdeaPad 3 15ITL6
Petrillo	Camper Operaciones	Calidad y Seguridad	Toshiba	Dynabook Portege X40-J
Machachi	Camper Oil Services	Calidad y Seguridad	HP	Hp Laptop 15-fd0053la
Machachi	Camper TTHH	Administrativo y TTHH	Dell	Inspiron 14-3467 (laptop)
Petrillo	Camper Operaciones	Operaciones	Lenovo	IdeaPad 3 17IIL05
Petrillo	Teletrabajo	Calidad y Seguridad	HP	HP 250 G10
Guayaquil	Linde Bulk	Calidad y Seguridad	Dell	Inspiron 15 3511 (laptop)
NNUU	Oficina 1203	Administrativo y TTHH	HP	Laptop 14-dq1004la

Guayaquil	Indura	Operaciones	Dell	Latitude 5430
Petrillo	Camper Operaciones	Operaciones	HP	HP 250 15.6 inch G10 Notebook PC
Petrillo	Camper Operaciones	Operaciones	Dell	Inspiron 15 3511 (laptop)
Guayaquil	Linde (Cilindros Sur)	Operaciones	Toshiba	Dynabook Satellite Pro C40-J
Machachi	Linde Turubamba	Calidad y Seguridad	Toshiba	Dynabook Satellite Pro C40-J
Guayaquil	Linde (Cilindros Sur)	Operaciones Logísticas	HP	HP 348 G7
NNUU	Oficina 1402	Jurídico	HP	HP 348 G7
Guayaquil	Linde Norte	Operaciones	Dell	Inspiron 3558 (laptop)
NNUU	Oficina 1204	Financiero	Dell	Inspiron 15 3520 (laptop)
NNUU	Oficina 1204	Financiero	HP	Victus Laptop 16-d0510la
Tulcán	Oficina Almacén Temporal	Operaciones	HP	HP Laptop 14dq1004la
NNUU	Oficina 1605	Operaciones	Dell	Inspiron 15 3520 (laptop)

Machachi	Oficinas Santa María	Operaciones	Dell	Inspiron 3501(laptop)
Machachi	Oficinas Santa María	Operaciones	Toshiba	Dynabook Portege X40 -J
NNUU	Oficina 1605	Operaciones	Dell	Inspiron 15 3511(laptop)
Machachi	Oficinas Santa María	Operaciones	Dell	DC15251
Guayaquil	Linde Bulk	Operaciones	Dell	Latitude 7430
Petrillo	Bodega	Mantenimiento	HP	HP 250 G10
NNUU	Oficina 1203	Calidad y Seguridad	HP	HP 250 G10
Machachi	Camper Recursos Humanos	Administrativo y TTHH	HP	HP 250 G10
NNUU	Oficina 1203	Gerencia	Dell	Latitude 7440
NNUU	Oficina 1203	Gerencia	Dell	Inspiron 15 5510 (laptop)
NNUU	Oficina 1402	Gerencia	Dell	Alienware
NNUU	Oficina 1203	Presidencia	Dell	Latitude 15 3520

NNUU	Oficina 1605	Gerencia	Microsoft	SURFACE PRO
NNUU	Oficina 1204	Gerencia	HP	HP Probook 440 14 inch G10 Notebook PC
NNUU	Oficina 1204	Gerencia	Dell	Inspiron 15 5510(laptop)
Guayaquil	Agencia de aduana Sytsa	Gerencia	Apple	MacBook Air PRO M2
Machachi	Camper Gerencia	Gerencia	Apple	MacBook Air
NNUU	Oficina 1203	Gerencia	Apple	iMac 2017
Machachi	Camper Presidencia	Presidencia	Dell	Latitude 3440

Nota: Sytsa Cia. Ltda (2025)

3.4 Registro de sistemas de información

- ERP Odoo
- Plataforma de correo electrónico
- CloudFleet
- ICDSOFT
- Controlador de Dominio
- Silogtran
- Nigisu
- Antivirus corporativo Kaspersky
- Cortafuegos y seguridad de red mediante MikroTik

3.5 Registro de personal

3.5.1 Personal con acceso a datos

El siguiente personal pertenece a las diferentes jefaturas de la organización quienes son los responsables de la administración del acceso a datos sensibles de la empresa y a la infraestructura tecnológica, bases de datos, redes, sistemas y controles de acceso de la organización.

Tabla 6

Personal a cargo del acceso a datos.

Cargo	Área	Departamento
Gerencia Comercial	Comercial	Ventas
Gerente de Operaciones	Logística	Logística
Gerente de Finanzas	Contabilidad	Contabilidad
Gerente de Administración	Administración	Compras
Gerente de Administración	Talento Humano	Recursos Humanos
Gerente de Calidad	Calidad	Calidad y Seguridad

Nota: Sytsa Cia. Ltda. (2026)

3.5.2 Personal sin acceso a datos

El personal operativo y de apoyo que no requiere acceso directo a sistemas, redes o bases de datos de la organización realiza sus funciones sin acceso a información sensible.

Dentro de este grupo se incluye personal de:

- Personal de limpieza
- Personal de custodia
- Mecánicos
- Conductores

Este personal no administra sistemas de información ni mantiene privilegios de acceso sobre la base de datos corporativos.

3.5.3 Accesos físicos

Los controles físicos de acceso son un conjunto de medidas, procedimientos y dispositivos de seguridad implementados por las organizaciones para regular, supervisar y restringir el ingreso de personas, vehículos y materiales a las instalaciones y a los sistemas de la empresa. Estos controles tienen como objetivo prevenir accesos no autorizados, proteger los activos críticos y garantizar la integridad de la cadena de suministro.

1. **Control de acceso a instalaciones:** Las normas BASC establecen que las instalaciones deben contar con mecanismos que permitan identificar, registrar y controlar el ingreso de empleados, visitantes y proveedores. Entre los principales controles físicos se encuentran:

- **Identificación del personal:** Todos los empleados deben portar credenciales o identificaciones visibles dentro de las instalaciones.
- **Registro y control de visitantes:** Los visitantes deben ser registrados, autorizados y acompañados durante su permanencia en la empresa.
- **Control de ingreso y salida de vehículos:** Debe verificarse la identidad del conductor, el motivo de ingreso y realizar inspecciones cuando sea necesario.

- **Procedimientos para personas no autorizadas:** Se deben establecer protocolos para detectar, confrontar y retirar a personas no autorizadas dentro de la empresa.

2. Seguridad física del perímetro

Las instalaciones deben contar con infraestructura de seguridad que limite el acceso y proteja las áreas críticas. Entre las medidas recomendadas se incluyen:

- Cercas o muros perimetrales que delimiten claramente el área de la empresa.
- Puertas y garitas de control vigiladas.
- Sistemas de iluminación adecuados en zonas externas e internas.
- Sistemas de vigilancia electrónica como cámaras CCTV.
- Control de llaves, cerraduras y accesos a áreas restringidas.

3. Control de acceso a áreas sensibles

Las áreas críticas como bodegas, centros de documentación, sistemas informáticos o zonas de carga deben contar con accesos restringidos y autorizaciones específicas. Para ello se implementan medidas como:

- Tarjetas de acceso o sistemas electrónicos de control.
- Registros de ingreso a áreas restringidas.

- Supervisión por personal de seguridad.
- Monitoreo mediante cámaras de vigilancia.

Estas medidas permiten garantizar que solo personal autorizado y debidamente identificado pueda acceder a dichas áreas.

3.6 Registro de prestadores de servicio

Las siguientes empresas brindan servicios tecnológicos relacionados exclusivamente con la infraestructura, sistemas y plataformas administradas por el Departamento de TI.

Tabla 7

Empresas prestadoras de servicio de Internet.

Empresa	Tipo de soporte	Servicios
Saitel	Proveedor de Internet	Conectividad empresarial
Megadatos	Proveedor de Internet	Conectividad empresarial
Fibramax	Proveedor de Internet	Conectividad empresarial
Otecel - Claro Ecuador	Licencia	Microsoft Office 365

Nota: Sytsa Cia. Ltda. (2026)

3.6.1 Con acceso a datos catalogados

La empresa cuenta con 61 proveedores que no tienen acceso o manejo de documentación sensible. Los cuales se encuentran descritos en la ¨Matriz de Evaluación Documental de Proveedores¨ (SIG-SYTSA-SFPV-FOR-022 V,02)

3.6.2 Sin acceso a datos catalogados

La empresa cuenta con 25 proveedores que tienen acceso o manejo de documentación sensible. Los cuales se encuentran descritos en la ¨Matriz de Evaluación Documental de Proveedores¨ (SIG-SYTSA-SFPV-FOR-022 V,02)

3.7 Sistemas de captación de imágenes y audio

La organización utiliza el Ecosistema Hikvision (iVMS-4200 para PC / Hik-Connect para dispositivos móviles).

3.7.1 Número de cámaras

El sistema cuenta con un despliegue total de 98 cámaras distribuidas en las diferentes sucursales de la organización a nivel nacional.

3.7.2 Zonas de influencia

- Sucursal de Petrillo: 20 cámaras (Sistema operativo)
- Sucursal de Alóag: 37 cámaras (Divididas en secciones SLB y Sytsa Frontal)

- Sucursal de Tulcán: 21 cámaras (Sistema operativo)
- Sucursal de Guayaquil: 20 cámaras (Sistema operativo)

3.7.3 Sistema de tratamiento y almacenamiento

El almacenamiento se gestiona de forma local mediante hardware especializado de la marca Hikvision, garantizando la integridad de los datos sin dependencia de terceros.

- Capacidad Total: 32 TB (Distribuidos en 4 discos duros de 8 TB cada uno).
- Tiempo de Retención: Aproximadamente 90 días de grabación continua.
- Gestión: Grabación cíclica automatizada por el servidor de video.

3.7.4 Usuarios autorizados

A continuación, se detalla el personal que cuenta con credenciales de acceso al sistema (monitoreo en vivo y/o revisión de grabaciones):

Tabla 8

Personal autorizado de control de accesos al sistema.

Cargo	Área
Presidente	Presidencia
Gerente General	Gerencia
Jefe de área	Tecnología de la Información

Nota: Sytsa Cia. Ltda. (2026)

3.8. Dispositivos. Medidas de seguridad.

3.8.1 Análisis de las medidas de seguridad de los dispositivos.

La infraestructura tecnológica de la organización está compuesta por equipos informáticos utilizados en las actividades administrativas y operativas, incluyendo computadoras de escritorio, laptops, equipos de red y plataformas tecnológicas que permiten el funcionamiento de los sistemas de información de la empresa.

El objetivo se basa en proteger la información institucional y garantizar la continuidad operativa de los sistemas, es por ello que la organización ha implementado diversas medidas de seguridad tecnológica que permiten reducir riesgos asociados al acceso no autorizado, pérdida de información o incidentes de seguridad informática.

La empresa SYTSA S.A. utiliza como medida de seguridad el Authenticathor de Microsoft en las cuentas de OFFICE 365, cuenta con un dominio donde pueden acceder el Administrador, el equipo de operaciones del TI y los usuarios UDB. Por consecuencia al proteger las cuentas online mediante la verificación en dos pasos que nos ofrece el Authenticathor permite tener seguridad en los equipos, y para el ingreso de equipos electrónicos mediante el uso de contraseña, tenemos Kaspersky como antivirus ante las amenazas en los equipos celulares como en los de computación.

La empresa a pesar de no contar con servidores, el área de TI tiene acceso a la consola de administración del Hosting la misma que tiene doble factor de autenticación con Microsoft

Authenticathor. También cuentan con gestores de correo como es Office 365 y Roundcube Webmail.

Los sistemas operativos que más se utilizan son WINDOWS y MACOS los cuales son actualizados cada 6 meses cuando se hace el mantenimiento de los equipos, sin embargo, los computadores se actualizan automáticamente cuando Microsoft lanza actualizaciones. De igual manera el antivirus Kaspersky se encuentra en una actualización constante cada hora.

Para la creación de contraseñas en los correos y el ingreso de computadoras se exige mantener un nivel de seguridad favorable en él se incluyen letras, números o caracteres especiales, se actualizan cada vez que el usuario desea en el caso de office, contrario al Webmail que se debe cambiar la contraseña una vez cada 3 meses. El antivirus a su vez cuneta con un plan en el cual el uso de su licencia le permite mantener actualizaciones diarias.

Entre las principales medidas de seguridad implementadas en los dispositivos y sistemas se encuentran las siguientes:

- Antivirus corporativo Kaspersky

Los equipos informáticos utilizados dentro de la organización cuentan con el antivirus corporativo Kaspersky instalado, el cual permite la protección contra amenazas informáticas tales como virus, malware, spyware, ransomware y otros programas maliciosos que puedan comprometer la seguridad de la información.

El antivirus permite realizar análisis de seguridad en los dispositivos, detectar archivos potencialmente peligrosos y prevenir la ejecución de software malicioso que pueda afectar el funcionamiento de los sistemas o comprometer la confidencialidad de los datos almacenados.

- Cortafuegos y seguridad de red mediante MikroTik

La infraestructura de red de la organización se encuentra administrada mediante dispositivos MikroTik, los cuales funcionan como cortafuegos y controladores de tráfico de red.

Los equipos MikroTik permiten establecer políticas de seguridad que regulan el acceso a la red, controlar el tráfico de datos, administrar conexiones de internet y restringir accesos no autorizados desde redes externas. Asimismo, estos dispositivos permiten segmentar la red y monitorear la actividad de los dispositivos conectados a la infraestructura tecnológica.

- Control de acceso a dispositivos y sistemas

El acceso a los dispositivos informáticos se realiza mediante credenciales de usuario asignadas al personal autorizado. Cada usuario accede a los equipos y sistemas de acuerdo con las funciones que desempeña dentro de la organización, lo que permite mantener un control sobre el uso de los recursos tecnológicos.

3.8.2 Propuesta de mejora de las medidas de seguridad.

A pesar de las medidas de seguridad actualmente implementadas, es posible fortalecer la protección de la información mediante la adopción de prácticas adicionales orientadas a reducir riesgos tecnológicos y mejorar el control sobre los dispositivos y sistemas informáticos.

Entre las mejoras que pueden implementarse se encuentran las siguientes:

- Fortalecimiento de políticas de seguridad informática

Establecer políticas internas que definan el uso adecuado de los equipos informáticos, el manejo de contraseñas seguras y las responsabilidades del personal en relación con la protección de la información.

- Gestión de actualizaciones de software

Mantener actualizados los sistemas operativos, aplicaciones y herramientas de seguridad instaladas en los equipos, con el fin de reducir vulnerabilidades que puedan ser explotadas por amenazas informáticas.

- Control de acceso basado en roles

Reforzar el control de acceso a los sistemas de información mediante la asignación de permisos de acuerdo con las funciones de cada usuario dentro de la organización, limitando el acceso únicamente a la información necesaria para el desempeño de sus actividades.

- Monitoreo de seguridad de la red

Fortalecer las actividades de monitoreo de la red corporativa utilizando las herramientas disponibles en la infraestructura MikroTik, lo que permitirá detectar comportamientos inusuales, intentos de acceso no autorizado o actividades que puedan representar un riesgo para la seguridad de la información.

- Capacitación del personal en seguridad de la información

Promover buenas prácticas de seguridad informática entre los colaboradores de la organización mediante capacitaciones periódicas que permitan sensibilizar al personal sobre riesgos como correos maliciosos, uso indebido de dispositivos o manejo inadecuado de información confidencial.

Las medidas de seguridad actualmente implementadas en los dispositivos y sistemas tecnológicos de la organización permiten mantener un nivel de protección adecuado frente a amenazas informáticas comunes. Sin embargo, el fortalecimiento continuo de las políticas de seguridad, el monitoreo de la infraestructura tecnológica y la capacitación del personal contribuirán a mejorar la protección de la información y reducir los riesgos asociados a la seguridad informática.

Finalmente se debe contar con un estudio de seguridad que englobe a todos los puestos de trabajo dentro de la organización, así como es importante que se implemente un proceso para el

tratamiento de la información en la cual permita observar de manera holística las posibles brechas de seguridad que puedan ocasionar una infiltración, hurto o mal uso de información de la empresa.

3.9. Puestos de trabajo.

3.9.1 Análisis de las medidas de seguridad de cada puesto de trabajo, según la información tratada.

El Departamento de TI es responsable de la administración de la infraestructura tecnológica, sistemas informáticos, plataformas tecnológicas y medidas de seguridad asociadas a los dispositivos y redes de la organización. Sin embargo, la definición de funciones, responsabilidades, análisis de riesgos laborales, clasificación de puestos de trabajo y evaluación de las actividades realizadas por cada cargo dentro de la empresa son competencias propias de otras áreas organizacionales.

Por ejemplo, en el área de Talento Humano cuentan con computadores de escritorio en los cuales su sistema operativo es Microsoft. El Autentificador de Microsoft les otorga el acceso una vez realizado la verificación en dos pasos con el celular, además las computadoras se encuentran ancladas al dominio del departamento de TI.

Para el uso de las aplicaciones internas, los permisos de los programas como Odoo, Isolución y CloudFleet se asignan según de las funciones de cada colaborador, limitando su uso al

personal que no cuenta con las competencias necesarias o que no necesita de información adicional a sus labores diarias.

El departamento de Talento Humano utiliza documentación de soporte mixto, manteniendo información del personal como contratos, hojas de vida, historial laboral en soporte papel que son almacenados en archiveros dentro del lugar de trabajo. La documentación digital como es el caso de los datos personales, vivienda, números de cuenta, comprobantes de pagos, resultados de exámenes preocupacionales, entre otros, se lo almacena en la computadora donde se debe realizar una copia de seguridad en la nube de office. El uso de discos externos se encuentra limitado solamente para usuarios autorizados, generalmente para cargos de jefatura y coordinación.

3.9.2 Acuerdo de confidencialidad.

ACUERDO DE CONFIDENCIALIDAD Y TRATAMIENTO DE DATOS PERSONALES

Empresa: SYTSA CIA. LTDA.

1. **Datos identificativos del trabajador**

Nombre completo: _____

Número de cédula o identificación: _____

Cargo o puesto de trabajo: _____

Área o departamento: _____

Correo electrónico corporativo: _____

Mediante la firma del presente documento, el trabajador declara conocer y aceptar las obligaciones derivadas del acceso a información y datos personales en el ejercicio de sus funciones.

2. **Actividad de tratamiento y acceso a la información**

El trabajador, en el ejercicio de sus funciones laborales, podrá tener acceso a información y datos personales pertenecientes a clientes, proveedores, colaboradores o terceros vinculados con SYTSA CIA. LTDA.

El acceso a dichos datos se realizará únicamente para el cumplimiento de sus funciones laborales y conforme a las políticas internas de seguridad y protección de datos de la organización.

3. **Obligación de confidencialidad**

El trabajador se compromete a mantener estricta confidencialidad respecto de toda información y datos personales a los que tenga acceso.

No podrá divulgar, compartir, copiar o utilizar dicha información para fines distintos a los establecidos por la empresa, ni revelarla a terceros no autorizados, incluso después de finalizada la relación laboral.

4. **Obligación de cumplimiento de medidas de seguridad**

El trabajador se compromete a cumplir con las medidas técnicas y organizativas de seguridad establecidas por la empresa, entre ellas:

- Uso adecuado de sistemas informáticos y credenciales de acceso.

- Protección de contraseñas y accesos a sistemas corporativos.

- Uso responsable del correo electrónico corporativo.

- No instalar software no autorizado.

- Notificar cualquier incidente de seguridad o posible vulneración de datos personales.

5. **Consecuencias de vulnerar las obligaciones**

El incumplimiento de las obligaciones de confidencialidad y seguridad podrá dar lugar a sanciones disciplinarias internas, terminación de la relación laboral y posibles responsabilidades civiles o administrativas conforme a la normativa vigente.

6. **Finalidad del tratamiento de los datos del trabajador**

Los datos personales del trabajador serán recopilados y tratados por SYTSA CIA. LTDA. con las siguientes finalidades:

- Gestión de la relación laboral.

- Administración de nómina y beneficios laborales.

- Cumplimiento de obligaciones legales y contractuales.

- Gestión de seguridad informática y control interno.

- Control de acceso a instalaciones o sistemas.

7. **Tiempo de almacenamiento de los datos**

Los datos personales del trabajador serán conservados durante la vigencia de la relación laboral en soporte papel en el área de Talento Humano con copia de seguridad subido a la nube y posteriormente durante el tiempo necesario para cumplir con obligaciones legales, laborales, fiscales o administrativas.

8. **Ejercicio de derechos del trabajador**

El trabajador podrá ejercer los derechos de acceso, rectificación, actualización, eliminación, oposición y portabilidad de sus datos personales.

Para ejercer estos derechos podrá comunicarse a:

Correo electrónico: _____

Dirección: _____

9. **Datos del delegado de Protección de Datos (DPD)**

Delegado de Protección de Datos: _____

Correo electrónico: _____

Teléfono: _____

10**. Sistema de videovigilancia**

Se informa al trabajador que SYTSA CIA. LTDA. puede contar con sistemas de videovigilancia en determinadas áreas de sus instalaciones con la finalidad de garantizar la seguridad de las personas, proteger los bienes e instalaciones y prevenir incidentes o actividades ilícitas.

11**. Sistema de localización GPS**

En caso de que el trabajador utilice vehículos o dispositivos corporativos, estos podrán contar con sistemas de geolocalización (GPS) con fines de control logístico, seguridad de los activos y optimización de rutas de trabajo.

12. **Uso de datos biométricos**

En caso de utilizarse sistemas biométricos (como huella dactilar o reconocimiento facial) para control de acceso o asistencia, estos datos serán tratados exclusivamente para fines laborales y con medidas de seguridad reforzadas.

☐ Acepto

☐ No acepto

13. **Aceptación**

Mediante la firma del presente documento, el trabajador declara haber leído y aceptado las condiciones establecidas en este acuerdo de confidencialidad y protección de datos.

Lugar: _____

Fecha: ____ / ____ / _____

Por la empresa

SYTSA CIA. LTDA.

Nombre: _____

Cargo: _____

Firma: _____

El trabajador

Nombre: _____

Cédula: _____

Firma: _____

3.10. Encargado del tratamiento.

3.10.1 Contrato E. Tratamiento.

CONTRATO DE ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

Por una parte, SYTSA CIA. LTDA., con RUC No. _____, domiciliada en _____, representada legalmente por _____, en calidad de _____, a quien en adelante se le denominará "EL RESPONSABLE DEL TRATAMIENTO".

Y, por otra parte, _____, con RUC/C.I. No. _____, domiciliado en _____, representado por _____, en calidad de _____, a quien en adelante se le denominará "EL ENCARGADO DEL TRATAMIENTO". Las partes acuerdan lo siguiente:

Primera: Objeto

El presente acuerdo tiene por objeto regular el tratamiento de datos personales por parte del responsable del tratamiento, el cual consistirá en:

• Recopilación, registro, organización y uso de datos personales.

• Tratamiento de información como nombres, apellidos, correos electrónicos, números telefónicos y demás datos necesarios.

• Gestión administrativa, comercial y operativa relacionada con los servicios contratados.

• Envío de comunicaciones relacionadas con la prestación de servicios.

El responsable del tratamiento se compromete a tratar los datos únicamente para las finalidades aquí establecidas.

Segunda: Alcance laboral

El encargado reconoce que el tratamiento de datos puede involucrar información de trabajadores, ex trabajadores y postulantes, conforme a las disposiciones del Ministerio de Trabajo.

Tercera: Antecedentes

El encargado del tratamiento ha contratado previamente a SYTSA S.A. para la prestación de servicios relacionados con su actividad comercial.

Para la correcta ejecución del contrato y cumplimiento de obligaciones legales, el responsable del tratamiento requiere acceder a datos personales bajo custodia del encargado del tratamiento. La LOPDP regula las obligaciones en materia de protección de datos personales en el Ecuador.

En cumplimiento de lo dispuesto en el artículo 68 numeral 9, en concordancia con el artículo 34 y el artículo 47 numeral 10 de la LOPDP, las Partes suscriben el presente acuerdo.

El presente instrumento constituye parte integrante y accesoria del contrato principal celebrado entre las Partes

Cuarta: Finalidad

La finalidad del contrato consiste en documentar las instrucciones del responsable del tratamiento de datos garantizando que los datos del encargado del tratamiento sean seguros, confidenciales bajo estricto cumplimiento normativo de la LOPDP y establece obligaciones específicas para proteger los datos personales al ser gestionados por terceros.

Quinta: Tipo de datos

El responsable del tratamiento tendrá acceso a datos personales de clientes, empleados o usuarios recogidos por el encargado según se necesite. Entre los datos recogidos se detallan los siguientes:

- Datos personales identificativos (Nombres, apellidos, cédula o RUC correo)
- Datos de contacto (Número de teléfono, dirección)
- Datos laborales (Formación de estudios, hoja de vida)
- Datos financieros (Cuentas bancarias)

Sexta: Obligaciones del responsable de tratamiento

El responsable se obliga a:

- Tratar los datos personales únicamente para las finalidades establecidas.
- Actuar conforme a las instrucciones documentadas del encargado.
- Informar al encargado en caso de que una instrucción contravenga la normativa.
- Mantener estricta confidencialidad sobre los datos tratados.
- No comunicar datos a terceros sin autorización expresa del encargado.
- Suscribir acuerdos de confidencialidad con su personal y colaboradores.
- Implementar medidas de seguridad adecuadas.
- Suprimir o devolver los datos al finalizar el contrato, salvo obligación legal de conservación.
- Apoyar al encargado en la atención de derechos de los titulares.
- Notificar incidentes de seguridad o vulneraciones de datos personales.

Séptima: Subcontratación

El responsable del tratamiento podrá subcontratar servicios relacionados con el tratamiento de datos, previa autorización del encargado. El sub responsable deberá:

- Cumplir con las mismas obligaciones del presente acuerdo.

- Garantizar medidas adecuadas de protección de datos. SYTSA S.A. será responsable por el cumplimiento del sub responsable.

Octava: Transferencias internacionales de datos

El responsable no realizará transferencias internacionales de datos personales sin autorización previa del encargado del tratamiento y bajo el cumplimiento de la normativa de la LOPDP.

Novena: Seguridad de la información

El responsable implementará medidas técnicas, organizativas y administrativas como controles de acceso, respaldo de información, cifrado y gestión de incidentes, para garantizar la seguridad de los datos personales.

Décima: Confidencialidad La obligación de confidencialidad:

El responsable y su personal deberán firmar acuerdos de confidencialidad conforme a la legislación laboral ecuatoriana y:

- Se mantendrá incluso después de terminado el contrato.
- Aplica a todo el personal y terceros involucrados.

Décima primera: Ley aplicable y jurisdicción

El presente acuerdo se rige por la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP). Las partes se someten a la jurisdicción de los tribunales competentes del Ecuador.

Décima segunda: Aceptación

Las Partes declaran haber leído, entendido y aceptado el contenido del presente acuerdo.

FIRMAS

El encargado

Nombre: _____

Cédula: _____

Fecha: //__

SYTSA S.A. (El responsable)

Nombre: _____

Cargo: _____

Fecha: //__

3.11.- Análisis web.

3.11.1 Análisis, configuración y Política de cookies.

La empresa SYTSA cuenta con un sitio web que presenta una estructura corporativa que está orientado a la parte informativa de los servicios que realiza. Analizaremos el sitio web de la empresa el cual se ingresa con la siguiente página: https://sytsa.com.ec.

El sitio web de la empresa es una página segura con protocolo (https) y tiene un certificado valido, el cual mostraremos a continuación.

Figura 7

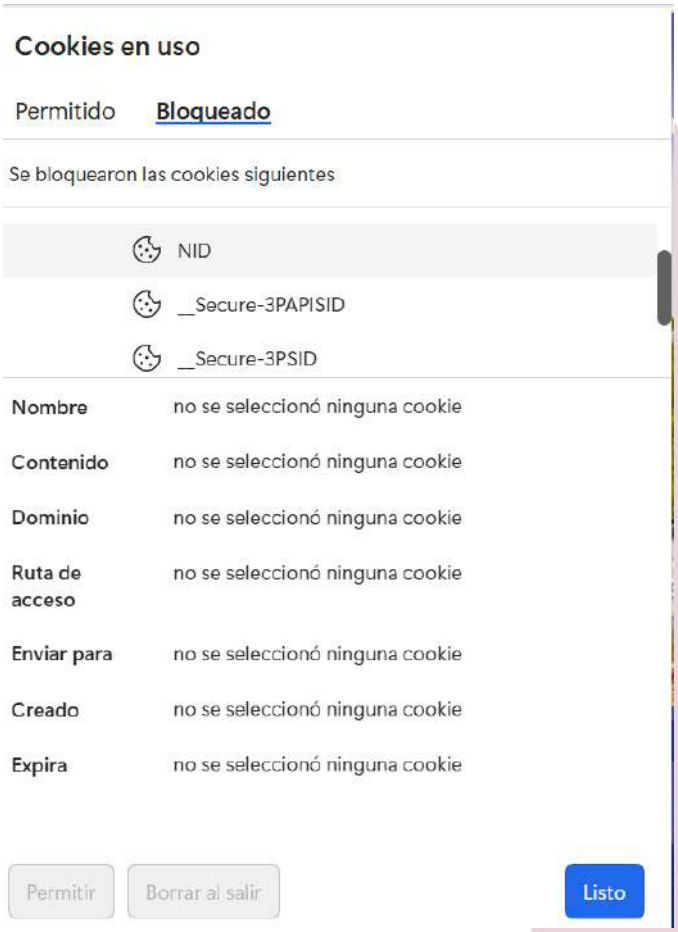
Visualizador de certificados

Nota: Fuente (SYTSA, 2023)

El certificado de seguridad es válido y cuenta que es emitido por la página de la empresa sytsa.com.ec, esta proporcionado por R13 organización Let's Encryt, el periodo de validez del certificado fue emitido el 26 de enero de 2026 y vence el 26 abril de 2026.

Figura 8

Uso de cookies



Nota: Fuente (SYTSA, 2023)

Analizando las cookies que se encuentran en el sitio web de la empresa se ha rastreado 3 cookies de Google, las cuales son: NID, _Secure-3PAPASID, _Secure-3PSID. No se evidencia un banner de consentimiento de cookies al ingresar al sitio y tampoco una política de cookies visible.

Recomendamos a la organización incrementar un banner de consentimiento y políticas de cookies en el sitio web, a continuación, les presentaremos un esquema de banner de consentimiento para que puedan insertar al sitio web.

Figura 9

Banner de uso de cookies

Nota: Fuente (SYTSA, 2023)

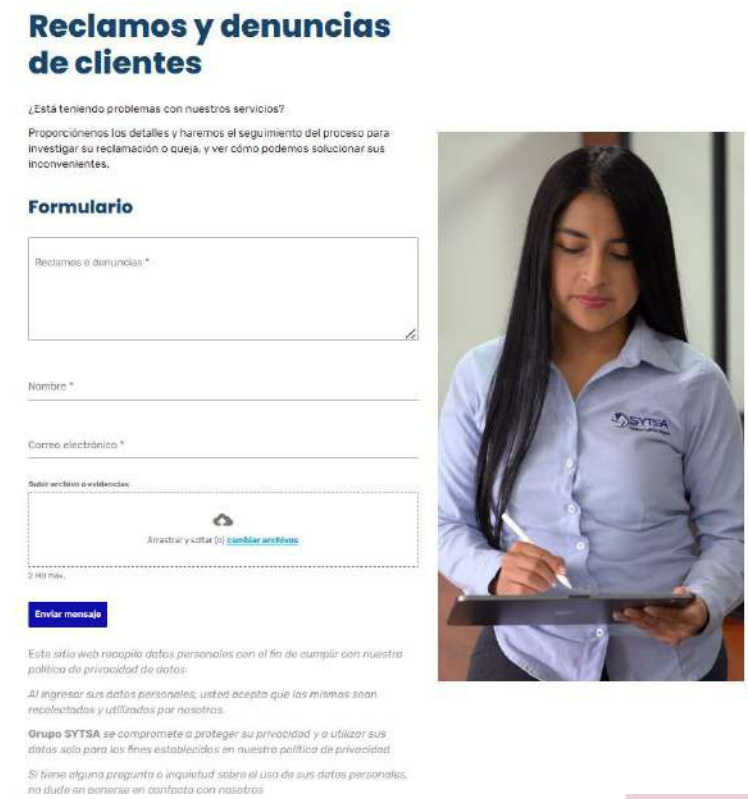
3.11.2 Formularios de contacto, newsletter, trabaja conmigo, registro.

El sitio web de la empresa cuenta con dos formularios, uno de contacto y otro de reclamos y denuncias de clientes, los dos formularios cuentan con el principio de minimización y no contiene política de privacidad.

Recomendamos que se agregue una política de privacidad visible en la página web para que los usuarios estén en conocimientos de los tratamientos de los datos que se obtienen en los formularios, a continuación, le generaremos una política de privacidad para que pueda ser utilizada para la página.

Figura 10

Números de contacto para de asistencia y servicio al cliente



Nota: Fuente (SYTSA, 2023)

Política de Privacidad

SYTSA se compromete a garantizar la protección y confidencialidad de los datos personales de los usuarios que acceden a su sitio web, conforme a la legislación vigente en materia de protección de datos personales.

Responsable: SYTSA

Domicilio: Quito, Núñez de vela y Naciones Unidas, Edificio Metropolitan

Correo electrónico: correo@sytsa.com

Teléfono: 0999443825

El responsable del tratamiento de los datos personales es SYTSA, quien determina los fines y medios del tratamiento de la información recabada a través del sitio web.

Los datos personales proporcionados por los usuarios a través de formularios de contacto, reclamos o denuncias de clientes disponible en el sitio web serán utilizados con las siguientes finalidades:

- Gestionar solicitudes de información, consultas o servicios.
- Enviar información sobre productos, servicios o novedades de SYTSA, siempre que el usuario haya otorgado su consentimiento.
- Cumplir con obligaciones legales o contractuales derivadas de la relación con el usuario.

El tratamiento de los datos personales se basa en:

- El consentimiento expreso del usuario al aceptar esta Política de Privacidad.
- El cumplimiento de obligaciones legales aplicables a SYTSA.
- El interés legítimo de SYTSA en mantener relaciones comerciales y mejorar sus servicios.

Los datos personales se conservarán durante el tiempo necesario para cumplir con la finalidad para la que fueron recabados y mientras el usuario no solicite su supresión. Posteriormente, se mantendrán bloqueados durante los plazos legalmente establecidos para atender posibles responsabilidades.

SYTSA no cederá los datos personales a terceros, salvo obligación legal o cuando sea necesario para la prestación de un servicio contratado.

En caso de transferencias internacionales de datos, SYTSA garantizará que se realicen conforme a las normas y garantías establecidas por la legislación vigente.

SYTSA no realiza decisiones automatizadas ni elaboración de perfiles que produzcan efectos jurídicos o afecten significativamente al usuario.

SYTSA cuenta con un delegado de Protección de Datos (DPD) encargado de supervisar el cumplimiento de la normativa y atender las solicitudes relacionadas con la protección de datos.

Contacto del DPD: correo.dpd@sytsa.com

Los usuarios pueden ejercer en cualquier momento los siguientes derechos:

- Acceso: conocer qué datos personales se están tratando.
- Rectificación: solicitar la corrección de datos inexactos o incompletos.
- Supresión: pedir la eliminación de sus datos cuando ya no sean necesarios.
- Oposición: oponerse al tratamiento de sus datos por motivos legítimos.
- Limitación: solicitar la restricción del tratamiento en determinadas circunstancias.
- Portabilidad: recibir sus datos en un formato estructurado y transferible.

Para ejercer estos derechos, el usuario puede enviar una solicitud al correo electrónico correo@sytsa.com, adjuntando una copia de su documento de identidad.

SYTSA se reserva el derecho de modificar la presente Política de Privacidad para adaptarla a cambios legislativos o a nuevas prácticas internas. Cualquier modificación será publicada en esta misma página.

3.11.3 Aviso legales.

El sitio web de la empresa no cuenta con aviso legal en la página, recomendamos que se debe de ponerse el aviso legal para el conocimiento de los usuarios, a continuación, les redactaremos un aviso legal para que pueda ser tomado en cuenta.

Aviso Legal

En cumplimiento con la legislación vigente, se informa que el presente sitio web pertenece a SYTSA, empresa dedicada al desarrollo de soluciones tecnológicas y servicios informáticos.

Titular: SYTSA

Domicilio: Quito, Núñez de vela y Naciones Unidas, Edificio Metropolitan

Correo electrónico de contacto: correo@sytsa.com

Teléfono: 0999443825

Sitio web: www.sytsa.com

El acceso y uso de este sitio web atribuye la condición de usuario, implicando la aceptación plena y sin reservas de todas las disposiciones incluidas en este aviso legal.

El sitio web de SYTSA tiene como finalidad ofrecer información sobre los servicios, productos y proyectos desarrollados por la empresa, así como facilitar el contacto con clientes, proveedores y colaboradores.

Todos los contenidos del sitio web, incluyendo textos, imágenes, logotipos, gráficos, archivos, diseño y estructura, son propiedad exclusiva de SYTSA o de terceros que han autorizado su uso.

Queda prohibida la reproducción, distribución, comunicación pública o transformación de dichos contenidos sin la autorización expresa y por escrito de SYTSA.

El usuario se compromete a hacer un uso adecuado del sitio web y de sus contenidos, evitando cualquier acción que pueda causar daños a los sistemas de SYTSA o de terceros, o que vulnere la legislación vigente, la buena fe o el orden público.

El sitio web puede contener enlaces a páginas externas. SYTSA no se responsabiliza del contenido, exactitud o fiabilidad de dichas páginas, ni de los daños que puedan derivarse de su uso.

SYTSA garantiza la confidencialidad y seguridad de los datos personales proporcionados por los usuarios, conforme a la normativa vigente en materia de protección de datos. Para más información, puede consultarse la Política de Privacidad disponible en este sitio web.

El sitio web utiliza cookies propias y de terceros para mejorar la experiencia del usuario y analizar el tráfico. El uso de cookies se regula en la Política de Cookies, donde se detallan los tipos de cookies utilizadas y las opciones de configuración disponibles.

SYTSA no se hace responsable de los daños o perjuicios derivados del uso del sitio web, incluyendo errores u omisiones en los contenidos, falta de disponibilidad o transmisión de virus o programas maliciosos.

El presente aviso legal se rige por la legislación del país en el que SYTSA tiene su domicilio social. Cualquier controversia que surja en relación con el sitio web será sometida a los juzgados y tribunales competentes de dicha jurisdicción.

SYTSA se reserva el derecho de modificar, actualizar o eliminar cualquier información contenida en este sitio web, así como este aviso legal, sin previo aviso y en cualquier momento.

3.12.- Medidas de seguridad.

3.12.1 Análisis, uso y medidas de seguridad en el uso de navegadores.

En la empresa SYTSA, los navegadores web constituyen una herramienta esencial para el acceso a plataformas corporativas, sistemas en la nube y servicios de comunicación, lo que los convierte en un punto crítico en términos de seguridad de la información.

El uso del navegador EDGE se manifiesta como el navegador predeterminado en la empresa debido a que SYTSA S.A. utiliza como medida de seguridad el Authenticathor de Microsoft en las cuentas de OFFICE 365, cuenta con un dominio donde pueden acceder el Administrador, el equipo de operaciones del TI y los usuarios UDB. Es por eso que el navegador EDGE está directamente relacionado con actividades como acceso a sistemas ERP, plataformas logísticas, correo electrónico corporativo y herramientas de gestión documental. Esto implica la exposición a riesgos como ataques de phishing, descarga de software malicioso, robo de credenciales y acceso a sitios web no seguros.

En este contexto, la organización ha implementado las siguientes medidas de seguridad:

- Control de navegación mediante el antivirus corporativo Kaspersky.
- Protección contra amenazas web como phishing y malware.
- Uso de sistemas operativos actualizados (Windows y Mac).
- Gestión centralizada mediante dominio corporativo.
- Restricción del uso de dispositivos externos.
- Actualización constante del antivirus.

Se recomienda a la empresa el uso limitado de varios navegadores dentro de la jornada laboral y mantener una restricción de búsqueda y de páginas web ajenas a las actividades del cargo. Así también se debe restringir la instalación de extensiones y utilizar herramientas de gestión centralizada.

Al mantener más de un navegador web aumenta el riesgo de un ataque cibernético, eleva el riesgo de infecciones por malware y el robo de credenciales o la fuga de datos personales.

3.12.2 Hosting y Servidores

La empresa SYTSA no cuenta con servidores físicos propios, opera principalmente mediante servicios en la nube administrados por proveedores externos, la cual el departamento de TI tiene acceso a la consola del hosting para su monitoreo y control

3.12.2.1 Medidas de seguridad.

- Acceso restringido a consolas de administración.
- Doble factor de autenticación (2FA) mediante Microsoft Authenticathor.
- Gestión de accesos basada en roles.
- Copias de seguridad en la nube (Office 365).
- Políticas de contraseñas seguras.
- Supervisión por el Departamento de TI.

A medida del crecimiento de la empresa se recomienda cambiar el hosting compartido por un servido propio de la empresa debido a que un servidor VPS brinda un rendimiento superior, un mayor control en niveles de seguridad en el sistema operativo y se adapta mucho mejor a grandes proyectos.

Para el hosting que se encuentra en la empresa se recomienda implementar medidas activas como el uso de certificados SSL, mantener y cumplir con las actualizaciones periódicas del software, mantener las copias de seguridad diarias de manera automática y además implementar el uso de protocolos seguros y firewalls para bloquear peticiones maliciosas.

3.12.2.2 Prestadores de servicios.

Entre los principales proveedores se encuentran:

- Cloudfleet: gestión de flotas.
- Silogtran: sistema logístico.
- ISOLUCION: gestión documental.
- Killka: soporte ERP Odoo.
- Saitel, Megadatos, Fibramax: internet.
- OTECEL – Claro: licencias Office 365.

3.12.3 Gestores de Correo electrónico.

La empresa utiliza Microsoft Office 365 y Roundcube Webmail.

3.12.3.1. Medidas de seguridad.

- Doble factor de autenticación.
- Contraseñas seguras.
- Control de accesos por roles.
- Protección mediante antivirus.
- Copias de seguridad en la nube.
- Administración centralizada.

3.12.3.2Prestadores de servicios.

Microsoft Office 365:

Plataforma en la nube con alta disponibilidad, respaldo automático y autenticación multifactor.

Roundcube Webmail:

Plataforma de correo web con acceso sencillo, pero con menor nivel de seguridad en comparación con soluciones empresariales avanzadas.

CAPÍTULO 4: PLAN DIRECTOR DE SEGURIDAD (PDS)

Un Plan Director de Seguridad (PDS) define y prioriza un conjunto de proyectos en materia de seguridad de la información, con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis detallado de la situación inicial (INCIBE, 2023). En el caso de SYTSA, esto significa no solo listar problemas, sino ordenarlos según lo que puede paralizar la operación en un futuro.

El PDS constituye una hoja de ruta estratégica que permite a la organización planificar, organizar y gestionar las actuaciones necesarias para proteger sus activos de información, alineándose con los objetivos estratégicos del negocio. Su desarrollo implica la participación de todos los niveles de la organización, desde la alta dirección hasta los usuarios finales, y considera aspectos técnicos, organizativos y legales.

Para la empresa SYTSA, dedicada a soluciones logísticas y tecnológicas, la implementación de un PDS resulta especialmente relevante dado que sus operaciones dependen críticamente de sistemas de información, plataformas tecnológicas (ERP Odoo, CloudFleet, Silogtran) y datos sensibles de clientes, proveedores y colaboradores.

Beneficios principales de implementar un PDS en SYTSA:

En el contexto de SYTSA, la implementación de un Plan Director de Seguridad (PDS) aporta beneficios que trascienden al cumplimiento normativo y se alinean directamente con la sostenibilidad operativa de la organización. Entre los principales se destaca la priorización de inversiones en seguridad basada en riesgos reales y no en percepciones subjetivas, lo cual resulta fundamental en una empresa donde los recursos tecnológicos y financieros son limitados. Asimismo, el PDS permite proteger activos críticos identificados durante el diagnóstico, tales como el ERP Odoo, las bases de datos de clientes y los sistemas de gestión de flotas CloudFleet y Silogran, cuya indisponibilidad afectaría directamente la continuidad de la cadena logística.

Desde el ámbito normativo, el PDS facilita la evaluación del grado de cumplimiento de SYTSA con la Ley Orgánica de Protección de Datos Personales (LOPDP). Finalmente, el carácter cíclico del PDS introduce un mecanismo de mejora continua que contrasta con la gestión reactiva de incidentes que hasta ahora ha predominado en la organización.

4.1. Check List PDS

A continuación, se presenta la evaluación inicial del cumplimiento de los controles establecidos para el Plan Director de Seguridad en la empresa SYTSA. Los controles se clasifican por nivel (Básico B / Avanzado A) y podrán tener el siguiente alcance (Procesos PRO, Tecnología TEC, Personas PER).

Tabla 9

Controles iniciales del Check List PDS

Nivel	Alcance	Control	Cumple
A	PRO	Analizar la situación actual de la empresa	☒
A	PRO	Alinear el PDS con la estrategia de la empresa	☒
A	PRO	Definir los proyectos a ejecutar	☐
A	PRO	Clasificar y priorizar los proyectos	☐
B	PRO	Aprobar el PDS	☐
A	PRO	Ejecución del PDS	☐
A	PRO	Certificación en seguridad	☐

Fuente: (INCIBE, 2023)

SYTSA se encuentra en una fase inicial. Se ha realizado un análisis de la situación actual (Capítulo 3) y se ha comenzado a alinear el PDS con la estrategia. Restan definir, priorizar, aprobar y ejecutar los proyectos, así como considerar futuras certificaciones.

4.1.1. Análisis de la situación actual de la Organización

SYTSA presenta la siguiente situación actual en materia de seguridad:

Tabla 10

Aspectos positivos de seguridad en SYTSA.

Área	Situación actual
Política de seguridad	Se ha definido un Acuerdo de Confidencialidad y Tratamiento de Datos Personales para empleados.
Control de acceso	Se utiliza Autenticación de dos factores (2FA) con Microsoft Authenticator para Office 365.
Antivirus	Cuenta con Kaspersky como antivirus corporativo, con actualizaciones constantes.
Cortafuegos	Implementa dispositivos MikroTik como firewall y controlador de red.
Copias de seguridad	Se realizan copias en la nube mediante Office 365.
Videovigilancia	Sistema Hikvision con 98 cámaras y almacenamiento local de 32 TB (90 días de retención).
Accesos físicos	Control de perímetro, garitas, credenciales y registro de visitantes.

Sytsa Cia. Ltda. (2026)

Aspectos para mejorar (controles que no cumple o cumple parcialmente):

Tabla 11.

Aspectos para mejorar en seguridad en SYTSA.

Área	Brecha identificada
Documento formal	No existe un documento único de "Política de Seguridad de la Información" formalmente aprobado.
Comité de Seguridad	No se evidencia un Comité de Seguridad formal establecido.
Inventario de activos	No se dispone de un inventario formal de activos TIC (equipos, sistemas, datos).
Gestión de vulnerabilidades	No se evidencia un proceso formal de gestión de vulnerabilidades.
Plan de continuidad	No se han definido ni probado planes de continuidad de negocio.
Portal web	El sitio web no cuenta con política de cookies visible, banner de consentimiento ni política de privacidad.
Formación	No se evidencia un plan de formación y concienciación en ciberseguridad para empleados.

Servidores propios	SYTSA no cuenta con servidores físicos propios, opera con hosting compartido.
Configuración de redes	Se evidencia el uso de múltiples navegadores sin restricciones, lo que aumenta el riesgo.

Sytsa Cia. Ltda. (2026)

4.1.2. Plan estratégico en materia tecnológica

Actualmente, SYTSA no cuenta con un Plan Estratégico formal en materia tecnológica documentado. Sin embargo, a partir del análisis realizado, se establecen los siguientes objetivos estratégicos para el PDS:

Objetivos del PDS para SYTSA:

1. **Corto plazo (0-6 meses):**
    - Elaborar y aprobar la Política de Seguridad de la Información.
    - Implementar un inventario formal de activos TIC.
    - Instalar banner de cookies y política de privacidad en el sitio web.
    - Realizar una campaña de sensibilización básica en ciberseguridad para empleados.

2. **Mediano plazo (6-18 meses):**
    - Establecer un Comité de Seguridad con responsabilidades definidas.
    - Implementar un proceso formal de gestión de vulnerabilidades.
    - Migrar de hosting compartido a servidor VPS o servidor propio.
    - Desarrollar y probar planes de continuidad de negocio.
3. **Largo plazo (18-36 meses):**
    - Obtener certificación ISO 27001 (Sistemas de Gestión de Seguridad de la Información).
    - Implementar un SOC (Centro de Operaciones de Seguridad) interno o externalizado.
    - Alcanzar un nivel de madurez en ciberseguridad equivalente a estándares internacionales.

4.2. VERIFICACIÓN DE CONTROLES

A continuación, se presenta la verificación de los 30 controles de seguridad aplicables a SYTSA, basada en la información recopilada en el Capítulo 3.

Tabla 12

Verificación de controles de seguridad (30 controles).

Identificador	Aspecto a evaluar	Respuesta	Responsable	Fecha
ID_0001	¿La organización ha definido un documento con la política de seguridad de la información?	No	-	-
ID_0002	¿La política de seguridad de la información se revisa periódicamente?	No	-	-

ID_0003	¿Se han definido las responsabilidades en materia de seguridad de la información?	Parcial Se ha establecido una estructura para la definición de responsabilidades en seguridad informática en base a la ISO 27001 para asignar tareas y dar seguimiento.	Jefatura TI / Gerencia	-
ID_0004	¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?	No	-	-
ID_0005	¿Los contratos y acuerdos con terceras partes tienen en	Sí Existe un acuerdo de confidencialidad para proveedores, clientes y personal interno que	Departamento Jurídico	No registrada

	consideración los requisitos de seguridad de la organización?	maneje documentación o sistemas con información delicada.		
ID_0006	¿Se dispone de un inventario de activos?	No	-	-
ID_0007	¿Se ha definido quien es el responsable de los activos?	No	-	-
ID_0008	¿Se comprueban las referencias de todos los candidatos a empleo?	Sí Como parte del proceso de selección se verifica referencias profesionales, antecedentes, nivel de estudios, portafolio (si aplica) y demás información que sustente su experiencia.	Talento Humano	No registrada

ID_0009	¿Se han implantado perímetros de seguridad para proteger las áreas de acceso restringido?	Sí Existen tarjetas de acceso que deben estar registrados en la base de datos de la empresa para que solo el personal autorizado pueda entrar a las diferentes áreas	Jefe de Seguridad Física	No registrada
ID_0010	¿Los equipos TIC críticos de la organización están ubicados en salas de CPD?	No (hosting externo)	-	-
ID_0011	¿Se han definido y documentado los procedimientos operacionales TIC?	Parcial Se ha definido los procedimientos operacionales y se encuentra en proceso de actualización de	Jefatura TI	-

		activos de hardware y licencias para su documentación		
ID_0012	¿Las copias de seguridad se realizan regularmente de acuerdo con la política de back up establecida?	Sí Dentro de la política de seguridad se establece realizar una copia de seguridad diaria, de las operaciones que posteriormente serán guardadas en la nube de la empresa.	Jefatura TI	No registrada
ID_0013	¿Se verifica regularmente la correcta realización de las copias de seguridad?	Sí El departamento de TI se asegura en automatizar los reportes de error y revisar las fechas de las últimas copias de seguridad que se realicen.	Jefatura TI	No registrada

ID_0014	¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?	Parcial Se debe definir un cronograma y los equipos con mayor criticidad de la empresa	Jefatura TI	-
ID_0015	¿Se registran las actividades de los administradores y operadores de sistema?	Parcial Se registran las actividades de mantenimiento, cambio o uso de información del sistema	Jefatura TI	-
ID_0016	¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?	Sí Solo puede tener uso del sistema los altos mandos (Gerente General) un delegado de gerencia y el departamento de TI	Jefatura TI	No registrada
ID_0017	¿Se ha definido, documentado e implantado un proceso formal	Sí	Jefatura TI	No registrada

	para la asignación de contraseñas?	Dentro de la matriz de requisitos legales y cumplimientos internos se integra el proceso de asignación de contraseñas y accesos	
ID_0018	¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?	Sí El departamento de TI junto a TH socializa la importancia del uso adecuado de contraseñas, protección de datos y de seguridad de la información	Jefatura TI – Talento Humano No registrada
ID_0019	¿Los usuarios se aseguran de proteger los equipos desatendidos?	Parcial Se recomienda bloquear la pantalla del colaborador cada que se encuentre lejos de su puesto de trabajo.	Todos los empleados -

ID_0020	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?	Si Las cuentas de usuario son unipersonales	Jefatura TI	No registrada
ID_0021	¿Se controla la instalación de software en sistemas en producción?	Parcial El departamento de TI debe mantener actualizados los accesos de los equipos de TIC para evitar la instalación de softwares ajenos a los de la empresa	Jefatura TI	-
ID_0022	¿Existe un proceso formal para la gestión de las	No	-	-

	vulnerabilidades técnicas de los sistemas en uso?			
ID_0023	¿Se ha definido, documentado e implantado un proceso formal para la gestión de los incidentes de seguridad?	Parcial Dentro de la matriz de riesgos se detalla la gestión de incidentes de seguridad	Jefatura TI	-
ID_0024	¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?	No	-	-
ID_0025	¿Se han definido, documentado e implantado planes de continuidad de negocio?	No	-	-

ID_0026	¿Los planes de continuidad de negocio se revisan y prueban formalmente?	No	-	-
ID_0027	¿Todos los requisitos relevantes de carácter legal se mantienen identificados?	Parcial Dentro de la matriz de requisitos legales y cumplimientos se detalla solamente requisitos relevantes a la empresa	Departamento Jurídico	-
ID_0028	¿Se han implementado procedimientos para asegurar el cumplimiento de los requisitos legales?	Parcial Dentro de la matriz de requisitos legales y cumplimientos se detalla los procedimientos que se deben cumplir	Departamento Jurídico	-

ID_0029	¿Se han establecido e implantado procedimientos para la protección y privacidad de la información?	Sí Existe un acuerdo de confidencialidad donde se detallan las cláusulas que la persona encargada de manejar información cumpla con el procedimiento de la protección de datos	DPD / Jurídico	No registrada
ID_0030	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad?	No	-	-

Sytsa Cia. Ltda. (2026)

4.3. INVENTARIO DE ACTIVOS

El inventario de activos es un documento fundamental dentro de cualquier sistema de gestión de seguridad de la información, ya que permite identificar, clasificar y asignar responsables a todos los recursos tecnológicos, informáticos y de información que posee una organización. Sin un inventario actualizado, resulta imposible evaluar correctamente los riesgos ni establecer medidas de protección adecuadas. A continuación, se presenta el análisis de activos de SYTSA, incluyendo su tipología, ubicación, responsable y una valoración inicial del riesgo inherente.

4.3.1. Análisis de riesgos (Inventario de activos)

En esta sección se listan los activos identificados en SYTSA y se realiza una valoración cualitativa del riesgo inherente para cada uno de ellos, entendiendo por riesgo inherente aquel que existe antes de aplicar medidas de mitigación. Esta valoración se ha realizado en base a la observación directa de las vulnerabilidades y al conocimiento de la operación de la empresa, sin aplicar todavía una fórmula matemática de probabilidad e impacto.

Tabla 13.

Inventario de activos de SYTSA

Identificador	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ACT-001	ERP Odoo	Sistema ERP corporativo para gestión administrativa, comercial y operativa	Jefatura TI	Software SaaS (Lógico)	Hosting externo (Killka)	Sí
ACT-002	CloudFleet	Plataforma de gestión de flotas y transporte	Jefatura TI	Software SaaS (Lógico)	Cloud	Sí
ACT-003	Silogran	Sistema logístico de transportes	Jefatura TI	Software SaaS (Lógico)	Cloud	Sí
ACT-004	ISOLUCION	Sistema de gestión documental y calidad	Jefatura TI	Software SaaS (Lógico)	Cloud	No

ACT-005	Nigisu	Sistema de gestión de infraestructura y cámaras	Jefatura TI	Software (Lógico)	Servidor local	No
ACT-006	Microsoft Office 365	Plataforma de correo y productividad corporativa	Jefatura TI	Software SaaS (Lógico)	Cloud (Microsoft)	No
ACT-007	Roundcube Webmail	Cliente de correo web alternativo	Jefatura TI	Software (Lógico)	Hosting	No
ACT-008	Antivirus Kaspersky	Protección antivirus corporativa	Jefatura TI	Software licencia (Lógico)	Equipos locales	No
ACT-009	MikroTik (Firewall)	Cortafuegos y controlador de red	Jefatura TI	Hardware (Físico)	Sala técnica (NNUU)	No

ACT-010	Cámaras Hikvision (98)	Sistema de videovigilancia (98 cámaras)	Jefatura TI	Hardware (Físico)	Sucursales nacionales	No
ACT-011	Servidor de video Hikvision	Almacenamiento local de grabaciones (32 TB)	Jefatura TI	Hardware (Físico)	Sala técnica	No
ACT-012	Equipos de cómputo (laptops/desk tops)	Aprox. 80+ equipos Dell, HP, Lenovo, Apple	Jefatura TI	Hardware (Físico)	Oficinas y sucursales	No

ACT-013	Celulares corporativos (271)	Dispositivos móviles para comunicación operativa	Jefatura TI	Hardware (Físico)	Personal de campo y oficinas	No
ACT-014	Base de datos de clientes	Información personal y contractual de clientes	Director Comercial	Información (Lógico)	Servidores/Cloud	Sí
ACT-015	Base de datos de proveedores	Información financiera y comercial de proveedores	Gerente Administrativo	Información (Lógico)	Servidores/Cloud	Sí
ACT-016	Base de datos de empleados	Datos personales, laborales y biométricos	Talento Humano	Información (Lógico)	Servidores/Cloud	Sí

ACT-017	Sitio web sytsa.com.ec	Portal corporativo informativo	Jefatura TI	Sitio web (Lógico)	Hosting externo	No
ACT-018	Redes Wi-Fi corporativas	Redes internas para empleados y visitantes	Jefatura TI	Infraestructura (Físico)	Sucursales	No

Sytsa Cia. Ltda. (2026)

4.4. ANÁLISIS DE RIESGOS

Partiendo del inventario de activos presentado en el apartado anterior, se ha procedido a realizar un análisis de riesgos cuantitativo (semicuantitativo) únicamente para aquellos activos que fueron calificados como Críticos (Sí) en la tabla 4.3.1, ya que son los que requieren una priorización inmediata. Para cada uno de estos activos se ha asignado una probabilidad de ocurrencia (1 = Baja, 2 = Media, 3 = Alta) y un impacto potencial (1 = Bajo, 2 = Medio, 3 = Alto), calculando el nivel de riesgo como el producto de ambos factores. Los resultados se presentan en la siguiente tabla.

Tabla 14.

Análisis de riesgos cuantitativo.

Activo	Amenaza principal	Probabilidad (1-3)	Impacto (1-3)	Riesgo (P×I)
ERP Odoo	Ransomware / Ciberataque	3	3	9
CloudFleet	Indisponibilidad del servicio por fallo del proveedor	2	3	6

Silogran	Indisponibilidad del servicio por fallo del proveedor	2	3	6
Base de datos clientes	Filtración de datos personales	2	3	6
Base de datos proveedores	Filtración de información financiera	2	2	4
Base de datos empleados	Pérdida de confidencialidad de datos personales	2	2	4

Sytsa Cia. Ltda. (2026)

4.5. CLASIFICACIÓN Y PRIORIZACIÓN

Una vez finalizado el análisis de riesgos cuantitativo del apartado anterior, se procede a clasificar y priorizar únicamente aquellos riesgos cuyo valor numérico sea superior a 4. Los riesgos con valor igual o inferior a 4 no se catalogan a priori, ya que se consideran dentro de niveles aceptables o tolerables para la organización. A continuación, se presentan los riesgos identificados con valor superior a 4, junto con las medidas propuestas para su mitigación, el responsable de cada acción, el tipo de medida (organizativa o técnica), el coste estimado, la fecha prevista de ejecución y la periodicidad de revisión.

Tabla 15.

Clasificación y priorización de iniciativas de mitigación.

Identificador	Título	Descripción de la medida	Responsable	Tipo	Coste estimado	Fecha prevista	Revisión
IN-001	Mitigación riesgo ERP Odoo (Riesgo 9)	Migrar del hosting compartido actual a un servidor VPS o servidor dedicado, implementar respaldos diarios automatizados y configurar un firewall gestionado. Adicionalmente, desarrollar un plan de contingencia específico para el ERP.	Jefatura de TI	Técnica	5.000−10.000	3 meses	Mensual

IN-002	Plan de continuidad para CloudFleet (Riesgo 6)	Establecer un acuerdo de nivel de servicio (SLA) formal con el proveedor de CloudFleet que garantice tiempos de respuesta y disponibilidad. Definir y documentar un procedimiento manual alternativo para la gestión de flotas en caso de caída del sistema.	Gerencia de Operaciones	Organizativa	1.000−2.500	2 meses	Trimestral
IN-003	Plan de continuidad para Silogran (Riesgo 6)	Al igual que con CloudFleet, formalizar un SLA con el proveedor de Silogran y documentar un procedimiento alternativo para la gestión logística de	Gerencia de Operaciones	Organizativa	1.000−2.500	2 meses	Trimestral

		transportes en caso de indisponibilidad del sistema.					
IN-004	Protección de datos de clientes (Riesgo 6)	Implementar cifrado de las bases de datos que contienen información de clientes. Revisar y actualizar los consentimientos informados conforme a la Ley Orgánica de Protección de Datos (LOPDP). Realizar auditorías trimestrales de acceso a datos sensibles para detectar accesos no autorizados.	Jefatura TI	Técnica / Organizativa	2.000−4.000	4 meses	Semestral

Sytsa Cia. Ltda. (2026)

Nota: Los riesgos con valor igual a 4 (Base de datos de proveedores y Base de datos de empleados) no se incluyen en esta tabla por encontrarse en el umbral de tolerancia establecido por la organización. No obstante, se recomienda mantener su monitorización periódica.

4.6. CHECK LIST PDS (Verificación final)

Una vez definidas las iniciativas de mitigación para los riesgos con valor superior a 4, se procede a realizar una nueva verificación de los controles del Checklist PDS. Esta verificación final permite comparar la situación inicial de SYTSA con la situación esperada tras la implementación de las medidas propuestas, evidenciando el progreso alcanzado gracias al Plan Director de Seguridad.

A continuación, se presenta la tabla comparativa entre el estado inicial y el estado esperado post implantación.

Tabla 16.

Comparativa del Checklist PDS – Estado inicial vs estado esperado.

Nivel	Alcance	Control	Estado inicial	Estado esperado (post implantación)
A	PRO	Analizar la situación actual de la empresa	☒	☒
A	PRO	Alinear el PDS con la estrategia de la empresa	☐	☒
A	PRO	Definir los proyectos a ejecutar	☐	☒
A	PRO	Clasificar y priorizar los proyectos	☐	☒
B	PRO	Aprobar el PDS	☐	☐
A	PRO	Ejecución del PDS	☐	☐
A	PRO	Certificación en seguridad	☐	☐

Sytsa Cia. Ltda. (2026)

Análisis comparativo:

En el estado inicial, SYTSA únicamente presentaba el primer control (análisis de la situación actual) marcado como cumplido, gracias al diagnóstico realizado en el capítulo tercero del presente proyecto. El resto de los controles se encontraban pendientes, lo que reflejaba una ausencia de planificación estructurada en materia de ciberseguridad.

Tras la elaboración del Plan Director de Seguridad, se han definido y priorizado cuatro iniciativas concretas (IN-001 a IN-004) orientadas a mitigar los riesgos cuantificados con valor superior a 4. Estas iniciativas están alineadas con la estrategia de la empresa y cuentan con responsables asignados, plazos de ejecución, costes estimados y periodicidad de revisión. Una vez que el documento sea aprobado por la alta dirección, el control de aprobación del PDS pasará a estar marcado como cumplido. La ejecución de las iniciativas dará inicio en el plazo establecido, dando cumplimiento al sexto control.

En cuanto a la certificación en seguridad, se mantiene como un objetivo a largo plazo, una vez que el sistema de gestión de la seguridad de la información haya alcanzado un nivel de madurez suficiente para afrontar con éxito una auditoría conforme a la norma ISO 27001 o equivalentes. Por ello, este control permanece pendiente en el estado esperado, con previsión de ser abordado en un horizonte de 24 a 36 meses.

Tabla 17

Resumen de evolución de los controles del PDS.

Indicador	Estado inicial	Estado esperado
Controles cumplidos (☒)	1 de 7 (14%)	6 de 7 (86%)
Controles pendientes (☐)	6 de 7 (86%)	1 de 7 (14%)

Sytsa Cia. Ltda. (2026)

CAPITULO 5. Propuesta de implementación de un sistema de gestión basado en la norma ISO 31000:2018 en la empresa SYTSA S.A.

La norma ISO 31000:2018 es una guía internacional que establece principios y directrices para la gestión de riesgos dentro de una organización. Su aplicación permite identificar, analizar, evaluar y tratar los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos y operacionales de una empresa, contribuyendo así a una mejor toma de decisiones y al fortalecimiento de sus procesos. En la actualidad, las empresas del sector logístico y de transporte se enfrentan constantemente a diferentes riesgos relacionados con la seguridad, la operación, el cumplimiento legal, la tecnología, el entorno económico y la cadena de suministro. Por esta razón, contar con un sistema de gestión de riesgos se ha convertido en una necesidad importante para garantizar la continuidad de las operaciones y la protección de los recursos organizacionales.

Transportes y Servicios Asociados SYTSA Cía. Ltda., dedicada al transporte de carga pesada, servicios logísticos y operaciones aduaneras a nivel nacional e internacional, mantiene el compromiso de brindar servicios seguros, confiables y eficientes. Debido a la naturaleza de sus actividades, la organización se encuentra expuesta a riesgos operacionales, viales, físicos, legales y de seguridad en la cadena logística, por lo que resulta fundamental implementar herramientas que permitan prevenir y controlar dichos riesgos de manera oportuna.

5.1. Objeto y campo de aplicación

El objeto del Sistema de Gestión de Riesgos (SGR) de la empresa Transportes y Servicios Asociados SYTSA Cía. Ltda., se fundamenta en los lineamientos de la norma ISO 31000:2018. Su finalidad es proporcionar un enfoque sistemático, estructurado e integral para la gestión de los riesgos que puedan afectar el logro de los objetivos organizacionales.

En concordancia con dicha norma, la gestión del riesgo tiene como propósito la creación y protección del valor, contribuyendo a la mejora del desempeño organizacional, al fortalecimiento de la toma de decisiones y a la sostenibilidad del negocio.

En este contexto, el Sistema de Gestión de Riesgos tiene como objeto:

- Identificar, analizar y tratar los riesgos asociados a la cadena logística y al transporte de carga.
- Prevenir eventos relacionados con actividades ilícitas, tales como narcotráfico, contrabando y terrorismo, conforme al enfoque BASC.
- Garantizar la seguridad física, vial y operacional en todas las actividades de la organización.
- Asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.
- Fortalecer la resiliencia organizacional frente a amenazas internas y externas.

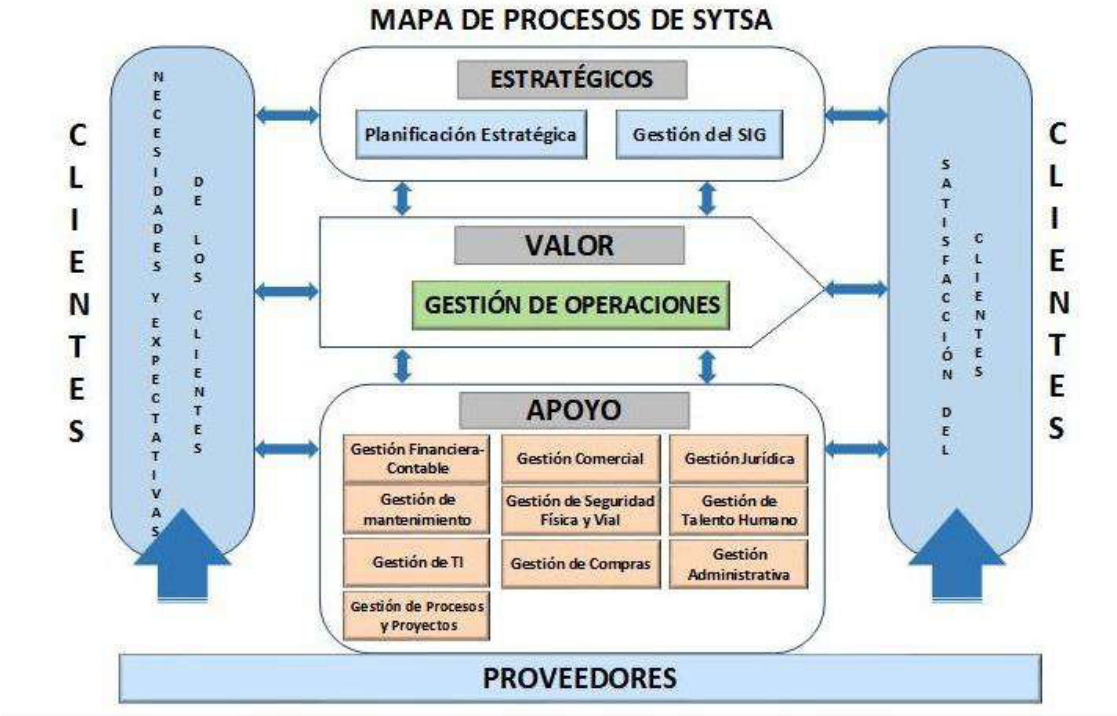
De esta manera, el Sistema de Gestión de Riesgos se constituye como una herramienta clave para la gestión estratégica y operativa de la organización, adoptando los siguientes enfoques:

- Integral: aplicado a todos los niveles y procesos de la organización.
- Preventivo: orientado a la mitigación de riesgos antes de su materialización.
- Basado en procesos: alineado con el Sistema de Gestión en Control y Seguridad BASC (SGCS).
- Dinámico: adaptable a los cambios del entorno interno y externo.

El alcance del SGR institucional es transversal, siendo aplicado en cada uno de los procesos descritos en el mapa de proceso interno, con gestión organizacional y operativa a nivel nacional como valor agregado de servicio para las partes interesadas como clientes, proveedores y trabajadores haciendo énfasis en la seguridad y tratamiento de información.

Figura 11

Mapa de procesos de SYTSA S.A.



Elaborado por: SYTSA S.A

5.2. Referencias normativas

La siguiente propuesta de implementación del sistema de gestión tiene como referencias normativas los siguientes marcos:

Norma principal:

- ISO 31000:2018 – Gestión del riesgo – Directrices

Normas secundarias y estándares de referencia:

- BASC V6-2022 – Seguridad en la cadena de suministro
- ISO 9001:2015 – Sistemas de gestión de la calidad – Requisitos
- ISO 14001:2015 – Sistemas de gestión ambiental – Requisitos
- ISO 45001:2018 – Sistemas de gestión de seguridad y salud en el trabajo
- ISO 27001:2022 – Seguridad de la información – Sistemas de gestión
- ISO 27701:2019 – Gestión de la privacidad de la información
- ISO 22301:2019 – Continuidad del negocio

Normativa legal ecuatoriana:

- Constitución del Ecuador 2008

- Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP)
- Reglamento General a la Ley Orgánica de Protección de Datos Personales
- Código de Trabajo del Ecuador
- Ley de Seguridad y Salud en el Trabajo del Ecuador
- Normas técnicas de ciberseguridad del Ministerio de Telecomunicaciones
- Código de comercio
- Superintendencia de Compañías, Valores y Seguros (SCVS)
- Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial (LOTTTSV)

Normativa interna:

- Política de seguridad de la información de SYTSA (en proceso de elaboración)
- Reglamento de protección de datos de SYTSA S.A
- Acuerdo de confidencialidad y tratamiento de datos personales de SYTSA
- Matriz de requisitos legales y cumplimientos internos de SYTSA

La integración de estas normas permite que el sistema de gestión de riesgos: Sea transversal a todos los sistemas de gestión existentes, garantice una visión holística del riesgo, fortalezca la seguridad de la cadena logística, facilite auditorías, certificaciones y cumplimiento regulatorio.

5.3. Términos y definiciones

Para efectos del Sistema de Gestión de Riesgos de SYTSA, se adoptan los términos establecidos en la ISO 31000:2018.

- **Administración/gestión de riesgos:** Proceso sistemático para la administración de riesgos dentro de la organización que posee estructura y funciones definidas para alcanzar sus objetivos.
- **Consecuencia:** Resultado de un evento que afecta a los objetivos, pudiendo ser directa o indirecta.
- **Control:** Actividad de monitoreo de procesos y aplicación de medidas preventivas, correctivas y de mejora para evitar eventos no deseados.
- **Evento:** Ocurrencia o cambio de circunstancias que puede generar una o varias consecuencias.
- **Fuente de riesgo:** Elemento que tiene el potencial de generar un riesgo, ya sea de forma individual o en combinación con otros factores.

- **Parte interesada:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.
- **Probabilidad:** Posibilidad de que ocurra un evento, evaluada de manera cualitativa o cuantitativa.
- **Riesgo:** Posibilidad de ocurrencia de un evento que impacte los objetivos, medido en términos de probabilidad y consecuencia

Términos específicos de SYTSA:

- **Cadena logística:** Conjunto de procesos interrelacionados que SYTSA ejecuta para el transporte y almacenamiento de carga desde el origen hasta el destino final.
- **CloudFleet:** Plataforma tecnológica utilizada por SYTSA para la gestión y monitoreo de flotas de transporte.
- **ERP Odoo:** Sistema corporativo utilizado por SYTSA para la gestión administrativa, comercial y operativa.
- **Hosting compartido:** Modalidad de alojamiento web en la que SYTSA no cuenta con servidores físicos propios.
- **Silogran:** Sistema logístico de transportes utilizado por SYTSA para la gestión de operaciones de carga.

5.4 Principios

La norma ISO 31000:2018 establece ocho principios fundamentales que constituyen la base sobre la cual se sustenta el Sistema de Gestión de Riesgos. Estos principios deben ser aplicados y personalizados en SYTSA para garantizar la efectividad del sistema.

5.4.1 Integrada

La gestión de riesgos debe estar integrada en todas las actividades de la organización, formando parte de la estructura, procesos y cultura organizacional. No debe ser tratada como una actividad independiente, sino como un elemento clave en la toma de decisiones.

En SYTSA, la integración de la gestión de riesgos implica que todos los procesos organizacionales deben incorporar la identificación y evaluación de riesgos como parte de sus actividades habituales. Esto incluye las áreas administrativas, operativas, financieras y tecnológicas.

Para lograr una integración efectiva, SYTSA implementará las siguientes acciones:

- **Cultura de gestión del riesgo:** Se fomentará una cultura institucional donde la gestión del riesgo sea parte del día a día de todos los colaboradores, desde la alta dirección hasta el personal operativo.

- **Responsabilidad compartida:** Se asignarán responsabilidades claras en todos los niveles jerárquicos, asegurando que cada área y cada trabajador conozca su rol en la gestión del riesgo.
- **Integración en procesos:** Se incorporarán matrices de riesgos en cada proceso identificado en el mapa de procesos de SYTSA, especialmente en los procesos de operaciones, TI, seguridad física y talento humano.
- **Vinculación con otros sistemas:** La gestión de riesgos se vinculará con otros sistemas de gestión existentes en SYTSA, como el Sistema de Gestión de Calidad y el Sistema de Gestión en Control y Seguridad BASC.

La implementación de este principio permitirá a la organización mejorar la toma de decisiones, anticiparse a eventos adversos y fortalecer su resiliencia organizacional.

5.4.2 Estructurada y Exhaustiva

La gestión de riesgos debe seguir un enfoque estructurado y completo que garantice resultados coherentes, comparables y confiables.

SYTSA implementará una metodología formal para la gestión de riesgos que incluya las siguientes fases principales:

1. **Identificación de riesgos:** Se identificarán todas las fuentes de riesgo, eventos y consecuencias que puedan afectar los objetivos de SYTSA, incluyendo riesgos operativos, tecnológicos, financieros y de seguridad de la información.

2. **Análisis de riesgos:** Se analizarán las causas, probabilidad de ocurrencia y posibles consecuencias de cada riesgo identificado, utilizando herramientas cualitativas y cuantitativas.

3. **Evaluación de riesgos:** Se compararán los niveles de riesgo estimados con los criterios de riesgos establecidos por SYTSA para determinar qué riesgos requieren tratamiento prioritario.

4. **Tratamiento del riesgo:** Se implementarán medidas para evitar, reducir, transferir o aceptar los riesgos, según corresponda.

5. **Monitoreo y revisión:** Se establecerán mecanismos de seguimiento continuo para verificar la efectividad de los controles y la evolución de los riesgos.

Herramientas a utilizar en SYTSA:

- Matriz de riesgos (cualitativa y cuantitativa)
- Mapas de calor (heat maps)
- Indicadores clave de riesgo (KRI)

- Procedimientos documentados para cada fase

La aplicación de este principio permitirá obtener información confiable, mejorar la priorización de riesgos y garantizar la trazabilidad del proceso de gestión de riesgos en toda la organización.

5.4.3 Adaptativa

La gestión de riesgos debe estar alineada con el contexto externo e interno de la organización y con sus objetivos.

En la empresa SYTSA, la gestión del riesgo será diseñada y aplicada de manera específica conforme a las características propias de la organización, su entorno operativo y su modelo de negocios basado es soluciones tecnológicas e industrial; la misma que se adaptara al contexto de la empresa y a los diferentes cambios que la misma necesitara en su entorno operativo, tecnológico, organizacional y comercial.

La adaptación del sistema de gestión de riesgos implica que no se utilizara un enfoque genérico, sino que se ajustara a los elementos internos y externos que afecten a la empresa. Las herramientas que se utilizaran serán ajustadas a los procesos claves de la empresa y se realizaran monitoreos periódicos para su valoración.

Los riesgos no se gestionarán de forma aislada, si no como parte del cumplimiento de los objetivos organizacionales y se alinearan con los objetivos estratégicos; los cuales estarán

directamente vinculado con: la continuidad del negocio, la calidad del servicio técnico, la innovación tecnológica y la satisfacción del cliente.

La adaptación continua del sistema permitirá que la gestión de riesgos sea relevante y efectiva frente a los cambios del entorno y de la organización.

5.4.4 Inclusiva

La gestión de riesgos debe considerar las necesidades, percepciones y opiniones de las partes interesadas, promoviendo su participación activa.

En SYTSA, la gestión del riesgo se desarrollará bajo un enfoque inclusivo, promoviendo la participación activa y oportuna de todas las partes interesadas relevantes, tanto internas como externas, con el fin de enriquecer la toma de decisiones para fortalecer la identificación y tratamiento de los riesgos. Este principio reconoce que la diversidad de perspectiva permite una mejor compresión de los riesgos y sus posibles impactos, por eso primeramente se identificaran las partes interesadas internas y externas; después se llevara a cabo la implementación de talleres, reuniones, encuestas y canales de comunicación directa (reportes de incidentes) para recopilar información valiosa desde distintos niveles organizacionales y garantizar la inclusión efectiva.

La inclusión de todas las partes interesadas permitirá una mejor identificación de riesgos, mayor compromiso organizacional y decisiones más acertadas.

5.4.5 Dinámica

La gestión de riesgos debe ser dinámica, permitiendo identificar y responder oportunamente a los cambios que se produzcan en el contexto de la organización.

La gestión del riesgo permite anticipar, detectar, reconocer y responder a los riesgos que tienden a cambiar, aparecer o desaparecer según el contexto interno o externo de la empresa. Para poner en marcha el principio del dinamismo, SYTSA S.A. enfatiza la necesidad de tener una respuesta óptima, ágil y proactiva en la cual se desarrolle las capacidades internas que permitan a las organizaciones tener un control de los sistemas para detectar cambios en los indicadores claves de riesgo.

Se debe realizar evaluaciones periódicas de los riesgos y analizar los escenarios vulnerables que puedan tener posibles cambios para anticipar y mantener una postura proactiva en el entorno empresarial. De igual manera, es importante actualizar las estrategias de gestión del riesgo periódicamente para asegurar la resiliencia, la continuidad del negocio y la protección de activos frente a amenazas nuevas o que puedan evolucionar con el tiempo. Por último, es necesario desarrollar protocolos con un enfoque flexible y adaptativo para detectar y responder riesgos emergentes de forma rápida y segura.

El dinamismo del sistema permitirá a SYTSA anticiparse a nuevas amenazas, adaptarse rápidamente a los cambios y mantener una posición resiliente frente a la incertidumbre.

5.4.6 Mejor información disponible

El sistema de gestión del riesgo se basa en recopilar información histórica y actualizada con datos precisos y relevantes para una evaluación y una diligencia efectiva de los riesgos.

La empresa SYTSA S.A. debe tener en cuenta explícitamente cualquier limitación e incertidumbre de la información y por ello se recomienda en invertir en sistemas de recopilación y análisis de datos, fomentar una cultura de transparencia en el intercambio y manejo de la información, mantener un compromiso con la mejora continua, fomentar una cultura orientada a la toma de decisiones y a formar colaboradores que puedan interpretar, utilizar y gestionar datos de manera efectiva.

Para un correcto manejo de información se debe tomar en cuenta:

- Datos históricos y sus fuentes de información.
- Detección temprana de riesgos emergentes
- Identificación de patrones y tendencias
- Análisis en tiempo real
- Anticipación de escenarios futuros
- Limitaciones

El uso de la mejor información disponible permitirá a SYTSA tomar decisiones más informadas, reducir la incertidumbre y mejorar la efectividad de los controles implementados.

5.4.7 Factores humanos y culturales

La gestión del riesgo debe considerar los comportamientos, percepciones y valores de las personas, así como la cultura organizacional, ya que estos factores influyen en la efectividad del sistema.

La gestión del riesgo dentro de SYTSA reconoce que los factores humanos y culturales constituyen elementos fundamentales para el adecuado funcionamiento del sistema de gestión basado en la norma ISO 31000:2018, debido a que el comportamiento de las personas, la cultura organizacional, la comunicación interna y la percepción del riesgo influyen directamente en la identificación, análisis, tratamiento y control de los riesgos corporativos.

En este contexto, SYTSA promoverá una cultura institucional orientada a la prevención, la responsabilidad compartida y la mejora continua, fomentando la participación activa de todos los niveles jerárquicos en las actividades relacionadas con la gestión del riesgo. La alta dirección será responsable de impulsar políticas y lineamientos que fortalezcan la concienciación sobre la importancia de gestionar adecuadamente los riesgos operativos, tecnológicos, estratégicos y de seguridad de la información presentes en la organización.

SYTSA garantizará que el personal cuente con las competencias, conocimientos y recursos necesarios para cumplir sus funciones de manera segura y eficiente, promoviendo programas permanentes de capacitación, sensibilización y formación relacionados con:

- Gestión integral de riesgos.
- Seguridad de la información.
- Protección de activos tecnológicos.
- Continuidad del negocio.
- Manejo seguro de la información.
- Buenas prácticas en el uso de herramientas tecnológicas.
- Prevención de incidentes operativos y tecnológicos.

La organización reconoce que el error humano constituye uno de los principales factores asociados a incidentes operativos y vulnerabilidades de seguridad, especialmente en entornos tecnológicos y logísticos altamente dinámicos. Por tal motivo, se implementarán controles orientados a minimizar riesgos derivados de:

- Uso inadecuado de sistemas informáticos.
- Manejo incorrecto de información confidencial.

- Incumplimiento de procedimientos internos.
- Accesos no autorizados.
- Fallas en la comunicación organizacional.
- Omisión de controles de seguridad.
- Resistencia al cambio organizacional.

Con el fin de fortalecer la cultura preventiva, SYTSA promoverá mecanismos de comunicación interna que permitan reportar incidentes, vulnerabilidades, desviaciones o amenazas sin temor a represalias, fomentando un entorno organizacional basado en la transparencia, la confianza y la mejora institucional.

La gestión de los factores humanos también considerará aspectos relacionados con:

- Carga laboral.
- Fatiga.
- Estrés ocupacional.
- Clima organizacional.
- Adaptación tecnológica.
- Nivel de experiencia del personal.

- Capacidad de respuesta ante incidentes.

Estos elementos podrán influir en la toma de decisiones y en la efectividad de los controles implementados.

Adicionalmente, SYTSA promoverá una cultura de protección de la información y de los activos tecnológicos mediante el establecimiento de políticas de acceso, control de privilegios, autenticación segura y uso responsable de dispositivos corporativos, considerando las características operativas y tecnológicas de la empresa.

En concordancia con la norma ISO 31000:2018, SYTSA reconoce que la gestión del riesgo debe adaptarse al contexto humano y cultural de la organización, integrándose en todos los procesos y actividades institucionales, con la finalidad de fortalecer la resiliencia organizacional, mejorar la capacidad de respuesta y contribuir al cumplimiento de los objetivos estratégicos de la empresa.

5.4.8 Mejora Continua

La gestión de riesgos debe ser un proceso de mejora continua, mediante la revisión y actualización periódica de los análisis, controles y tratamientos implementados.

SYTSA establecerá un proceso permanente de mejora continua del sistema de gestión de riesgos basado en la norma ISO 31000:2018, con el propósito de garantizar la eficacia, eficiencia

y actualización constante de los mecanismos de identificación, análisis, evaluación, tratamiento y monitoreo de riesgos organizacionales.

La mejora continua permitirá fortalecer progresivamente la capacidad de la organización para enfrentar escenarios de incertidumbre, responder oportunamente ante incidentes y adaptarse a cambios internos y externos que puedan afectar el cumplimiento de los objetivos estratégicos y operacionales de la empresa. Para tal efecto, SYTSA implementará procesos sistemáticos de seguimiento, revisión y evaluación periódica del desempeño del sistema de gestión de riesgos, considerando aspectos relacionados con:

- Eficacia de los controles implementados.
- Cumplimiento de políticas y procedimientos.
- Incidentes registrados.
- Riesgos emergentes.
- Vulnerabilidades tecnológicas.
- Cambios normativos.
- Resultados de auditorías y revisiones internas.
- Retroalimentación del personal y partes interesadas.

SYTSA realizará revisiones periódicas del marco de gestión del riesgo con la finalidad de identificar oportunidades de mejora, corregir desviaciones y fortalecer continuamente los procesos organizacionales asociados a la gestión de riesgos. Estas revisiones deberán considerar:

- Cambios tecnológicos.
- Nuevas amenazas cibernéticas.
- Modificaciones en los procesos operativos.
- Actualización de infraestructura tecnológica.
- Cambios regulatorios.
- Variaciones en el contexto organizacional y del mercado.

Como parte del proceso de mejora continua, SYTSA establecerá indicadores de desempeño que permitan evaluar el comportamiento del sistema de gestión de riesgos y medir la efectividad de las acciones implementadas. Entre los principales indicadores se considerarán:

- Número de incidentes registrados.
- Tiempo de respuesta ante incidentes.
- Nivel de cumplimiento de controles.
- Riesgos mitigados.

- Porcentaje de capacitaciones ejecutadas.
- Vulnerabilidades identificadas y corregidas.
- Resultados de auditorías internas.

La alta dirección será responsable de promover una cultura organizacional orientada a la mejora continua, asegurando la asignación de recursos técnicos, humanos y tecnológicos necesarios para mantener actualizado el sistema de gestión de riesgos y garantizar su adecuada implementación. Adicionalmente, SYTSA fomentará la retroalimentación continua entre departamentos y áreas operativas, con el objetivo de identificar oportunidades de optimización y fortalecer la toma de decisiones basada en riesgos.

Toda mejora implementada deberá documentarse adecuadamente mediante registros, informes técnicos, actualizaciones de procedimientos y evidencias de seguimiento, garantizando la trazabilidad y control de las acciones correctivas y preventivas ejecutadas por la organización.

En concordancia con la norma ISO 31000:2018, SYTSA reconoce que la mejora continua constituye un elemento esencial para asegurar que el sistema de gestión de riesgos permanezca adecuado, eficiente y alineado con las necesidades estratégicas, operativas y tecnológicas de la empresa, permitiendo fortalecer la resiliencia organizacional y la continuidad del negocio frente a escenarios cambiantes de riesgo e incertidumbre.

5.5 Marco de referencia

La norma ISO 31000:2018 establece que el marco de referencia permite integrar la gestión del riesgo en todos los procesos organizacionales, asegurando que la gestión de riesgos forme parte de la gobernanza, liderazgo, cultura y toma de decisiones de la empresa. En el caso de SYTSA, el marco de referencia se adapta a las características de la empresa, sus procesos operativos y el contexto logístico nacional e internacional en el que desarrolla sus actividades.

5.5.1 Generalidades

La gestión del riesgo en SYTSA se fundamenta en los principios establecidos por la norma ISO 31000:2018, los cuales promueven un enfoque estructurado, dinámico e integrado en todas las actividades de la organización. El objetivo principal del marco de referencia es garantizar que la gestión de riesgos forme parte de los procesos estratégicos, operacionales y administrativos de la empresa.

Debido a la naturaleza de las operaciones de transporte de carga pesada y logística internacional, SYTSA se encuentra expuesta a riesgos operacionales, viales, legales, tecnológicos, financieros y de seguridad física. Por esta razón, la organización requiere establecer mecanismos de prevención y control que permitan minimizar impactos negativos sobre la continuidad de sus actividades.

El marco de referencia propuesto considera la participación de todos los niveles organizacionales, incluyendo gerencia general, coordinadores operativos, supervisores, conductores y personal administrativo. Esto permitirá fortalecer la cultura organizacional orientada a la prevención y gestión adecuada de riesgos.

Asimismo, la gestión del riesgo debe alinearse con los objetivos estratégicos de la empresa y con los requisitos de seguridad BASC, permitiendo fortalecer la seguridad de la cadena logística, el cumplimiento legal y la protección de los activos organizacionales.

El sistema propuesto busca establecer procedimientos claros para la identificación, evaluación, tratamiento, monitoreo y seguimiento de riesgos, contribuyendo a mejorar la toma de decisiones y la capacidad de respuesta ante incidentes o eventos adversos.

5.5.2 Liderazgo y compromiso

La norma ISO 31000:2018 establece que el liderazgo y compromiso de la alta dirección son fundamentales para garantizar la eficacia del sistema de gestión de riesgos. En SYTSA, la gerencia general deberá asumir un rol activo en la implementación, mantenimiento y mejora continua del sistema.

La alta dirección será responsable de promover una cultura organizacional basada en la prevención, el cumplimiento normativo y la gestión eficiente de riesgos. Para ello, deberá

establecer políticas, objetivos y lineamientos alineados con las necesidades operativas y estratégicas de la empresa.

El liderazgo organizacional también implica garantizar que los recursos necesarios se encuentren disponibles para la gestión del riesgo. Esto incluye capacitación al personal, herramientas tecnológicas, controles de monitoreo, sistemas de seguridad, mantenimiento de flota y mecanismos de comunicación interna.

La siguiente tabla detalla los principales roles, responsabilidades y mecanismos de participación dentro del Sistema de Gestión de Riesgos propuesto para SYTSA, conforme a los lineamientos de la norma ISO 31000:2018.

La gerencia deberá asegurar que las responsabilidades y autoridades relacionadas con la gestión del riesgo sean claramente definidas y comunicadas a todos los colaboradores. Cada trabajador deberá comprender su rol dentro del sistema y participar activamente en la identificación y reporte de situaciones de riesgo.

Dentro de las operaciones de SYTSA, el compromiso de la dirección permitirá fortalecer la seguridad vial, la protección de la carga, la prevención de actividades ilícitas y el cumplimiento de estándares internacionales relacionados con la cadena logística y el transporte terrestre.

En este sentido, los indicadores asignados a la Gerencia General se orientan a medir directamente la rendición de cuentas estratégica relacionada con el desempeño del Sistema de

Gestión de Riesgos, el cumplimiento de objetivos organizacionales, la ejecución de auditorías y la mejora continua del sistema, más allá de la reducción general de incidentes.

Finalmente, el liderazgo y compromiso de la organización contribuirán a fortalecer la confianza de clientes, proveedores y demás partes interesadas, mejorando la reputación y sostenibilidad de la empresa.

Tabla 18

Liderazgo y compromiso

Cargo / Área	Responsabilidades dentro del SGR	Autoridad asignada	Participación en la gestión del riesgo	Indicadores de seguimiento	Fórmula de evaluación del KPI
Gerencia General	Aprobar políticas, objetivos y recursos del SGR.	Aprobación estratégica y toma de decisiones.	Liderar y supervisar el sistema.	Cumplimiento de objetivos estratégicos del SGR; cumplimiento de auditorías internas y externas; nivel de ejecución del plan anual de gestión de riesgos; cumplimiento de metas BASC y acciones correctivas implementadas.	Promedio de cumplimiento general ponderado de todos los proyectos / Número de incidentes con recargo o no conformidad por parte del cliente.
Coordinación Operativa	Supervisar operaciones y	Coordinar acciones preventivas.	Identificar y reportar riesgos operacionales.	Número de incidentes y cumplimiento de controles.	Índice de coordinación operativa ICO:

	controles logísticos. Verificar cumplimiento de normas de seguridad.	Detener actividades inseguras.	Monitorear condiciones de riesgo.	Inspecciones y hallazgos detectados.	% Cumplimiento de controles / (1 + número de incidentes)
Conductores	Cumplir procedimientos de conducción segura.	Aplicar controles en ruta.	Reportar incidentes y riesgos.	Accidentes e infracciones registradas.	(% checklist realizados / % checklist previstos) + (Número de incidentes con reportes realizados / número incidentes con reportes no realizados) + (Número de accidentes /

					número de accidentes previstos) + (Número de eventos de seguridad vial / número de eventos de seguridad vial previstos).
Talento Humano	Gestionar capacitaciones y competencias.	Coordinar formación del personal.	Promover cultura preventiva.	Horas de capacitación ejecutadas.	Número de trabajadores con capacitación completa y vigente / Número de trabajadores con capacitación no vigente o incompleta.

Área Administrativa	Gestionar recursos financieros.	Aprobar presupuestos operativos.	Apoyar sostenibilidad sistema.	del	Control presupuestario.

Índice financiero:

% Ejecución 40%: 100 - 100% - (Gasto Real / Presupuesto Planificado × 100).

% Eficiencia 25% = Costo Estándar por Km / Costo Real por Km × 100.

Flujo de caja 20% = Caja Disponible / Egresos Mensuales × 100, máximo 100%

Tecnología y GPS	Administrar monitoreo y trazabilidad.	Controlar sistemas de seguimiento.	Monitorear rutas y alertas.	Disponibilidad del sistema GPS.	Rentabilidad operativa 15%: Utilidad Operativa / Ingresos × 100 Número de incidentes o no conformodidades del cliente/ Número de incidentes o no conformodidades del cliente esperados
Proveedores y Contratistas	Cumplir políticas y requisitos de seguridad.	Aplicar controles contractuales.	Reportar riesgos detectados.	Evaluación de proveedores.	Número de requerimientos realizados a provedores / Número de requerimientos con incidentes o novedades.

5.5.3 Integración

La integración constituye uno de los principios fundamentales de la norma ISO 31000:2018, ya que establece que la gestión del riesgo debe formar parte de todos los procesos organizacionales y no funcionar de manera independiente o aislada.

En SYTSA, la integración de la gestión del riesgo de manera transversal permitirá incorporar criterios de prevención y control en las actividades operativas, administrativas y estratégicas de la empresa. Esto incluye procesos relacionados con transporte de carga, seguridad vial, mantenimiento de vehículos, logística, gestión documental y control de la cadena de suministro.

La integración del sistema permitirá que la identificación y evaluación de riesgos se realice de manera continua durante la ejecución de las actividades diarias. De esta forma, la empresa podrá anticiparse a posibles amenazas y establecer medidas de control oportunas.

Dentro de las operaciones logísticas de SYTSA, la integración de la gestión del riesgo será aplicada en actividades como planificación de rutas, monitoreo satelital, control de tiempos de conducción, inspección de unidades, control documental y verificación de cumplimiento de normas de seguridad.

La integración también permitirá fortalecer el cumplimiento de estándares BASC, así como otros sistemas de gestión implementados por la organización relacionados con seguridad vial,

seguridad ocupacional y control operacional. Adicionalmente, la organización deberá considerar factores internos y externos que puedan afectar sus actividades, tales como cambios normativos, condiciones de las vías, riesgos de robo de carga, amenazas del entorno, factores climáticos y riesgos asociados a operaciones internacionales.

La correcta integración de la gestión del riesgo permitirá a SYTSA mejorar su desempeño organizacional, reducir incidentes operacionales y fortalecer la continuidad de sus actividades, contribuyendo a la sostenibilidad y competitividad de la empresa.

5.5.4 Diseño

Dentro de la norma ISO 31000:2018, el diseño del marco de referencia describe la estructura en la cual la empresa SYTSA utilizará para gestionar los riesgos persistentes de tal manera que este sistema se adapte de manera efectiva alineado a la cultura organizacional y los objetivos estratégicos que posee. En esta fase se analiza el contexto de la organización lo que nos permite tener una visión holística de los factores internos y externos que puedan afectar a la empresa. Así también se integra los recursos necesarios para la gestión de riesgos y se designa a los responsables que tienen como objetivo mantener una comunicación asertiva que permita comprender las expectativas y las diferentes perspectivas sobre los riesgos inherentes en todas las áreas de la organización.

Para concluir, SYTSA SA debe valorar la efectividad del marco de referencia mediante la evaluación del sistema de gestión de riesgos respecto a los objetivos establecidos alineado al contexto volátil de la empresa y a su capacidad de adaptación al cambio. En base a los resultados del sistema, la empresa debe realizar auditorías periódicas que permitan identificar las áreas de mejora para aplicar medidas correctivas o preventivas, sometiéndose a un proceso de mejora continua que le permitirá estar preparada ante posibles eventos que puedan afectar la continuidad del negocio.

5.5.4.1 Comprensión de la organización y su contexto

La empresa SYTSA S.A.S., en el marco del diseño e implementación del Manual de Gestión del Riesgo basado en la Norma ISO 31000:2018, debe desarrollar una comprensión integral de su organización y del contexto en el que opera, con el propósito de identificar los factores internos y externos que puedan influir en el logro de sus objetivos estratégicos, operativos, financieros y legales.

La comprensión del contexto organizacional constituye una etapa fundamental dentro del diseño del marco de referencia para la gestión del riesgo, debido a que permite identificar las condiciones que pueden generar amenazas, oportunidades o vulnerabilidades para la organización. Mediante el siguiente análisis FODA podemos identificar los factores con mayor relevancia en el sistema de gestión de riesgos:

Tabla 19

Análisis FODA

FORTALEZAS	OPORTUNIDADES
Compromiso inicial de la Alta Dirección con la implementación de la ISO 31000.	Crecimiento de estándares internacionales relacionados con gestión del riesgo.
Interés organizacional en fortalecer los procesos internos y administrativos.	Posibilidad de mejorar la competitividad empresarial mediante certificaciones y buenas prácticas.
Existencia de personal con experiencia operativa y administrativa.	Avances tecnológicos aplicables a la automatización y control de riesgos.
Capacidad de establecer políticas y procedimientos organizacionales.	Acceso a capacitaciones y programas especializados en gestión del riesgo y seguridad de la información.
Disposición para fortalecer la seguridad de la información y continuidad del negocio.	Mayor confianza de clientes y partes interesadas al implementar sistemas de gestión.
Identificación preliminar de procesos estratégicos y operativos.	Implementación de herramientas tecnológicas para monitoreo y seguimiento de riesgos.
Interés en mejorar la cultura organizacional y el cumplimiento normativo.	Adaptación a nuevas oportunidades de mercado mediante procesos más seguros y eficientes.

DEBILIDADES	AMENAZAS
Falta de procedimientos documentados en algunos procesos organizacionales.	Riesgos de ciberseguridad y ataques informáticos.
Deficiencias en la comunicación interna.	Cambios constantes en normativas legales y regulatorias.
Dependencia de personal clave para determinadas actividades críticas.	Incremento de la competencia en el mercado.
Limitaciones presupuestarias para implementación de controles especializados.	Inestabilidad económica y financiera.
Escasa cultura organizacional orientada a la gestión integral del riesgo.	Riesgos reputacionales derivados de incidentes operacionales o tecnológicos.
Necesidad de fortalecer procesos de capacitación y concientización.	Fallas tecnológicas o interrupciones en sistemas de información.
Procesos de identificación y evaluación de riesgos aún en desarrollo.	Cambios tecnológicos acelerados que generen nuevas vulnerabilidades.
Debilidad en mecanismos de seguimiento y control interno.	Exigencias crecientes de clientes y organismos de control.

Contexto Interno de SYTSA S.A.S.

Para el análisis del contexto interno, SYTSA S.A.S. deberá considerar los siguientes elementos:

- La estructura organizacional de la empresa.
- Las funciones y responsabilidades de cada área.
- Los procesos operativos y administrativos.
- La cultura organizacional.
- Las políticas internas y procedimientos establecidos.
- Los recursos humanos, tecnológicos y financieros disponibles.
- El nivel de conocimiento y capacitación del personal.
- Los sistemas de información utilizados.
- La capacidad de respuesta ante incidentes o situaciones de riesgo.

Dentro de este análisis, la empresa deberá identificar aquellas situaciones que puedan afectar negativamente el cumplimiento de sus objetivos institucionales, tales como:

- Falta de procedimientos documentados.
- Deficiencias en la comunicación interna.

- Riesgos operacionales.
- Riesgos tecnológicos y de ciberseguridad.
- Dependencia de personal clave.
- Limitaciones presupuestarias.
- Incumplimiento de políticas internas.

Asimismo, será importante evaluar las fortalezas organizacionales que permitan mejorar la capacidad de gestión del riesgo dentro de SYTSA S.A.S.

Contexto Externo de SYTSA S.A.S.

En relación con el contexto externo, la empresa deberá analizar todos aquellos factores ajenos a la organización que puedan impactar sus actividades y operaciones, entre ellos:

- Factores legales y regulatorios aplicables en Ecuador.
- Cambios económicos y financieros.
- Competencia del mercado.
- Avances tecnológicos.
- Condiciones políticas y sociales.
- Requisitos de clientes y proveedores.

- Riesgos reputacionales.
- Amenazas relacionadas con seguridad de la información y protección de datos.
- Normativa vigente relacionada con gestión de riesgos y continuidad del negocio.

El análisis del contexto externo permitirá a SYTSA S.A.S. anticiparse a posibles amenazas y establecer mecanismos preventivos que contribuyan a minimizar impactos negativos sobre la organización.

Partes Interesadas

Como parte de la comprensión de la organización y su contexto, SYTSA S.A.S. deberá identificar las necesidades y expectativas de las partes interesadas, entre las cuales se incluyen:

- Accionistas.
- Gerencia.
- Trabajadores.
- Clientes.
- Proveedores.
- Entidades de control y regulación.
- Comunidad y sociedad en general.

La identificación de estas partes interesadas permitirá establecer criterios adecuados para la gestión del riesgo y fortalecer la toma de decisiones organizacionales.

Importancia para la Gestión del Riesgo

La correcta comprensión de la organización y su contexto permitirá que SYTSA S.A.S. pueda:

- Identificar riesgos de manera más efectiva.
- Establecer criterios adecuados de evaluación del riesgo.
- Mejorar la toma de decisiones.
- Fortalecer la planificación estratégica.
- Incrementar la capacidad de prevención y respuesta.
- Garantizar el cumplimiento normativo.
- Proteger los recursos y la reputación institucional.

Por tanto, este análisis se convierte en una base esencial para el diseño e implementación del Sistema de Gestión del Riesgo bajo los lineamientos de la ISO 31000:2018.

5.5.4.2 Articulación del compromiso con la gestión del riesgo

La Alta Dirección de SYTSA S.A.S. deberá demostrar liderazgo y compromiso con la gestión del riesgo, garantizando que esta se encuentre integrada en todos los niveles y procesos de la organización, conforme a los lineamientos establecidos en la Norma ISO 31000:2018.

La articulación del compromiso implica que la gestión del riesgo no sea considerada únicamente como una actividad aislada, sino como un elemento estratégico que apoye el cumplimiento de los objetivos institucionales y fortalezca la sostenibilidad organizacional.

Compromiso de la Alta Dirección

La Gerencia de SYTSA S.A.S. deberá asumir un rol activo dentro del proceso de gestión del riesgo mediante las siguientes acciones:

- Aprobar políticas y lineamientos de gestión del riesgo.
- Promover una cultura organizacional orientada a la prevención.
- Asignar recursos necesarios para la implementación del sistema.
- Establecer responsabilidades claras dentro de la organización.
- Participar en la toma de decisiones relacionadas con riesgos críticos.
- Supervisar el cumplimiento de los controles establecidos.

- Impulsar procesos de mejora continua.

La participación activa de la Alta Dirección permitirá fortalecer la eficacia del sistema y generar compromiso por parte de todos los colaboradores.

Integración de la Gestión del Riesgo en los Procesos Organizacionales

SYTSA S.A.S. deberá integrar la gestión del riesgo dentro de:

- Procesos estratégicos.
- Procesos operativos.
- Procesos administrativos.
- Procesos financieros.
- Procesos tecnológicos.
- Gestión de talento humano.
- Seguridad de la información.
- Cumplimiento legal y regulatorio.

La integración permitirá que los riesgos sean considerados en todas las actividades y decisiones organizacionales, reduciendo la posibilidad de incidentes que afecten la continuidad de las operaciones.

Cultura Organizacional y Concientización

La empresa deberá fomentar una cultura de gestión del riesgo mediante:

- Capacitaciones periódicas.
- Programas de sensibilización.
- Comunicación interna efectiva.
- Participación del personal en la identificación de riesgos.
- Difusión de políticas y procedimientos.

El fortalecimiento de la cultura organizacional contribuirá a que todos los colaboradores comprendan la importancia de identificar, reportar y gestionar riesgos de manera oportuna.

Comunicación del Compromiso

La Alta Dirección deberá comunicar formalmente su compromiso con la gestión del riesgo a través de:

- Políticas institucionales.
- Manuales y procedimientos.
- Reuniones organizacionales.
- Capacitaciones internas.

- Comunicados oficiales.

Esto permitirá que todos los niveles de la organización conozcan sus responsabilidades y participen activamente en el sistema de gestión del riesgo.

Beneficios de la Articulación del Compromiso

La adecuada articulación del compromiso con la gestión del riesgo permitirá a SYTSA S.A.S.:

- Mejorar la capacidad de respuesta ante incidentes.
- Reducir pérdidas operacionales.
- Fortalecer el cumplimiento normativo.
- Proteger la información y activos de la empresa.
- Mejorar la toma de decisiones.
- Incrementar la confianza de clientes y partes interesadas.
- Garantizar la continuidad del negocio.

En consecuencia, el compromiso institucional representa un elemento clave para asegurar la eficacia y sostenibilidad del Manual de Gestión del Riesgo basado en la ISO 31000:2018 dentro de SYTSA S.A.S.

5.5.4.3 Asignación de roles, autoridades, responsabilidades y obligaciones de rendir cuentas en la organización

De acuerdo con los lineamientos establecidos en la Norma ISO 31000:2018, la empresa de Transportes y Servicios Asociados SYTSA Cía. Ltda. deberá definir claramente los roles, autoridades, responsabilidades y obligaciones de rendición de cuentas dentro del marco de gestión de riesgos, con el propósito de garantizar una adecuada administración de los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos, operativos y tecnológicos de la organización.

La correcta asignación de responsabilidades permitirá fortalecer la gobernanza corporativa y fomentar una cultura organizacional orientada a la prevención, control y tratamiento oportuno de los riesgos. Asimismo, facilitará que cada colaborador conozca sus funciones específicas dentro del sistema de gestión de riesgos y comprenda el impacto de sus decisiones y actividades sobre la continuidad operativa de la empresa, por ello, resulta indispensable establecer una estructura organizacional que permita gestionar estos riesgos de manera eficiente e integral.

La Alta Dirección será responsable de liderar y promover el marco de gestión de riesgos, asegurando que las políticas, objetivos y estrategias estén alineados con los principios de la norma ISO 31000:2018. Además, deberá aprobar los lineamientos generales, proporcionar el apoyo institucional necesario y fomentar una cultura preventiva dentro de toda la organización.

Los directores y responsables de cada área deberán identificar, analizar y reportar los riesgos asociados a sus procesos, así como implementar medidas de control y seguimiento que permitan reducir la probabilidad e impacto de eventos adversos. Cada líder departamental tendrá la obligación de supervisar el cumplimiento de los procedimientos establecidos y comunicar oportunamente cualquier incidente o vulnerabilidad detectada.

El área de Tecnología de la Información tendrá una participación fundamental dentro del sistema de gestión de riesgos debido a la naturaleza tecnológica de SYTSA. Esta área será responsable de gestionar riesgos relacionados con seguridad informática, disponibilidad de sistemas, protección de la información, accesos no autorizados, respaldo de datos y continuidad tecnológica.

Asimismo, se propone la creación de un Comité de Gestión de Riesgos conformado por representantes de las principales áreas de la organización, cuya función será coordinar las actividades relacionadas con la gestión del riesgo, supervisar la implementación del sistema y promover la mejora continua del marco de referencia establecido bajo ISO 31000:2018.

Tabla 20

Roles y responsabilidad dentro del Sistema de Gestión de Riegos

Cargo o Área	Responsabilidad
Alta Dirección (Gerencia General)	Aprobar políticas, objetivos y estrategias de gestión de riesgos.
Comité de Gestión de Riesgos	Supervisar la implementación y seguimiento del sistema de gestión de riesgos.
Área de Tecnología	Gestionar riesgos tecnológicos y de seguridad de la información.
Jefes Departamentales	Identificar, evaluar y reportar riesgos asociados a sus procesos.
Talento Humano	Coordinar programas de capacitación y concientización sobre gestión de riesgos.
Personal Operativo y Administrativo	Cumplir procedimientos y reportar incidentes o vulnerabilidades detectadas.

5.5.4.4 Asignación de recursos

La Empresa SYTSA deberá garantizar la asignación de recursos necesarios para implementar, mantener y mejorar continuamente el sistema de gestión de riesgos basado en la Norma ISO 31000:2018. La disponibilidad adecuada de recursos permitirá asegurar la eficacia del marco de gestión de riesgos y contribuirá al cumplimiento de los objetivos estratégicos, operacionales y tecnológicos de la organización.

La asignación de recursos constituye un elemento esencial para fortalecer la capacidad de la empresa frente a eventos adversos que puedan afectar sus servicios tecnológicos, infraestructura, activos de información y operaciones comerciales. Por ello, la organización deberá destinar recursos financieros, humanos, tecnológicos y físicos suficientes para la correcta gestión de riesgos.

En relación con los recursos humanos, SYTSA deberá contar con personal competente y capacitado en gestión de riesgos, seguridad de la información, continuidad del negocio y manejo de incidentes tecnológicos. La empresa promoverá programas permanentes de formación y concientización dirigidos a todos los niveles organizacionales.

Respecto a los recursos tecnológicos, la empresa deberá disponer de herramientas, plataformas y sistemas especializados que permitan identificar, monitorear y controlar riesgos asociados a los procesos tecnológicos e industriales. Asimismo, SYTSA deberá asignar recursos

financieros adecuados para cubrir inversiones relacionadas con infraestructura tecnológica, adquisición de equipos, implementación de controles de seguridad, auditorías internas, mantenimiento preventivo de vehículos de transporte, contratación de servicios especializados en talleres de repuestos de vehículos y ejecución de programas de capacitación en seguridad vial.

La empresa también deberá establecer procesos de planificación y seguimiento presupuestario que permitan evaluar periódicamente la disponibilidad y utilización eficiente de los recursos asignados al sistema de gestión de riesgos.

Tabla 21

Recursos necesarios para la implementación del Sistema de Gestión de Riesgos

Tipo de recurso	Descripción
Recursos Humanos	Personal capacitado en gestión de riesgos, ciberseguridad, seguridad vial y continuidad del negocio.
Recursos Tecnológicos	Software de monitoreo, antivirus, firewalls y herramientas de análisis de riesgos.
Recursos Financieros	Presupuesto destinado a capacitación, auditorías, infraestructura, mantenimiento de vehículos y controles de seguridad.

Recursos Físicos	Instalaciones, equipos tecnológicos, centros de datos, talleres de mantenimiento, vehículos de transporte pesado y sistemas de protección física.
Recursos de Capacitación	Programas de formación y concientización para el personal (seguridad física, ciberseguridad, seguridad vial)
Recursos para Continuidad Operativa	Planes de contingencia, respaldos de información, mecanismos de recuperación ante incidentes.

5.5.4.5 Establecimiento de la comunicación y la consulta

La empresa SYTSA SA establecerá un enfoque integral en el cual se relacione la comunicación y la consulta para apoyar al marco de referencia de la norma ISO 31000:2018 la cual facilitará la aplicación eficaz de la gestión del riesgo. Para ello, la empresa implementará un proceso de comunicación oportuna, transparente y bidireccional a todas las partes interesadas, fomentando una cultura de gestión proactiva de riesgos en todos los niveles jerárquicos de la organización.

Este proceso permitirá incorporar la experiencia, el conocimiento local y las percepciones de los diversos actores para enriquecer la toma de decisiones y la apertura de realizar consultas sobre el tema enriqueciendo una retroalimentación continua de los colaboradores para mejorar la

identificación y la evaluación de los riesgos. Para desarrollar este plan de comunicación integral se debe contemplar las siguientes acciones:

- *Definición de objetivos.* - Fomentar una cultura de gestión de riesgos donde se profundice la concientización, la transparencia de la información y la retroalimentación continua a los trabajadores.
- *Difusión interna.* – Establecer lineamientos claros, protocolos de seguridad y emitir reportes específicos de cada área con el fin de socializar a todos los trabajadores sobre el proceso del sistema mediante carteleras informativas físicas en áreas comunes y plataformas digitales internas.
- *Inducción y capacitación.* – Realizar talleres y reuniones de capacitación de acuerdo a los perfiles de cada puesto de trabajo en los cuales se priorice la importancia de reportar incidentes laborales, identificación de riesgos y el uso de canales de comunicación propios de la empresa
- *Partes externas.* – Establecer un proceso de comunicación para el personal externo como proveedores, clientes o entidades reguladoras que requieran conocer las medidas de continuidad del negocio o vulnerabilidades relacionadas a datos personales.
- *Canales de comunicación.* – Fomentar el uso de correos electrónicos mediante la intranet corporativa en la cual se establezca políticas de seguridad para la actualización periódica

del sistema a toda la organización y para dar cumplimiento a las obligaciones de la ley orgánica de protección de datos personales.

- *Formato de informes.* – Se debe definir plantillas estandarizadas que contengan la descripción del riesgo, el nivel del riesgo, el responsable de tratar el riesgo, planes de acción, el monitoreo del avance del riesgo, los resultas y los planes de mejora que se deben seguir.

Para un control exhaustivo de las rutas de los choferes y garantizar el cumplimiento de los horarios de entrega, se implementan dispositivos GPS para geolocalizar la flota y permite la visualización exacta, la velocidad y la dirección de cada unidad. Además, es responsabilidad de cada chofer reportar cualquier anormalidad en la ruta como cierre de caminos, accidentes que impidan la circulación del transporte o cualquier tipo de altercado que retrase o imposibilite la entrega de las cargas en el horario planificado mediante los canales oficiales de comunicación ya sean estos el reporte vía telefónica (llamada o mensajes de WhatsApp), y de ser necesario, se debe aplicar un protocolo de emergencia vial que consiste en la regla nemotécnica PAS (Proteger, Avisar, Socorrer).

El plan de comunicación debe ser monitoreado eventualmente para evaluar si la información entregada es veraz, si los canales de información son adecuados y efectivos y si la empresa se adapta al contexto cambiante del entorno en que desarrolla sus actividades.

5.5.5 Implementación

La implementación del sistema de gestión de riesgos representa la fase operativa en la cual SYTSA SA ejecuta los principios, las políticas y los procesos definidos en el marco normativo y estratégico. El proceso de implementación se alinea a los objetivos establecidos, lo que garantiza la participación activa de las partes interesadas y permite la integración progresiva de una cultura organizacional resiliente. Para ello se requiere:

- *Identificar el riesgo.* – Se determina el escenario, las condiciones cambiantes y las amenazas que pueden afectar el cumplimiento de los objetivos.
- *Análisis del riesgo.* – Evaluar el nivel del riesgo (probabilidad x impacto) de los riesgos identificados mediante la matriz de riesgos o mapas de calor.
- *Evaluación del riesgo.* – Mediante los resultados expuestos se podrá realizar una comparación de los niveles de riesgo versus los criterios de aceptación de la empresa y de esa manea se priorizarán los riesgos que requieran un plan de acción inmediato para ser tratados.
- *Tratamiento del riesgo.* – Se ejecutarán planes de acción que permitan evitar, mitigar, compartir o aceptar el riesgo con mayor grado de priorización. Para ello el encargado del tratamiento del riesgo deberá utilizar los recursos necesarios de la empresa y deberá llevar el monitoreo y control del plan de acción.

- *Comunicación y consulta.* – Durante el proceso se garantizará la comunicación asertiva de las partes interesadas promoviendo la transparencia y la participación de los colaboradores.
- *Monitoreo y control.* – Se debe dar seguimiento periódico a todos los riesgos para garantizar la efectividad del plan de acción y el cumplimiento de las estrategias establecidas.
- *Actualización.* – Se debe actualizar los registros del mapa de calor y matrices de cada área de trabajo para mantener un monitoreo continuo ante posibles riesgos que puedan encontrarse.
- *Retroalimentación.* – La retroalimentación permite que se mantenga un enfoque dinámico y participativo que asegura dentro del marco de gestión el desarrollo organizacional y la participación de las partes interesadas, también contribuye a realizar evaluaciones periódicas del sistema lo que permite identificar áreas de mejora y aplicar acciones correctivas o preventivas

5.5.6 Valoración

La valoración del marco de referencia de gestión de riesgos tiene como propósito medir periódicamente el desempeño del sistema implementado, verificando su idoneidad, eficacia y alineamiento con los objetivos estratégicos y operacionales de SYTSA. Conforme a lo establecido en la norma ISO 31000:2018, la organización debe evaluar si el marco de gestión de riesgos

permanece adecuado para apoyar el logro de sus metas y si los recursos asignados están siendo utilizados de manera eficiente.

5.5.6.1 Indicadores de desempeño

Para llevar a cabo la valoración, SYTSA definirá un conjunto de indicadores clave de desempeño (KPIs) que permitan medir tanto el funcionamiento del sistema de gestión de riesgos como la efectividad de los controles implementados, vinculados directamente a los riesgos críticos identificados en el análisis previo (ERP Odoo, CloudFleet, Silogran, bases de datos, cámaras, etc.)

Tabla 22

Indicadores de desempeño del Sistema de Gestión de Riesgos

Indicador	Descripción	Línea base	Meta	Frecuencia	Responsable
Porcentaje de riesgos críticos con plan de tratamiento	Riesgos con puntuación >4 (Tabla 15 del PDS) que cuentan con plan implementado	0% (inicial)	≥90%	Trimestral	Comité de Gestión de Riesgos
Cumplimiento de planes de tratamiento	Porcentaje de acciones ejecutadas frente a lo planificado (IN-001 a IN-004)	–	≥85%	Mensual	Jefes departamentales
Tiempo de respuesta ante incidentes de seguridad	Tiempo promedio entre detección y contención (incidentes cibernéticos o de seguridad física)	No medido	<2 horas	Mensual	Área de TI / HSE

Disponibilidad de sistemas críticos	Porcentaje de tiempo operativo de ERP Odoo, CloudFleet y Silogran	No medido formalmente	≥99.5%	Mensual	Área de TI
Reducción de incidentes operativos	Variación en número de accidentes, robos de carga, fallas tecnológicas graves respecto al semestre anterior	Línea base del año 0	≥15% anual	Semestral	Coordinación Operativa
Horas de capacitación en gestión de riesgos	Total de horas de formación impartidas al personal	0 horas	≥20 horas por persona/año	Trimestral	Talento Humano
Porcentaje de colaboradores capacitados	Colaboradores que han recibido al menos 8 horas de formación en riesgos	0%	≥90%	Semestral	Talento Humano

Eficacia de controles tecnológicos	Porcentaje de controles (antivirus, firewall, 2FA, copias de seguridad) operativos y actualizados	Parcial	100%	Mensual	Área de TI
Cumplimiento normativo	Porcentaje de requisitos legales (LOPDP, BASC, LOTTTSV) con evidencia de cumplimiento	Variable por norma	100%	Semestral	Dpto. Jurídico / HSE
Incidentes de fuga de datos	Número de eventos de acceso no autorizado a bases de datos de clientes, proveedores o empleados	0	0 (tolerancia cero)	Mensual	Área de TI

5.5.6.2 Metodología de valoración

La valoración se realizará siguiendo un proceso estructurado que incluye las siguientes actividades:

1. **Revisión documental**: Análisis de registros del sistema de gestión de riesgos, incluyendo matrices de riesgos, planes de tratamiento, informes de incidentes, actas del Comité de Gestión de Riesgos y resultados de indicadores.
2. **Auditorías internas**: El área de Calidad y Seguridad ejecutará auditorías internas periódicas (al menos una vez al año) para verificar la implementación y eficacia del marco de referencia. Estas auditorías se basarán en la lista de verificación del Plan Director de Seguridad (Tabla 16).
3. **Encuestas y consultas a partes interesadas**: Se recopilará la percepción de colaboradores, proveedores y clientes sobre la cultura de riesgos y la efectividad de los controles, mediante encuestas anónimas semestrales.
4. **Análisis de tendencias**: Evaluación de la evolución de los indicadores de desempeño, identificación de desviaciones y correlación con eventos o cambios internos/externos.
5. **Revisión por la alta dirección**: La Gerencia General y el Comité de Gestión de Riesgos sostendrán una reunión de valoración **cada seis meses** para analizar los resultados de los

indicadores, las auditorías y las consultas, y determinar si el marco de referencia sigue siendo adecuado.

5.5.6.3 Criterios de aceptación del desempeño

Para que el marco de referencia se considere eficaz, SYTSA deberá cumplir con los siguientes criterios mínimos:

Tabla 23

Criterios de aceptación del desempeño

Criterio	Estándar mínimo
Riesgos críticos con plan de tratamiento	≥80%
Cumplimiento de planes de tratamiento	≥85%
Reducción anual de incidentes operativos	≥15%
Personal capacitado en gestión de riesgos	≥90%
Disponibilidad de sistemas críticos	≥99%
Sanciones regulatorias por incumplimiento	0 (cero)
Incidentes de fuga de datos	0 (cero)

Si durante la valoración se detecta que uno o más criterios no se cumplen, el Comité de Gestión de Riesgos deberá elaborar un **plan de acciones correctivas** en un plazo no mayor a 30 días, con responsables y fechas claras.

5.5.6.4 Registro de la valoración

Todos los resultados de la valoración serán documentados en un Informe de Valoración del SGR, que contendrá:

- Fecha y alcance de la valoración.
- Resultados de cada indicador (tabla comparativa).
- Hallazgos de auditorías internas.
- Resultados de encuestas a partes interesadas.
- Análisis de tendencias y desviaciones.
- Conclusiones sobre la idoneidad y eficacia del marco.
- Plan de acciones correctivas (si aplica).
- Fecha de la próxima valoración.

El informe será aprobado por el Comité de Gestión de Riesgos y presentado a la Gerencia General.

5.5.7 Mejora

La norma ISO 31000:2018 establece que el marco de referencia de gestión de riesgos debe ser objeto de mejora continua, adaptándose a los cambios internos y externos que afecten a la organización. En SYTSA, la mejora se aborda desde dos dimensiones complementarias: la adaptación (5.5.7.1) y la mejora continua (5.5.7.2).

5.5.7.1 Adaptación

La adaptación implica que SYTSA debe realizar el seguimiento continuo de su entorno y modificar el marco de gestión de riesgos cuando se produzcan cambios significativos que puedan afectar la eficacia del sistema. A continuación, se muestran los factores que pueden desencadenar una adaptación y los procedimientos de adaptación.

Tabla 24

Factores que pueden desencadenar una adaptación

Categoría	Ejemplos aplicables a SYTSA
Cambios normativos	Modificaciones en LOPDP, nuevas regulaciones aduaneras, actualizaciones de estándares BASC, reformas al Código de Trabajo
Transformaciones tecnológicas	Migración de hosting compartido a VPS, implementación de nuevo ERP, adopción de herramientas de ciberseguridad avanzadas (SOC)
Variaciones en el mercado	Ingreso de nuevos competidores logísticos, cambios en la demanda de transporte de carga, fluctuaciones económicas
Eventos internos	Reestructuración organizacional, rotación de personal clave, ampliación de operaciones a nuevas provincias, adquisición de nueva flota
Lecciones aprendidas de incidentes	Materialización de un ciberataque, robo de carga, accidente vial grave, fuga de información de clientes
Cambios en el contexto externo	Condiciones climáticas extremas, crisis de seguridad en zonas de operación, pandemia, variación de precios de combustible

Tabla 25

Procedimiento de adaptación

Fase	Descripción	Responsable	Plazo
1. Detección del cambio	Cualquier colaborador o área reporta un cambio relevante mediante el formulario "Solicitud de revisión del marco"	Todos los colaboradores	Inmediato
2. Análisis del impacto	El Comité de Gestión de Riesgos evalúa si el cambio afecta la idoneidad, adecuación o eficacia del sistema	Comité de Gestión de Riesgos	15 días
3. Modificación documentada	Si es necesario adaptar el marco, se actualizan políticas, procedimientos, matrices de riesgos o planes de tratamiento	Comité / Jefes departamentales	30 días

4. Comunicación y capacitación	Los cambios se comunican a toda la organización y, si procede, se imparte capacitación adicional	Talento Humano / Comité	15 días posteriores a la modificación
5. Seguimiento	Se monitorea la efectividad de la adaptación durante al menos tres meses, utilizando los indicadores definidos	Comité de Gestión de Riesgos	3 meses

5.5.7.2 Mejora continua

La mejora continua es un principio transversal que busca que SYTSA fortalezca progresivamente su sistema de gestión de riesgos mediante el aprendizaje, la experiencia y la implementación de acciones correctivas y preventivas. La organización adoptará el **ciclo PHVA (Planificar-Hacer-Verificar-Actuar)** como base para la mejora continua, integrando los resultados de la valoración (5.5.6) y de la adaptación (5.5.7.1).

Tabla 26

Acciones específicas para la mejora continua en SYYSA (ciclo PHVA)

Fase PHVA	Actividades en SYTSA	Responsable	Plazo
Planificar	Identificar oportunidades de mejora a partir de indicadores, auditorías, incidentes y lecciones aprendidas. Definir metas de mejora anuales	Comité de Gestión de Riesgos	Anual (diciembre)
Hacer	Ejecutar los planes de mejora priorizados (ver ejemplos en tabla siguiente)	Jefes departamentales / TI	Según cronograma
Verificar	Medir los resultados de las acciones de mejora mediante los KPIs definidos en 5.5.6.1 y auditorías internas	Calidad y Seguridad / Auditoría interna	Trimestral
Actuar	Estandarizar las mejoras que hayan demostrado ser eficaces (actualizar procedimientos, políticas, matrices). Si una mejora no funcionó, analizar causas y proponer una nueva acción	Comité de Gestión de Riesgos	Semestral

Tabla 27

Ejemplos concretos de mejora continua para SYTSA (basados en el diagnóstico previo, el Plan Director de Seguridad y los riesgos identificados):

Plazo	Acción de mejora	Norma/Enfoque	Riesgo que aborda	Responsable	Indicador de cumplimiento
0-6 meses Corto Plazo	Implementar inventario formal de activos TIC	ISO 27001	Pérdida de activos, robo de información	Jefatura TI	100% activos registrados
0-6 meses Corto Plazo	Campaña integral de ciberseguridad (phishing, ransomware, contraseñas seguras)	ISO 27001	Robo de credenciales y malware	TH / TI	95% personal capacitado
0-6 meses Corto Plazo	Implementar Comité de Seguridad de la Información	ISO 27001	Falta de gobernanza	Gerencia / TI	Comité formalizado

0-6 meses Corto Plazo	Actualizar matriz legal y requisitos regulatorios	ISO 9001	Incumplimiento legal	Jurídico	100% requisitos actualizados
0-6 meses Corto Plazo	Fortalecer inspecciones preoperacionales digitales	ISO 39001	Accidentes y fallas mecánicas	Operaciones	100% inspecciones ejecutadas
6-12 meses Mediano Plazo	Implementar gestión formal de vulnerabilidades	ISO 27001	Ciberataques	TI	Vulnerabilidades críticas corregidas
6-12 meses Mediano Plazo	Desarrollar Plan de Continuidad del Negocio	ISO 22301	Interrupción operativa	SIG	Plan aprobado
6-12 meses Mediano Plazo	Ejecutar simulacros de robo de carga y contingencias BASC	BASC	Contaminación y robo de carga	Seguridad BASC	2 simulacros/año
6-12 meses Mediano Plazo	Programa de control de fatiga y conducción segura	ISO 39001	Accidentes de tránsito	Operaciones / HSE	Reducción de incidentes

6-12 meses Mediano Plazo	Homologación y reevaluación de asociados de negocio críticos	BASC	Proveedores de alto riesgo	Compras	100% evaluados
12-24 meses Largo Plazo	Implementar tablero de indicadores KRI y KPI de riesgos	ISO 31000	Falta de monitoreo	SIG	Indicadores implementados
12-24 meses Largo Plazo	Migrar servicios críticos a infraestructura más robusta	ISO 27001	Caída de sistemas	TI	Disponibilidad >99%
12-24 meses Largo Plazo	Fortalecer monitoreo satelital con geocercas avanzadas	BASC / ISO 39001	Robo de carga y desvíos	Monitoreo	100% rutas críticas controladas
12-24 meses Largo Plazo	Programa de auditorías integradas basadas en riesgos	ISO 31000	No conformidades recurrentes	SIG	100% programa ejecutado
12-24 meses Largo Plazo	Implementar cultura de mejora continua basada en riesgos	ISO 9001 e ISO 31000	Desempeño organizacional	Gerencia	Cumplimiento >90% acciones

5.5.7.3 Revisión anual del marco de referencia

Además de las acciones de adaptación y mejora continua, SYTSA realizará una revisión anual completa del marco de referencia, en la que participará la alta dirección y el Comité de Gestión de Riesgos. Esta revisión evaluará:

Tabla 28

Revisión anual del marco de referencia

Aspecto por revisar	Pregunta guía
Vigencia y pertinencia de la política de gestión de riesgos	¿Sigue reflejando los objetivos y la cultura actual de SYTSA?
Suficiencia de los recursos asignados	¿Los recursos humanos, tecnológicos y financieros son adecuados?
Eficacia del proceso de comunicación y consulta	¿Los canales establecidos funcionan? ¿Las partes interesadas participan?
Integración de la gestión de riesgos	¿El SGR está realmente incorporado en todos los procesos clave?
Cumplimiento de objetivos estratégicos	¿La gestión de riesgos ha contribuido a reducir incidentes y mejorar la toma de decisiones?
Resultados de la valoración	¿Se han alcanzado las metas de los indicadores?

Documento de salida de la revisión anual:

El resultado de esta revisión anual se documentará en un Acta de Revisión por la Dirección, que contendrá:

- Fecha, lugar y asistentes.
- Análisis de cada aspecto evaluado.
- Conclusiones y fortalezas identificadas.
- Debilidades u oportunidades de mejora.
- Decisiones adoptadas (modificar la política, asignar recursos adicionales, cambiar responsables).
- Plan de acción para el año siguiente con responsables y plazos.
- Fecha de la próxima revisión anual.

5.6 Proceso

La gestión del riesgo al ser un proceso estructurado y sistemático impacta de manera positiva en la toma de decisiones, la anticipación disciplinada ante actividades, sucesos, conflictos, etc., permitirá identificar amenazas y oportunidades a través de la identificación, el análisis, evaluación, la acción y la verificación una vez que se ha identificado un riesgo.

5.6.1 Generalidades

En SYTSA la implementación de la gestión de riesgos, basada en la norma ISO 31000, impulsará la toma de decisiones proactiva debido a su estructura cimentada en sus principios. Empezando con que la gestión del riesgo debe ser integrada a todas las actividades, con el fin de garantizar resultados consistentes el siguiente principio propone que debe ser estructurada y exhaustiva, al tratarse de un proceso que garantiza estabilidad y seguridad otro de sus principios es que debe ser adaptada tanto al entorno interno como externo, en relación a esto destaca el principio que menciona que debe ser inclusiva involucrando a todas las partes interesadas y su forma de respuesta debe ser dinámica ante cambios del entorno. Todo esto debe estar estratégicamente alineado con los tres últimos principios que son mejor información disponible, los factores humanos y culturales y la mejora continua.

Estos principios serán la guía en SYTSA para gestionar los efectos de incertidumbre sobre sus objetivos y soporte en la prevención de accidentes, reducción de pérdidas, fortalecimiento de controles BASC así como el cumplimiento legal.

5.6.2 Comunicación y consulta

La norma ISO 31000:2018 tiene como objetivo el asegurar que todas las partes interesadas que conforman una organización logren comprender los riesgos y las acciones que se deben tomar para poder controlarlos. La base para esta toma de decisiones se establece a la comunicación, que

busca promover la toma de conciencia y la comprensión de los riesgos; y de la consulta, que implica el intercambio de información fundamentada y retroalimentación bidireccional.

SYTSA establecerá mecanismos de comunicación y consulta con personal operativo, supervisores, clientes, proveedores y autoridades. La información relacionada con riesgos será compartida mediante reportes operativos, reuniones, auditorías internas, capacitaciones y plataformas tecnológicas.

La empresa deberá fomentar un canal de comunicación que asegure la confiabilidad del estado del negocio mediante la realización de informes trimestrales donde se pueda dejar un registro de la evolución de los riesgos y comprobar si las acciones correctivas que se implementaron contribuyeron a mitigar los riesgos existentes. Así también es importante contar con reuniones mensuales junto con el comité de dirección en la que se encuentren involucradas todas las áreas de la organización para mantener una comunicación alineada y transparente, donde se pueda hablar de los problemas a resolver que afecte la continuidad de las funciones de los trabajadores.

Toda información de interés común debe ser enviada únicamente por los canales oficiales de la empresa, como es el correo electrónico empresarial y las implantadas por SYTSA. S.A, debido a que permite centralizar la comunicación oficial, resguardar la información confidencial y combatir el efecto de los rumores y las filtraciones de información.

Tabla 29

Responsabilidades individuales y difusión de información

Etapa	Responsable	Proceso	Frecuencia	Tipo de comunicación
Identificación del riesgo	Colaboradores (Todos los niveles jerárquicos de la organización)	Realizar un reporte de los riesgos y vulnerabilidades encontrados y clasificarlos por nivel de criticidad con el fin de controlar, monitorear y reportar los hallazgos a la junta directiva para la toma de decisiones e implementar acciones correctivas.	Periódico (cada que se presente un riesgo)	Lista de verificación, informes mensuales, reuniones mensuales
Análisis del riesgo	Jefaturas de cada departamento - Alta dirección - Gerencia	Identificar los riesgos que representan un mayor peligro para la operabilidad de la empresa y realizar la toma de decisiones e implementar controles que permitan frenar la amenaza.	Trimestral	Informes trimestrales, reuniones trimestrales

Valoración del riesgo	Nivel intermedio (jefaturas, responsable de SSO, responsable de TI, Talento Humano)	Evaluar el nivel del riesgo encontrado para otorgar medidas preventivas o correctivas según el nivel de criticidad de tal manera que se pueda concluir si el riesgo puede ser tolerable o si representa una amenaza	Trimestral	Canales de comunicación empresarial, informes, reuniones, reportes trimestrales.
Control y monitoreo del Riesgo	Coordinador de Rutas / jefe de Seguridad	Tomar acciones que permitan reducir la probabilidad de ocurrencia de un riesgo con el fin de minimizar el impacto mediante políticas de seguridad y manuales de procedimientos que garanticen las operaciones diarias en cada puesto de trabajo.	Periódico	Lista de verificación, reportes semanales, evaluaciones de desempeño, correo empresarial

Valoración del riesgo	Nivel intermedio (jefaturas, responsable de SSO, responsable de TI, Talento Humano)	Evaluar el nivel del riesgo encontrado para otorgar medidas preventivas o correctivas según el nivel de criticidad de tal manera que se pueda concluir si el riesgo puede ser tolerable o si representa una amenaza	Trimestral	Canales de comunicación empresarial, informes, reuniones, reportes trimestrales.
Control y monitoreo del Riesgo	Coordinador de Rutas / jefe de Seguridad	Tomar acciones que permitan reducir la probabilidad de ocurrencia de un riesgo con el fin de minimizar el impacto mediante políticas de seguridad y manuales de procedimientos que garanticen las operaciones diarias en cada puesto de trabajo.	Periódico	Lista de verificación, reportes semanales, evaluaciones de desempeño, correo empresarial

El objetivo principal de SYTSA S.A es que al infundir un sistema de comunicación bidireccional permita integrar a todas las áreas de la organización para obtener una visión holística de los criterios de los riesgos asegurando una información basada en hechos donde los datos sean veraces, comprensibles y transparentes lo que permita la aceptación y la toma de decisiones.

5.6.3 Alcance, Contexto y Criterios

Antes de lanzarse a identificar riesgos, hay que poner límites. No se puede gestionar todo al mismo tiempo, sobre todo en una operación logística que abarca múltiples rutas, horarios y tipos de carga. Esta etapa nos ayuda a enfocar los esfuerzos donde realmente importa.

5.6.3.1 Generalidades

El establecimiento del alcance, el análisis del contexto y la definición de criterios son la brújula del proceso. Nos dicen hasta dónde llegamos, qué estamos considerando como parte del entorno y con qué reglas vamos a medir la importancia de un riesgo. Sin esto, cualquier evaluación sería arbitraria y probablemente inútil para la toma de decisiones.

En SYTSA, esta etapa se realiza al inicio del diseño del sistema y se revisa cada vez que hay cambios significativos en la operación (por ejemplo, una nueva ruta internacional o la incorporación de un tipo de carga peligrosa que no se manejaba antes).

5.6.3.2 Definición del Alcance

Para el Sistema de Gestión de Riesgos (SGR) de SYTSA, el alcance inicial se ha delimitado a los siguientes procesos logísticos, considerados críticos para la seguridad de la carga y la continuidad del servicio:

Tabla 30

Procesos de seguridad de la carga

Proceso incluido	Justificación
Transporte terrestre de carga (rutas nacionales)	Es el eje del negocio. Concentra la mayor exposición a accidentes viales, robos y fatiga de conductores.
Rutas de alta peligrosidad (zonas con antecedentes de robo de carga o condiciones geográficas adversas)	El nivel de riesgo es significativamente más alto y requiere controles especiales como escoltas, geocercas y comunicación satelital.
Monitoreo satelital y trazabilidad (sistema CloudFleet)	Es el principal control preventivo para detectar desvíos, velocidades anormales o inmovilizaciones no programadas. Su falla implica una pérdida de visibilidad sobre la carga.

Mantenimiento preventivo de la flota	Las fallas mecánicas en ruta no solo generan retrasos, sino que pueden provocar accidentes graves. Un vehículo en mal estado es un riesgo latente.
Seguridad física en patios y bodegas	El ingreso no autorizado a las instalaciones donde se almacena carga (especialmente productos de alto valor o peligrosos) es una amenaza concreta.
Gestión documental de la cadena de custodia	Los errores en guías de remisión, manifiestos de carga o documentación aduanera pueden derivar en retenciones, multas o pérdida de mercancía.

Límites del alcance:

El SGR cubre las operaciones bajo control directo de SYTSA, es decir, vehículos de propiedad de la empresa, personal con relación laboral directa y bodegas operadas por SYTSA. Los tramos donde la carga es transferida a transportistas asociados (subcontratados) o donde se utilizan patios de terceros se abordan como riesgos de cadena de suministro, evaluándose a través de los acuerdos de servicio y las auditorías a proveedores.

Recursos:

Para la implementación de este proceso, SYTSA cuenta con el historial de incidentes de los últimos dos años, el personal experimentado de operaciones y seguridad, y los sistemas tecnológicos ya implementados (CloudFleet, ERP Odoo, Silogran). Como recurso adicional pendiente, se ha identificado la necesidad de adquirir una herramienta digital para la gestión centralizada de la matriz de riesgos y el seguimiento de acciones correctivas, que actualmente se lleva en hojas de cálculo.

5.6.3.3 Contextos Externo e Interno

El transporte de carga no ocurre en un laboratorio. SYTSA opera en el mundo real, con calles, carreteras, condiciones climáticas cambiantes y una situación de seguridad ciudadana que varía día a día. Entender el contexto es fundamental para anticipar, no solo reaccionar.

Tabla 31

Contexto externo

Factor	Descripción y efecto en SYTSA	Sustento metodológico
Político - Legal	La Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial (LOTTTSV) se actualiza periódicamente. El incumplimiento de las horas de conducción o la falta de documentación en regla puede generar multas elevadas. Además, el estándar BASC V6 exige controles más rigurosos contra el contrabando y el narcotráfico, lo que implica inversiones en procedimientos y tecnología.	Informes de auditorías internas semestrales enfocadas en la revisión de documentación. Check list de la matriz de requisitos legales
Económico	La fluctuación del precio del combustible impacta directamente los costos operativos y puede incentivar prácticas inseguras (como forzar jornadas para compensar gastos). La alta competencia en el sector logístico presiona las tarifas	Matriz de costos operativos. Reportes mensuales.

	a la baja, y existe el riesgo de que algunos clientes prioricen precio sobre seguridad.	Matriz de criticidad de rutas
Social - Delincuencia	Existen corredores viales específicos (hacia la costa, a la frontera norte y en ciertos tramos de la sierra centro) con alta incidencia de robos de carga, secuestros de conductores y extorsión. Esta situación ha empeorado en los últimos años y requiere medidas activas como escoltas armadas en rutas críticas.	Mapa de identificación de zonas rojas. Bitácoras de siniestros Reportes de la Policía Nacional.
Tecnológico	Los sistemas de monitoreo GPS con corte de combustible remoto ofrecen una oportunidad valiosa para proteger la carga. Sin embargo, la dependencia de la	Mapa de cobertura de las operadoras

	conectividad celular es una vulnerabilidad en zonas rurales o de montaña. También existe el riesgo creciente de ciberataques que podrían inutilizar la plataforma de trazabilidad.	Informes de auditorías semestrales de seguridad de datos
		Fichas técnicas de los proveedores de sistema de monitoreo GPS
Ambiental	Las condiciones climáticas extremas (El Niño, deslaves, crecidas de ríos) pueden cerrar vías durante horas o días, obligando a desvíos improvisados por rutas no controladas y aumentando la exposición a robos.	Reportes de estado de las vías mediante medios oficiales

Tabla 32

Contexto Interno

Factor	Descripción y estado en SYTSA	Interacción entre áreas internas
Cultura organizacional	Si bien la gerencia ha mostrado compromiso con la seguridad, todavía existe una brecha entre el discurso y la práctica en el personal operativo. Algunos conductores ven los controles como una traba, no como una protección. La alta rotación de personal en conducción dificulta mantener una formación homogénea en cultura de riesgo.	El departamento de Seguridad, respaldado por la gerencia, en conjunto con el área de talento humano impulsaran la cultura preventiva desde un enfoque proactivo no reactivo ante la materialización de un riesgo.

Infraestructura y flota	La flota está en buen estado general gracias a un plan de mantenimiento preventivo. Sin embargo, no todos los vehículos cuentan con sistemas de comunicación de respaldo (radio de alta frecuencia) para zonas sin cobertura celular, y algunos equipos de monitoreo GPS son de generaciones anteriores con menor precisión.	El departamento de Seguridad junto con el área de Mantenimiento verificará la infraestructura, así como el estado de los vehículos para colocarlo en la planificación mensual y efectuar las actividades conforme el nivel de importancia que presenten.
Procesos internos	Los procedimientos de control de acceso a patios y de inspección de carga previa al sellado son en gran parte manuales (listas de chequeo en papel), lo que los hace vulnerables a errores humanos y a la manipulación no detectada.	El departamento de seguridad junto con el área de sistemas trabajara en conjunto para lograr la digitalización de documentos en un 100% como medida de prevención y seguridad de datos.

Talento humano	Existe una buena base de conductores con experiencia en rutas nacionales, pero la formación en estándares BASC y en protocolos contra el robo de carga es aún incipiente. Se requiere un programa de capacitación más estructurado y con evaluaciones prácticas.	El departamento de Talento humano junto con el área de seguridad levantará el plan de capacitación en base al análisis de necesidades corporativas, competencias y conocimientos.

5.6.3.4 Definición de los Criterios de Riesgo

Para que la evaluación de riesgos no sea un ejercicio subjetivo, SYTSA ha definido criterios claros, basados en la experiencia operativa y en los umbrales que la gerencia considera aceptables o inaceptables. Estos criterios se aplican a todos los procesos incluidos en el alcance.

Tabla 33

Escala de probabilidad de ocurrencia

Nivel	Descripción	Valor	Referencia operativa
Muy baja	Casi nunca ocurre. No se tiene registro en los últimos 5 año	1	Una vez cada 5 años aproximadamente
Baja	Ocurre ocasionalmente. Se tiene algún registro aislado en el historial.	2	Una vez cada 2 años aproximadamente.
Media	Ocurre con cierta regularidad. Ya se ha presentado varias veces en la operación.	3	Una vez al año (una falla de sistema GPS recurrente).

Alta	Es frecuente. Ocurre varias veces al año en diferentes unidades o rutas.	4	Varias veces al año (ejemplo: incidentes menores de tránsito).
Crítico	Es casi permanente. Ocurre con gran regularidad en la operación diaria.	5	Mensualmente o incluso semanalmente (ejemplo: quejas por tiempos de espera en aduanas).

Tabla 34

Escala de impacto

Nivel	Descripción	Consecuencias concretas	Valor
Insignificante	Afectación muy leve, se resuelve con acciones internas sencillas.	Sin pérdida económica significativa. Retraso menor a 1 hora en la entrega. No afecta la imagen del cliente.	1
Menor	Interrupción parcial de una operación, pero se puede recuperar.	Pérdidas operativas de hasta $500. Retraso de hasta medio turno. Queja informal de un cliente.	2

Moderado	Afectación considerable a una ruta o a un cliente específico.	Daños materiales de entre 1.000y1.000*y*5.000. Pérdida de la carga en un tramo. Multa leve de tránsito.	3
Mayor	Paralización de una unidad de negocio o pérdida de un cliente importante.	Lesiones graves de un conductor o ayudante. Pérdida de un contrato importante. Multa regulatoria de hasta $10.000.	4
Crítico	Impacto severo en la continuidad del negocio o la reputación de SYTSA.	Fatalidad de un colaborador. Pérdida de la certificación BASC. Sanción grave de una autoridad. Quiebre de stock de un cliente clave.	5

Matriz de riesgos:

Con los valores de probabilidad (1 a 5) e impacto (1 a 5), el nivel de riesgo se calcula multiplicando ambos factores, obteniendo un puntaje de 1 a 25.

Tabla 35

Mapa de calor del riesgo

Impacto → **Probabilidad ↓**	**1 (Insignificante)**	**2 (Moderado)**	**3 (Importante)**	**4 (Mayor)**	**5 (Crítico)**
5 Muy alta	**5**	**10**	**15**	**20**	**25**
4 Alta	4	8	12	16	**20**
3 Media	3	6	9	12	15
2 Baja	2	4	6	8	10
1 Muy baja	1	2	3	4	5

Tabla 36

Clasificación de los niveles del riesgo

Rango	Nivel	Significado	Acción requerida
1 al 5	Muy Bajo	Riesgo sin afectación, Riesgo aceptable	Asumir el riesgo debido a qu no afecta directamente a la continuidad del negocio
6 al 10	Bajo	Riesgo moderado. Requiere atención.	Definir e implementar acciones específicas de mitigación en un plazo de 3 a 6 meses.
10 al 15	Medio	Riesgo moderado. Requiere atención.	Definir e implementar acciones específicas de mitigación en un plazo de 3 a 6 meses.
16 al 20	Alto	Riesgo importante. Requiere intervención de jefatura.	Elaborar un plan de tratamiento detallado, con responsables y presupuesto asignado. Seguimiento mensual.
21 al 25	Crítico	Riesgo inaceptable. Amenaza directa a la continuidad.	Tratamiento inmediato por parte de la Gerencia. Suspensión temporal de la actividad si no se puede controlar.

Clasificación de los niveles de riesgo:

Estos criterios se aplican de manera consistente en todas las áreas de SYTSA, lo que permite comparar riesgos operativos (como un accidente de tránsito) con riesgos administrativos (como una sanción regulatoria) bajo una misma lógica.

5.6.4 Evaluación del riesgo

5.6.4.1 Generalidades

SYTSA requiere evaluar de manera sistemática los riesgos que puedan afectar la continuidad del negocio, la seguridad de la cadena logística, el cumplimiento legal, la seguridad de la información y el logro de los objetivos estratégicos. La evaluación del riesgo constituye la base para la toma de decisiones y la asignación eficiente de recursos.

5.6.4.2 Identificación del riesgo

Realizar un reporte de los riesgos y vulnerabilidades encontrados y clasificarlos por nivel de criticidad con el fin de controlar, monitorear y reportar los hallazgos a la junta directiva para la toma de decisiones e implementar acciones correctivas.

5.6.4.3 Análisis del riesgo

El análisis considera fuentes de riesgo, eventos, causas, consecuencias, controles existentes, probabilidad de ocurrencia e impacto potencial. La metodología utiliza una escala de 1 a 5 para probabilidad e impacto.

Tabla 37

Escala de probabilidad

Nivel	Descripción	Valor
Muy Baja	Evento excepcional	1
Baja	Poco frecuente	2
Media	Ocasional	3
Alta	Frecuente	4
Muy Alta	Recurrente	5

Tabla 38

Escala de Impacto

Nivel	Descripción	Consecuencia	Valor
Insignificante	Sin afectación	Impacto mínimo	1
Menor	Leve	Retrasos	2
Moderado	Importante	Pérdidas operativas	3
Mayor	Significativo	Daño legal o reputacional	4
Crítico	Severo	Fatalidades o paralización	5

5.6.4.4 Valoración del Riesgo

La valoración permite priorizar los riesgos para definir acciones de tratamiento. Se utiliza una matriz 5x5 de probabilidad e impacto.

Tabla 39

Matriz de probabilidad x impacto

I→ P ↓	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
Ca2	2	4	6	8	10
1	1	2	3	4	5

Nota. - Clasificación: Bajo (1-5), Moderado (6-10), Alto (11-15) y Crítico (16-25).

Tabla 40

Matriz Integral de Riesgos de SYTSA

Proceso	Riesgo	Categoría	Causa	P	I	Valor	Nivel	Control	Tratamiento
Administrativo y legal	Vencimiento documental	Legal	Falta de seguimiento y cumplimiento interno	3	4	12	Alto	Seguimiento y control	Auditoria mensual.
Operaciones	Accidente de tránsito	Vial	Exceso velocidad	5	5	25	Crítico	GPS	Programa vial
Operaciones	Fatiga de conductores	SST	Jornadas extensas	4	5	20	Crítico	Control rutas	Pausas y monitoreo
Operaciones	Volcamiento	Operacional	Condiciones vía	4	5	20	Crítico	Capacitación	Control conducción
Operaciones	Bloqueo de vías	Operacional	Conflictos/social	3	4	12	Alto	Monitoreo	Rutas alternas

Seguridad BASC	Robo de carga	BASC	Delincuencia	4	5	20	Crítico	GPS	Geocercas
Seguridad BASC	Contaminación de carga	BASC	Manipulación ilícita	4	5	20	Crítico	Inspecciones	Controles BASC
Seguridad BASC	Secuestro de unidad	BASC	Crimen organizado	3	5	15	Alto	Monitoreo	Protocolos
Mantenimiento	Falla de frenos	Operacional	Desgaste	4	5	20	Crítico	Checklist	MP preventivo
Mantenimiento	Neumáticos defectuosos	Operacional	Falta inspección	4	4	16	Crítico	Inspección	Reposición
TI	Phishing	Ciberseguridad	Correos maliciosos	4	4	16	Crítico	Filtros	Capacitación
TI	Ransomware	Ciberseguridad	Malware	4	5	20	Crítico	Backups	EDR

TI	Filtración de datos	Información	Acceso indebido	4	5	20	Crítico	Permisos	DLP
TI	Shadow IT	Tecnológico	Apps no autorizadas	3	4	12	Alto	Políticas	Control software
TI	Pérdida de dispositivos	Información	Robo/extravío	3	4	12	Alto	Inventario	Cifrado
TI	Ataque cadena suministro	Tecnológico	Proveedor comprometido	3	5	15	Alto	Evaluación	Homologación
Videovigilancia	Hacking cámaras	Tecnológico	Credenciales débiles	3	5	15	Alto	Contraseñas	Segmentación
Videovigilancia	Vulnerabilidades IoT	Tecnológico	Equipos sin actualizar	4	4	16	Crítico	Actualización	Gestión vulnerabilidades
Compras	Proveedor crítico no homologado	Estratégico	Falta evaluación	3	4	12	Alto	BASC	Homologación

Jurídico	Incumplimiento legal	Legal	Desactualización	3	5	15	Alto	Matriz legal	Auditorías
Financiero	Fraude interno	Financiero	Controles débiles	3	5	15	Alto	Segregación	Monitoreo
Talento Humano	Rotación de conductores	TH	Mercado laboral	3	3	9	Moderado	Capacitación	Retención
SIG	No conformidades recurrentes	Estratégico	Falta seguimiento	3	4	12	Alto	Auditorías	Acciones correctivas
Continuidad	Ausencia de BCP	Continuidad	Falta planificación	4	5	20	Crítico	Parcial	Plan continuidad
Continuidad	Sin pruebas de continuidad	Continuidad	Falta simulacros	4	4	16	Crítico	N/A	Pruebas

Comercial	Pérdida cliente estratégico	Reputacional	Incumplimientos	3	4	12	Alto	Seguimiento	Plan comercial
TI	Sin inventario TIC	Gobernanza	Falta control activos	4	4	16	Crítico	Parcial	Inventario
TI	Sin comité de seguridad	Gobernanza	Falta estructura	3	4	12	Alto	Parcial	Comité seguridad
TI	Sin gestión vulnerabilidades	Gobernanza	Proceso inexistente	4	5	20	Crítico	N/A	Programa formal
Información	Suplantación identidad	Fraude	Datos expuestos	3	5	15	Alto	Accesos	MFA
Información	Malware documentos	Ciberseguridad	Archivos infectados	4	4	16	Crítico	Antivirus	Sandbox

El análisis evidencia que los riesgos críticos se concentran en operaciones, seguridad BASC, continuidad del negocio, control documental y seguridad de la información, requiriendo prioridad en la asignación de recursos y controles.

5.6.5 Tratamiento del riesgo

5.6.5.1 Generalidades

El tratamiento del riesgo constituye la fase del proceso en la cual SYTSA selecciona e implementa medidas orientadas a modificar los riesgos identificados y valorados previamente. El objetivo fundamental es reducir la probabilidad de ocurrencia, mitigar el impacto potencial o, en los casos más críticos, eliminar la fuente del riesgo cuando sea posible.

En el contexto de SYTSA, una empresa de transporte de carga pesada y logística, el tratamiento del riesgo no es un ejercicio teórico. Implica decisiones concretas que afectan la operación diaria: desde la reasignación de rutas ante un incremento de robos de carga, hasta la inversión en nuevos sistemas de monitoreo satelital o la contratación de escoltas armadas en corredores viales de alta peligrosidad.

El tratamiento del riesgo se aplica de manera diferencial según el nivel de criticidad obtenido en la valoración (Bajo, Moderado, Alto o Crítico). Para los riesgos calificados como Bajos o Moderados, se implementan controles rutinarios dentro de los procesos

existentes. Para los riesgos calificados como Altos o Críticos, se requiere la elaboración de planes de tratamiento específicos, con asignación de recursos, responsables definidos y plazos de ejecución claros.

Es importante señalar que el tratamiento del riesgo no siempre elimina completamente la amenaza. En muchos casos, lo que se logra es reducir el nivel de riesgo a un rango aceptable según los criterios definidos por la organización. Además, cualquier tratamiento implementado puede introducir nuevos riesgos (riesgos secundarios), los cuales deben ser identificados y gestionados en un nuevo ciclo del proceso.

5.6.5.2 Selección de las opciones para el tratamiento del riesgo

Para cada riesgo identificado en la matriz integral de SYTSA (Tabla 3 del apartado 5.6.4), la organización evaluará las opciones disponibles para su tratamiento. La selección de la opción más adecuada dependerá del nivel de riesgo, los recursos disponibles, la factibilidad operativa y el análisis costo-beneficio.

Las opciones de tratamiento consideradas por SYTSA son las siguientes:

Tabla 41

Opciones de tratamiento de la empresa SYTSA.

Opción	Descripción	Aplicación en SYTSA
Evitar el riesgo	Decidir no iniciar o no continuar con la actividad que genera el riesgo.	Suspender operaciones en una ruta específica cuando las condiciones de seguridad (robos, secuestros, conflictos sociales) superan los umbrales aceptables, hasta que la situación se normalice.
Reducir el riesgo (mitigar)	Implementar controles para disminuir la probabilidad de ocurrencia o el impacto potencial.	Es la opción más utilizada en SYTSA. Incluye: instalación de GPS con corte de combustible, implementación de geocercas, contratación de escoltas armados en rutas críticas, mantenimiento preventivo de flota, capacitación a conductores en conducción a la defensiva y estándares BASC.

Compartir el riesgo (transferir)	Trasladar parte o toda la responsabilidad del riesgo a un tercero.	Contratación de seguros de carga y de responsabilidad civil. Externalización de rutas o tramos de alto riesgo a transportistas especializados (siempre que estén homologados bajo estándares BASC).
Aceptar el riesgo (retener)	Decisión informada de no tomar ninguna acción adicional, asumiendo el nivel de riesgo existente.	Se aplica cuando el riesgo está valorado como Bajo (1-5) o Moderado (6-10), o cuando el costo del tratamiento es desproporcionado en relación con el impacto potencial. Ejemplo: pequeñas demoras por tráfico no crítico.
Aumentar el riesgo (para oportunidades)	Incrementar el nivel de exposición para aprovechar una oportunidad de negocio.	Aunque menos frecuente en el sector logístico por su naturaleza de control de pérdidas, podría aplicarse al abrir una nueva ruta internacional con mayor rentabilidad, pero también mayor exposición, aceptando un nivel de riesgo controlado y monitoreado permanentemente.

La selección de la opción se realizará mediante un análisis que considere los beneficios esperados, los costos de implementación, las obligaciones legales (LOTTTSV, LOPDP, estándares BASC) y las expectativas de las partes interesadas (clientes, aseguradoras, entes de control).

Tabla 42

Criterios para la selección de opciones según nivel de riesgo

Nivel de riesgo (valor)	Opción prioritaria	Acción esperada
Bajo (1-5)	Aceptar	Monitoreo rutinario dentro de los procesos normales. No requiere acciones adicionales.
Moderado (6-10)	Reducir (con controles básicos)	Implementar controles complementarios de bajo costo. Definir acciones en un plazo de 3 a 6 meses.
Alto (11-15)	Reducir (con controles reforzados) o Compartir	Elaborar plan de tratamiento detallado, con presupuesto y responsables asignados. Seguimiento mensual.
Crítico (16-25)	Evitar o Reducir (con controles intensivos)	Tratamiento inmediato por parte de la Gerencia. Suspensión temporal de la actividad si no es posible controlar el riesgo.

5.6.5.3 Preparación e implementación de los planes de tratamiento del riesgo

Una vez seleccionada la opción de tratamiento para cada riesgo crítico o alto, SYTSA elaborará un *Plan de Tratamiento del Riesgo* que especifique la manera en que se implementarán las acciones acordadas.

Tabla 43

Contenido mínimo del Plan de Tratamiento del Riesgo

Componente	Descripción
Riesgo identificado	Nombre y código del riesgo según la matriz integral de riesgos.
Nivel de riesgo inherente	Valoración obtenida (P x I) antes del tratamiento.
Opción de tratamiento seleccionada	Evitar, reducir, compartir o aceptar.
Acciones propuestas	Descripción detallada de las medidas a implementar.
Beneficios esperados	Reducción de probabilidad e impacto esperada.
Responsables	Persona o cargo encargado de ejecutar el plan.
Recursos necesarios	Presupuesto, personal, equipos, tecnología, capacitación.
Fecha de inicio y fin	Plazo de ejecución de las acciones.
Indicadores de seguimiento	Métrica que permitirá verificar la eficacia del tratamiento.
Riesgos secundarios identificados	Nuevos riesgos que podrían surgir como consecuencia del tratamiento.
Periodicidad de revisión	Frecuencia con la que se evaluará el avance y la efectividad.

Tabla 44

Plan de Tratamiento para riesgos críticos priorizados (basado en la Tabla 3 del apartado 5.6.4)

Riesgo	Nivel (PxI)	Opción	Acciones propuestas	Responsable	Plazo	Recursos estimados
Accidente de tránsito (exceso velocidad / distracción)	25 (Crítico)	Reducir	Implementar programa de conducción segura con reentrenamiento obligatorio para conductores con infracciones. Fortalecer monitoreo GPS en tiempo real. Instalar sistemas de alerta de fatiga (cámaras en cabina).	Gerencia de Operaciones / HSE	3 meses	USD 15.000 - 25.000
Fatiga de conductores (jornadas extensas)	20 (Crítico)	Reducir	Control automatizado de horas de conducción (no exceder 5 horas continuas). Aplicar pausas activas obligatorias. Rotación	Operaciones / Talento Humano	2 meses	USD 5.000 - 10.000

			de conductores en rutas de larga distancia. Evaluaciones médicas periódicas.			
Robo de carga (delincuencia)	20 (Crítico)	Reducir / Compartir	Implementar geocercas en rutas críticas. Contratar escoltas armadas para cargas de alto valor en corredores de alta peligrosidad. Contratar seguro de carga con cobertura ampliada. Establecer rutas alternas seguras con monitoreo satelital.	Seguridad BASC / Monitoreo	2 meses	USD 20.000 - 40.000
Contaminación de carga (manipulación ilícita)	20 (Crítico)	Reducir	Aplicar inspecciones BASC aleatorias en origen y destino. Implementar sellos de seguridad inviolables (candados y precintos de alta seguridad). Capacitación a conductores en protocolos anticontaminación. Auditorías a proveedores logísticos.	Seguridad BASC	3 meses	USD 8.000 - 15.000

Ransomware / Ciberataque	20 (Crítico)	Reducir	Migrar de hosting compartido a servidor VPS o dedicado. Implementar respaldos diarios automatizados fuera de la red corporativa. Configurar firewall gestionado y segmentación de red. Contratar EDR (Endpoint Detection and Response). Capacitación al personal en identificación de phishing.	TI	4 meses	USD 12.000 - 20.000
Filtración de datos (acceso indebido)	20 (Crítico)	Reducir	Implementar DLP (Data Loss Prevention) en correo y terminales. Cifrado de bases de datos de clientes. Autenticación de dos factores (2FA) obligatoria para accesos remotos. Revisión trimestral de permisos y accesos.	TI	3 meses	USD 8.000 - 15.000
Ausencia de BCP (plan de continuidad)	20 (Crítico)	Evitar / Reducir	Elaborar Plan de Continuidad del Negocio (BCP) para procesos críticos (monitoreo satelital, centro de control de flota). Definir procedimientos manuales alternativos para caída de sistemas	Gerencia / TI / Operaciones	6 meses	USD 10.000 - 20.000

			(CloudFleet, Silogran). Realizar pruebas de restauración cada 6 meses.				
Fallas de frenos (desgaste)	20 (Crítico)	Reducir	Implementar checklist de pre-arranque obligatorio con registro digital. Establecer plan de mantenimiento preventivo mensual con reemplazo de pastillas y zapatas de freno por kilometraje. Auditorías semanales a talleres.	Mantenimiento	1 mes	USD 5.000 - 10.000
Sin gestión de vulnerabilidades	20 (Crítico)	Evitar	Implementar programa formal de gestión de vulnerabilidades (escaneos mensuales de puertos y servicios, actualización de parches de seguridad en 15 días). Contratar prueba de penetración anual (pentesting).	TI	3 meses	USD 7.000 - 12.000

Procedimiento de implementación de los planes:

1. **Aprobación del plan:** Los planes de tratamiento para riesgos Altos o Críticos serán presentados al Comité de Gestión de Riesgos para su revisión y aprobación. La Gerencia General autorizará la asignación de recursos necesarios.

2. **Asignación de responsables:** Cada plan tendrá un "dueño del riesgo" (responsable principal) que rendirá cuentas sobre la ejecución del plan y la eficacia de los controles.

3. **Ejecución:** El responsable ejecuta las acciones según el cronograma definido, utilizando los recursos asignados y documentando cada avance.

4. **Monitoreo:** El avance del plan será revisado en las reuniones mensuales del Comité de Gestión de Riesgos. Los indicadores definidos en el plan serán reportados mediante el dashboard de KRI (Indicadores Clave de Riesgo).

5. **Evaluación del riesgo residual:** Una vez implementadas las acciones de tratamiento, se recalculará el nivel del riesgo (probabilidad e impacto residuales). El objetivo es que el riesgo residual se ubique en niveles Bajo o Moderado (1-10). Si el riesgo residual se mantiene en nivel Alto o Crítico, se deberá definir un tratamiento adicional.

6. **Documentación:** Todos los planes ejecutados y los resultados obtenidos serán registrados en la matriz de riesgos actualizada, en los informes de seguimiento y en el repositorio documental del Sistema de Gestión de Riesgos.

Riesgos secundarios a considerar:

El tratamiento del riesgo puede generar nuevos riesgos que deben ser identificados y gestionados. Por ejemplo:

- La contratación de escoltas armados para proteger la carga introduce riesgos de accidentes por vehículos adicionales en la caravana, así como riesgos de responsabilidad civil por uso de armas.
- La migración de hosting compartido a VPS puede generar riesgos de configuración incorrecta de firewalls durante la transición, exponiendo temporalmente los sistemas.
- La implementación de geocercas puede generar riesgos de falsas alarmas que desensibilicen al centro de monitoreo.

Estos riesgos secundarios deberán ser incorporados en la matriz de riesgos y gestionados con el mismo nivel de rigurosidad que los riesgos primarios.

5.6.6 Seguimiento y revisión

La empresa realizará revisiones periódicas de la matriz de riesgos, evaluará el desempeño de los controles y analizará la ocurrencia de incidentes o desviaciones que puedan afectar el cumplimiento de los objetivos organizacionales.

Objetivos del Seguimiento y Revisión

Objetivo general. - Verificar la eficacia y pertinencia de las actividades de gestión del riesgo implementadas en SYTSA S.A.S.

Objetivos específicos:

- Evaluar la efectividad de los controles establecidos.
- Identificar riesgos emergentes y cambios en los riesgos existentes.
- Verificar el cumplimiento de los planes de tratamiento.
- Apoyar la toma de decisiones basada en información objetiva.
- Promover la mejora continua del sistema de gestión del riesgo.

Responsables:

- *Gerencia general.* – Aprobar resultados, asignar recursos y tomar decisiones estratégicas.
- *Responsable del sistema de gestión.* – Coordinar actividades de seguimiento y consolidar informes.
- *Líderes de proceso.* – Monitorear riesgos de sus áreas y reportar desviaciones.
- *Colaboradores.* – Informar incidentes, eventos y riesgos emergentes.

Indicadores de Seguimiento

- *Cumplimiento de planes de tratamiento*

Fórmula: (Planes ejecutados / Planes programados) x 100

Meta: ≥ 90 %

- *Riesgos controlados*

Fórmula: (Riesgos con controles eficaces / Total de riesgos identificados) x 100

Meta: ≥ 85 %

- *Actualización de la matriz de riesgos*

Fórmula: (Matrices actualizadas / Matrices programadas) x 100

Meta: 100 %

Metodología de Seguimiento

El seguimiento se desarrollará mediante revisión documental, análisis de indicadores, verificación de controles, reuniones de seguimiento, evaluación de incidentes y actualización periódica de la matriz de riesgos. Los resultados deberán registrarse y comunicarse a la dirección para la adopción de acciones de mejora.

Tabla 45

Frecuencia

Actividad	Frecuencia
Seguimiento de riesgos críticos	Mensual
Revisión de controles	Trimestral
Actualización de la matriz de riesgos	Semestral
Informe de gestión del riesgo	Semestral
Revisión por la dirección	Anual

Nota: La frecuencia podrá ajustarse cuando existan cambios significativos en el contexto organizacional o cuando se materialicen riesgos de alta criticidad

Registros Generados

Matriz de riesgos actualizada, informes de seguimiento, registros de incidentes, planes de acción, actas de reunión e indicadores de gestión del riesgo.

Mejora Continua

La información obtenida durante el seguimiento y revisión será utilizada para fortalecer controles, actualizar evaluaciones, optimizar procesos y mejorar la capacidad de respuesta de SYTSA S.A.S. frente a los riesgos identificados. La organización fomentará una cultura preventiva orientada a la mejora continua y al cumplimiento de los objetivos estratégicos.

5.6.7 Registro e informe

En SYTSA, el registro e informe permitirá evidenciar la gestión realizada sobre los riesgos asociados a los procesos realizados en las actividades operativas y actividades administrativas.

Los registros constituyen la evidencia documental del sistema de gestión de riesgos y permiten demostrar el cumplimiento de los objetivos organizacionales, así como la eficacia de los controles implementados. La información documentada será utilizada por la Alta Dirección para la toma de decisiones estratégicas, asignación de recursos y priorización de acciones de mejora.

Los registros deberán incluir como mínimo: identificación del riesgo, categoría, proceso afectado, causas, consecuencias, evaluación de probabilidad e impacto, nivel de riesgo inherente, controles existentes, responsables, planes de tratamiento, indicadores de seguimiento y estado de implementación.

Los informes de riesgos serán consolidados trimestralmente y presentados a la Gerencia General, permitiendo evaluar tendencias, riesgos emergentes, desviaciones, oportunidades de mejora y cumplimiento de objetivos.

5.6.7.1 Medios de comunicación

La comunicación efectiva constituye un elemento transversal dentro del proceso de gestión de riesgos. SYTSA implementará mecanismos de comunicación interna y externa que permitan garantizar que las partes interesadas reciban información oportuna, confiable y pertinente sobre los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos.

Objetivos de la comunicación:

- Fortalecer la cultura organizacional de gestión de riesgos.
- Promover la participación de todas las áreas.
- Facilitar la toma de decisiones basada en información objetiva.
- Garantizar la rendición de cuentas.
- Mantener informadas a las partes interesadas.

Comunicación interna:

- Correo
- electrónico corporativo.
- Reuniones de seguimiento.
- Comité de Gestión de Riesgos
- Intranet corporativa.
- Informes ejecutivos.
- Capacitaciones y talleres.

Comunicación externa:

- Clientes.
- Proveedores estratégicos.
- Entidades regulatorias.
- Organismos gubernamentales.
- Socios comerciales.

Toda comunicación relacionada con riesgos críticos deberá realizarse de manera inmediata mediante los canales oficiales definidos por la organización.

Tabla 46

Matriz de Comunicación de Riesgos

Información	Responsable	Destinatario	Frecuencia	Medio
Informe de riesgos	Coordinador de Riesgos	Gerencia	Trimestral	Reunión e informe
Indicadores KPI/KRI	Analista	Jefaturas	Mensual	Dashboard
Incidentes críticos	Responsable del proceso	Alta Dirección	Inmediata	Correo y llamada
Capacitaciones	Talento Humano	Personal	Semestral	Talleres

5.6.7.2 CRONOGRAMA DE ACTIVIDADES PARA LA IMPLEMENTACIÓN DE PROCESOS DE MEJORA ANTE LOS RIESGOS DETECTADOS

Con la finalidad de asegurar la mejora continua del Sistema de Gestión de Riesgos, SYTSA establecerá un cronograma anual de actividades orientado al seguimiento, control, revisión y fortalecimiento de los controles implementados.

El cronograma permitirá verificar el cumplimiento de los planes de tratamiento, evaluar la eficacia de los controles, detectar riesgos emergentes y mantener actualizado el Manual de Gestión de Riesgos.

Tabla 47

Cronograma de actividades

Actividad	Responsable	Frecuencia	Entregable	Indicador	Objetivo
Revisión de riesgos	Coord. Riesgos	Trimestral	Informe	% riesgos revisados	Actualizar matriz
Planes de tratamiento	Jefes de área	Semestral	Plan actualizado	% acciones ejecutadas	Reducir exposición
Comité de riesgos	Alta Dirección	Trimestral	Acta	Reuniones ejecutadas	Tomar decisiones
Seguimiento KPI/KRI	Analista	Mensual	Dashboard	Indicadores	Monitorear desempeño
Capacitación	Talento Humano	Semestral	Registro	% personal capacitado	Fortalecer cultura
Auditoría interna	Auditor	Anual	Informe auditoría	No conformidades detectadas	Verificar cumplimiento
Revisión del manual	Comité	Anual	Nueva versión	Actualización ejecutada	Mejora continua

5.6.8 Auditoría Interna

5.6.8.1 Objetivos

Verificar la eficacia del Sistema de Gestión de Riesgos, evaluar la efectividad de los controles, determinar oportunidades de mejora y asegurar la conformidad con los lineamientos establecidos por SYTSA y la ISO 31000:2018.

5.6.8.2 Proceso de la Auditoría Interna

- Planificación: definición del alcance, criterios, procesos, riesgos críticos y cronograma.
- Ejecución: revisión documental, entrevistas, inspecciones en campo y verificación de evidencias.
- Informe: emisión de hallazgos, observaciones, oportunidades de mejora y no conformidades.
- Seguimiento: validación de acciones correctivas y verificación de eficacia.

Tabla 48

Proceso de la auditoría interna

Proceso	Riesgo crítico	Frecuencia	Responsable	Prioridad
Operaciones	Accidentes, fatiga,	Trimestral	Auditor Interno	Alta
Seguridad BASC	Robo y contaminación	Trimestral	Auditor Interno	Alta
TI	Ciberseguridad	Semestral	Auditor Interno	Alta
Mantenimiento	Fallas críticas	Trimestral	Auditor Interno	Alta
Compras	Asociados críticos	Semestral	Auditor Interno	Media
SIG	No conformidades	Semestral	Auditor Interno	Media
TTHH	Cumplimiento de capacitación.	Mensual	Auditor Interno	Media
Jurídico, Administrativo	Documentación vencida	Mensual	Auditor Interno	Media

5.6.8.3 No conformidades y acciones correctivas

Las no conformidades identificadas durante las auditorías se gestionarán mediante los formatos corporativos de acciones correctivas y cierre de observaciones de SYTSA. Cada hallazgo deberá incluir análisis de causa raíz, responsable, fecha compromiso, seguimiento y verificación de eficacia.

Tabla 49

No conformidades y acciones correctivas

No conformidad	Causa raíz	Acción correctiva	Responsable	Plazo	Eficacia
Exceso de velocidad recurrente	Falta control	Reentrenamiento y monitoreo	Operaciones	30 días	Auditoría
Capacitación BASC vencida	Falta seguimiento	Programa capacitación	TH	15 días	Verificación registros
Sin respaldo actualizado	Incumplimiento TI	Automatizar respaldos	TI	10 días	Prueba restauración

CAPITULO 6

6. CONCLUSIONES Y APLICACIONES

6.1. Conclusiones generales

La presente investigación permite desarrollar una propuesta integral para el diseño de un Manual de Gestión de Riesgos basado en los lineamientos de la norma ISO 31000:2018 para la empresa SYTSA S.A., organización dedicada a la prestación de soluciones logísticas integrales. El estudio evidencia que, aunque la empresa cuenta con procesos organizacionales definidos y sistemas de gestión orientados a la calidad, seguridad y eficiencia operativa, no dispone de una metodología formal que permitiera gestionar los riesgos de manera estructurada, sistemática y alineada con estándares internacionales.

A través del diagnóstico organizacional realizado se identifica que la gestión de riesgos se desarrolla principalmente de manera reactiva, limitando la capacidad de anticipación frente a eventos que podrían afectar el cumplimiento de los objetivos estratégicos de la organización. En este contexto, la propuesta desarrollada constituye una herramienta que facilita la identificación, análisis, evaluación, tratamiento, seguimiento y comunicación de los riesgos en todos los niveles de la empresa.

6.2. Conclusiones específicas

Se identifica y se categoriza los principales riesgos internos y externos que pueden afectar el desempeño de la organización, incluyendo riesgos operativos, tecnológicos, estratégicos, financieros, de seguridad de la información y de continuidad del negocio.

Asimismo, se identifican los procesos organizacionales que requieren la incorporación de mecanismos de gestión del riesgo, alineándolos con la estructura organizacional y los objetivos estratégicos de la empresa. Finalmente, se establece lineamientos metodológicos para la valoración, tratamiento, monitoreo y revisión de los riesgos.

6.2.1. Análisis del cumplimiento de los objetivos de la investigación

El estudio permite identificar y categorizar riesgos críticos en las áreas de operaciones, seguridad BASC, tecnología de la información, mantenimiento y continuidad del negocio, entre los que destacan accidentes de tránsito, robo de carga, fatiga de conductores, ransomware, fallas de frenos y ausencia de un Plan de Continuidad del Negocio. Frente a esta realidad, se recomienda implementar un plan de tratamiento priorizado para los riesgos clasificados como Críticos (puntuación 16-25), que incluya acciones concretas como un programa de conducción segura con reentrenamiento obligatorio para conductores con infracciones, la implementación de geocercas en rutas críticas con escoltas armados en corredores de alta peligrosidad, la migración de hosting compartido a servidor VPS o dedicado con respaldos diarios automatizados, y el establecimiento

de un checklist de pre-arranque obligatorio con registro digital para prevenir fallas mecánicas. Asimismo, se recomienda establecer un sistema de vigilancia del contexto externo que incluya un mapa de criticidad de rutas actualizado mensualmente y una matriz de requisitos legales actualizada semestralmente por el Departamento Jurídico.

6.2.2. Contribución a la gestión empresarial

El diagnóstico permite establecer una línea base que evidencia que SYTSA carece de un inventario formal de activos TIC, un Comité de Seguridad establecido, un proceso formal de gestión de vulnerabilidades, un Plan de Continuidad del Negocio, y una política de cookies y privacidad en su sitio web. Para cerrar estas brechas y medir el progreso del sistema, se recomienda implementar los controles identificados como "No cumplidos" en el Checklist PDS en un plazo de seis meses, lo que incluye la elaboración y aprobación de la Política de Seguridad de la Información, la creación del Comité de Seguridad, la implementación del inventario formal de activos TIC, el establecimiento de un proceso de gestión de vulnerabilidades con escaneos mensuales, y el desarrollo del Plan de Continuidad del Negocio para procesos críticos como el monitoreo satelital y el centro de control de flotas. Adicionalmente, se recomienda instalar en el sitio web de SYTSA un banner de consentimiento de cookies y una política de privacidad visible en un plazo de treinta días, cumpliendo con los requisitos de la Ley Orgánica de Protección de Datos Personales.

El manual diseñado incorpora los principios, el marco de referencia y el proceso de gestión del riesgo definidos por la ISO 31000:2018, incluyendo un anexo de Procedimientos Normalizados de Trabajo (PNT). Para asegurar que estos procesos sean implementados, se recomienda aprobar formalmente el Manual de Gestión de Riesgos por parte de la Alta Dirección y difundirlo a toda la organización a través de los canales oficiales, designando un responsable del Sistema de Gestión de Riesgos que lidere su implementación y actualización. Asimismo, se sugiere constituir formalmente el Comité de Gestión de Riesgos con representantes de las principales áreas, que se reunirá mensualmente durante los primeros seis meses y trimestralmente después, para coordinar y supervisar las actividades del sistema. También se recomienda implementar el procedimiento para la creación de PNTs contenido en el anexo del manual, comenzando por los procesos críticos: inspección preoperacional de vehículos, protocolo de respuesta a robos de carga y procedimiento de reporte de incidentes de ciberseguridad.

6.2.3. Contribución a nivel académico

Desde el ámbito académico, la presente investigación aporta evidencia práctica sobre la aplicación de la norma ISO 31000:2018 en una organización ecuatoriana del sector logístico.

El estudio demuestra la importancia de adaptar los lineamientos teóricos establecidos por estándares internacionales a contextos empresariales específicos, constituyéndose en una referencia metodológica para futuras investigaciones relacionadas con la gestión de riesgos.

6.2.4. Contribución a nivel personal

El desarrollo de esta investigación permite fortalecer las competencias profesionales y académicas de los autores en materia de gestión de riesgos, análisis organizacional, planificación estratégica y aplicación de estándares internacionales.

Asimismo, fortalece capacidades de análisis crítico, trabajo colaborativo, investigación aplicada y resolución de problemas, competencias fundamentales para el ejercicio profesional.

6.3. Limitaciones a la Investigación

Durante el desarrollo de la investigación se presentaron algunas limitaciones relacionadas con el acceso restringido a determinada información estratégica y financiera de la organización debido a criterios de confidencialidad empresarial.

Además, el alcance del estudio se centró en el diseño del Manual de Gestión de Riesgos y no en su implementación y evaluación posterior, por lo que los beneficios esperados deberán ser validados una vez que la organización adopte formalmente la metodología propuesta.

Finalmente, dado que la propuesta fue desarrollada considerando las características particulares de SYTSA S.A., su aplicación en otras organizaciones requerirá procesos de adaptación que contemplen las condiciones específicas de cada contexto empresarial.

Bibliografía

Aven, T. (21 de 12 de 2015). *sciencedirect*. Obtenido de Risk assessment and risk management: Review of recent advances on their foundation: https://pdf.sciencedirectassets.com/271700/1-s2.0-S0377221716X00082/1-s2.0-S0377221715011479/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEHoaCXVzLWVhc3QtMSJHMEUCIQC2H2w0XNqdWWLoS9bgQ5BtJwEe1TKn%2FdgCpY2TuQP11AIgXcHB%2FCx1A%2Fe0ko81sObHTFEfX3O3IUapFAe5H6

Castellanos, A. (2015). *ecoeediciones*. Obtenido de Logística Comercial Internacional: https://www.ecoeediciones.com/wp-content/uploads/2015/07/Logistica-Comercial-Internacional.pdf?srsltid=AfmBOorhunkzqI5629mcpOn8N-EMbbMBxDCHC2A9RlPdjBMMe3nVDvWW

Christopher, M. (2016). *ACADEMIA*. Obtenido de Logística y gestión de la cadena de suministro - 5ª edición : https://www.academia.edu/144414061/Logistics_and_Supply_Chain_Management_5th_edition_Christopher_M

Hopkin. (2018). *SCIENTIFIC RESEARCH AN ACADEMIC PUBLISHER*. Obtenido de La influencia de las operaciones de control preventivo de COSO en la movilización de ingresos en las escuelas ugandesas: https://www.scirp.org/reference/referencespapers?referenceid=2779304

INCIBE. (2023). *INCIBE (Instituto Nacional de Ciberseguridad de España).* Obtenido de Plan Director de Seguridad.: https://www.incibe.es/

Standardization, I. O. (s.f). *ISO: Organización Internacional de Normalización*. Obtenido de ISO: Normas mundiales para bienes y servicios de confianza: https://www.iso.org/es/home

SYTSA. (2023). *SYTSA*. Obtenido de SYTSA Soluciones Logísticas Integradas: https://sytsa.com.ec/soluciones-logisticas-globales/

ANEXO: PROCEDIMIENTO PARA LA CREACIÓN DE PROCEDIMIENTOS NORMALIZADOS DE TRABAJO (PNT)

Código: ANX-SGR-PNT-001

Versión: 1.0

Fecha de emisión: Mayo, 2026

1. OBJETIVO

Establecer una metodología única, clara y obligatoria para la elaboración, revisión, aprobación, difusión y actualización de los Procedimientos Normalizados de Trabajo (PNT) relacionados con la gestión de riesgos operativos, de seguridad vial y de integridad de la carga en SYTSA.

2. ALCANCE

Este procedimiento aplica a todos los colaboradores, jefaturas y áreas de SYTSA que tengan la responsabilidad de generar, modificar o controlar PNTs vinculados a:

- La operación de transporte de carga (conducción, descansos, inspección de vehículos).
- La seguridad física en patios y bodegas (control de accesos, custodia de mercancía).
- El monitoreo satelital y la trazabilidad (uso del sistema CloudFleet, reporte de novedades).

- El mantenimiento preventivo de la flota.
- La respuesta a emergencias (derrames, accidentes, robos de carga).
- El cumplimiento de estándares BASC y normativa legal aplicable.

3. RESPONSABLES

Tabla 50

Responsables del procedimiento

Rol	Responsabilidad
Dueño del proceso (Jefe de Operaciones, Jefe de Mantenimiento, Supervisor HSE, etc.)	Identificar la necesidad del PNT, redactar el borrador y asegurar que el contenido refleje fielmente la actividad real.
Supervisor HSE	Revisar que el PNT mitigue adecuadamente los riesgos identificados y que no contravenga la normativa de seguridad vigente.
Jefe de TI (cuando el PNT involucre sistemas informáticos)	Validar la viabilidad técnica de los pasos relacionados con software, GPS o plataformas digitales.

Comité de Gestión de Riesgos	Aprobar los PNTs que aborden riesgos clasificados como ALTOS o CRÍTICOS en la matriz de riesgos.
Talento Humano	Coordinar las capacitaciones sobre los nuevos PNTs y mantener los registros de asistencia.
Unidad de Calidad / SIG	Gestionar el formato único, la numeración de versiones, el archivo de documentos y el retiro de versiones obsoletas.

4. DESARROLLO DEL PROCEDIMIENTO (CICLO DE VIDA DEL PNT)

El ciclo de vida de un PNT consta de 8 pasos secuenciales, descritos a continuación.

Paso 1: Identificación de la necesidad

El dueño del proceso, basado en una o más de las siguientes situaciones, detecta que se requiere un nuevo PNT o una actualización de uno existente:

- Un incidente o accidente ocurrido (lección aprendida).
- Un hallazgo de auditoría interna o externa (incluyendo auditorías BASC).
- Un cambio en la normativa legal (LOTTTSV, LOPDP, Código de Trabajo).
- Una actualización del estándar BASC.

- Una sugerencia fundamentada del personal operativo (conductores, ayudantes, supervisores de patio).
- Un cambio tecnológico (nuevo sistema de monitoreo, nueva versión del ERP).

Paso 2: Redacción del borrador

El dueño del proceso redacta el borrador utilizando **el formato único de SYTSA** (ver punto 5 de este anexo). El borrador debe incluir obligatoriamente los siguientes campos:

- **Código del PNT:** Identificador único (ej. PNT-OPE-012).
- **Versión:** 1.0, 1.1, 2.0, etc.
- **Fecha de emisión y próxima revisión.**
- **Proceso al que pertenece.**
- **Título claro y descriptivo** (ej. "Procedimiento para el sellado de contenedores de exportación").
- **Objetivo:** Redactado en infinitivo, debe responder qué se busca lograr.
- **Alcance:** Delimita dónde, cuándo y a quién aplica el procedimiento.
- **Responsabilidades:** Tabla que asigna cada paso a un cargo específico.

- **Desarrollo:** Lista numerada de pasos, escrita en lenguaje claro, directo y en voz activa. Cada paso debe ser una instrucción ejecutable ("El conductor verifica...", "El supervisor registra...").
- **Registros asociados:** Formatos, listas de chequeo, reportes que se generan como evidencia.
- **Anexos (si aplica):** Fotografías, diagramas, flujogramas.

Paso 3: Revisión técnica y de riesgos

El borrador se envía al **Supervisor HSE** y, si corresponde, al **Jefe de TI**. Estos revisan:

- Que los pasos propuestos sean técnicamente viables.
- Que no introduzcan nuevos riesgos no identificados.
- Que estén alineados con la normativa de seguridad y con los estándares BASC.
- Que el lenguaje sea comprensible para el personal operativo.

Si se detectan observaciones, el borrador regresa al dueño del proceso para ajustes. Este ciclo se repite hasta que el contenido es técnicamente aceptable.

Paso 4: Prueba de campo (validación operativa)

Antes de cualquier aprobación formal, el PNT se prueba **en condiciones reales de trabajo**. El dueño del proceso selecciona al menos a dos colaboradores del nivel operativo (por ejemplo, dos conductores con al menos un año de experiencia, o dos ayudantes de patio). Se les pide que ejecuten los pasos del PNT y que respondan:

- ¿Hay alguna instrucción que no se entienda?
- ¿Falta algún paso importante que se hace en la realidad y no está escrito?
- ¿Sobra algún paso que es innecesario o que nunca se hace?

Las observaciones recogidas se incorporan al borrador antes de la versión final.

Paso 5: Aprobación y oficialización

- Si el PNT aborda riesgos clasificados como **BAJOS o MEDIOS** (puntaje 1 a 9 en la matriz de riesgos), la aprobación final recae en el **Jefe de Área** y el **Gerente de Operaciones**.
- Si el PNT aborda riesgos clasificados como **ALTOS o CRÍTICOS** (puntaje 10 a 25), requiere además la aprobación expresa del **Comité de Gestión de Riesgos** en sesión ordinaria o extraordinaria.

La aprobación se documenta mediante las firmas en el formato del PNT (campo "Aprobado por").

Paso 6: Capacitación y difusión

- **Talento Humano** programa una capacitación práctica (charla de 15 a 30 minutos) con todo el personal afectado por el nuevo PNT.
- Se pasa lista de asistencia y se resuelven dudas.
- El PNT se publica en la **intranet corporativa** y en las **carteleras físicas** de las áreas operativas (patios, comedores, sala de conductores).
- Las versiones anteriores del PNT se retiran de cualquier punto de acceso físico o digital.

Paso 7: Implementación y control

- El PNT entra en vigencia a partir de la fecha planificada en el formato.
- Durante las **auditorías internas** (al menos una vez al año), los auditores verifican el cumplimiento del PNT mediante observación directa y revisión de registros.
- Cualquier desviación o incumplimiento detectado se registra como hallazgo y se gestiona a través del plan de acciones correctivas del Sistema de Gestión de Riesgos.

Paso 8: Revisión y actualización

Todo PNT se revisa al menos **una vez al año** durante la Revisión por la Dirección del SGR. Si se detectan cambios en el contexto (nueva normativa, nuevos riesgos, cambios tecnológicos) o se identifican lecciones aprendidas de incidentes, se inicia un nuevo ciclo de actualización (volver al Paso 1).

5. FORMATO ÚNICO DE PNT (PLANTILLA OBLIGATORIA)

La siguiente plantilla debe ser utilizada por todas las áreas de SYTSA para la elaboración de PNTs.

Tabla 51

Formato PNT - SYTSA

Campo	Contenido
Código	[Ej. PNT-OPE-005]
Versión	[Ej. 2.0]
Fecha de emisión	[dd/mm/aaaa]
Fecha de próxima revisión	[dd/mm/aaaa]
Proceso	[Ej. Transporte de carga / Mantenimiento / Seguridad física]

Título	[Ej. Procedimiento para la inspección preoperacional del vehículo]
Elaborado por	[Nombre y cargo]
Revisado por	[Nombre y cargo]
Aprobado por	[Nombre y cargo]
1. OBJETIVO	[Texto redactado en infinitivo]
2. ALCANCE	[Texto que delimita la aplicación]
3. RESPONSABILIDADES	[Tabla: Cargo / Responsabilidad en el PNT]
4. DESARROLLO	[Lista numerada de pasos, en voz activa]
5.REGISTROS ASOCIADOS	[Lista de formatos o evidencias que se generan]
6. ANEXOS	[Fotografías, diagramas, flujogramas, listas de chequeo]

---

6. REGISTROS Y CONTROL DE VERSIONES

La Unidad de Calidad / SIG mantiene un **Registro Maestro de PNTs**, que debe contener al menos los siguientes campos:

- Código del PNT
- Título

- Versión vigente
- Fecha de última actualización
- Próxima fecha de revisión
- Responsable del proceso

Las versiones obsoletas deben ser archivadas (no eliminadas) en una carpeta separada, etiquetada como "Histórico de PNTs", con acceso restringido únicamente al personal autorizado.

7. REFERENCIAS

- ISO 31000:2018 – Gestión del riesgo – Directrices.
- Norma Técnica Ecuatoriana NTE INEN-ISO 31000.
- Política de Gestión de Riesgos de SYTSA.
- Matriz de riesgos operativos de SYTSA.
- Estándares BASC V6 – Seguridad en la cadena de suministro.