Maestría en

Gestión de Riesgos

Trabajo de investigación previo a la obtención del título de

Magíster en Gestión de Riesgos

AUTORES:

Byron Alejandro Liviapoma Díaz

Daniel Fernando Ortiz Sánchez

Henry Jhonny Pillajo Terán

Silvia Cecilia León Miranda

Stephanie Astrid Peréz Agreda

Ulbio Juvenal Noriega Avíles

TUTORES:

Paloma Manzano Martínez

Enrique Francisco Molina Suarez

Wilson Fabian Goyes Arroyo

David Genaro Benavides Gutiérrez

Diseño de un Sistema de Gestión de Riesgos basado en la ISO 31000:2018 en la organización Stratos Asesores Quito-Ecuador.

Quito, (marzo 2026)

Certificación de autoría

Nosotros, **Byron Alejandro Liviapoma Diaz, Daniel Fernando Ortiz Sánchez, Henry Jhonny Pillajo Terán, Silvia Cecilia León Miranda Stephanie Astrid Peréz Agreda y Ulbio Juvenal Noriega Avíles,** 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:
BYRON ALEJANDRO LIVIAPOMA DIAZ

Firma del graduado
Byron Alejandro Liviapoma Diaz

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DANIEL FERNANDO ORTIZ SANCHEZ

Firma del graduado
Daniel Fernando Ortiz Sánchez

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY JHONNY PILLAJO TERAN

Firma del graduado
Henry Jhonny Pillajo Terán

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
SILVIA CECILIA LEON MIRANDA

Firma del graduado
Silvia Cecilia León Miranda

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
STEPHANIE ASTRID PEREZ AGREDA

Firma del graduado
Stephanie Astrid Peréz Agreda

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ULBIO JUVENAL NORIEGA AVILES

Firma del graduado
Ulbio Juvenal Noriega Avíles

Autorización de derechos de propiedad intelectual

Nosotros, **Byron Alejandro Liviapoma Diaz, Daniel Fernando Ortiz Sánchez, Henry Jhonny Pillajo Terán, Silvia Cecilia León Miranda, Stephanie Astrid Peréz Agreda y Ulbio Juvenal Noriega Avíles**, en calidad de autores del trabajo de investigación titulado ***Diseño de un Sistema de Gestión de Riesgos basado en la ISO 31000:2018 en la organización Stratos Asesores Quito-Ecuador***, 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:
BYRON ALEJANDRO LIVIAPOMA DIAZ

Firma del graduado
Byron Alejandro Liviapoma Diaz

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DANIEL FERNANDO ORTIZ SANCHEZ

Firma del graduado
Daniel Fernando Ortiz Sánchez

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
HENRY JHONNY PILLAJO TERAN

Firma del graduado
Henry Jhonny Pillajo Terán

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
SILVIA CECILIA LEON MIRANDA

Firma del graduado
Silvia Cecilia León Miranda

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
STEPHANIE ASTRID PEREZ AGREDA

Firma del graduado
Stephanie Astrid Peréz Agreda

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ULBIO JUVENAL NORIEGA AVILES

Firma del graduado
Ulbio Juvenal Noriega Avíles

Aprobación de dirección y coordinación del programa

Nosotros, **Paloma Manzano Martínez y David Genaro Benavides Gutiérrez,** declaramos que los graduados: **Byron Alejandro Liviapoma Diaz, Daniel Fernando Ortiz Sánchez, Henry Jhonny Pillajo Terán, Silvia Cecilia León Miranda, Stephanie Astrid Peréz Agreda y Ulbio Juvenal Noriega Avíles,** 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 18:21:12 +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

Dedico este trabajo a mi papá, por su fortaleza y por la responsabilidad con la que ha enfrentado cada etapa de mi vida. Su ejemplo me enseña que el compromiso y la constancia no se dicen, se demuestran. Este logro también es fruto de todo lo que ha sembrado en mí.

A mi mamá, mi ángel en el cielo, porque, aunque su ausencia se siente, su recuerdo y sus enseñanzas siguen guiando mi camino.

Y a todas las personas que estuvieron presentes durante este proceso, que de una u otra manera aportaron para que hoy pueda culminar esta etapa.

Daniel Fernando Ortiz Sánchez

Dedico este trabajo a Dios, a mi familia y a Stratos Asesores, por ser pilares fundamentales en este camino.

Su guía, apoyo, confianza y colaboración hicieron posible la culminación de esta importante etapa académica.

Byron Alejandro Liviapoma Diaz

Dedico este logro a mis padres, por su amor incondicional, por los valores que inculcaron y por el pilar firme sobre el que he construido cada paso de mi vida.

A mis hermanas, por su apoyo constate, por sus palabras de ánimo y por acompañarme siempre en cada desafío.

Y de manera muy especial a mi hija quien es mi mayor inspiración. Por ella encuentro la fuerza, el valor y la motivación para seguir avanzando, superando obstáculos y soñando en grande. Este esfuerzo es también por ti y para ti.

Henry Jhonny Pillajo Terán

Dedico este logro a Dios por la fortaleza brindada, y a mi familia por su apoyo incondicional. Asimismo, a mis docentes y compañeros por el conocimiento compartido, y a este proceso que consolido mi resiliencia.

Silvia Cecilia León Miranda

Dedico este trabajo a mis padres, por su amor y apoyo incondicional; a mi hermano, por su compañía constante; y a mis docentes y compañeros, quienes con sus conocimientos y experiencias fueron piezas claves a lo largo de todo este proceso.

Stephanie Astrid Peréz Agreda

Dedico este proyecto a mi familia, por ser mi mayor apoyo y motor durante este proceso de formación. Gracias por su paciencia y por motivarme a seguir adelante en los momentos más exigentes.

A mis mentores, por compartir sus conocimientos y visión, fortaleciendo mi compromiso con una gestión responsable del riesgo.

Ulbio Juvenal Noriega Avíles

Agradecimientos

Queremos expresar nuestro agradecimiento a la Universidad Internacional del Ecuador (UIDE) y al programa de la Maestría en Gestión de Riesgos, por la formación recibida y por brindarnos las herramientas necesarias para desarrollar este proyecto con criterio técnico y visión práctica.

A nuestros docentes y directivos, por su orientación constante, sus observaciones oportunas y el nivel de exigencia que nos impulsó a fortalecer cada etapa del trabajo.

A la organización Stratos Asesores, por la confianza depositada en nuestro equipo y por facilitarnos la información requerida, haciendo posible que este estudio se sustente en una realidad organizacional concreta.

Y a cada integrante del equipo de trabajo, por el compromiso, la responsabilidad y el trabajo conjunto que hicieron posible alcanzar este objetivo común.

Resumen

El presente proyecto de aplicación tiene como objetivo diseñar un Sistema de Gestión de Riesgos basado en la norma ISO 31000:2018, alineado con las características específicas y necesidades de Stratos Asesores S.A.S. Para lo cual se realizó un levantamiento del contexto interno y externo de la organización, el reconocimiento de todos los procesos críticos y la implementación de una metodología para la gestión de riesgos. Más adelante se llevó a cabo el proceso de identificación, análisis, evaluación y priorización de los riesgos, desde una perspectiva operativa, tecnológica, financiera y de seguridad de la información y datos personales. En consecuencia, se desarrolló una matriz de riesgos para las áreas específicas de Asesoría en Riesgos y Precios de Trasferencia, se establecieron criterios de valoración en base a la probabilidad de impacto y se crearon planes de tratamiento con asignación de responsables, acciones, periodos de tiempo definidos y mecanismos de seguimiento. Esta propuesta facilita a Stratos Asesores S.A.S. una base metodológica para gestionar sus riesgos de manera ordenada, preventiva y alineada con sus objetivos. Su implementación permitiría fortalecer la planificación de proyectos, mejorar el seguimiento de actividades críticas, disminuir reprocesos, proteger la información de los clientes y respaldar la toma de decisiones de la Alta Dirección.

Palabras clave: Sistema de Gestión de Riesgos, ISO 31000:2018, análisis de riesgos, evaluación de riesgos, tratamiento de riesgos, protección de datos personales.

Abstract

The objective of this implementation project is to design a risk management system based on the ISO 31000:2018 standard, tailored to the specific characteristics and needs of Stratos Asesores S.A.S. To this end, an assessment of the organization's internal and external context was conducted, all critical processes were identified, and a risk management methodology was implemented. Subsequently, the process of identifying, analyzing, evaluating, and prioritizing risks was carried out from an operational, technological, financial, and information security and personal data perspective. Consequently, a risk matrix was developed for the specific areas of Risk Advisory and Transfer Pricing; evaluation criteria were established based on the probability of impact; and treatment plans were created, assigning responsible parties, actions, defined deadlines, and monitoring mechanisms. This proposal provides Stratos Asesores S.A.S. with a methodological framework to manage its risks in an orderly and preventive manner, in line with its objectives. Its implementation would strengthen project planning, improve the monitoring of critical activities, reduce duplication of work, protect client information, and support senior management decision-making.

Keywords: Risk Management System, ISO 31000:2018, risk analysis, risk assessment, risk treatment, personal data protection

Tabla de contenidos

Lista de tablas

Lista de figuras

Lista de anexos

CAPÍTULO 1.

Introducción

Stratos Asesores S.A.S., es una organización de servicios profesionales ubicada en Quito–Ecuador, con enfoque en la gestión de riesgos organizacionales y fiscalidad internacional. Su principal actividad se enfoca en la ejecución efectiva de proyectos, la calidad técnica de sus entregables y el cumplimiento de compromisos contractuales con sus clientes. Haciendo uso de herramientas corporativas tales como OneDrive, correo corporativo Outlook y Teams, para gestionar información y evidencias asociadas a los proyectos.

No obstante, como parte del análisis organizacional, se identifican oportunidades de mejora relacionadas con la gestión de tiempos en la entrega de informes, la estandarización de actividades y la organización en la ejecución de los proyectos. Asimismo, se evidencia la necesidad de fortalecer la planificación de cargas de trabajo, con el fin de optimizar la coordinación interna y mantener la calidad de los entregables. A esto se suman riesgos asociados al manejo y tratamiento de la información, que incluye la protección de datos personales y la gestión de accesos. La ausencia de un enfoque formal de gestión de riesgos limita la capacidad de anticipación frente a estas situaciones.

En este escenario, se propone el diseño de un Sistema de Gestión de Riesgos (SGR) basado en la norma ISO 31000: 2018, que se adapte a las características de la organización, con el objetivo de fortalecer la planificación, el control de los proyectos y la gestión de riesgos.

La finalidad del proyecto se enfoca en diseñar un Sistema de Gestión de Riesgos que permita identificar, analizar y tratar los riesgos relevantes de la organización, incorporando prácticas de seguridad de la información; para lo cual el documento se estructura en capítulos que abordan la introducción, el perfil organizacional, los lineamientos de seguridad, el desarrollo del Sistema de Gestión de Riesgos y finalmente las conclusiones.

1.1. Planteamiento del Problema e Importancia del Estudio

1.1.1. Definición del Proyecto

El presente proyecto de aplicación tiene como finalidad el diseño de un Sistema de Gestión de Riesgos (SGR) basado en la Norma ISO 31000:2018 para la organización Stratos Asesores S.A.S., una organización ecuatoriana que lleva 2 años en el mercado ubicada en Quito-Ecuador, que brinda atención a nivel nacional bajo modalidades presencial, híbrida y remota. La organización se encuentra conformada por dos líneas principales de servicio: Asesoría en Riesgos y Precios de Transferencia, y desarrolla sus actividades mediante un esquema de prestación de servicios por proyecto, apoyándose en herramientas corporativas de Microsoft 365, tales como OneDrive, correo corporativo Outlook y Teams, para la administración documental, la coordinación interna y el intercambio de información.

El proyecto surge ante la necesidad de fortalecer la gestión interna frente a riesgos operativos y de desempeño que pueden afectar el logro de objetivos y la calidad del servicio prestado comprometiendo la reputación y credibilidad de la firma frente a los clientes. Dado que la firma desarrolla sus actividades en un entorno dinámico y bajo un modelo de ejecución por proyectos, resulta pertinente considerar no solo los riesgos asociados a la operación y al

desempeño, sino también riesgos relacionados con la seguridad de la información, protección de datos personales y otras prácticas internas que inciden en el adecuado funcionamiento de la organización. En ese sentido, la propuesta incorpora una visión integral que contempla riesgos asociados a la planificación y desarrollo de proyectos, gestión de credenciales de acceso, altas, bajas y modificaciones de usuarios de las plataformas tecnológicas, privacidad de los datos personales de clientes, proveedores, aspirantes y empleados, y el tratamiento de la información obtenida mediante sistemas de videovigilancia.

Como respuesta a esta necesidad, se plantea el diseño un Sistema de Gestión de Riesgos (SGR) acorde al tamaño de Stratos Asesores S.A.S. (aproximadamente 17 colaboradores), alineado a la ISO 31000:2018, incorporando el establecimiento de contexto, definición de criterios de evaluación (probabilidad e impacto), identificación y valoración de riesgos por procesos y áreas, y la definición de planes de tratamiento y seguimiento. Su alcance abarcará los procesos relacionados con la prestación de servicios, gestión comercial y contratación, planificación, ejecución, control de calidad, gestión información y evidencias, cierre de proyectos. De igual forma, incluirá aspectos vinculados con la administración de accesos, altas, bajas y modificaciones de usuarios de las plataformas tecnológicas, privacidad de la información y el manejo de la videovigilancia dentro del entorno de la organización.

1.1.2. Naturaleza o Tipo de Proyecto

Este proyecto es de naturaleza de diseño y corresponde a un estudio de gestión de riesgos. Abarca el diseño y desarrollo de un sistema de gestión estructurado, con base en la norma ISO 31000:2018 (Organización Internacional de Normalización, 2018).

1.1.3. Objetivos

1.1.3.1. Objetivo general.

Diseñar un Sistema de Gestión de Riesgos basado en ISO 31000:2018 para Stratos Asesores S.A.S., mediante el establecimiento del marco, proceso y herramientas de aplicación, a fin de fortalecer la gestión de riesgos organizacionales asociados a la operación, seguridad de la información y la protección de los datos personales.

1.1.3.2. Objetivos específicos.

- Analizar el contexto organizacional (interno y externo) y los procesos clave de Stratos Asesores S.A.S. vinculados al logro de objetivos.
- Definir el marco de gestión de riesgos (política, roles, responsabilidades y mecanismo de reporte) acorde al tamaño de la organización.
- Diseñar una metodología para la identificación, análisis y evaluación de riesgos con base en criterios de probabilidad e impacto.
- Elaborar el registro de riesgos y priorizar riesgos críticos por área (Riesgos y Precios de Transferencia).
- Proponer planes de tratamiento para los riesgos priorizados, estableciendo acciones, responsables, plazos y evidencias.
- Definir un esquema de seguimiento y mejora mediante indicadores (KRIs) y una rutina de revisión periódica.
- Incorporar en el análisis de riesgos vinculados con la seguridad de la información y privacidad de los datos personales dentro de la organización.

1.1.4. Justificación e Importancia del Trabajo de Investigación

El proyecto de aplicación nace de la necesidad de proporcionar a Stratos Asesores S.A.S. un enfoque ordenado, consistente y sostenible para la gestión de aquellos riesgos que inciden directamente en el cumplimiento de sus objetivos institucionales y en calidad de los servicios ofrecidos. La ausencia de un enfoque sistemático para gestionar los riesgos puede derivar en situaciones que afecten la eficiencia operativa, calidad del trabajo realizado y la capacidad de respuesta de la organización frente a los escenarios adversos.

La importancia de este proyecto de aplicación radica en que propone una visión integral de la gestión de riesgos, adecuada a la realidad de la organización por su tamaño, pero con actividades que demandan organización, control y manejo responsable de la información. Desde esta perspectiva, no solo se consideran los riesgos vinculados con la operación y el desarrollo de los proyectos, sino también aspectos relacionados con la gestión de contraseñas, altas, bajas y modificaciones de usuarios de las plataformas tecnológicas, protección de datos personales de clientes, proveedores, aspirantes y empleados, y el tratamiento de la información derivada de los sistemas de videovigilancia.

Bajo un enfoque metodológico, la elección de la ISO 31000:2018 resulta adecuada ya que esta norma proporciona lineamientos reconocidos internacionalmente para incorporar la gestión de riesgos en la operación institucional y en la toma de decisiones. Además de tener un enfoque común para gestionar cualquier tipo de riesgo y utilizarse a lo largo de la vida de la organización sin importar su actividad o tamaño (Organización Internacional de Normalización, 2018).

Finalmente, a nivel académico y profesional, el proyecto de aplicación aporta un referente aplicable para organizaciones de servicios profesionales en Ecuador, al demostrar que la gestión de riesgos puede ser desarrollada de forma integral en organizaciones jóvenes con recursos limitados con el fin de fortalecer sus prácticas internas y mejorar su capacidad de anticipación, control y respuesta frente a los riesgos.

CAPÍTULO 2.

La Organización

3.1. Perfil de la organización

2.1.1. Nombre de la Empresa

STRATOS ASESORES S.A.S.

2.1.2. Misión, Visión, Valores

Misión: "Proporcionar asesoramiento especializado en gestión de riesgos organizacionales y fiscalidad, apoyar a la toma de decisiones informadas considerando el entorno de riesgos en el que se desenvuelven las organizaciones de hoy día."

Visión: "Ser la referencia regional de apoyo empresarial en temas de riesgos y fiscalidad internacional, ofreciendo soluciones innovadoras y adaptadas a las necesidades cambiantes del entorno empresarial."

Propósito: "Empoderar a las organizaciones y su personal para enfrentar retos presentes y futuros con confianza y resiliencia, siendo un socio estratégico orientado a la excelencia, el cumplimiento y la optimización fiscal; anticipar el caos y salvaguardar activos, contribuyendo a un mundo sostenible, seguro y estable."

2.1.3. Actividades, Marcas, Productos y Servicios

Los servicios de Stratos Asesores S.A.S., se ofrecen bajo el nombre comercial de la organización, como se presenta en la Figura 1.

Figura 1

Logo de la organización Stratos Asesores S.A.S.

Nota. Tomado del logotipo de la organización Stratos Asesores S.A.S., por Stratos Asesores, s.f., https://www.stratosasesores.com/ . Derechos reservados.

Stratos Asesores S.A.S., ofrece servicios profesionales en dos líneas principales:

a) Asesoría en Riesgos: apoyo para interiorizar y manejar un sistema de riesgos corporativo transversal, permitiendo identificar, evaluar, tratar y mantener riesgos que apoyen la estrategia organizacional.

   Dentro de esta área se destacan los siguientes servicios:

   - Cumplimiento (diseño de sistemas de gestión para requerimientos internos y externos).
   - Seguridad de información (diseño e implementación de sistemas basados en estándares internacionales, evaluaciones y revisión de

vulnerabilidades).

- Privacidad de datos (modelos regulatorios, apoyo en auditoría a responsables de datos).
    - Anticorrupción y antisoborno (evaluación y tratamiento de eventos de corrupción; herramientas de control).
    - Auditoría interna (planes de auditoría basados en riesgos y apoyo en ejecución).
    - Aseguramiento de procesos organizacionales y tecnológicos (reportes SOC 1, SOC 2, SOC 3).
    - Auditoría de sistemas (evaluaciones de control interno en TI).
    - Resiliencia empresarial / continuidad del negocio (diseño e implementación de sistemas de continuidad).

b) Precios de Transferencia / Fiscalidad Internacional: análisis y consultas sobre transacciones internacionales (convenios para evitar doble imposición y normativa vigente) y servicios especializados de precios de transferencia.

Dentro de esta área se destacan los siguientes servicios:

- Informe Integral de Precios de Transferencia (IIPT) y acompañamiento en obligaciones formales.
- Anexo de Operaciones con Partes Relacionadas (AOPR) y consideraciones de consistencia para evitar detecciones de riesgo y sanciones.

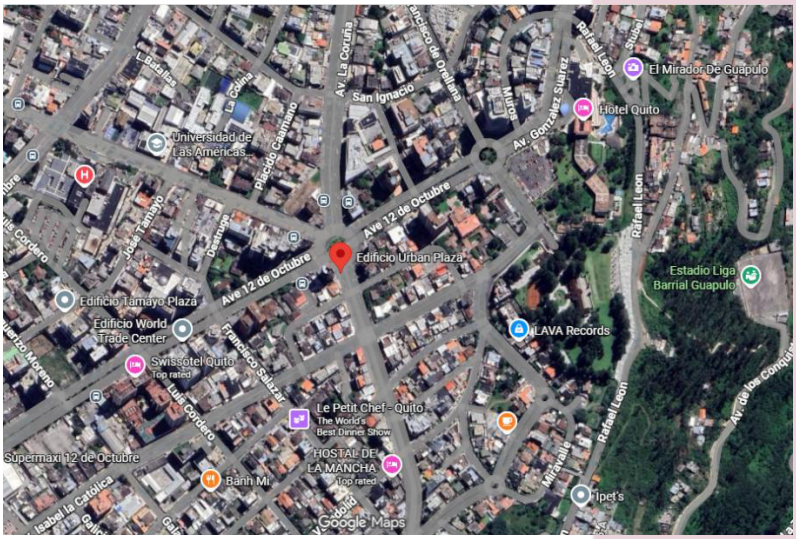
- Asesoría técnica en procesos contenciosos de precios de transferencia (defensa y estrategia legal/técnica).
- Consultas de Valoración Previa (CVP) (gestión integral del proceso).

2.1.4. Ubicación de la Sede

La sede se ubica en Quito, Ecuador, en: Av. 12 de octubre y Coruña, Edif. Urban Plaza, Piso 12, tal como se muestra en la Figura 2.

Figura 2

Ubicación de la organización Stratos Asesores S.A.S.



Nota. Tomado de *Google Maps*, por Google, 2026.

2.1.5. Ubicación de las Operaciones

Su operación principal se desarrolla en Quito-Ecuador.

Figura 3

Edificio Urban Plaza

2.1.6. Propiedad y Forma Jurídica

Stratos Asesores S.A.S., opera bajo la figura societaria S.A.S. (Sociedad por Acciones Simplificada) la cual fue fundada por Oswaldo Bravo – Socio Fundador y CEO de la organización y Karilin Arenas – Socia de Precios de Transferencia.

2.1.7. Mercados Servidos o Ubicación de sus Actividades de Negocio

La actividad principal de Stratos Asesores S.A.S. se ubica en Quito, Ecuador, en: Av. 12 de octubre y Coruña, Edif. Urban Plaza, Piso 12. Respecto a sus mercados servidos, puede

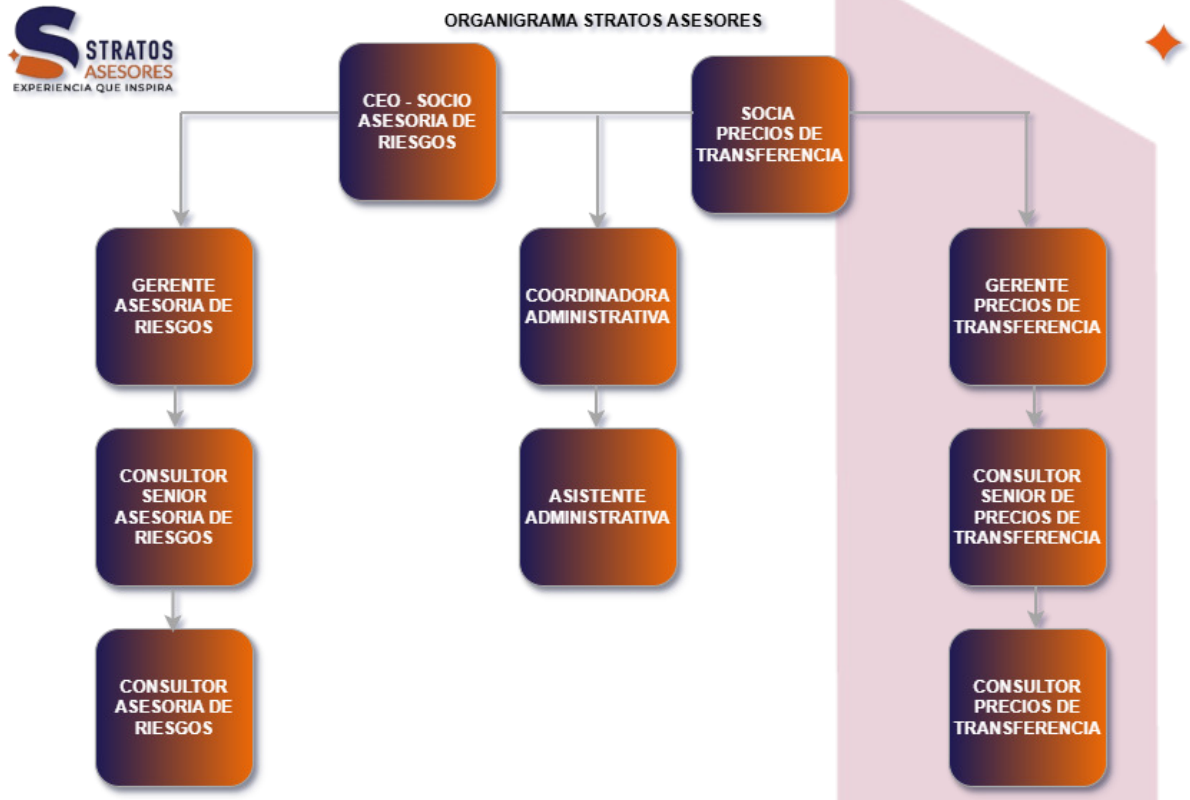
ofrecer servicios a nivel nacional, atendiendo clientes en distintas ciudades del Ecuador bajo modalidades presencial, hibrida o remota según el tipo de proyecto y la ubicación del cliente.

2.1.8. Tamaño de la Organización

Stratos Asesores S.A.S. cuenta actualmente con 17 colaboradores.

Figura 4

Organigrama Stratos Asesores S.A.S.



Stratos Asesores S.A.S. está constituida por dos áreas (Riesgos y Precios de Transferencia) las cuales ofrecen servicios bajo proyecto. Además, de contar con el

área Administrativa encargada de los procesos administrativos y financieros de la organización.

2.1.9. Información sobre Empleados y otros Trabajadores

Stratos Asesores S.A.S. cuenta con 17 colaboradores de los cuales son 11 son mujeres y 6 hombres entre un promedio de edad de 30 años. Los cuales están divididos en diferentes áreas, 5 colaboradores para el área de riesgos, 10 colaboradores para el área de precios de transferencia y 2 colaboradores para el área administrativa.

2.1.10. Procesos Claves Relacionados con el Objetivo Propuesto

Se identifican como procesos clave aquellos que impactan directamente en el cumplimiento de objetivos de la organización, la calidad del servicio y el control de riesgos operativos, reputacionales, contractuales y de seguridad de la información. En Stratos Asesores S.A.S., los procesos clave relacionados con el sistema propuesto son los siguientes:

1. **Gestión comercial y de contratación (inicio del proyecto)**
    a. Levantamiento de necesidades del cliente, elaboración de propuesta, definición de alcance, negociación, firma de contrato/orden de servicio.
    b. Relevancia para el SGR: define riesgos por alcance, expectativas, plazos y compromisos contractuales.
2. **Planificación y gestión del proyecto**
    a. Asignación de equipo (Riesgos / Precios / Administrativo según aplique), cronograma, hitos, plan de trabajo, gestión de cambios, coordinación con el cliente.

b. Relevancia: controla riesgos de retrasos, sobrecarga, dependencia de personas clave y desviaciones de alcance.

3. **Ejecución técnica del servicio**

   a. Desarrollo del trabajo según la línea de servicio ya sea del área de Riesgos o Precios de Transferencia.

   b. Relevancia se materializan riesgos de calidad técnica, documentación técnica, elaboración de informes y anexos.

4. **Gestión de información y evidencias**

   a. Recepción, clasificación, almacenamiento, control de accesos, versionamiento, respaldo, y custodia de evidencias/documentos del cliente.

   b. Relevancia: proceso crítico para riesgos de confidencialidad, integridad y disponibilidad de información (incidentes, pérdidas de evidencia, accesos no autorizados).

5. **Aseguramiento de calidad y revisión por partes**

   a. Revisión técnica y metodológica de entregables antes de su emisión, control de versiones, validación de evidencia y consistencia del informe.

   b. Revisión técnica y metodológica de entregables antes de su emisión, control de versiones, validación de evidencia y consistencia del informe.

6. **Entrega, y cierre y post-entrega**

   a. Presentación de resultados, entrega formal del producto, aceptación por el cliente, lecciones aprendidas, archivo/retención de documentación.

b. Relevancia: controla riesgos de insatisfacción, disputas contractuales, y define condiciones de conservación o devolución/eliminación de información.

7. **Gestión administrativa y financiera**
    a. Facturación, cobros, pagos, control de costos/horas, y soporte administrativo.
    b. Relevancia: impacta riesgos de liquidez, cumplimiento interno, y sostenibilidad del negocio.
8. **Gestión de talento y capacidad**
    a. Asignación de carga laboral, capacitación, respaldo de roles, continuidad operativa ante ausencias.
    b. Relevancia: reduce riesgos por dependencia de personas clave y sostiene la capacidad de ejecución.

Estos procesos constituyen el punto de partida para aplicar el proceso ISO 31000:2018 (identificación, análisis, evaluación, tratamiento y seguimiento), ya que permiten ubicar dónde se originan los riesgos y dónde deben definirse controles y acciones de tratamiento.

2.1.11. Principales Cifras, Ratios y Números que definen a la Empresa

Con base en la información financiera al 31 de diciembre de 2025, Stratos Asesores S.A.S. presenta un total de activos de USD 183.676,77, compuesto principalmente por activos corrientes de USD 181.279,50, destacando efectivo y equivalentes por USD 86.209,59 y cuentas por cobrar por USD 30.082,00. El activo no corriente asciende a USD 2.397,27 (propiedad, planta y equipo).

En cuanto a su estructura de financiamiento, la organización registra pasivos totales

por USD 153.214,64, los cuales son 100% corrientes, siendo las principales cuentas por pagar (USD 118.658,96), beneficios a empleados (USD 13.051,54) y provisiones locales (USD 21.504,14). El patrimonio total asciende a USD 30.462,13.

Desde la perspectiva de desempeño, durante 2025 la organización registró ingresos totales por USD 490.812,91 y una pérdida neta de USD -6.862,11, lo que representa un margen neto aproximado de -1,40%.

Como indicadores financieros relevantes para el presente proyecto (Sistema de Gestión de Riesgos ISO 31000:2018), se determinan: liquidez corriente de 1,18, prueba ácida de 1,09, capital de trabajo de USD 28.064,86, y nivel de endeudamiento de 83,42% (con una relación deuda/patrimonio de 5,03). Estas cifras constituyen una línea base para identificar riesgos asociados a liquidez de corto plazo, concentración de obligaciones corrientes, y sostenibilidad financiera vinculada al control de gastos y administración de cuentas por cobrar.

Tabla 1

Análisis de Indicadores de Liquidez y Riesgos Asociados

Indicador Financiero	Resultado	Interpretación	Riesgo Asociado
Liquidez corriente	1.18	La organización dispone de USD 1,18 en activos corrientes por cada USD 1 de pasivos corrientes.	Posible presión de liquidez si aumentan las obligaciones a corto plazo.
Prueba ácida	1.09	La organización puede cubrir sus deudas a corto plazo sin depender de inventarios.	Riesgo moderado si las cuentas por cobrar no se recuperan a tiempo.

Capital de trabajo	$ 28.064,86	Existe un excedente de activos corrientes sobre pasivos corrientes para operar.	Riesgo de reducción de liquidez si no se controla el gasto o se retrasan cobros.
Nivel de endeudamiento	83.42%	Alto porcentaje de los activos financiados con deuda.	Riesgo financiero elevado por dependencia del financiamiento externo.
Relación deuda/patrimonio	5.03	Por cada USD 1 de patrimonio existen USD 5,03 de deuda.	Riesgo de sostenibilidad financiera y presión sobre la estructura de capital.

Nota. La información expuesta es a partir del análisis de los indicadores financieros.

2.1.12. Modelo de Negocio

Stratos Asesores S.A.S opera bajo un modelo de negocio de servicios profesionales, basado en la prestación de consultorías y trabajos especializados por proyectos. Sus líneas principales de negocio se organizan en: Asesoría en Riesgos (incluye consultorías y auditorías informáticas/tecnológicas, entre otros servicios asociados) y Precios de Transferencia / Fiscalidad Internacional. La generación de valor se materializa mediante entregables técnicos, informes y acompañamiento especializado para la toma de decisiones y el cumplimiento de requerimientos del cliente.

El ciclo de negocio se estructura, de forma general, en: (1) prospección y levantamiento de necesidades, (2) elaboración de propuesta y contratación, (3) planificación del proyecto y asignación de recursos, (4) ejecución técnica y recolección/análisis de información, (5) control de calidad mediante revisión por pares, y (6) entrega, cierre y soporte post-entrega. La modalidad de prestación de servicios puede ser presencial, híbrida o remota, lo que permite atender clientes en todo el Ecuador.

Los principales recursos del modelo son: el conocimiento especializado del equipo, la metodología de trabajo, la capacidad de gestión de proyectos y el manejo adecuado de información del cliente. Como repositorio principal de información se utiliza OneDrive, lo que exige controles sobre acceso, orden documental y control de versiones. La rentabilidad depende del control de tiempos/hora-hombre, la eficiencia en ejecución, la correcta definición de alcance, la calidad del entregable y la gestión de cobranza, variables que se consideran relevantes para el diseño del Sistema de Gestión de Riesgos basado en ISO 31000:2018.

2.1.13. Grupos de Interés Internos y Externos

Para el diseño del Sistema de Gestión de Riesgos (ISO 31000:2018), se identifican los siguientes grupos de interés (stakeholders), considerando su influencia sobre los objetivos y su relación con los riesgos:

a) Grupos de interés internos

CEO/Socios: responsables de definir objetivos, prioridades y apetito de riesgo; aprueban políticas y decisiones estratégicas.

Gerencia (Riesgos y Precios de Transferencia): dueños de procesos y "risk owners" principales; gestionan riesgos en la operación diaria.

Equipo consultor: ejecutan proyectos, levantan evidencia, realizan análisis y elaboran entregables; su desempeño y cumplimiento metodológico impactan calidad, plazos y reputación.

Área administrativa: gestiona facturación, cobranzas, pagos y soporte operativo; influye en riesgos de liquidez y cumplimiento interno.

b) Grupos de interés externos

Clientes (organizaciones contratantes): definen requerimientos, entregan información, validan resultados y condicionan riesgos por alcance, tiempos y cumplimiento contractual.

Proveedores y aliados (tecnología y servicios): por ejemplo, servicios de nube (OneDrive/Microsoft), herramientas de comunicación, y proveedores especializados; influyen en continuidad y seguridad de la información.

Entidades reguladoras y de control: marcos normativos que impactan los servicios prestados por Stratos Asesores o los compromisos con clientes.

Instituciones financieras: relacionadas con servicios bancarios, pagos y obligaciones.

Competencia y mercado: influyen en expectativas del cliente, presión por tiempos, precios y reputación.

La identificación de estos grupos permite definir necesidades de comunicación, criterios de riesgo y responsabilidades de seguimiento dentro del sistema ISO 31000:2018

2.1.14. Otros Datos de Interés

Cobertura nacional y modalidad flexible: Stratos Asesores S.A.S. presta servicios en todo el Ecuador mediante esquemas presencial, híbrido o remoto, lo que exige coordinación efectiva y controles claros para mantener consistencia en calidad y entrega.

Modelo por proyecto fijo: la estructura de precio fijo vuelve especialmente relevante la gestión de riesgos de alcance, estimación de esfuerzo, asignación de recursos, y control de cambios, ya que afectan directamente rentabilidad.

Contratos y Acuerdos de confidencialidad (NDA): la existencia de contratos y acuerdos de confidencialidad formaliza obligaciones de cumplimiento y protección de información, incrementando la criticidad de los controles de custodia documental y manejo de evidencias.

Gestión de información en OneDrive: el repositorio central implica la necesidad de políticas y prácticas para permisos de acceso, segregación por cliente, control de versiones, respaldo y trazabilidad.

Control de calidad establecido: la revisión por pares previa a la entrega es un control interno relevante que reduce el riesgo de errores técnicos, reproceso e inconformidades del cliente, y debe integrarse como control existente en el análisis de riesgos.

Línea base financiera 2025: la información al 31/12/2025 permite disponer de una línea base para riesgos financieros (liquidez de corto plazo, obligaciones corrientes y sostenibilidad) y para la definición de indicadores de seguimiento en el sistema ISO 31000:2018.

CAPÍTULO 3.

Manual de Documentos de Seguridad

3.1. Análisis de Riesgos

Identificación de la organización y de sus centros de trabajo

Stratos Asesores S.A.S es una organización dedicada a la asesoría en gestión de riesgos organizacionales, fiscalidad y precios de transferencia. Se encuentra ubicada en la ciudad de Quito, Ecuador, en: Av. 12 de octubre y Coruña, Edif. Urban Plaza, Piso 12.

3.1.1. Identificación de la Organización y de sus Centros de Trabajo

Stratos Asesores S.A.S es una organización dedicada a la asesoría en gestión de riesgos organizacionales, fiscalidad y precios de transferencia. Se encuentra ubicada en la ciudad de Quito, Ecuador, en: Av. 12 de Octubre y Coruña, Edif. Urban Plaza, Piso 12.

3.1.2. Representante Legal y Responsable de Seguridad

El representante legal de la organización es Oswaldo Bravo, quien se encarga de la dirección y toma de decisiones estratégicas de la organización. Por su parte, Mayra Conchambay. es la responsable de seguridad, encargada de liderar la implementación y supervisión de las normativas de seguridad en la organización.

3.1.3. Actividades de la Organización

La organización brinda apoyo a las empresas para interiorizar y gestionar sistemas de riesgos corporativos de manera transversal, permitiendo identificar, evaluar, tratar y gestionar los riesgos que pueden influir en el cumplimiento de la estrategia organizacional. Asimismo,

realiza análisis y consultas sobre transacciones internacionales y servicios especializados de precios de transferencia.

3.1.4. Tratamientos de la Organización y sus Riesgos

En la Tabla 2 se muestra el tratamiento, los datos tratados, los riesgos principales y controles de la organización Stratos Asesores S.A.S.

Tabla 2

Tratamientos de la organización y sus riesgos

Tratamiento	Datos tratados	Riesgos principales	Controles/medidas
Gestión de clientes	Identificación; contacto; datos de representantes; contractuales (contratos, propuestas, etc.); financieros y facturación	Acceso no autorizado; envío erróneo; pérdida documental	Repositorio OneDrive por cliente; gestión de permisos y control de versiones
Gestión de posibles clientes	Identificación; contacto; datos comerciales	Acceso no autorizado; fuga de información; pérdida de la información	Repositorio de OneDrive con acceso restringido
Gestión de proyectos y evidencias	Documentos del cliente; evidencias; informes; datos sensibles según proyecto	Fuga de información; alteración; pérdida; uso fuera de alcance	Segregación por proyecto; revisión por pares; acceso mínimo
Área Administrativa	Datos de empleados (hojas de vida, datos de cuentas bancarias, historial laboral)	Exposición; incumplimiento; pérdida	Carpetas restringidas; acceso área administrativa
Finanzas/contabilidad	Facturas; pagos; RUC; cuentas	Fraude; error; pérdida; divulgación	Controles administrativos; aprobaciones; respaldo

Proveedores	Contratos; facturas; datos de contacto	Fuga; incumplimiento contractual	Contratos; cláusulas de confidencialidad; evaluación mínima
Aspirantes	Hojas de vida	Fuga de información; alteración; pérdida	Carpetas restringidas; acceso área administrativa
Videovigilancia	Rostro, fecha y hora ingreso/salida	Acceso no autorizado; filtración de videos; falta de información a los clientes; conservación excesiva de grabaciones	Responsable de la administración de la videovigilancia; acceso restringido al sistema de videovigilancia; señalética visible; uso exclusivo para seguridad; controles de acceso por roles, contraseñas, bitácora de acceso

Nota. Los riesgos y controles se determinaron a partir del análisis de las actividades de tratamiento de datos personales.

3.1.5. Consentimientos y Notas Informativas

Consentimiento para el Tratamiento de Datos Personales de STRATOS ASESORES S.A.S.

En cumplimiento de lo dispuesto en la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) y su respectivo reglamento, STRATOS ASESORES S.A.S. informa a los titulares de datos personales sobre los aspectos relacionados con el tratamiento de su información:

1. **Responsable del tratamiento:**

STRATOS ASESORES S.A.S. con RUC 1793212161001 es la entidad responsable del tratamiento de los datos personales. La organización se encuentra ubicada en la ciudad de Quito, Ecuador, en la Av. 12 de octubre y Coruña, Edif. Urban Plaza, Piso 12.

2. Finalidad del tratamiento:

Los datos personales recopilados serán utilizados para gestionar la relación comercial, atender solicitudes o requerimientos, proporcionar información sobre los servicios ofrecidos por la organización, realizar comunicaciones relacionadas con actividades de marketing y cumplir con las obligaciones legales y contractuales aplicables.

3. Datos personales que se recopilan:

La organización podrá recopilar datos personales como nombres y apellidos, número de cédula o pasaporte, dirección, teléfono, correo electrónico, entre otros datos que resulten necesarios para la prestación de los servicios ofrecidos.

4. Almacenamiento y Periodo de conservación de los datos:

Los datos personales serán conservados durante el tiempo necesario para cumplir con las finalidades para las cuales fueron recopilados, considerando además los plazos establecidos por la normativa vigente y las posibles obligaciones legales o contractuales que pudieran surgir posteriormente a la finalización de la relación comercial. Estos datos serán almacenados en los repositorios digitales de la organización, quedando debidamente integrados en el Registro de Actividad de Tratamiento denominado “Gestión de clientes”.

5. Derechos del titular:

Usted, como titular de los datos personales, podrá ejercer los derechos reconocidos en la normativa vigente, entre ellos los derechos de acceso, rectificación, cancelación, oposición y revocación del consentimiento, conforme a lo establecido en la Ley Orgánica de Protección de Datos Personales y su Reglamento. Para el ejercicio de estos derechos, el titular podrá dirigir su solicitud a los canales de contacto oficiales de la organización vinculados al registro de gestión mencionado anteriormente.

6. Revocación del consentimiento:

Usted podrá retirar en cualquier momento el consentimiento otorgado para el tratamiento de sus datos personales mediante solicitud escrita y firmada electrónicamente dirigida a administracionsgb@stratos.ec y/o pboada@stratos.ec, o de manera presencial. La revocación del consentimiento no afectará la legalidad del tratamiento realizado con anterioridad.

7. Transferencias de datos:

La organización podrá compartir información personal con terceros relacionados con el desarrollo de sus actividades. Dichas transferencias se realizarán únicamente cuando el titular haya otorgado su consentimiento previo y siempre garantizando el cumplimiento de las medidas de protección y confidencialidad establecidas en la normativa vigente.

8. Seguridad de los datos:

STRATOS ASESORES S.A.S. adopta medidas técnicas y organizativas orientadas a garantizar la protección de los datos personales, evitando accesos no autorizados, pérdida, alteración o cualquier tratamiento indebido de la información.

9. Consentimiento:

Mediante la firma del presente documento, usted autoriza de manera expresa el tratamiento de sus datos personales conforme a las condiciones descritas en el presente documento y confirma haber sido debidamente informado sobre sus derechos como titular de los datos.

Firma del Titular: _____

Nombre completo: _____

RUC / Cédula: _____

Fecha: _____

3.2. Registro de Actividades de Tratamiento

3.2.1. Grupos de Información

Stratos Asesores S.A.S, ubicada en Quito, Ecuador, es una organización dedicada a la asesoría en gestión de riesgos organizacionales, servicios especializados en fiscalidad y precios de transferencia. En el desarrollo de sus actividades, la organización realiza el tratamiento de diferentes tipos de datos personales vinculados con sus procesos administrativos, comerciales y operativos. Entre estos se encuentran datos de clientes, proveedores y empleados, así como información necesaria para la gestión contable y fiscal relacionada con la prestación de sus servicios.

Estas actividades se realizan en cumplimiento de la normativa vigente en materia de protección de datos personales, aplicando medidas técnicas y organizativas orientadas a garantizar la seguridad y confidencialidad de la información tratada.

Grupo de información: empleados

La organización gestiona datos personales de sus empleados como parte del manejo de la relación laboral y para cumplir con las obligaciones legales. Estas actividades son coordinadas principalmente por el área de Talento Humano, encargada de los procesos relacionados con la administración del personal.

Entre las principales actividades vinculadas a este tratamiento se encuentran:

- Contratación del personal de acuerdo con los perfiles y requisitos establecidos por la organización.
- Gestión y archivo de la documentación laboral y de las hojas de vida de los colaboradores.
- Elaboración y pago de sueldos o nómina, asegurando el cumplimiento de las obligaciones salariales.
- Afiliación y seguimiento de los trabajadores al sistema de seguridad social.
- Desarrollo de programas de capacitación y formación orientados al fortalecimiento de las competencias del personal.
- Aplicación de encuestas de clima laboral y satisfacción de los colaboradores.
- Supervisión del cumplimiento de la normativa laboral y promoción del bienestar del personal.

Base legal del tratamiento: ejecución del contrato laboral, cumplimiento de obligaciones legales en materia laboral y seguridad social, así como intereses legítimos de la organización.

Medidas de seguridad: acceso restringido a la información laboral, controles de acceso a los sistemas, uso de contraseñas y aplicación de políticas internas de privacidad y protección de datos.

Grupo de información: clientes

Stratos Asesores S.A.S trata datos personales de sus clientes con el objetivo de gestionar la relación comercial y desarrollar los servicios profesionales que ofrece la organización, principalmente gestión de riesgos organizacionales, fiscalidad y precios de transferencia.

Las actividades relacionadas con este tratamiento incluyen:

- Gestión de la base de datos de clientes y administración de la información comercial.
- Atención de consultas, solicitudes y requerimientos realizados por los clientes.
- Segmentación de la base de clientes para la gestión de servicios y comunicación comercial.
- Elaboración y entrega de informes derivados de los servicios prestados.
- Facturación y gestión administrativa relacionada con la ejecución de contratos de servicios.
- Aplicación de encuestas de satisfacción.

- Análisis del comportamiento y nivel de satisfacción de los clientes.
- Seguimiento y evaluación del desempeño de los servicios brindados.

Base legal del tratamiento: ejecución de la relación contractual con los clientes, cumplimiento de obligaciones legales y consentimiento del titular.

Grupo de información: proveedores

La organización también gestiona información personal de proveedores que participan en el desarrollo de sus actividades. Este tratamiento tiene como finalidad facilitar la administración de las relaciones comerciales con terceros que suministran bienes o prestan servicios a la organización.

Las principales actividades relacionadas con este tratamiento son:

- Registro y gestión administrativa de proveedores.
- Administración de un sistema centralizado para la gestión de la información de proveedores.
- Procesos de contratación de proveedores para la prestación de bienes o servicios.
- Seguimiento de los servicios que prestan los proveedores.
- Control y gestión de los pagos relacionados con los servicios contratados.
- Evaluación del desempeño de los proveedores y aplicación de mecanismos de retroalimentación.
- Aplicación de incentivos o penalizaciones de acuerdo con el cumplimiento de los acuerdos establecidos.

Base legal del tratamiento: ejecución de relaciones contractuales con proveedores y cumplimiento de obligaciones legales aplicables.

Grupo de información: aspirantes

La organización gestiona datos personales de los aspirantes como parte del proceso de selección y contratación de personal. Estas actividades son coordinadas principalmente por el área de Talento Humano, encargada de los procesos relacionados con la administración del personal.

Entre las principales actividades vinculadas a este tratamiento se encuentran:

- Recepción y registro de hojas de vida entregada por los aspirantes
- Gestión de entrevistas y pruebas técnicas vinculadas al proceso de selección.
- Verificación de referencias personales y laborales.

Base legal del tratamiento: ejecución de medias contractuales a petición del titular para participar en el proceso de selección, evaluación y eventual contratación del aspirante.

Medidas de seguridad: acceso restringido a la información laboral, controles de acceso a los sistemas, uso de contraseñas y aplicación de políticas internas de privacidad y protección de datos.

Grupo de información: videovigilancia

La organización también gestiona información personal de los empleados, clientes, proveedores o cualquier otra persona que ingresa o haga uso de las instalaciones de la organización. Este tratamiento tiene como finalidad contribuir a la seguridad física del personal, visitantes y de los activos de la organización, mediante la captación de imágenes

que permitan la prevención, monitoreo, control de accesos, detectar y contar con evidencia ante eventos que puedan afectar el normal desarrollo de las actividades de la organización.

Las principales actividades relacionadas con este tratamiento son:

- Captación y grabación de imágenes de las personas que ingresan a las instalaciones de la organización.
- Monitoreo de las áreas vigiladas (acceso principal, zona de acceso a oficinas y puestos de trabajo) con fines de seguridad.
- Revisión y consulta de grabaciones cuando sea necesario verificar situaciones que afecten la seguridad.
- Eliminación de las grabaciones una vez cumplido el plazo de conservación (promedio de 2 meses)
- Almacenamiento y conservación temporal de las grabaciones obtenidas por el sistema de videovigilancia.
- Gestión de accesos al sistema de videovigilancia para asegurar que solo el administrador pueda visualizar o manipular las grabaciones.

Base legal del tratamiento: ejecución de relaciones contractuales con proveedores y cumplimiento de obligaciones legales aplicables.

3.2.2. Sistemas de Tratamiento y Niveles de Seguridad

En la organización se identifican distintos grupos de información relacionados con empleados, clientes, aspirantes, proveedores y videovigilancia. Para cada uno de ellos se determinan los sistemas de tratamiento utilizados y el nivel de seguridad correspondiente. El

tratamiento de los datos puede realizarse mediante sistemas físicos (papel), digitales o mixtos, según el medio en el que se almacene o gestione la información. De igual manera, el nivel de seguridad se define considerando la naturaleza de los datos personales y los riesgos asociados a su manejo. La clasificación de estos elementos se presenta en la Tabla 3:

Tabla 3

Sistemas de tratamiento y niveles de seguridad

Grupos de información	Sistemas de tratamiento	Niveles de seguridad
Empleados	Mixto (físico y digital)	Alto
Clientes	Mixto (físico y digital)	Bajo
Proveedores	Digital	Bajo
Aspirantes	Digital	Bajo
Videovigilancia	Digital	Bajo

Nota. Los niveles de seguridad fueron concluyentes considerando la naturaleza de los datos tratados, los sistemas de tratamiento utilizados y los riesgos asociados.

3.2.3. Finalidades, Categorías de Datos, de Interesados y de Destinatarios

3.2.3.1. Gestión de Empleados.

Finalidad del tratamiento:

Administrar los recursos humanos de la organización, lo que incluye procesos de contratación, gestión de nómina, afiliación y seguimiento en el sistema de seguridad social, gestión de beneficios laborales, programas de capacitación y formación del personal, administración de la información contenida en los currículos vitae de los empleados.

Categorías de datos:

- **Datos de identificación:** nombres, apellidos, número de cédula de identidad, dirección, teléfono y correo electrónico.
- **Datos laborales:** historial laboral, contratos de trabajo, evaluaciones de desempeño, información sobre formación profesional y currículos vitae.
- **Datos financieros:** información de cuentas bancarias utilizada para el pago de remuneraciones.
- **Datos relacionados con la seguridad social:** número de afiliación y registros asociados al sistema de seguridad social.

Categorías de interesados:

- Empleados de la organización.

Categorías de destinatarios:

- Administraciones públicas como el Instituto Ecuatoriano de Seguridad Social (IESS) y el Servicio de Rentas Internas (SRI).
- Entidades bancarias utilizadas para el procesamiento de pagos y depósitos de remuneraciones.
- Aseguradoras encargadas de la gestión de seguros laborales o beneficios del personal.
- Proveedores de servicios relacionados con formación, capacitación o auditoría.

3.2.3.2. Gestión de Clientes.

Finalidad del tratamiento:

Gestionar la relación comercial con los clientes de la organización, que incluye la prestación de los servicios profesionales (riesgos organizacionales y precios de transferencia), facturación, atención a consultas o requerimientos, el análisis de información con fines de marketing.

Categorías de datos:

- **Datos de identificación:** nombres, apellidos, número de cédula, RUC o pasaporte, dirección, teléfono y correo electrónico.
- **Datos de facturación:** dirección de facturación e información necesaria para la emisión de comprobantes de pago.
- **Datos de pago:** información de tarjetas de crédito o débito y datos bancarios utilizados para procesar pagos.

Categorías de interesados:

- Clientes de los servicios de gestión de riesgos organizacionales y fiscalidad.

Categorías de destinatarios:

- Proveedores de servicios de pago utilizados para el procesamiento de transacciones.
- Organizaciones de mensajería encargadas del envío o entrega de documentación.
- Entidades o sistemas de control de acceso y seguridad utilizados en las instalaciones de la organización.

3.2.3.3. Gestión de Proveedores.

Finalidad del tratamiento:

Administrar la relación comercial con los proveedores de la organización, lo que incluye procesos de contratación de bienes o servicios, gestión administrativa y contable de proveedores, control y seguimiento de los servicios prestados, así como la gestión de pagos.

Categorías de datos:

- **Datos de identificación:** nombres, apellidos, número de cédula o RUC, dirección, teléfono y correo electrónico.
- **Datos contractuales:** información relacionada con contratos, acuerdos comerciales y servicios prestados.
- **Datos financieros:** información bancaria utilizada para la gestión de pagos a proveedores.
- **Datos de facturación:** información necesaria para la emisión y registro de facturas o comprobantes de pago.

Categorías de interesados:

- Proveedores que suministran bienes o prestan servicios a Stratos Asesores S.A.S.

Categorías de destinatarios:

- Entidades bancarias utilizadas para la gestión de pagos a proveedores.
- Administraciones públicas cuando sea necesario para el cumplimiento de obligaciones legales o tributarias.

- Proveedores de servicios contables o auditoría vinculados a la gestión administrativa de la organización.

3.2.3.4. Gestión de Aspirantes.

Finalidad del tratamiento:

Gestionar su participación en los procesos de contratación, selección y eventual contratación del aspirante, permitiendo a la organización recibir, registrar, analizar y evaluar la información proporcionada por los aspirantes para verificar su idoneidad para cubrir el puesto ofertado, coordinar entrevistas y pruebas de selección.

Categorías de datos:

- **Datos de identificación:** nombres, apellidos, número de cédula de identidad, dirección, teléfono y correo electrónico.
- **Datos laborales:** currículos vitae, referencias laborales e información sobre formación profesional.

Categorías de interesados:

- Los aspirantes

Categorías de destinatarios:

- Administraciones públicas como el Instituto Ecuatoriano de Seguridad Social (IESS) y el Servicio de Rentas Internas (SRI).

3.2.3.5. Gestión de Videovigilancia.

Finalidad del tratamiento:

Contribuir a la seguridad física del personal, visitantes y de los activos de la organización, mediante la captación de imágenes que permitan la prevención, monitoreo, control de accesos, detectar y contar con evidencia ante eventos que puedan afectar el normal desarrollo de las actividades de la organización.

Categorías de datos:

- **Datos de video:** imágenes captadas por los sistemas de videovigilancia instalados en las instalaciones de la organización.

Categorías de interesados:

- Empleados, clientes, visitantes, aspirantes y proveedores

Categorías de destinatarios:

- Cuerpos y fuerza de seguridad del estado
- Compañías aseguradoras

3.2.4. Encargados de los Tratamientos

La organización cuenta con proveedores externos que prestan servicios tecnológicos, contables, financieros, médicos, soluciones de videovigilancia para el desarrollo de las actividades de la organización. A continuación, se identifican los proveedores que brindan estos servicios:

Proveedor de almacenamiento en la nube y correo corporativo

- **Razón social:** SIEMPREOK S.AS
- **Localidad:** Quito-Ecuador

- **Servicio:** Venta de licencias de Microsoft para almacenamiento en la nube y correo corporativo.

Proveedor de servicios contables

- **Razón social:** INTELIGENCORP CONSULTORES CIA. LTDA
- **Localidad:** Quito-Ecuador
- **Servicio:** Prestación de servicios de contabilidad y preparación de impuestos

Proveedor de servicio financiero

- **Razón social:** BANCO PICHINCHA CA
- **Localidad:** Ecuador
- **Servicio:** Prestador de servicios financieros.

Proveedor de servicios legales

- **Razón social:** HUGO R. H. L.
- **Localidad:** Quito- Ecuador
- **Servicio:** Prestador del servicio legal para asesoría, revisión, gestión y acompañamiento jurídico, con acceso a datos identificativos de clientes.

Proveedor de servicios de mensajería y logística

- **Razón social:** MARCELO G.T.
- **Localidad:** Quito- Ecuador
- **Servicio:** Prestador de servicios de mensajería para el traslado, entrega y recepción de documentación y correspondencia vinculada a la organización.

Proveedor de seguro corporativo

- **Razón social:** BMI IGUALAS MEDICAS DEL ECUADOR S.A
- **Localidad:** Ecuador
- **Servicio:** Prestador de servicios de seguro médico corporativo

Proveedor de servicio de contable y facturación electrónica

- **Razón social:** ZUKALO S.A. CONTIFICO
- **Localidad:** Guayaquil-Ecuador
- **Servicio:** Prestador de servicios contabilidad en línea, facturación electrónica y reportes contables y financieros

Proveedor de cámaras de seguridad CCTV y sistema de control de acceso físico

- **Razón social:** SIEMPREOK S.AS
- **Localidad:** Quito-Ecuador
- **Servicio:** Soluciones de videovigilancia y sistema de control de acceso físico bajo plataforma de IP para gestión de ingreso y salida de empleados, aspirantes, clientes, proveedores y visitantes.

Proveedor de servicios de TI

- **Razón social:** SIEMPREOK S.AS
- **Localidad:** Quito-Ecuador
- **Servicio:** Servicio de soporte y mantenimiento de infraestructura tecnológica

Proveedor de servicios de selección y contratación de personal

- **Razón social:** TOP TALENT BUSINESS INTELLIGENCE
- **Localidad:** Quito-Ecuador

- **Servicio:** Servicio de apoyo al proceso de selección de personal, responsable de aplicar pruebas psicológicas y de razonamiento lógico a los candidatos preseleccionados.

3.3. Registro de Dispositivos (Digital)

Stratos Asesores S.A.S., utiliza distintos dispositivos digitales para el desarrollo de sus actividades administrativas y de gestión de información. A continuación, se presenta el registro de los principales equipos utilizados, indicando su tipo, finalidad, ubicación y área responsable.

Ordenadores de escritorio y laptops

- **Tipo de dispositivo:** Laptop
- **Cantidad:** 17
- **Modelo y especificaciones:** Dynabook, sistema operativo Windows 11 Pro.
- **Finalidad:** Uso en actividades administrativas, contabilidad, gestión de recursos humanos, procesamiento de datos, así como en la prestación de servicios relacionados con gestión de riesgos organizacionales y fiscalidad.
- **Ubicación:** Oficina central.
- **Área responsable:** Personal administrativo y profesional de la organización.

Impresoras y escáneres

- **Tipo de dispositivo:** Impresoras y escáneres multifuncionales
- **Cantidad:** 1
- **Modelo y especificaciones:** Ricoh C4500.

- **Finalidad:** Impresión de documentos administrativos como facturas, contratos y roles de pago, así como digitalización de documentos físicos a formato digital.
- **Ubicación:** Oficina central.
- **Área responsable:** Área administrativa.

Dispositivos de control de acceso (tarjetas de acceso)

- **Tipo de dispositivo:** Sistema de control de acceso
- **Cantidad:** 1
- **Modelo y especificaciones:** Hikvision, sistema de 4 puertas modelo DS-K28042022062, control bajo plataforma IP
- **Finalidad:** Control de acceso al piso 12.
- **Ubicación:** Área de espera.
- **Área responsable:** Nicolás A.

Cámaras de seguridad

- **Tipo de dispositivo:** Cámaras de videovigilancia
- **Cantidad:** 3
- **Modelo y especificaciones:** Hikvision, NVR-8-A0820190910CCRRD60250941WCVU
- **Finalidad:** Seguridad de videovigilancia del piso 12.
- **Ubicación:** Acceso principal, zona de acceso a oficinas y puestos de trabajo.
- **Área responsable:** Nicolás A.

Dispositivos móviles (celular)

- **Tipo de dispositivo:** Celular
- **Cantidad:** 1
- **Modelo y especificaciones:** Motorola 50 Fusion
- **Finalidad:** Celular corporativo de comunicación administrativa y redes sociales.
- **Ubicación:** Oficina central
- **Área responsable:** Coordinadora Administrativa

Dispositivos de conectividad de red

- **Tipo de dispositivo:** Amplificador Wifi
- **Cantidad:** 1
- **Modelo y especificaciones:** Ubiquiti - Wireless access point - U7 Pro Access Point Wifi7, Banda 5 & 6 GHz
- **Finalidad:** Permite la conexión a internet
- **Ubicación:** Oficina central
- **Área responsable:** Prestador de servicio de TI

Dispositivos de conectividad de red

- **Tipo de dispositivo:** Router/switch/firewall/controlador central
- **Cantidad:** 1
- **Modelo y especificaciones:** Ubiquiti UDMPro 1U Rackmount 10Gbps UniFi

MultiApplication

- **Finalidad:** Centralizar y administrar la red de una organización, actuando como puerta de enlace principal para controlar el tráfico, la seguridad, los dispositivos UniFi y los servicios de red desde una sola plataforma.
- **Ubicación:** Cuarto de equipos TI.
- **Área responsable:** Prestador de servicio de TI

Dispositivos de almacenamiento

- **Tipo de dispositivo:** NAS (Almacenamiento conectado a la red)
- **Cantidad:** 1
- **Modelo y especificaciones:** Synology DS224+ capacidad 2TB
- **Finalidad:** Permite almacenar información digital
- **Ubicación:** Cuarto de equipos de TI.
- **Área responsable:** Prestador de servicio de TI.

3.4. Registro de Sistemas de Información. (Software, Seguridad, entre otros.)

La organización utiliza distintos sistemas de información y herramientas tecnológicas que permiten la gestión de datos, la comunicación interna y externa, así como la seguridad de la información. A continuación, se presentan los principales sistemas utilizados en el desarrollo de las actividades de la organización:

Software de gestión:

Facturación Contifico: Sistema utilizado para la emisión de comprobantes electrónicos conforme a la normativa del Servicio de Rentas Internas.

Sistema de almacenamiento en la nube:

OneDrive: Plataformas de almacenamiento en la nube que permiten guardar, compartir y respaldar información de manera segura.

Sistema de correo corporativo:

Outlook: Herramienta de comunicación utilizada para el envío y recepción de correos electrónicos y documentos entre clientes, empleados y proveedores.

Sistema de comunicación corporativa:

Microsoft Teams: Plataforma utilizada para la comunicación interna del equipo de trabajo, realización de reuniones virtuales y compartición de información.

Sistemas de seguridad:

Hikvision iVMS: Plataforma utilizada para la gestión del sistema de videovigilancia.

Plataforma IP Hikvision: Software utilizado para el control de accesos y registro de asistencia del personal.

Protección de datos y ciberseguridad

ESET Endpoint Security: Software de seguridad instalado en los equipos de trabajo que proporciona protección antivirus, antimalware y defensa frente a ataques informáticos o amenazas en la red.

3.5. Registro de Personal

3.5.1. Con Acceso a Datos

- Socio de precios de transferencia.
- Socio de asesoría en riesgos.
- Gerencia de precios de transferencia.
- Gerencia de asesoría en riesgos.
- Consultores de precios de transferencia.
- Consultores de asesoría en riesgos.
- Coordinadora administrativa.
- Asistente administrativa.

3.5.2. Sin Acceso a Datos

Guardias de seguridad.

3.5.3. Accesos Físicos

- Socio de precios de transferencia.
- Socio de asesoría en riesgos.
- Gerencia de precios de transferencia.
- Gerencia de asesoría en riesgos.
- Consultores de precios de transferencia.
- Consultores de asesoría en riesgos.
- Coordinadora administrativa.
- Asistente administrativa.

- Guardias de seguridad.

3.6. Registro de Prestadores de Servicio

3.6.1. Con Acceso a Datos Catalogados

El registro de prestadores de servicio con acceso a datos catalogados permite identificar a los proveedores externos involucrados en actividades realizadas para Stratos Asesores S.A.S. y con acceso a información que contiene datos personales. Este registro contribuye al control de dichos proveedores y al cumplimiento de la normativa vigente en la protección de datos personales, así como de las políticas internas de la organización relacionadas con la seguridad de la información.

NICOLAS A.

Descripción del servicio: prestador de servicios de administración de cámaras de videovigilancia y sistemas de control de acceso física para gestión de ingreso y salida de empleados, proveedores, clientes, aspirantes y visitantes.

Tipos de datos accedidos: Datos personales de empleados, clientes, proveedores, aspirantes y visitantes, incluyendo imágenes captadas por los sistemas de videovigilancia, registros de ingreso y salida, datos de identificación y de ser el caso credencial (fecha de nacimiento de empleados) utilizadas para el control de acceso a las instalaciones de la organización.

3.6.2. Sin Acceso a Datos Catalogados

OTECEL S.A.

Descripción del servicio: prestador de servicios de planes celulares corporativos para los empleados y socios de la organización. El prestador del servicio no interactúa con sistemas informáticos ni accede a datos personales.

DISMOF SILVA

Descripción del servicio: provisión de materiales y equipos de oficina utilizados en las actividades administrativas de la organización, tales como papel bond, tóner, teclados, mouse, soportes para laptops, ventiladores, esferos y lápices. El personal responsable de este servicio no accede a información confidencial ni a sistemas que gestionen datos personales.

MEGADATOS S.A.

Descripción del servicio: prestación del servicio de internet de fibra óptica en las instalaciones donde opera la organización. El personal técnico encargado del mantenimiento o soporte del servicio de internet no tiene acceso a información confidencial ni a los sistemas que almacenan datos personales.

CORPORACIÓN NACIONAL DE TELECOMUNICACIONES - CNT EP

Descripción del servicio: prestación de servicio de telecomunicaciones para telefonía fija de la organización. El prestador del servicio no interactúa con sistemas informáticos ni accede a datos personales.

EDGAR F.T.G.

Descripción del servicio: prestación de servicios de limpieza orientados al mantenimiento, higiene y conservación de las instalaciones de la organización. El personal de

limpieza no tiene acceso a información confidencial ni a los sistemas que almacenan datos personales.

3.7. Sistemas de Captación de Imágenes y Audio

3.7.1. Número de Cámaras

La organización cuenta con 3 cámaras de seguridad ubicadas en: área de espera, pasillo y área operativa.

3.7.2. Zonas de Influencia

Las cámaras cubren áreas como acceso principal, zona de acceso a oficinas y puestos de trabajo y un tiempo de almacenamiento promedio de 2 meses.

3.7.3. Sistema de Tratamiento y Almacenamiento

Las grabaciones se almacenan en servidores internos con acceso restringido por un período de sesenta días.

3.7.4. Usuarios Autorizados

El acceso a las grabaciones está limitado a personal de seguridad y socios de Stratos Asesores S.A.S, quienes deben seguir protocolos de protección de datos y sin autorización previa para la revisión de imágenes.

3.8. Dispositivos Medidas de seguridad

3.8.1. Análisis de las Medidas de Seguridad de los Dispositivos

En Stratos Asesores S.A.S., la gestión de la información se apoya en dispositivos tecnológicos y plataformas corporativas que permiten trabajar con datos de clientes, empleados, proveedores y documentación interna. Estos recursos se utilizan en actividades

administrativas, contables, de recursos humanos y en la prestación de servicios vinculados con gestión de riesgos organizacionales y fiscalidad.

Entre los principales dispositivos y sistemas utilizados por la organización se encuentran las laptops corporativas con sistema operativo Windows 11 Pro, el correo corporativo Outlook, las plataformas de almacenamiento en la nube OneDrive, Microsoft Teams para la comunicación interna, el software de seguridad ESET Endpoint Security, el sistema de videovigilancia Hikvision, la plataforma IP Hikvision para el control de accesos, la impresora y escáner multifuncional Ricoh C4500 y el celular corporativo Motorola 50 Fusion.

Tabla 4

Análisis de las medidas de seguridad de los dispositivos

Dispositivo o sistema	Descripción y uso	Medidas de seguridad
Laptops corporativas Dynabook	Equipos utilizados en actividades administrativas, contabilidad, recursos humanos, procesamiento de datos y prestación de servicios profesionales. Funcionan con Windows 11 Pro.	Sistema operativo licenciado y actualizado; acceso mediante usuario y contraseña personal; administración de cuentas locales con segregación de privilegios; protección mediante ESET Endpoint Security. Si bien existe un procedimiento de cambio de contraseña, no se ha implementado un cambio periódico efectivo y verificable de contraseñas, por lo que este aspecto constituye una oportunidad de mejora. Candados físicos de seguridad para laptops.
Correo corporativo Outlook	Herramienta institucional para el envío y recepción de correos y archivos entre clientes, empleados y proveedores.	Acceso mediante credenciales corporativas; uso restringido a fines laborales; control de acceso por usuario; servicio actualizado.

OneDrive	Plataforma de almacenamiento en la nube utilizada para guardar, compartir y respaldar información.	Gestión de permisos de acceso; segregación por cliente; segregación por áreas (riesgos y precios de transferencia); control de versiones; respaldo de información; trazabilidad documental; acceso restringido al personal autorizado.
Microsoft Teams	Plataforma de comunicación, reuniones virtuales y distribución de información del equipo de trabajo, clientes y proveedores.	Acceso mediante cuentas corporativas; uso institucional; integración con el entorno Microsoft 365; servicio actualizado.
ESET Endpoint Security	Software de seguridad instalado en los equipos de trabajo.	Protección antivirus, antimalware y defensa frente a ataques informáticos o amenazas en la red; actualización por parte del prestador del servicio; prohibición de desactivar el antivirus y sus actualizaciones.
Impresora y escáner multifuncional Ricoh C4500	Equipo utilizado para impresión de facturas, contratos y roles de pago, así como para digitalización de documentos físicos.	Uso centralizado en la oficina; apoyo al control documental; custodia de archivos físicos por parte del área administrativa; retiro inmediato de documentos impresos para evitar el acceso de personas no autorizadas.
Sistema de control de acceso Hikvision	Sistema de 4 puertas, modelo DS-K28042022062, bajo plataforma IP, utilizado para controlar el acceso al piso 12.	Restricción de acceso físico a las instalaciones; control mediante plataforma especializada; acceso permitido solo a personal autorizado.
Cámaras de videovigilancia Hikvision	Sistema de videovigilancia instalado en acceso principal, zona de acceso a oficinas y puestos de trabajo.	Monitoreo de áreas críticas; grabaciones almacenadas en servidores del proveedor; acceso restringido a las imágenes; tiempo de almacenamiento promedio de dos meses o sesenta días.
Celular corporativo Motorola 50 Fusion	Dispositivo usado para comunicación administrativa y redes sociales institucionales.	Uso corporativo controlado; acceso restringido al dispositivo; manejo por la coordinadora administrativa; sistema y aplicaciones actualizados.

Nota. Las medidas de seguridad identificadas pertenecen a los controles implementados en los dispositivos y sistemas utilizados para el tratamiento de datos personales.

La organización mantiene controles para el acceso a la información mediante administración de cuentas locales con segregación de privilegios y credenciales personales. El uso de plataformas como Outlook, OneDrive y Teams permite gestionar documentos y comunicaciones dentro de un entorno corporativo con permisos de acceso, control de versiones, respaldo y trazabilidad. A ello se suma la protección de los equipos mediante ESET Endpoint Security y el control físico de ingreso a través del sistema Hikvision, lo que contribuye a reducir riesgos asociados con accesos no autorizados, pérdida de información, alteración de documentos o exposición indebida de datos personales.

3.8.2. Propuesta de Mejora de las Medidas de Seguridad

Para fortalecer la protección de la información en Stratos Asesores S.A.S., es necesario mejorar varios controles relacionados con el uso de dispositivos, el acceso a plataformas corporativas, la gestión de contraseñas, el respaldo de la información y la seguridad física.

3.8.2.1. Gestión de Contraseñas y Accesos.

El acceso a los equipos y plataformas corporativas debe fortalecerse mediante reglas claras para el uso de credenciales. Esto es importante porque la contraseña constituye una de las primeras barreras de protección frente al acceso no autorizado a la información.

Acciones:

- Implementar una revisión periódica de la implementación de la política de contraseñas robustas, evitando el uso de fechas de nacimiento, números de

cédula o combinaciones fáciles de identificar.

- Definir un cambio obligatorio y periódico de contraseñas para los equipos, correo corporativo y plataformas de almacenamiento.
- Reforzar el bloqueo del acceso después de intentos fallidos y revisar periódicamente los usuarios habilitados.
- Evaluar la implementación de un segundo factor de autenticación en las plataformas que contienen información más sensible.
- Implementar un gestor de contraseñas para guardar, organizar, compartir y controlar accesos a contraseñas dentro de la organización.

3.8.2.2. Actualización de Sistemas y Software.

La seguridad de los dispositivos también depende del mantenimiento continuo de sus sistemas y aplicaciones. Por ello, es necesario asegurar que tanto el sistema operativo como las herramientas corporativas y el software de protección se mantengan actualizados.

Acciones:

- Verificar de forma periódica la actualización del sistema operativo Windows 11 Pro.
- Mantener actualizados Outlook, OneDrive, Microsoft Teams y las demás herramientas corporativas.
- Supervisar de manera regular el funcionamiento de ESET Endpoint Security para asegurar que permanezca activo y actualizado.
- Comprobar la vigencia de las licencias de software y de los servicios

tecnológicos utilizados por la organización.

- Designar responsables internos para el control de actualizaciones y la revisión del entorno tecnológico.

3.8.2.3. Protección de la Información Almacenada.

La información institucional se conserva principalmente en plataformas corporativas de almacenamiento como OneDrive. Esto permite mantener orden documental, control de versiones y trazabilidad, pero requiere una revisión constante de permisos y accesos.

Acciones:

- Revisar periódicamente los permisos de acceso en OneDrive.
- Mantener la segregación de la información por cliente, proveedor y por proyecto.
- Reforzar el control de versiones y la trazabilidad de los archivos compartidos.
- Restringir la descarga o almacenamiento de archivos sensibles fuera de los medios autorizados por la organización.
- Implementar cifrado de controles de disco en los equipos que almacenan información sensible de la organización.

3.8.2.4. Copias de Seguridad y Recuperación de Información.

El respaldo de la información es indispensable para garantizar su disponibilidad y recuperación ante incidentes. Por ello, resulta necesario formalizar este proceso y definir claramente su periodicidad y responsables.

Acciones:

- Establecer una política formal de copias de seguridad con periodicidad definida.
- Asignar un responsable de la supervisión periódica de los permisos de acceso a la información almacenada en OneDrive.
- Establecer un mecanismo secundario de respaldo para la información de mayor criticidad para la operación, cumplimiento legal y atención a clientes.
- Limitar el acceso a los respaldos únicamente al personal autorizado.

3.8.2.5. Seguridad Física y Manejo de Documentos.

Además de los sistemas digitales, la organización también utiliza dispositivos y recursos físicos que requieren control y resguardo. Esto incluye documentos impresos, equipos compartidos, cámaras de videovigilancia y sistemas de control de acceso.

Acciones:

- Guardar los documentos físicos con datos personales en archivadores cerrados o en espacios de acceso restringido.
- Evitar que documentos impresos permanezcan expuestos en bandejas o escritorios compartidos.
- Mantener restringido el acceso a grabaciones de videovigilancia y a los registros de control de acceso.
- Modificar los tiempos de grabaciones de imágenes (30 días) y revisar periódicamente los permisos asignados a estos sistemas.

3.8.2.6. Seguimiento y Mejora Continua.

La seguridad de la información requiere seguimiento permanente. No basta con contar con herramientas tecnológicas, también es necesario revisar de forma periódica si las medidas aplicadas siguen siendo suficientes frente a los riesgos existentes.

Acciones:

- Realizar revisiones internas periódicas sobre el estado de seguridad de los dispositivos y sistemas.
- Identificar debilidades en contraseñas, permisos, respaldos y accesos.
- Documentar hallazgos y acciones correctivas para dar seguimiento a las mejoras.
- Capacitar al personal sobre el uso seguro de equipos, contraseñas, correo corporativo y plataformas institucionales.

3.9. Puestos de Trabajo

3.9.1. Análisis de las Medidas de Seguridad de Cada Puesto de Trabajo, Según la Información Tratada

El área administrativa concentra el manejo de información laboral, contractual, financiera y comercial, tanto en soporte digital como en soporte físico. Por esta razón, resulta el espacio más representativo para analizar las medidas de seguridad aplicadas dentro de la organización, ya que en ella se manejan distintos tipos de datos personales y documentación sensible que requieren control, resguardo y acceso restringido.

En esta área se utilizan equipos corporativos, correo institucional, plataformas de almacenamiento en la nube y documentación física bajo custodia interna. Esto implica que las medidas de seguridad no solo deben proteger los archivos digitales, sino también los documentos impresos, la circulación interna de la información y el acceso a los espacios donde se resguarda.

Tabla 5

Análisis de las medidas de seguridad del área Administrativa

Información tratada	Soporte	Lugar de resguardo	Medidas de seguridad
Datos de empleados, como hojas de vida, historial laboral, contrato, roles de pagos y datos de cuentas bancarias	Mixto (digital y papel)	Carpetas restringidas y archivos físicos administrativos	Acceso restringido al personal autorizado; uso de equipos corporativos con Windows 11 Pro; ingreso mediante credenciales personales; protección mediante ESET Endpoint Security; custodia física de documentos dentro del área administrativa
Datos de clientes, como información de contacto, datos contractuales, propuestas, contratos, acuerdos, facturación y documentación comercial	Mixto (digital y papel)	OneDrive y archivos físicos administrativos	Gestión documental con permisos de acceso por usuario; control de versiones; respaldo de información; trazabilidad documental; resguardo físico de documentos en espacios de acceso restringido
Información financiera y contable, como facturas, pagos, RUC, cuentas y registros administrativos	Mixto (digital y papel)	Sistemas institucionales, correo corporativo y archivo administrativo	Controles administrativos; aprobaciones internas; acceso limitado a personal autorizado; uso de Outlook para comunicaciones; respaldo de información; control sobre la circulación interna de documentos impresos

Comunicaciones administrativas y seguimiento operativo	Digital	Outlook, Teams y plataformas corporativas	Uso de cuentas institucionales; acceso mediante credenciales; manejo de información dentro de medios autorizados; control sobre el intercambio de archivos y comunicaciones

Nota. Con base en la información recopilada durante el desarrollo de la investigación.

El área administrativa combina soportes digitales y físicos, por lo que las medidas de seguridad deben aplicarse de forma complementaria en ambos entornos. El acceso restringido, la gestión documental con permisos, el respaldo de información, la trazabilidad de archivos, las aprobaciones internas y la custodia física de documentos permiten reducir riesgos de acceso no autorizado, pérdida documental, alteración de registros y divulgación indebida de información personal.

3.9.2. Acuerdo de Confidencialidad

Entre **STRATOS ASESORES S.A.S.**, con domicilio en la ciudad de Quito, legalmente representada por Oswaldo Bravo, en adelante denominada **LA ORGANIZACIÓN**; y **(Nombre del trabajador)**, portador de la cédula de identidad No. **(_____)**, en adelante denominado **EL TRABAJADOR**, se acuerda lo siguiente:

PRIMERA. OBJETO

El presente acuerdo tiene por objeto regular el deber de confidencialidad y el cumplimiento de las medidas de seguridad que EL TRABAJADOR debe observar respecto de la información a la que accede en el ejercicio de sus funciones dentro de LA ORGANIZACIÓN.

SEGUNDA: DEFINICIONES

Se entiende por Información Confidencial toda aquella relativa a:

- Datos personales de empleados, clientes, proveedores u otras partes interesadas.
- Información financiera, comercial, operativa, tecnológica y estratégica de LA ORGANIZACIÓN.
- Procedimientos internos, políticas de seguridad, medidas de protección de datos, contraseñas, códigos de acceso y otros recursos relacionados con dispositivos, redes o sistemas.
- Documentación relacionada con procesos de producción, trazabilidad, control de calidad, nóminas, inventarios, entre otros.

TERCERA: OBLIGACIONES DEL TRABAJADOR

EL TRABAJADOR se compromete a:

- Mantener absoluta reserva sobre la información a la que tenga acceso;
- Utilizar la información únicamente para el cumplimiento de sus funciones;
- No divulgar, copiar, reproducir, transferir, extraer o compartir información confidencial sin autorización expresa;
- Cumplir las medidas de seguridad establecidas por LA ORGANIZACIÓN para la protección de la información;
- Utilizar únicamente los equipos, cuentas, plataformas y medios autorizados;
- Custodiar adecuadamente la documentación física y digital bajo su responsabilidad;

- Informar de inmediato cualquier incidente, pérdida, acceso no autorizado o situación que comprometa la seguridad de la información.

CUARTA. VIGENCIA

La obligación de confidencialidad tendrá vigencia durante toda la relación laboral o contractual entre EL TRABAJADOR y LA ORGANIZACIÓN, y continuará aun después de su terminación, mientras la información mantenga su carácter confidencial o su divulgación pueda generar afectación a LA ORGANIZACIÓN o a terceros.

QUINTA. SANCIONES

El incumplimiento de las obligaciones establecidas en este acuerdo podrá dar lugar a las acciones administrativas, laborales, civiles o penales que correspondan, de conformidad con la gravedad del hecho y el perjuicio ocasionado.

La vulneración de la confidencialidad, el uso indebido de datos, la inobservancia de medidas de seguridad o la divulgación no autorizada de información podrá ser considerada falta grave, sin perjuicio de las responsabilidades adicionales que correspondan.

SEXTA. JURISDICCIÓN Y MARCO LEGAL

El presente acuerdo se regirá por la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, su Reglamento, el Código del Trabajo y demás normativa ecuatoriana aplicable.

Para la interpretación, ejecución y cumplimiento del presente acuerdo, las partes se someten a la jurisdicción de los jueces competentes de la ciudad de Quito.

SÉPTIMA. FINALIDAD Y USO DE LOS DATOS DEL TRABAJADOR

LA ORGANIZACIÓN tratará los datos personales de EL TRABAJADOR exclusivamente para fines vinculados con la relación laboral o contractual, tales como gestión administrativa interna, pago de remuneraciones, cumplimiento de obligaciones legales, control de accesos, seguridad institucional, archivo documental, administración de personal y demás actividades relacionadas con la operación de la organización.

Los datos personales de EL TRABAJADOR no serán utilizados para fines distintos a los aquí previstos, salvo obligación legal o autorización expresa cuando corresponda.

OCTAVA. TIEMPO DE ALMACENAMIENTO DE LOS DATOS

Los datos personales de EL TRABAJADOR serán conservados durante el tiempo que se mantenga la relación laboral o contractual y, posteriormente, por el plazo necesario para cumplir obligaciones legales, laborales, contables, tributarias o de archivo.

Una vez cumplida la finalidad del tratamiento y agotados los plazos legales de conservación, los datos serán eliminados, bloqueados o conservados únicamente cuando exista una obligación legal que lo justifique.

NOVENA. VIDEOVIGILANCIA

EL TRABAJADOR declara conocer que las instalaciones de LA ORGANIZACIÓN pueden contar con sistemas de videovigilancia con fines de seguridad, control de accesos y protección de personas, bienes e información.

En caso de que LA ORGANIZACIÓN implemente sistemas de localización GPS para control de vehículos, dispositivos o actividades laborales, EL TRABAJADOR será informado previamente sobre su finalidad, alcance y condiciones de uso.

En caso de que LA ORGANIZACIÓN implemente sistemas biométricos de identificación o control, EL TRABAJADOR será informado de manera previa, clara y suficiente sobre su existencia, finalidad y condiciones aplicables.

DÉCIMA. EJERCICIO DE DERECHOS

EL TRABAJADOR podrá ejercer sus derechos de acceso, rectificación y actualización, eliminación, oposición, portabilidad y demás derechos reconocidos por la normativa vigente, mediante solicitud presentada ante LA ORGANIZACIÓN a través de los canales institucionales establecidos para tal efecto.

Dónde ejercerlos: En la oficina de LA ORGANIZACIÓN, ubicada en la ciudad de Quito, Ecuador, en la Av. 12 de octubre y Coruña, Edif. Urban Plaza, Piso 12, o mediante correo electrónico a: administracionsgb@stratos.ec y/o pboada@stratos.ec.

Plazo de respuesta: LA ORGANIZACIÓN dará respuesta a la solicitud en un plazo máximo de treinta (30) días hábiles, de conformidad con la Ley Orgánica de Protección de Datos Personales.

ACEPTACIÓN

Leído que fue el presente acuerdo, las partes manifiestan su conformidad con el contenido y lo suscriben en señal de aceptación.

LA ORGANIZACIÓN

STRATOS ASESORES S.A.S.

Representante legal: Oswaldo Bravo

Firma: _____

EL TRABAJADOR

Nombre: _____

Cédula: _____

Firma: _____

Lugar y fecha: _____

3.10. Encargado del Tratamiento

3.10.1. Contrato E. Tratamiento

Con el fin de regular el acceso y tratamiento de datos personales por parte del Encargado del Tratamiento que presta servicios a Stratos Asesores S.A.S., se desarrolla el siguiente contrato de encargado del tratamiento. Este instrumento establece las condiciones bajo las cuales el encargado podrá acceder a información personal por cuenta de la organización, así como las obligaciones, límites y medidas de seguridad que deberá cumplir durante toda la relación contractual.

3.10.1.1. Contrato de Encargado del Tratamiento de Datos Personales.

CONTRATO DE ENCARGADO DEL TRATAMIENTO

Por una parte, STRATOS ASESORES S.A.S., en adelante EL RESPONSABLE DEL TRATAMIENTO; y, por otra parte, BMI IGUALAS MEDICAS DEL ECUADOR S.A, en adelante EL ENCARGADO DEL TRATAMIENTO, celebran el presente contrato, de conformidad con las siguientes cláusulas:

PRIMERA. Identificación de las partes

Responsable del Tratamiento

Razón social: STRATOS ASESORES S.A.S.

RUC: 1793212161001

Dirección: Av. 12 de Octubre y Coruña, Edif. Urban Plaza, piso 12, Quito – Ecuador

Representante legal: Oswaldo Vladimir Bravo Arellano

Encargado del Tratamiento

Nombre o razón social: BMI IGUALAS MEDICAS DEL ECUADOR S.A

RUC / identificación: 1791927559001

Dirección: Pichincha / Quito / Iñaquito / Av. De Los Shyris N35-174 y Suecia

Representante legal: Hugo Javier Alvarez Clavijo

SEGUNDA. Identificación del Delegado de Protección de Datos Personales

Nombre: Mayra Del Pilar Conchambay

Cargo: Responsable de seguridad / punto de contacto en protección de datos

Correo electrónico: mconchambay@stratos.ec

Teléfono: 0983964548

TERCERA. Objeto del contrato

El presente contrato tiene por objeto regular el tratamiento al que EL ENCARGADO DEL TRATAMIENTO accederá por cuenta de EL RESPONSABLE DEL TRATAMIENTO, únicamente para la prestación de los servicios contratados.

CUARTA. Duración

Este contrato tendrá vigencia durante todo el tiempo que dure la relación contractual entre las partes y mientras EL ENCARGADO DEL TRATAMIENTO mantenga acceso a la información tratada por EL RESPONSABLE DEL TRATAMIENTO.

QUINTA. Naturaleza del tratamiento

El tratamiento podrá comprender, según la naturaleza del servicio prestado, actividades de acceso, consulta, organización, uso, registro, almacenamiento, revisión, respaldo, actualización, conservación o eliminación de información.

SEXTA. Finalidad del tratamiento

La finalidad del tratamiento será exclusivamente la ejecución de los servicios contratados por STRATOS ASESORES S.A.S., sin que EL ENCARGADO DEL TRATAMIENTO pueda utilizar la información para fines propios, ajenos o incompatibles con el objeto contractual.

SÉPTIMA. Tipo de datos tratados

EL ENCARGADO DEL TRATAMIENTO podrá acceder, de acuerdo con la naturaleza del servicio contratado, a los siguientes tipos de datos:

- Datos identificativos;
- Datos de contacto;
- Datos laborales;

OCTAVA. Categoría de interesados

La información tratada podrá corresponder, según el servicio prestado, a las siguientes categorías de titulares:

- Empleados;

NOVENA. Instrucciones para el tratamiento

EL ENCARGADO DEL TRATAMIENTO se obliga a tratar la información únicamente conforme a las instrucciones de EL RESPONSABLE DEL TRATAMIENTO.

En consecuencia, no podrá:

- Utilizar los datos para fines distintos a los autorizados;
- Ceder, transferir o comunicar información a terceros sin autorización previa;
- Conservar la información por más tiempo del necesario para la prestación del servicio, salvo obligación legal;
- Tratar la información fuera del alcance definido por EL RESPONSABLE DEL TRATAMIENTO.

DÉCIMA. Obligaciones del Encargado del Tratamiento

EL ENCARGADO DEL TRATAMIENTO se obliga a:

- Guardar reserva y confidencialidad respecto de toda la información a la que tenga acceso;
- Aplicar medidas técnicas, organizativas y administrativas adecuadas para proteger la información;
- Limitar el acceso a la información únicamente al personal autorizado y estrictamente necesario;
- Garantizar que el personal bajo su dependencia conozca y cumpla el deber de confidencialidad;

- Evitar accesos no autorizados, pérdida, alteración, divulgación indebida o uso incorrecto de la información;
- Informar de manera inmediata cualquier incidente o vulneración de seguridad;
- Colaborar con EL RESPONSABLE DEL TRATAMIENTO en la atención de requerimientos o solicitudes relacionadas con la información tratada;
- Permitir verificaciones razonables del cumplimiento de las obligaciones aquí establecidas, cuando así lo requiera EL RESPONSABLE DEL TRATAMIENTO.

DÉCIMA PRIMERA. Obligaciones del responsable del Tratamiento

EL RESPONSABLE DEL TRATAMIENTO se obliga a:

- Proporcionar instrucciones claras sobre el tratamiento que debe realizarse;
- Facilitar acceso únicamente a la información necesaria para la prestación del servicio.
- Supervisar el cumplimiento de las condiciones pactadas;
- Definir las finalidades del tratamiento y los controles aplicables;
- Coordinar con EL ENCARGADO DEL TRATAMIENTO la atención de incidentes y requerimientos relacionados con la información tratada;
- Informar oportunamente cualquier cambio relevante en las condiciones del tratamiento.

DÉCIMA SEGUNDA. Medidas de seguridad y confidencialidad

EL ENCARGADO DEL TRATAMIENTO deberá mantener medidas de seguridad acordes con la naturaleza de la información tratada y con los riesgos asociados al servicio prestado. Estas medidas incluirán, según corresponda:

- Control de accesos a sistemas y documentos;
- Uso de credenciales personales e intransferibles;
- Protección frente a malware, accesos no autorizados y pérdida de información;
- Resguardo de documentación física y digital;
- Respaldo de información;
- Control sobre la circulación, consulta y uso de los datos.

Toda la información tratada tendrá carácter confidencial y no podrá ser divulgada ni utilizada para fines distintos a los autorizados.

DÉCIMA TERCERA. Subcontratación

EL ENCARGADO DEL TRATAMIENTO no podrá subcontratar total o parcialmente el tratamiento de la información sin autorización previa, expresa y por escrito de EL RESPONSABLE DEL TRATAMIENTO.

En caso de autorización, el subencargado deberá asumir las mismas obligaciones de confidencialidad, seguridad y limitación del tratamiento establecidas en el presente contrato.

DÉCIMA CUARTA. Comunicación de brechas de seguridad

En caso de incidente, acceso no autorizado, pérdida, alteración, divulgación indebida o cualquier brecha de seguridad que afecte la información tratada, EL ENCARGADO DEL

TRATAMIENTO deberá comunicarlo de forma inmediata a EL RESPONSABLE DEL TRATAMIENTO.

La comunicación deberá contener, al menos:

- Descripción del incidente;
- Tipo de datos comprometidos;
- Fecha y circunstancias en que ocurrió;
- Posibles titulares afectados;
- Medidas adoptadas de forma inicial;
- Acciones propuestas para contener, corregir o mitigar sus efectos.

DÉCIMA QUINTA. Acuerdo de finalización de la relación

Una vez finalizada la relación contractual, EL ENCARGADO DEL TRATAMIENTO deberá, según la instrucción de EL RESPONSABLE DEL TRATAMIENTO:

- Devolver la información a la que tuvo acceso;
- Eliminarla de forma segura;
- Bloquearla, cuando exista obligación legal de conservación;
- Cesar de inmediato cualquier tratamiento posterior no autorizado.

Cuando sea requerido, EL ENCARGADO DEL TRATAMIENTO deberá dejar constancia de la devolución, eliminación o bloqueo de la información.

DÉCIMA SEXTA. Jurisdicción y marco legal

El presente contrato se regirá por la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, su Reglamento General y demás normativa ecuatoriana aplicable.

Para la interpretación y cumplimiento del presente contrato, las partes se someten a la jurisdicción de los jueces competentes de la ciudad de Quito.

DÉCIMA SÉPTIMA. Aceptación

Leído que fue el presente contrato, las partes manifiestan su conformidad con su contenido y lo suscriben en señal de aceptación.

EL RESPONSABLE DEL TRATAMIENTO

STRATOS ASESORES S.A.S.

Representante legal: Oswaldo Vladimir Bravo Arellano

Firma: _____

EL ENCARGADO DEL TRATAMIENTO

BMI IGUALAS MEDICAS DEL ECUADOR S.A

Representante legal: Hugo Javier Alvarez Clavijo

Firma: _____

Lugar y fecha: _____

3.11. Análisis Web

3.11.1. Análisis, Configuración y Política de Cookies

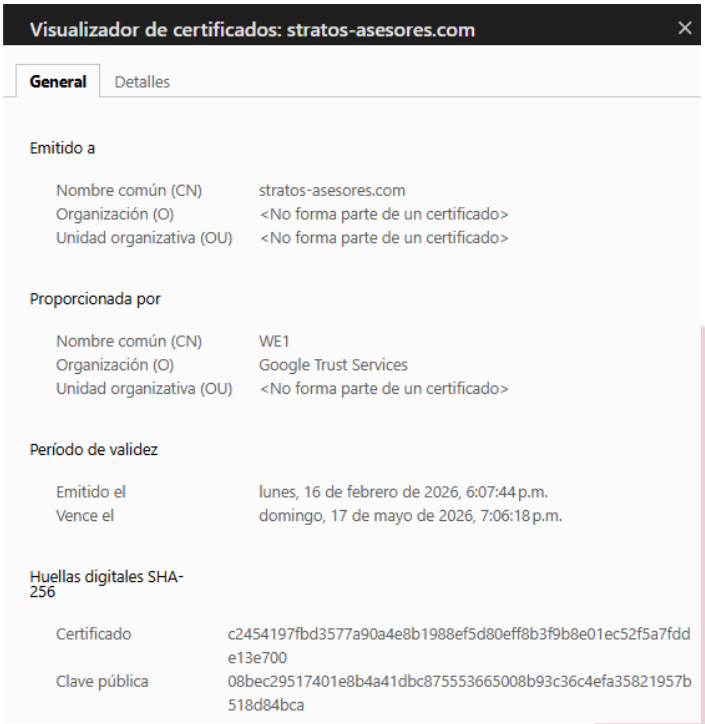
Las cookies son archivos de pequeño tamaño que se almacenan en el ordenador o en el dispositivo móvil al ingresar a un sitio web. Sirven para facilitar el funcionamiento de la página, conservar ciertas preferencias de navegación y conocer de forma general cómo se utiliza el sitio.

- **Análisis:** La página web de Stratos Asesores S.A.S. https://www.stratos-asesores.com/, constituye un espacio digital de carácter corporativo, orientado a mostrar la identidad de la firma, sus áreas de servicio, su equipo de trabajo y sus canales de contacto. También cuenta con un espacio de suscripción por correo electrónico y con una sección para el contacto directo. Sin embargo, la interfaz pública no incluye un aviso inicial sobre cookies, ni un panel de gestión, ni un enlace visible que explique su uso. Esta situación evidencia que el portal todavía puede reforzarse en términos de transparencia y de control sobre los datos que se generan durante la navegación, conforme a la Ley Orgánica de Protección de Datos Personales y a la normativa aplicable en materia de comercio electrónico y uso de medios digitales.

La página web de Stratos Asesores S.A.S. presenta un certificado digital vigente, emitido para el dominio stratos-asesores.com y proporcionado por Google Trust Services. Además, se detalla su período de validez, lo que respalda el uso de una conexión segura durante el acceso a la página, de acuerdo con la Figura 5:

Figura 5

Visualizador del certificado de seguridad del sitio web stratos-asesores.com



Nota. Captura de pantalla tomada del visualizador de certificados del navegador web Google Chrome.

La página web de Stratos Asesores S.A.S. funciona bajo protocolo HTTPS, que corresponde a una versión segura del protocolo de navegación y ayuda a proteger la comunicación entre el sitio y el usuario. Esta medida aporta una base adecuada de seguridad para la navegación y para el intercambio de información a través del portal.

- **Configuración:** La gestión de cookies debe permitir que cada usuario decida de manera clara y sencilla si acepta todas, si rechaza aquellas que no resultan indispensables o si prefiere configurarlas por categorías. En el caso de Stratos

Asesores, conviene incorporar un banner inicial que haga posible esa elección desde el primer acceso, sin obligar al visitante a aceptar configuraciones predeterminadas. Esta configuración debe poder presentarse a través de un panel visible dentro de la página, de manera que el usuario tenga la posibilidad de guardar su elección y modificarla posteriormente cuando lo considere necesario.

- **Permitir o bloquear cookies:** El usuario debe contar con la posibilidad de habilitar o deshabilitar total o parcialmente las cookies no esenciales, manteniendo el acceso normal al contenido principal del sitio. Esta opción debe presentarse de forma clara, diferenciando aquellas cookies que son necesarias para el funcionamiento básico de la página de aquellas que cumplen funciones adicionales.
- **Eliminar cookies:** Las cookies almacenadas en el ordenador o dispositivo móvil pueden poder eliminarse mediante la configuración del navegador o desde las opciones habilitadas en la página web.
- **Gestionar cookies de terceros:** Los usuarios de la página web de Stratos Asesores S.A.S. podrán bloquear o permitir las cookies de terceros, las cuales no provienen directamente del sitio web visitado. Esta información debe presentarse de forma clara para que el usuario conozca qué tecnologías corresponden a servicios externos.

- **Política de cookies:** La política de cookies debe explicar de manera clara qué

tipos de cookies pueden utilizarse en el sitio web, para qué sirven, cuánto tiempo permanecen activas y de qué forma pueden ser aceptadas, rechazadas o eliminadas. Esta información debe mantenerse accesible desde un enlace visible dentro de la página. Entre los aspectos que contempla esta política se encuentran los siguientes:

- **Cookies técnicas:** Las cookies técnicas son aquellas que resultan necesarias para el funcionamiento básico de la página, como la estabilidad de determinados módulos, la navegación segura o la operatividad de componentes esenciales.
- **Cookies de análisis:** Las cookies de análisis permiten conocer tendencias de uso, recorridos dentro del sitio y posibles oportunidades de mejora en la experiencia digital. En caso de incorporarse, su uso debe explicarse de manera expresa.
- **Cookies de rendimiento:** Las cookies de rendimiento permiten evaluar el funcionamiento de la página y ayudan a identificar aspectos que pueden mejorarse para ofrecer una navegación más fluida y eficiente.
- **Cookies publicitarias:** Las cookies publicitarias se utilizan para mostrar contenidos promocionales o mensajes más ajustados a determinados intereses del usuario. Si llegaran a implementarse, su uso deberá informarse de forma clara y diferenciada.
- **Finalidad de las cookies:** La finalidad de las cookies debe estar

orientada a mejorar la operatividad de la página, facilitar la navegación, conservar determinadas preferencias y, de ser el caso, obtener información general que contribuya a optimizar el portal.

- **Cómo se utilizan las cookies:** Estas tecnologías operan desde el navegador y pueden almacenarse por distintos periodos, según su naturaleza. Su aplicación debe responder a finalidades concretas y previamente definidas dentro del sitio web.
- **Cómo se controlan las cookies:** El control de las cookies debe realizarse mediante un mecanismo visible y de fácil uso que permita aceptar, rechazar o personalizar la configuración por categorías. Esta herramienta debe dar al usuario la posibilidad de guardar su selección y modificarla posteriormente cuando lo considere necesario.

3.11.2. Formularios de Contacto, Newsletter, Trabaja conmigo, Registro

La página web de Stratos Asesores S.A.S. funciona como un canal institucional que permite presentar a la organización y facilitar la interacción con personas interesadas en sus servicios. El formulario de contacto y el espacio de suscripción por correo electrónico convierten a la página en un medio de comunicación directa, más allá de su función informativa.

- **Formularios de contacto:** En la sección “Contáctenos”, la página web de Stratos Asesores S.A.S. cuenta con un formulario mediante el cual se solicitan nombre, correo electrónico, dirección, referencia sobre cómo conoció a la

organización y mensaje. Este formulario permite canalizar consultas, solicitudes o requerimientos de una manera directa y ordenada. Junto a ello, la organización pone a disposición de los usuarios otros medios de contacto para una comunicación más formal y específica, entre ellos el teléfono institucional, los correos electrónicos administracion@stratos.ec y obravo@stratos.ec, y la dirección ubicada en la Av. 12 de octubre y Coruña, Edif. Urban Plaza, Piso 12, Quito, Ecuador. Esta información permite tanto el contacto digital como una atención más directa cuando sea necesario.

Como medida de mejora, debe reforzarse con una Política de Privacidad visible y accesible desde el propio formulario, junto con una casilla obligatoria de aceptación antes del envío. De esta manera, el usuario podrá conocer con claridad quién es el responsable del tratamiento, qué datos se recogen, con qué finalidad se utilizan, cuánto tiempo se conservarán, a través de qué medios puede ejercer sus derechos y en qué condiciones se realizará el tratamiento de la información proporcionada.

Figura 6

Formulario de contacto de la página web de Stratos Asesores S.A.S.

Nota. Captura de pantalla, tomada de la página web de Stratos Asesores S.A.S., s.f.

La Figura 6 muestra el formulario de contacto disponible en la página web de la organización, junto con los medios adicionales de contacto institucional. Su incorporación en este apartado permite evidenciar los datos que actualmente se solicitan al usuario y fundamenta la propuesta de mejora en añadir una casilla visible de aceptación de la Política de Privacidad antes del envío del formulario.

Como mejora del formulario de contacto de la página web de Stratos Asesores S.A.S., se propone incorporar una Política de Privacidad visible, clara y accesible desde el mismo formulario. Su finalidad es informar al usuario sobre el tratamiento de los datos personales que proporcione a través del sitio, así como garantizar mayor transparencia antes del envío de

cualquier consulta o solicitud.

- **Política de Privacidad**

En la página web de Stratos Asesores S.A.S no se observó la implementación de una política de privacidad tal cual se observa en la Figura 6. Por lo cual se propone implementar la siguiente Política de Privacidad en su página web:

POLÍTICA DE PRIVACIDAD

En Stratos Asesores S.A.S. respetamos la privacidad y protegemos los datos personales de nuestros usuarios, clientes, prospectos y demás titulares de datos. La presente Política de Privacidad tiene por objeto informar cómo recopilamos, utilizamos, almacenamos, protegemos y tratamos los datos personales obtenidos a través de nuestro sitio web, conforme a la normativa aplicable en materia de protección de datos personales en el Ecuador.

1. Responsable del tratamiento

El responsable del tratamiento de los datos personales es Stratos Asesores S.A.S., con domicilio en Av. 12 de Octubre y Coruña, Edif. Urban Plaza, Piso 12, Quito, Ecuador.

Para consultas relacionadas con privacidad y protección de datos personales, el titular podrá comunicarse a: administracion@stratos.ec

2. Datos personales que recopilamos

A través de nuestro sitio web podemos recopilar los siguientes datos personales:

a) Formulario de contacto

- Nombre;
- Correo electrónico;

- Dirección;
- Información sobre cómo conoció a la organización;
- Mensaje o consulta enviada por el usuario.

b) Formulario de suscripción

- Correo electrónico.

Stratos Asesores S.A.S. tratará únicamente los datos personales necesarios, pertinentes y limitados a las finalidades informadas.

3. Finalidades del tratamiento

Los datos personales recopilados a través del sitio web serán utilizados para las siguientes finalidades:

a) Respecto del formulario de contacto

- Atender solicitudes de información, consultas o requerimientos;
- Responder mensajes enviados por los usuarios;
- Dar seguimiento a solicitudes comerciales o informativas;
- Mantener registro de comunicaciones y solicitudes recibidas.

b) Respecto de la suscripción

- Enviar boletines, novedades, invitaciones, noticias, información corporativa o comunicaciones comerciales relacionadas con los servicios de Stratos Asesores S.A.S.

4. Base de legitimación

El tratamiento de los datos personales se realizará con base en el consentimiento del titular, cuando este sea necesario, así como en las demás bases legales permitidas por la normativa aplicable.

En el caso del formulario de contacto, el envío voluntario de la información por parte del titular constituye manifestación de conocimiento y aceptación del tratamiento para atender su requerimiento.

En el caso de la suscripción, el tratamiento del correo electrónico tendrá como base el consentimiento del titular para el envío de comunicaciones informativas o comerciales.

5. Conservación de los datos

Los datos personales serán conservados durante el tiempo necesario para cumplir con las finalidades descritas en esta política, así como durante los plazos que resulten aplicables conforme a obligaciones legales, regulatorias o de resguardo documental.

Posteriormente, los datos serán eliminados o bloqueados de manera segura, según corresponda.

6. Transferencia o comunicación de datos

Stratos Asesores S.A.S. no compartirá los datos personales con terceros, salvo cuando ello sea necesario para cumplir obligaciones legales, atender requerimientos de autoridad competente o apoyarse en proveedores que presten servicios relacionados con la operación del sitio web o la gestión de comunicaciones, bajo las debidas medidas de confidencialidad y protección de datos.

7. Seguridad de la información

Stratos Asesores S.A.S. aplica medidas administrativas, técnicas y organizativas razonables para proteger los datos personales frente a pérdida, acceso no autorizado, alteración, divulgación o uso indebido.

8. Derechos de los titulares

El titular podrá ejercer los derechos que le reconozca la normativa aplicable, incluyendo, entre otros:

- Acceso;
- Rectificación y actualización;
- Eliminación;
- Oposición;
- Portabilidad;
- Suspensión del tratamiento, cuando corresponda.

Para ejercer estos derechos, podrá enviar su solicitud al correo:

administracion@stratos.ec

La solicitud deberá permitir identificar al titular y detallar claramente el requerimiento correspondiente.

9. Uso de cookies

El sitio web de Stratos Asesores S.A.S. utiliza cookies estrictamente necesarias para garantizar el funcionamiento adecuado de la página, incluyendo la gestión de sesión y otras funcionalidades técnicas esenciales.

A la fecha de emisión de la presente política, no se contempla el uso de cookies analíticas, publicitarias o de terceros asociadas a herramientas de seguimiento o perfilamiento, tales como Google Analytics, Meta Pixel u otras similares.

En caso de incorporarse este tipo de tecnologías, Stratos Asesores S.A.S. informará previamente a los usuarios, implementará los mecanismos de información y, de ser aplicable, consentimientos correspondientes, y actualizará esta Política de Privacidad.

10. Suscripción y comunicaciones

Cuando el usuario se suscriba voluntariamente, autoriza el tratamiento de su correo electrónico para el envío de boletines, novedades, información corporativa y, en su caso, comunicaciones comerciales relacionadas con Stratos Asesores S.A.S.

El titular podrá solicitar en cualquier momento la cancelación de su suscripción o la supresión de sus datos de contacto mediante los canales habilitados por la organización.

11. Cambios a esta política

Stratos Asesores S.A.S. podrá modificar o actualizar esta Política de Privacidad cuando sea necesario por cambios legales, regulatorios, tecnológicos o de operación del sitio web. Las modificaciones serán publicadas en este mismo sitio.

12. Identificación del Delegado de Protección de Datos

Stratos Asesores S.A.S ha designado un Delegado de Protección de Datos, quien actúa como punto de contacto para consultas, solicitudes y asuntos relacionados con el tratamiento de datos personales.

Contacto del Delegado de Protección de Datos:

Nombre: Mayra del Pilar Conchambay

Correo electrónico: mconchambay@stratos.ec

Dirección: Av. 12 de Octubre y Coruña, Edif. Urban Plaza, Piso 12, Quito, Ecuador.

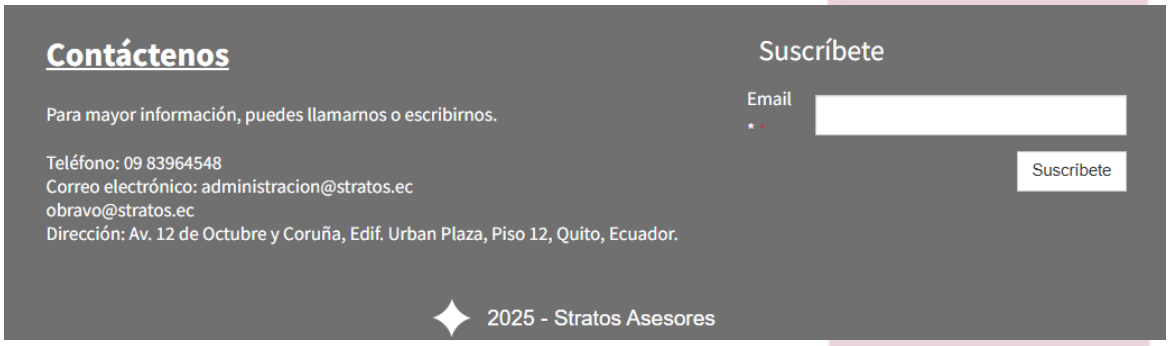
13. Contacto

Para cualquier consulta relacionada con esta Política de Privacidad o con el tratamiento de datos personales, puede escribir a: administracion@stratos.ec

- **Newsletter:** Tanto en la página principal como en la sección de contacto aparece un espacio de suscripción en el que el usuario puede ingresar su correo electrónico. Esa funcionalidad opera como un mecanismo de newsletter o de suscripción. Por ello, conviene acompañarla con una explicación breve sobre el tipo de información que se enviará, la frecuencia aproximada de contacto y la posibilidad de cancelar la suscripción en cualquier momento.

Figura 7

Espacio de suscripción de la página web de Stratos Asesores S.A.S.



Nota. Captura de pantalla tomada de la página web de Stratos Asesores S.A.S., s.f.

La figura 7 muestra el espacio de suscripción disponible en la página web de Stratos

Asesores S.A.S., donde el usuario puede registrar su correo electrónico para recibir comunicaciones futuras.

- **Trabaja conmigo:** El sitio no incorpora una sección específica para reclutamiento, carga de hojas de vida o postulación a vacantes. Por tanto, la página no cuenta con un módulo independiente orientado a captar información.
- **Registro:** La página tampoco incorpora un sistema de registro de usuarios, creación de cuentas, autenticación de clientes o acceso a áreas privadas. Su estructura está enfocada principalmente en brindar información institucional y facilitar el contacto abierto con quienes visitan el sitio.

La página web de Stratos Asesores S.A.S. cumple funciones informativas y de contacto, lo que facilita la interacción con sus visitantes. Aunque no cuenta con funciones más avanzadas como registro de usuarios o un módulo específico de reclutamiento, su estructura resulta adecuada para el propósito institucional de comunicación con los usuarios. La principal mejora en este punto consiste en incorporar una Política de Privacidad visible y una casilla de aceptación expresa antes del envío del formulario o del registro de una suscripción.

3.11.3. Avisos Legales

La página web de Stratos Asesores S.A.S. no presenta de forma visible una sección específica dedicada a los avisos legales, términos y condiciones de uso, política de privacidad u otra información relacionada con el uso del sitio. Esta falta de información hace que el usuario no pueda conocer con claridad las condiciones de uso de la página, más aún cuando

cuenta con formulario de contacto, datos institucionales y un espacio de suscripción por correo electrónico.

Esta falta de información puede generar dudas sobre el tratamiento de los datos personales, las condiciones de uso del sitio, la responsabilidad sobre el contenido publicado y los canales disponibles para consultas o reclamos. La Ley Orgánica de Protección de Datos Personales y la Ley de Comercio Electrónico, Firmas y Mensajes de Datos refuerzan la necesidad de que la página incorpore accesos visibles y permanentes al aviso de privacidad, los términos de uso y la identificación del responsable del sitio.

Como mejora del sitio web, se propone el siguiente texto de Aviso Legal:

AVISO LEGAL

1. TITULARIDAD DEL SITIO WEB

En cumplimiento con el deber de información vigente en la República del Ecuador, se detallan los datos del titular del portal:

Razón Social: Stratos Asesores S.A.S.

RUC: 1793212161001

Domicilio Legal: Av. 12 de octubre y Coruña, Edif. Urban Plaza, Piso 12, Quito, Ec.

Representante Legal: Oswaldo Bravo

Correo electrónico de contacto: administracionsgb@stratos.ec / pboada@stratos.ec

2. OBJETO DEL SITIO WEB

Este sitio tiene carácter informativo e institucional. Su finalidad es dar a conocer la identidad de Stratos Asesores S.A.S., sus servicios, su equipo de trabajo y sus canales de contacto.

3. CONDICIONES DE USUARIO

El usuario deberá utilizar esta página de forma adecuada y conforme a su finalidad informativa y de contacto. No se permitirá ningún uso que pueda alterar el funcionamiento del sitio o afectar la información publicada.

4. PROPIEDAD INTELECTUAL

Los textos, logotipos, diseños, imágenes y demás contenidos publicados en esta página son de uso institucional y no podrán ser reproducidos, distribuidos, modificados o utilizados sin autorización, salvo en los casos permitidos por la normativa aplicable.

5. PROTECCIÓN DE DATOS PERSONALES

Los datos personales que puedan recopilarse a través del formulario de contacto, del espacio de suscripción o de cualquier otro medio habilitado dentro del sitio serán tratados por Stratos Asesores S.A.S. de conformidad con la Ley Orgánica de Protección de Datos Personales. Dichos datos podrán utilizarse para atender consultas, responder solicitudes, gestionar requerimientos y mantener contacto con usuarios interesados en los servicios de la organización. Estos datos se conservarán únicamente durante el tiempo necesario para cumplir con la finalidad para la cual fueron recopilados o mientras exista una obligación legal que justifique su conservación. El detalle sobre finalidades, conservación, derechos del titular

y canales para ejercerlos deberá constar en la Política de Privacidad, la cual deberá mantenerse visible y accesible dentro de la página web.

6. USO DE COOKIES

Este sitio podrá utilizar cookies para facilitar la navegación, mejorar el funcionamiento de la página y conocer de forma general cómo se utiliza el sitio. Su uso deberá informarse de manera clara y accesible dentro del sitio web.

7. ENLACES EXTERNOS

En caso de que la página incluya enlaces a sitios de terceros, Stratos Asesores S.A.S. no asume responsabilidad por los contenidos, políticas o prácticas de dichos sitios externos.

8. LIMITACIÓN DE RESPONSABILIDAD

Stratos Asesores S.A.S. procurará mantener la información del sitio actualizada y su funcionamiento en condiciones adecuadas de seguridad. No obstante, no garantiza la ausencia absoluta de errores técnicos, interrupciones del servicio o eventos externos que puedan afectar temporalmente la disponibilidad de la página.

9. MODIFICACIONES

Stratos Asesores S.A.S. podrá actualizar o modificar el presente Aviso Legal cuando resulte necesario. La versión vigente deberá mantenerse disponible dentro de la página web.

3.12. Medidas de Seguridad

3.12.1. Análisis, Uso y Medidas de Seguridad en el Uso de Navegadores

En Stratos Asesores S.A.S., el uso de navegadores web constituye un componente esencial para el desarrollo de las actividades diarias, especialmente en el

acceso a plataformas corporativas como Microsoft 365, así como para la consulta de información y gestión de proyectos.

El uso de estos navegadores implica riesgos asociados a la seguridad de la información, particularmente en un entorno donde se gestionan datos personales de clientes, empleados y proveedores.

En este contexto, cabe precisar que Stratos Asesores S.A.S. no establece el empleo de un navegador determinado para el desarrollo de las actividades diarias. Sin embargo, los navegadores que frecuentemente utilizan son Google Chrome (para el ingreso a plataformas bancarias) y Microsoft Edge (para el acceso a OneDrive, plataformas en la nube empleadas para la gestión y almacenamiento de información relacionada con clientes, proveedores, empleados y aspirantes).

Esta práctica utilizada en la organización, a pesar de no estar documenta, se basa en las seguridades de cada navegador. Google Chrome ofrece advertencias frente a sitios sospechosos y protección de navegación segura para el acceso a plataformas bancarias **(Google, s. f.)**. Por su parte, Microsoft Edge incorpora Microsoft Defender SmartScreen para ayudar a proteger frente a sitios de phishing, malware y descargas potencialmente maliciosas, lo que aporta seguridad en el acceso a OneDrive **(Microsoft, 2025)**.

Uso de navegadores web en la organización.

El uso de navegadores en la organización se encuentra vinculado principalmente a:

- Acceso a la plataforma en la nube (OneDrive) para almacenamiento y gestión documental.

- Consulta de información técnica y normativa para el desarrollo de servicios.

Estas actividades implican el manejo constante de información sensible, lo que exige la aplicación de controles de acceso, uso de credenciales y restricción a plataformas autorizadas, tal como se evidencia en las prácticas actuales de la organización.

Riesgos asociados al uso de navegadores web

Los principales riesgos asociados a la organización son:

- Acceso a sitios web maliciosos que puedan comprometer la seguridad de los equipos.
- Ataques de phishing dirigidos a credenciales corporativas.
- Descarga de software malicioso que afecte los dispositivos corporativos.
- Exposición o fuga de información confidencial mediante navegación insegura.
- Acceso no autorizado a información almacenada en la nube.

Estos riesgos se relacionan directamente con la gestión de accesos, protección de datos personales y seguridad de la información, aspectos considerados dentro del alcance del Sistema de Gestión de Riesgos.

Medidas de seguridad propuestas

Con el objetivo de fortalecer la seguridad de la información en Stratos Asesores S.A.S. se proponen las siguientes medidas de tratamiento de riesgos para el uso de navegadores web:

- Estandarización del uso de navegadores web en la totalidad de los equipos corporativos.
- Implementación de políticas de control de acceso mediante credenciales

personales e intransferibles.

- Restricción de acceso a sitios web no autorizados o identificados como fuentes de riesgo.
- Prohibición técnica para la instalación de extensiones y complementos no autorizados por la organización.
- Ejecución de programas de capacitación periódica al personal sobre riesgos de navegación y ciberseguridad.
- Evitar el almacenamiento automático de contraseñas en navegadores.
- Desactivar las cookies de terceros para evitar la recopilación innecesaria de información.

Estas medidas complementan los controles ya existentes en la organización, tales como el acceso restringido, uso de credenciales y protección de dispositivos, fortaleciendo así la seguridad en el entorno digital.

3.12.2. Hosting y Servidores

3.12.2.1. Medidas de Seguridad.

En Stratos Asesores S.A.S se utiliza el hosting provisto por Ecuaweb y de forma complementaria se usa Cloudflare como una capa adicional de protección ya que actúa como intermediario entre los usuarios y el servidor alojado en el hosting permitiendo filtrar tráfico malicioso, mitigar ataques de denegación de servicio (DoS), mejorar la velocidad de acceso al sitio y reforzar la protección del servidor principal.

Asimismo, la página web cuenta con certificado digital Secure Sockets Layer (SSL) y dentro de la configuración del hosting se tiene activada la opción AutoSSL la que permite validar y renovar automáticamente el certificado digital y exista conexiones seguras bajo el protocolo HTTPS para proteger la información transmitida entre la página web y los usuarios.

De igual manera, el servicio de hosting de Ecuaweb permite a Stratos Asesores S.A.S tener copias de seguridad, incluyendo respaldos completos o parciales de la cuenta y opciones de restauración en caso de que se presenten incidentes o fallos de seguridad para recuperar la información.

3.12.2.2. Prestadores de Servicios.

Stratos Asesores S.A.S cuenta con el prestador de servicios Ecuaweb para alojar su página web y como complemento de protección y seguridad cuenta con Cloudflare.

3.12.3. Gestores de Correo electrónico

3.12.3.1. Medidas de Seguridad.

En Stratos Asesores S.A.S se tiene configurado Microsoft 365 para el servicio de correo electrónico. Dentro de la configuración del servidor se cuenta con Sender Policy Framework (SPF) la cual autoriza que servidores o servicios están autorizados para enviar correos desde el dominio de Stratos Asesores. También disponen de DomainKeys Identified mail (DKIM) el cual firma digitalmente los correos para asegurar que no han sido modificados. Finalmente, tienen el Domain-based Message Authentication, Reporting, and Conformance (DMARC) que permite establecer una política para los correos que no superen las validaciones de autenticidad, pudiendo aplicar acciones de monitoreo, cuarentena o

rechazo, mejorando la seguridad contra el phishing, suplantación de identidad y falseo de direcciones de correo electrónico.

De igual manera, Stratos Asesores tiene activado el doble factor de autenticación (MFA) dentro de Microsoft 365 para proteger frente a accesos no autorizados a las cuentas corporativas de los empleados.

Stratos Asesores S.A.S tiene cuentas individuales y compartidas. Las cuentas compartidas son info@stratos.ec y administracion@stratos.ec que están destinadas a fines institucionales tales como la atención a clientes, proveedores, aspirantes o gestión interna.

3.12.3.2. Prestadores de Servicios.

Stratos Asesores S.A.S cuenta con el prestador de servicios Microsoft 365 para correo electrónico corporativo.

CAPÍTULO 4.

Plan Director de Seguridad

4.1. Descripción Plan Director de Seguridad y Beneficios para la Empresa

En el contexto actual, en el que las organizaciones están expuestas a múltiples riesgos, resulta indispensable contar con herramientas que permitan anticiparse y actuar de manera organizada frente a posibles amenazas. En este sentido, el Plan Director de Seguridad (PDS) se establece como un instrumento de planificación que guía la gestión de la seguridad dentro de una organización, permitiendo identificar, organizar y priorizar un conjunto de iniciativas (acciones o mini proyectos) orientadas a reducir los riesgos hasta niveles aceptables, a partir de una evaluación inicial.

A través del Plan Director de Seguridad (PDS) se definen lineamientos y medidas alineadas con las necesidades específicas de la organización, basadas en el análisis integral de vulnerabilidades, amenazas y riesgos. Asimismo, adopta un enfoque transversal, ya que integra medidas de seguridad física y lógica sobre la infraestructura tecnológica, el manejo seguro de la información, la protección del personal y la continuidad de las operaciones, fomentando la integración de la seguridad y los procesos habituales de trabajo.

La implementación de un Plan Director de Seguridad aporta beneficios como la mejora de la capacidad de prevención y respuesta ante incidentes, la definición de responsables y plazos de ejecución, y el fortalecimiento de una cultura de seguridad basada en buenas prácticas. De igual forma, facilita la toma de decisiones al establecer

un plan de acción con prioridades definidas y mecanismos de seguimiento, contribuyendo a la estabilidad y sostenibilidad de la organización.

En el caso de Stratos Asesores S.A.S., la operación diaria depende de forma crítica de los equipos corporativos, las herramientas de Microsoft 365, correo corporativo para la comunicación y entrega de productos y la conectividad a Internet. En consecuencia, el Plan Director de Seguridad permitirá reducir la probabilidad e impacto de incidentes sobre estos activos críticos mediante controles de acceso y permisos, orden y control documental, respaldo y recuperación, y buenas prácticas de uso. Con el fin de reducir el riesgo de interrupciones y de afectación reputacional por falles en entrega o manejo de información.

4.2. Checklist PDS

El checklist del Plan Director de Seguridad constituye una herramienta inicial de diagnóstico que permite verificar, de manera sintética, si la organización dispone de los elementos mínimos necesarios para planificar e implementar un Plan Director de Seguridad. Su propósito es establecer un punto de partida respecto al nivel de preparación de la organización, identificando los aspectos ya abordados y aquellos que requieren desarrollo para completar el ciclo del Plan Director de Seguridad.

En Stratos Asesores S.A.S., este instrumento se utiliza para confirmar la realización del análisis de la situación actual y la alineación del Plan Director de Seguridad con la estrategia organizacional. Asimismo, permite reconocer actividades que se ejecutarán en fases posteriores, tales como la definición de iniciativas, su clasificación y

priorización, la aprobación por parte de la dirección y el seguimiento de su ejecución. De esta manera, el checklist del Plan Director de Seguridad asegura la trazabilidad entre las fases descritas en el capítulo 4 y los entregables generados, proporcionando una visión clara del progreso del plan y de los pasos necesarios para su implantación.

Tabla 6

Checklist de PDS - Estado inicial

Nivel	Alcance	Control	
A	PRO	**Analizar la situación actual de la organización** Analizas detalladamente la situación actual de la organización para poder acometer un Plan Director de Seguridad.	☒
A	PRO	**Alinear el PDS con la estrategia de la organización** Tienes en cuenta la estrategia empresarial en su conjunto a la hora de diseñar el Plan Director de Seguridad.	☒
A	PRO	**Definir los proyectos a ejecutar** Estableces y defines en detalle las acciones concretas para alcanzar los niveles de seguridad deseados.	☐
A	PRO	**Clasificar y priorizar los proyectos** Agrupas y clasificas las acciones a ejecutar con el fin de priorizar aquellas que nos proporcionen mayores beneficios en relación a su coste.	☐
B	PRO	**Aprobar el PDS** Apruebas y publicas la versión definitiva del PDS.	☐
A	PRO	**Ejecución del PDS** Pones en marcha los proyectos acordados para alcanzar los objetivos de ciberseguridad definidos.	☐
A	PRO	**Certificación en seguridad** Consideras la implantación de un proceso de certificación que acredite el sistema de gestión de la seguridad de tu organización.	☐

4.2.1. Análisis de la Situación Actual de la Organización

En el contexto actual, Stratos Asesores S.A.S. no cuenta con un Plan Director de Seguridad formalmente establecido. Sin embargo, la organización sí dispone de lineamientos y controles base a través del Manual de Políticas de Seguridad de la Información la cual define roles y responsabilidades, así como políticas relacionadas con el uso de correo electrónico, contraseñas seguras, control de accesos y respaldos de información, seguridad física, gestión de riesgos, privacidad y continuidad.

En cuanto al entorno tecnológico la operación de organización se apoya principalmente en equipos corporativos, herramientas Microsoft 365 (OneDrive) como repositorio documental, correo corporativo como canal formal de comunicación y entrega, Teams como herramienta de coordinación y reuniones. El acceso a estas plataformas cuenta con autenticación multifactor (MFA) y a nivel de estaciones de trabajo, se dispone de antivirus ESET Endpoint Security. Los entregables, papeles de trabajo y documentación asociada a cliente, empleados y terceros se gestionan en OneDrive, y remiten al cliente mediante correo corporativo, por lo que la disponibilidad de Internet y los controles de gestión documental, permisos, control de versiones y prácticas de seguridad de envió resultan críticos para la continuidad del servicio.

Adicionalmente, la organización mantiene un sitio web corporativo con formulario de contacto; no obstante, el hosting y las modificaciones de diseño dependen de un proveedor externo (proveedor de internet), lo que introduce una dependencia de

terceros respecto a disponibilidad, tiempos de respuesta y administración del servicio. Esta condición refuerza la necesidad de definir controles mínimos de continuidad y gobernanza del servicio web dentro del Plan Director de Seguridad.

En síntesis, Stratos Asesores S.A.S. cuenta con controles iniciales y políticas formalizadas, pero requiere un Plan Director de Seguridad para integrar, ordenar y calendarizar dichas prácticas mediante una cartera de iniciativas priorizadas, con responsables, plazos, evidencias y revisiones periódicas. En coherencia con el enfoque del Plan Director de Seguridad, esta sección funciona como punto de partida para la verificación de controles (4.2) y el inventario de activos (4.3), los cuales permitirán sustentar el análisis de riesgos y la priorización de iniciativas en los apartados posteriores.

4.2.2. Plan Estratégico en Materia Tecnológica

En el caso específico de Stratos Asesores S.A.S., organización con dos años de trayectoria y un equipo de 17 colaboradores, la operación no depende de un sistema transaccional complejo; sin embargo, sí depende de forma crítica de sus equipos corporativos, la conectividad a Internet y de Microsoft 365 (OneDrive, correo corporativo y Teams). Adicionalmente, el área de Precios de Transferencia utiliza el sistema Stratos Rate Company, una herramienta basada en Inteligencia Artificial (IA) que apoya el análisis técnico al comparar clientes con organizaciones de industrias que cotizan en bolsa, aplicando criterios de comparabilidad y datos de Standard & Poor’s,

y al analizar bases de datos y documentos PDF para identificar actividades, productos, servicios, clientes y estimar el grado de comparabilidad.

En consecuencia, el plan estratégico tecnológico para Stratos Asesores S.A.S. debe enfocarse en fortalecer la infraestructura tecnológica existente, de manera que se asegure la confidencialidad, integridad y disponibilidad de la información, y se mantenga la continuidad operativa de los servicios. A partir de estos criterios, se proponen las siguientes acciones:

- Evaluación y diagnóstico de la infraestructura tecnológica: realizar un inventario de activos tecnológicos (físicos y lógicos), definiendo responsables y criticidad, para identificar vulnerabilidades, niveles de desactualización y necesidades de mejora.
- Gestión de accesos e identidad: fortalecer la gestión de accesos sobre Microsoft 365 y equipos corporativos, mediante el principio de mínimo privilegio, control de permisos por cliente y proyecto en OneDrive, y autenticación robusta (contraseñas seguras con renovación periódica, conforme a políticas internas).
- Mejora continua y seguimiento: establecer un seguimiento continuo del entorno tecnológico a través de revisiones periódicas y la actualización de las medidas implementadas (controles, accesos, respaldos y buenas prácticas), con el fin de adaptarse a cambios, riesgos y nuevas necesidades organizacionales.

- Protección del endpoint y prevención de malware: mantener y fortalecer la protección de los equipos corporativos mediante el uso de antivirus corporativo (ESET Endpoint Security), asegurando su correcta configuración, actualización y monitoreo; complementar con una gestión sistemática de parches y controles mínimos de seguridad en estaciones de trabajo, con el fin de reducir el riesgo de incidentes que afecten la operación o la integridad de la información.
- Respaldo, recuperación y continuidad operativa: formalizar y validar las estrategias de respaldo y recuperación existentes, asegurando que la información crítica se almacene en repositorios corporativos (OneDrive) y, de forma complementaria, en un NAS (Almacenamiento Conectado a la Red); definir procedimientos de restauración ante incidentes y realizar revisiones y pruebas periódicas para garantizar la disponibilidad de la información y la continuidad de las operaciones.
- Presencia digital (sitio web y formulario de contacto): fortalecer el control y la continuidad de la página web corporativa, considerando la dependencia actual del proveedor de internet para el hosting y cambios de diseño. Para ello, se establecerán medidas básicas de administración, respaldo y actualización del sitio, así como lineamientos mínimos para el manejo de la información recibida mediante el formulario de contacto, reduciendo la dependencia del proveedor actual.

- Gestión de herramientas especializadas del negocio: asegurar que las herramientas de soporte al trabajo técnico (incluida la utilizada por el área de Precios de Transferencia) cuenten con controles mínimos de acceso y uso, y que sus resultados se gestionen y resguarden conforme a los lineamientos corporativos de seguridad y confidencialidad.

Este plan estratégico constituye el marco de referencia para definir y priorizar las iniciativas del PDS en los apartados posteriores, asegurando que las acciones propuestas respondan a los riesgos identificados y a las necesidades reales de la organización.

4.3.Verificación de Controles

La verificación de controles constituye una etapa esencial dentro del Plan Director de Seguridad, ya que permite conocer de forma estructurada el estado actual de implementación de los controles y prácticas de seguridad en la organización. A partir de esta revisión se identifican fortalezas, brechas y oportunidades de mejora, lo que facilita orientar la toma de decisiones y sustentar la priorización de iniciativas de seguridad.

En Stratos Asesores S.A.S., esta verificación se realiza mediante un checklist de controles que evalúa aspectos relacionados con organización y gobernanza, seguridad lógica, gestión de accesos, protección de equipos, respaldo y continuidad, seguridad física, uso de herramientas corporativas y concientización. Esta revisión se apoya, además, en los lineamientos ya definidos en el Manual de Políticas de Seguridad de la

Información de la organización, el cual establece políticas y responsabilidades aplicables a los activos tecnológicos y al manejo de la información.

Para cada control se registra si se encuentra implementado, y cuando la respuesta es afirmativa se documenta una descripción breve, el responsable y la fecha de última actualización o referencia; cuando la respuesta es negativa, se considera como brecha a ser tratada mediante las iniciativas del Plan Director de Seguridad.

Los resultados de esta verificación se utilizarán como insumo directo para el inventario de activos, el análisis de riesgos y la clasificación y priorización de acciones (mini-proyectos) del Plan Director de Seguridad, asegurando coherencia entre la situación inicial, los riesgos identificados y las medidas propuestas.

Tabla 7

Verificación de controles

Identificador	Aspecto a evaluar	Respuesta	Responsable	Fecha
ID_0001	¿La organización ha definido un documento con la política de seguridad de la información?	Sí, se cuenta con un Manual de políticas de seguridad de la información.	Mayra C. (responsable de Seguridad de la información)	Marzo 2025
ID_0002	¿La política de seguridad de la información se revisa periódicamente?	Sí, se la revisa cada año y se la actualiza cuando sea necesario.	Mayra C. (responsable de Seguridad de la información)	Marzo 2025
ID_0003	¿Se han definido las responsabilidades en materia de seguridad de la información?	Sí, se han definido los roles y sus responsabilidades y en caso de incumplimiento se aplicarán sanciones.	Oswaldo B. y Karilin A. (Dirección General) / Mayra C. (responsable de Seguridad de la información) / Empleados	Mayo 2025
ID_0004	¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?	No		

(Continua)

(Continuación)

Identificador	Aspecto a evaluar	Respuesta	Responsable	Fecha
ID_0005	¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la organización? (Confidencialidad, propiedad intelectual, etc.).	Sí, la organización incorpora en sus contratos con terceras cláusulas orientadas a proteger la información, incluyendo confidencialidad, privacidad y propiedad intelectual.	Hugo R.H.L / Mayra C. (Gerencia de Riesgos) / Mayra B. (Gerencia de Precios de Transferencia) / Paola B. (Coordinadora Administrativa)	Enero 2025
ID_0006	¿Se dispone de un inventario de activos?	Sí, la organización dispone de un inventario de activos y el área administrativa se encarga de regularizar anualmente los activos.	Paola B. (Coordinadora Administrativa) / Dario U. (Proveedor de servicios de TI)	Enero 2025
ID_0007	¿Se ha definido quien es el responsable de los activos?	Sí, cada empleado es responsable del activo asignado para sus funciones en la organización.	Paola B. (Coordinadora Administrativa)	Enero 2025
ID_0008	¿Se comprueban las referencias de todos los candidatos a empleo?	Sí, la comprobación de referencias y validación de candidatos es realizada por el área administrativa.	Paola B. (Coordinadora Administrativa)	Cada que se abre una plaza de trabajo (14-04-2026)

(Continua)

(Continuación)

Identificador	Aspecto a evaluar	Respuesta	Responsable	Fecha
ID_0009	¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?	Sí, la organización ha definido las áreas seguras con controles de acceso con tarjeta y PIN de seguridad.	Mayra C. (responsable de Seguridad de la información)	Marzo 2025
ID_0010	¿Los equipos TIC críticos de la organización están ubicados en salas de CPD?	No		
ID_0011	¿Se han definido y documentado los procedimientos operacionales TIC?	No		
ID_0012	¿Las copias de seguridad se realizan regularmente de acuerdo con la política de backup establecida?	Sí, el proveedor externo de TI es el encargado de realizar el respaldo de la información crítica de la organización.	Dario U. (Proveedor externo de TI)	Marzo 2025
ID_0013	¿Se verifica regularmente la correcta realización de las copias se seguridad?	Sí, el proveedor externo de TI es el encargado de revisar si los respaldos de información crítica se realizaron correctamente.	Dario U. (Proveedor externo de TI)	Marzo 2025
ID_0014	¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?	No		

(Continua)

(Continuación)

Identificador	Aspecto a evaluar	Respuesta	Responsable	Fecha
ID_0015	¿Se registran las actividades de los administradores y operadores de sistema?	No		
ID_0016	¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?	Sí, los accesos se otorgan según el perfil y rol autorizado, los usuarios no cuentan con permisos de administrador por defecto y cualquier privilegio adicional debe ser solicitado y aprobado previamente.	Dario U. (Proveedor externo de TI)	Marzo 2025
ID_0017	¿Se ha definido, documentado e implantado un proceso formal para la asignación de contraseñas?	Sí, se han establecido los requisitos mínimos de contraseñas, cambio periódico, bloqueo por intentos fallidos, uso personal e intransferible para la plataforma de Microsoft Office 365.	Mayra C. (responsable de Seguridad de la información)	Marzo 2025
ID_0018	¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?	Sí, los empleados deben seguir los requisitos mínimos de contraseñas para la plataforma de Microsoft Office 365.	Mayra C. (responsable de Seguridad de la información)	Marzo 2025
ID_0019	¿Los usuarios se aseguran de proteger los equipos desatendidos? (¿Ej. bloqueando o cerrando la sesión?	Sí, las sesiones deben cerrarse automáticamente tras 15 minutos de inactividad.	Mayra C. (responsable de Seguridad de la información)	Marzo 2025

(Continua)

(Continuación)

Identificador	Aspecto a evaluar	Respuesta	Responsable	Fecha
ID_0020	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?	Sí, el usuario y contraseña asignados para el acceso a los servicios tecnológicos son de uso personal e intransferible. No hay uso de cuentas genéricas.	Dario U. (Proveedor externo de TI)	Marzo 2025
ID_0021	¿Se controla la instalación de software en sistemas en producción?	Sí, previo a la puesta en operación, se deben validar los requisitos de seguridad, buenas prácticas, aspectos técnicos y metodologías formalizadas aplicables.	Oswaldo B. (responsable de TI)	Marzo 2025
ID_0022	¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	No		
ID_0023	¿Se ha definido, documentado e implantado un proceso formal para la gestión de los incidentes de seguridad?	No		
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		

(Continua)

(Continuación)

Identificador	Aspecto a evaluar	Respuesta	Responsable	Fecha
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?	Sí, la a organización mantiene identificadas sus obligaciones legales y regulatorias, incluyendo las relacionadas con la Superintendencia de Compañías y el SRI.	Oswaldo B. (Socio de Asesoría de Riesgos)	Mayo 2024
ID_0028	¿Se han implementado procedimientos para asegurar el cumplimiento de los requisitos relevantes de carácter legal?	Sí, el cumplimiento de estos requisitos se gestiona mediante coordinación con el área legal y contabilidad externa, quienes controlan fechas, revisiones y obligaciones aplicables.	Oswaldo B. (Socio de Asesoría de Riesgos) / Paola B. (Coordinadora Administrativa) / Proveedor de servicios contables / HUGO R.H.L.	
ID_0029	¿Se han establecido e implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	No		
ID_0030	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?	No		

4.4. Inventario de Activos

El inventario de activos constituye un elemento fundamental del Plan Director de Seguridad, ya que permite identificar y documentar los activos tecnológicos que soportan la operación de la organización y sobre los cuales se aplicarán los controles de seguridad. Disponer de un inventario actualizado facilita determinar qué activos son más críticos, quiénes son sus responsables, dónde se encuentran y cuál es su función dentro de los procesos de la organización, estableciendo así una base objetiva para el análisis de riesgos.

En coherencia con las secciones anteriores (Checklist y Verificación de Controles), el inventario de activos permite vincular los controles existentes con los activos que protegen y, a partir de ello, identificar brechas y riesgos asociados. Para Stratos Asesores S.A.S., este inventario incluye activos físicos y lógicos tales como equipos corporativos, conectividad a Internet y red WiFi, plataformas corporativas (Microsoft 365: OneDrive, correo corporativo y Teams), herramientas de protección (antivirus ESET Endpoint Security), el NAS utilizado para respaldos y la presencia digital (sitio web y servicio de hosting).

La siguiente Tabla 8 representa el inventario inicial de activos tecnológicos de Stratos Asesores S.A.S., cuyo propósito es facilitar el control general de los activos administrados por la organización. Este registro identifica responsable, ubicación, tipo y nivel de criticidad, contribuyendo a una gestión ordenada y al seguimiento adecuado

de los activos. La información recopilada se emplea como base para el análisis de riesgos y la priorización de acciones del Plan Director de Seguridad.

Tabla 8

Inventarios de activos

Identificador	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_001	Laptops corporativas (17 equipos)	Equipos informáticos utilizados para la ejecución de actividades administrativas, análisis de información y prestación de servicios profesionales.	Empleados	Físico	Oficina	Sí
ID_002	OneDrive (Microsoft 365)	1. Plataforma de almacenamiento en la nube utilizada para la gestión, acceso y resguardo de documentos corporativos.	Proveedor de servicio de TI	Lógico	Nube	Sí
ID_003	Correo Outlook (Microsoft 365)	Sistema de correo electrónico corporativo utilizado para la comunicación interna y externa de la organización.	Proveedor de servicio de TI	Lógico	Nube	Sí
ID_004	Teams (Microsoft 365)	Herramienta de colaboración para mensajería, videollamadas y coordinación de actividades laborales.	Proveedor de servicio de TI	Lógico	Nube	No

(Continua)

(Continuación)

Identificador	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_005	ESET Endpoint Security	Software de seguridad informática destinado a la protección contra virus, malware y otras amenazas digitales.	Proveedor de servicio de TI	Lógico	Nube	No
ID_006	Celular corporativo	Dispositivo móvil asignado para la comunicación institucional y coordinación de actividades.	Coordinadora Administrativa	Físico	Oficina	No
ID_007	Sistema Contable Contifico	Sistema digital utilizado para la gestión de facturación electrónica y control contable de la organización.	Coordinadora Administrativa / Proveedor de servicios contables	Lógico	Web	No
ID_008	Página web	Plataforma digital que representa la presencia institucional de la organización en internet.	Megadatos S.A.	Lógico	Internet	No
ID_009	Amplificador Wifi Ubiquiti	Infraestructura de red inalámbrica que permite la conexión de dispositivos dentro de la organización para sus actividades la cual consta de 2 segmentaciones de red (empleados y visitantes).	Proveedor de servicio de TI	Físico	Oficina	Sí

(Continua)

(Continuación)

Identificador	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_010	Controlador Cloud Ubiquiti Udm-pro-max	Dispositivo que actúa como router, firewall y controlador central para administrar, segmentar y proteger la red corporativa.	Proveedor de servicio de TI	Físico	Oficina	Sí
ID_011	Software Stratos Rate Company	Sistema digital de comparación empresarial con IA	Gerente de Precios de Transferencia	Lógico	Nube	Sí
ID_012	Estación de Energía Bluetti AC70P	Equipo de respaldo eléctrico con capacidad de 1000 W / 864 Wh, utilizado para mantener temporalmente energizados equipos críticos ante cortes o variaciones del suministro eléctrico.	Coordinadora Administrativa	Físico	Oficina	No
ID_013	NAS Synology	Dispositivo de almacenamiento en red utilizado para respaldos de información de la organización.	Proveedor de servicio de TI	Físico	Oficina	No

4.4.1. Análisis de Riesgos (Inventario de Activos)

Con base en el inventario de activos tecnológicos presentado en el apartado 4.4, se procedió a realizar el análisis de riesgos utilizando la herramienta proporcionada por el docente. En primer lugar, los activos tecnológicos reales de Stratos Asesores S.A.S. fueron mapeados a la tipología de activos definida en el catálogo de la herramienta (por ejemplo: página web alojada por proveedor externo, ordenadores/servidor, conexión a Internet con WiFi, dispositivos móviles y herramientas en la nube), con el fin de mantener coherencia metodológica y trazabilidad entre inventario, amenazas y riesgos.

Tabla 9

Categorización de activos

Identificador	Activos de Stratos	Categoría
ID_001	Laptops corporativas (17 equipos)	Ordenador y algún servidor
ID_002	OneDrive (Microsoft 365)	Herramientas en la nube
ID_003	Outlook/Correo (Microsoft 365)	Herramientas en la nube
ID_004	Teams (Microsoft 365)	Herramientas en la nube
ID_005	ESET Endpoint Security	Ordenadores y algún servidor
ID_006	Celular Corporativo	Dispositivos móviles con datos y apps
ID_007	Contifico (contable)	Herramientas en la nube
ID_008	Página Web	Web alojada por tercero
ID_009	Ubiquiti AP (amplificador wifi)	Conexión a Internet con Wifi
ID_010	UDM Pro Max (firewall, switch, controlador central)	Conexión a Internet con Wifi
ID_011	Stratos rate company	Herramientas en la nube

ID_012	Bluetti AC70P	Conexión a Internet con Wifi (u Ordenadores)
ID_013	NAS Synology (backup)	Ordenadores y algún servidor

Posteriormente, se aplicó el cruce Amenaza–Activo, evaluando uno a uno los escenarios posibles mediante el catálogo de amenazas definido (por ejemplo: fuga de información, introducción de falsa información, difusión de software dañino, errores de configuración, entre otras). Para cada combinación se determinó si la amenaza era aplicable al activo mediante una decisión "Sí/No", considerando el contexto operativo de la organización.

Una vez completado este cruce, se ejecutó la función "Mostrar Activos", mediante la cual la herramienta generó automáticamente el listado de riesgos potenciales, desplegando únicamente aquellas combinaciones Activo–Amenaza que habían sido marcadas como aplicables (Sí). De esta forma, se obtuvo un conjunto depurado de escenarios a valorar, evitando analizar amenazas que no guardan relación con los activos identificados.

Tabla 10

Cruce amenaza-activo

ID Activo	Nombre del activo	Amenazas aplicables (SI) – resumen	Observación
ID_001	Laptops corporativas (17)	Fuga de información; Introducción de falsa información; Alteración; Corrupción; Difusión de software	Activo crítico; riesgo principal ligado a manejo de

		dañino; Acceso no autorizado; Errores de configuración; Robo	información y malware
ID_002	OneDrive (Microsoft 365)	Fuga; Introducción de falsa info; Alteración; Corrupción; Destrucción; Acceso no autorizado; Errores de usuarios/admin	Repositorio crítico; control por permisos y versiones
ID_010	WiFi (Ubiquiti AP + UDM)	Difusión de software dañino; Errores de configuración; Denegación de servicio; Fallo de servicios de comunicaciones	Conectividad crítica para operar Microsoft 365

A continuación, cada riesgo potencial fue cuantificado asignando valores de Probabilidad (P) e Impacto (I), conforme a la escala cualitativa definida por la metodología (1 a 3). En la Probabilidad, se utilizó la siguiente referencia: Bajo (1) cuando la amenaza podría materializarse como máximo una vez al año, Medio (2) cuando podría materializarse como máximo una vez al mes, y Alto (3) cuando podría materializarse como máximo una vez a la semana. De manera equivalente, para el Impacto, se consideró Bajo (1) cuando el daño derivado no tiene consecuencias relevantes para la organización, Medio (2) cuando el daño tiene consecuencias reseñables, y Alto (3) cuando el daño tiene consecuencias graves reseñables para la organización.

Finalmente, la herramienta calculó el nivel de riesgo mediante la multiplicación de ambos criterios, empleando la fórmula $R = P \times I$, generando un valor cuantitativo por cada combinación Activo–Amenaza. Este resultado constituye la base para el apartado

4.4, donde se consolidan los riesgos priorizados; de acuerdo con el umbral definido en este proyecto, se consideran para tratamiento y posterior priorización aquellas situaciones cuyo valor sea mayor a 4, las cuales se convierten en iniciativas dentro de la matriz de clasificación y priorización del PDS (apartado 4.5).

Tabla 11

Resumen del análisis de riesgos por activo (PxI)

Activo (catálogo docente)	N° amenazas evaluadas	Riesgo máx. (P×I)	Riesgos >4 (sí/no)	Amenazas principales (Top 3)
Web alojada por proveedor	10	4	No	Fuga información (2), Falsa información (4), Destrucción de información (3)
Ordenadores/NAS (backup)	12	6	Sí	Fuga información (6), Falsa información (6), Alteración de la información (6)
Internet con WiFi	8	3	No	Fuga información (3), Destrucción de información (3)
Herramientas nube (Microsoft 365)	10	6	Sí	Fuga información (6), Falsa información (6), Alteración de información (6)
Móvil corporativo	6	4	No	Fuga información (4), Falsa información (4)

4.5. Análisis de Riesgos

El análisis de riesgos constituye la fase del Plan Director de Seguridad (PDS) en la que se cuantifican y priorizan los escenarios identificados en el cruce Activo–Amenaza desarrollado en el apartado 4.3.1. Su finalidad es determinar, con base en criterios

objetivos, cuáles riesgos requieren tratamiento inmediato y cuáles pueden ser aceptados o gestionados mediante controles existentes, asegurando que las iniciativas del PDS se enfoquen en los aspectos de mayor impacto para la organización.

Para ello, se asigna a cada escenario una valoración de Probabilidad (P) e Impacto (I), según una escala definida por la metodología aplicada, y se calcula el nivel de riesgo mediante la fórmula $R = P \times I$. A partir de los resultados obtenidos, y conforme al umbral establecido para este proyecto, se consideran como riesgos prioritarios aquellos cuyo valor es mayor a 4 ($R > 4$), los cuales se trasladan al apartado 4.5 para su clasificación y priorización en forma de iniciativas, responsables, plazos y revisiones.

A continuación, se presentan los resultados del análisis de riesgos realizado a partir del cruce Activo–Amenaza desarrollado en el apartado 4.3.1. Para cada escenario identificado se asignó un valor de Probabilidad (P) e Impacto (I) en escala de 1 a 3, conforme a los criterios definidos por la metodología aplicada. La probabilidad se valoró como Bajo (1) cuando la amenaza podría materializarse como máximo una vez al año, Medio (2) cuando podría materializarse como máximo una vez al mes y Alto (3) cuando podría materializarse como máximo una vez a la semana. De forma equivalente, el impacto se valoró como Bajo (1) cuando el daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización, Medio (2) cuando el daño tiene consecuencias reseñables, y Alto (3) cuando el daño tiene consecuencias graves reseñables para la organización.

El nivel de riesgo se calculó mediante la fórmula R = P × I, obteniendo un valor cuantitativo para cada combinación Activo–Amenaza. Con base en los resultados, y de acuerdo con el criterio establecido para este Plan Director de Seguridad, se consideran riesgos prioritarios aquellos cuyo valor sea mayor a 4 (R > 4), dado que representan escenarios con probabilidad e impacto relevantes que requieren tratamiento mediante iniciativas específicas.

Tabla 12

Riesgos priorizados (R > 4)

Activo	Amenaza	Probabilidad	Impacto	Riesgo
Ordenadores e incluso algún servidor (web, correo electrónico)	Daños por agua	Medio (2)	Alto (3)	6
Ordenadores e incluso algún servidor (web, correo electrónico)	Fuga de información	Medio (2)	Alto (3)	6
Ordenadores e incluso algún servidor (web, correo electrónico)	Introducción de falsa información	Medio (2)	Alto (3)	6
Ordenadores e incluso algún servidor (web, correo electrónico)	Alteración de la información	Medio (2)	Alto (3)	6
Ordenadores e incluso algún servidor (web, correo electrónico)	Corrupción de la información	Alto (3)	Medio (2)	6
Conexión a Internet con wifi	Difusión de software dañino	Medio (2)	Alto (3)	6
Conexión a Internet con wifi	Errores de configuración	Medio (2)	Alto (3)	6
Herramientas para organizaciones en la nube	Fuga de información	Medio (2)	Alto (3)	6
Herramientas para organizaciones en la nube	Introducción de falsa información	Medio (2)	Alto (3)	6

Herramientas para organizaciones en la nube	Alteración de la información	Medio (2)	Alto (3)	6
Herramientas para organizaciones en la nube	Corrupción de la información	Medio (2)	Alto (3)	6
Herramientas para organizaciones en la nube	Destrucción de información	Medio (2)	Alto (3)	6

Nota. En el contexto de Stratos Asesores S.A.S., el término «servidor» corresponde a un NAS Synology utilizado como respaldo de información, y las herramientas para organizaciones en la nube incluyen Microsoft 365 (OneDrive, correo corporativo y Teams), entre otras herramientas de apoyo al negocio.

A partir de los riesgos priorizados (R > 4), se evidencia que los escenarios de mayor severidad se concentran principalmente en tres grupos de activos: (i) ordenadores y activos asociados al procesamiento de información, (ii) conectividad a Internet con WiFi, y (iii) herramientas en la nube. En el primer grupo destacan amenazas relacionadas con fuga, alteración, introducción de falsa información y corrupción de la información, así como daños por agua, lo que refleja la criticidad del entorno de trabajo y del manejo documental para la operación. En el segundo grupo, los riesgos priorizados corresponden a difusión de software dañino y errores de configuración, evidenciando que la red es un punto de entrada capaz de afectar múltiples servicios. Finalmente, en el grupo de herramientas en la nube, se presentan riesgos de fuga, destrucción, corrupción, alteración e introducción de información no validada, lo cual impacta directamente la confidencialidad e integridad de los entregables.

En consecuencia, estos riesgos se convierten en insumo directo para el apartado 4.6, donde se establecen las iniciativas de tratamiento, responsables, plazos, costos y

frecuencia de revisión, con el objetivo de reducir el nivel de riesgo a valores aceptables.

4.6. Clasificación y Priorización

La clasificación y priorización de iniciativas tiene como finalidad establecer qué acciones de seguridad deben ejecutarse con mayor urgencia en Stratos Asesores S.A.S. Para ello, se toma como base el resultado del análisis de riesgos presentado en el apartado 4.5, considerando únicamente aquellos escenarios cuyo nivel de riesgo supera el umbral definido ($R > 4$). En este sentido, las iniciativas propuestas se formulan como medidas concretas (organizativas y/o técnicas), asignando responsables, costos referenciales, fechas objetivo y frecuencias de revisión, con el fin de asegurar un seguimiento efectivo dentro del Plan Director de Seguridad.

Tabla 13

Registro, clasificación y priorización de iniciativas (basada en riesgos R>4)

Identificador	Título amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión	Prioridad
IN_001	Daños por agua (ordenadores/servidor)	Definir directrices para evitar líquidos cerca de laptops/NAS; ubicar el NAS en zona elevada/segura, lejos de filtraciones o derrames; señalización básica.	Área Administrativa / Responsable de Seguridad	Organizativa	USD 30	Junio 2026	Semestral	Alta
IN_002	Fuga de información (ordenadores/servidor)	Reforzar accesos en laptops (bloqueo automático, cuentas individuales, contraseñas seguras) y restringir uso de dispositivos externos; acceso al NAS solo a responsables autorizados, sin cuentas compartidas.	Responsable de Seguridad / Proveedor de servicio de TI	Técnica	USD 108	Junio 2026	Trimestral	Alta

(Continua)

(Continuación)

Identificador	Título amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión	Prioridad
IN_003	Introducción de falsa información (ordenadores/servidor)	Estandarizar plantillas y papeles de trabajo; definir responsables de edición y un punto de control (revisión por pares) antes de declarar un documento como final.	Responsable de Seguridad / Gerencias de área	Organizativa	USD 0	Junio 2026	Trimestral	Alta
IN_004	Alteración de la información (ordenadores/servidor)	Asegurar control de versiones en OneDrive para documentos críticos; limitar permisos de edición; mantener trazabilidad de cambios. Para respaldos en NAS, restringir permisos de borrado/modificación de carpetas de backup.	Responsable de Seguridad / Gerencias de área	Técnica	USD 0	Junio 2026	Trimestral	Alta

(Continua)

(Continuación)

Identificador	Título amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión	Prioridad
IN_005	Corrupción de la información (ordenadores/servidor)	Verificación mensual de estado de copias (sin errores) y prueba trimestral de restauración de un conjunto de archivos, para confirmar recuperabilidad.	Responsable de Seguridad / Proveedor de servicio de TI	Técnica	USD 36	Julio 2026	Trimestral	Alta
IN_006	Difusión de software dañino (conexión a Internet con WiFi)	Revisión mensual de seguridad WiFi (WPA2/WPA3, clave robusta, firmware, dispositivos conectados); separación de red de invitados si aplica; reforzar reglas de navegación segura.	Proveedor de servicio de TI / Responsable de Seguridad	Técnica	USD 50	Junio 2026	Mensual	Alta

(Continua)

(Continuación)

Identificador	Título amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión	Prioridad
IN_007	Errores de configuración (conexión a Internet con WiFi)	Verificar y documentar configuración del amplificador WiFi y controlador (contraseñas, segmentación, permisos, parámetros de seguridad); mantener respaldo de configuración.	Proveedor de servicio de TI	Técnica	USD 50	Junio 2026	Trimestral	Alta
IN_008	Fuga de información (herramientas en la nube)	Revisión mensual de accesos/permisos en OneDrive por cliente/proyecto; mantener repositorio de carga del cliente con permisos mínimos; evitar enlaces públicos y dejar evidencia de cambios.	Responsable de Seguridad / Gerencias de área	Técnica	USD 0	Junio 2026	Mensual	Alta
IN_009	Introducción de falsa información (herramientas en la nube)	Definir responsables para validar y aprobar la documentación recibida del cliente antes de su uso; mantener carpeta 'Validado/Final' con control de cambios.	Responsable de Seguridad / Gerencias de área	Organizativa	USD 0	Junio 2026	Trimestral	Alta

(Continua)

(Continuación)

Identificador	Título amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión	Prioridad
IN_010	Alteración de la información (herramientas en la nube)	Activar y revisar control de versiones en documentos críticos; limitar permisos de edición; conservar trazabilidad de cambios y responsables.	Responsable de Seguridad / Proveedor de servicio de TI	Técnica	USD 54	Junio 2026	Mensual	Alta
IN_011	Corrupción de la información (herramientas en la nube)	Asegurar que la información crítica se gestione en repositorios corporativos (OneDrive) y validar periódicamente la recuperabilidad: revisión mensual de incidencias y prueba trimestral de restauración/recuperación.	Responsable de Seguridad / Proveedor de servicio de TI	Técnica	USD 54	Julio 2026	Trimestral	Alta
IN_012	Destrucción de información (herramientas en la nube)	Configurar conservación/recuperación (papelera/retención) y control de eliminación; revisión mensual de permisos de borrado para evitar eliminaciones no autorizadas o accidentales.	Responsable de Seguridad / Proveedor de servicio de TI	Técnica	USD 36	Julio 2026	Mensual	Alta

Las iniciativas se agrupan en tres aspectos relacionados con los ordenadores o servidores, la conexión a internet con WiFi y las herramientas en la nube. Estos activos sostienen buena parte del trabajo diario en Stratos Asesores S.A.S., por lo que una falla podría afectar la continuidad de las actividades y el manejo seguro de la información.

En los ordenadores o servidor, las medidas buscan reducir riesgos físicos y digitales. Por eso se consideran acciones frente a daños por agua, fuga de información, alteración de archivos, corrupción de datos e ingreso de información incorrecta. En términos prácticos, esto implica cuidar mejor la ubicación de los equipos, controlar accesos, revisar permisos, mantener versiones de documentos y comprobar que la información pueda recuperarse si ocurre algún incidente.

En la conexión a Internet con WiFi, las acciones apuntan a fortalecer la configuración de la red y reducir la exposición a software dañino. Este punto es importante porque la red permite acceder al correo, a las plataformas en la nube y a los sistemas que usa la organización. Si la configuración no se revisa o existen accesos no controlados, el riesgo puede afectar a varios servicios al mismo tiempo.

En las herramientas en la nube, las iniciativas se enfocan en proteger la información frente a fuga, alteración, corrupción, destrucción o carga de datos no validados. Como Stratos utiliza estas plataformas para almacenar, compartir y gestionar documentos de trabajo, es necesario revisar permisos, controlar versiones, definir responsables y mantener respaldos útiles. La matriz permite dejar cada medida organizada con un

responsable, un coste estimado, una fecha de aplicación y una frecuencia de revisión, lo que facilita el seguimiento de las acciones propuestas.

Como parte del seguimiento de las iniciativas planteadas en la matriz, se considera necesario incorporar un plan de capacitación, sensibilización y comunicación sobre seguridad de la información. Este plan contempla capacitaciones breves al personal interno y externo que colabore con Stratos, recordatorios periódicos sobre buenas prácticas, comunicaciones internas sobre riesgos frecuentes y orientación básica para nuevos usuarios que accedan a equipos, red WiFi, herramientas en la nube, documentos de trabajo, cuentas, contraseñas y permisos de acceso.

La aplicación de los controles no depende únicamente de configuraciones técnicas, sino también de la forma en que las personas manejan la información en sus actividades diarias. Por ello, estas actividades abordarán temas como manejo seguro de documentos, prevención de correos sospechosos, cuidado de equipos, uso responsable de contraseñas, validación de información antes de compartirla y reporte oportuno de incidentes. Con esto se busca reducir errores humanos y fortalecer una cultura de seguridad acorde con las necesidades de la organización.

4.7. Checklist PDS

En esta sección se presenta el checklist final del Plan Director de Seguridad, con el propósito de evidenciar el grado de cumplimiento de las fases previstas, comparando el estado inicial con el resultado obtenido tras el desarrollo del Capítulo 4. Este checklist permite verificar que el Plan Director de Seguridad cuenta con los elementos

mínimos: análisis de situación actual, alineación con la estrategia tecnológica, definición de los proyectos a ejecutar y clasificación y priorización de los proyectos de la organización.

Tabla 14

Checklist PDS resultado final

Nivel	Alcance	Control	Resultado final	Evidencia / Referencia en el documento
A	PRO	Analizar la situación actual de la organización	☒	4.1.1 (Análisis situación actual) + Manual de Políticas de Seguridad de la Información (referencia interna)
A	PRO	Alinear el PDS con la estrategia de la organización	☒	4.1.2 (Plan estratégico tecnológico) + alineación a activos críticos (Microsoft 365/OneDrive, correo, WiFi, ESET, NAS, web)
A	PRO	Verificación de controles	☒	4.3 Verificación de controles + Tabla 7 (Verificación de valores de seguridad)
A	PRO	Inventario de activos tecnológicos	☒	4.4 Inventario de Activos + Tabla 8 (Inventario de activos)
A	PRO	Categorización de activos	☒	4.4.1 Análisis de Riesgos (Inventario de Activos + Tabla 9 (Categorización de activos)
A	PRO	Cruce amenaza-activo	☒	4.4.1 Análisis de Riesgos (Inventario de Activos + Tabla 10 (Cruce amenaza-activo)
A	PRO	Riesgo por activo (PxI)	☒	4.4.1 Análisis de Riesgos (Inventario de Activos + Tabla 11 (Riesgo por activo PxI)
A	PRO	Análisis de riesgos (riesgos priorizados R>4)	☒	4.5 Análisis de riesgos + Tabla 12 (Riesgos priorizados R>4)
A	PRO	Definir los proyectos a ejecutar	☒	4.6 Clasificación y Priorización + Tabla 13 (Registro,

				clasificación y priorización de iniciativas – basada en riesgos R>4)
A	PRO	Clasificar y priorizar los proyectos	☒	4.5 Análisis de Riesgos + Tabla 12 (Riesgos priorizados R>4) 4.6 Clasificación y Priorización + Tabla 13 (Registro, clasificación y priorización de iniciativas – basada en riesgos R>4))
B	PRO	Aprobar el PDS	☐	Pendiente: Acta de aprobación / validación por Dirección (socios y gerencias)
A	PRO	Ejecución del PDS	☐	Pendiente: Plan de implementación y seguimiento (cronograma) + evidencias de ejecución (capturas, reportes, actas)
B	PRO	Revisión periódica del PDS y actualización	☒	4.6 Clasificación y priorización + Tabla 13 (Registro, clasificación y priorización de iniciativas basadas en riesgos R>4)
A	PRO	Certificación en seguridad	☐	Futuro: Evaluación de certificación (según decisión de Dirección y recursos)

Con base en la comparación entre el checklist inicial y el checklist final, se evidencia un avance significativo en la estructuración del Plan Director de Seguridad (PDS), pasando de contar únicamente con el análisis de la situación actual y la alineación estratégica, a disponer de un PDS definido y documentado en sus componentes principales. En particular, el documento consolida tanto los controles del checklist inicial como los controles adicionales incorporados para evidenciar el recorrido integral del PDS: desde la verificación de controles e inventarios de activos

tecnológicos, hasta el análisis de riesgos (cruce amenaza-activo, valoración PxI y riesgos priorizados R>4) y la definición de iniciativas con responsables, costos, fechas y frecuencia de revisión.

Las actividades que permanecen pendientes corresponden a la aprobación formal por la Dirección y a la implantación de las iniciativas priorizadas, las cuales dependen de la decisión organizacional y de la asignación de recursos. En consecuencia, una vez aprobadas, dichas iniciativas deberán ejecutarse y monitorearse conforme a la planificación establecida en la sección 4.6 (Tabla 13) y a las revisiones definidas, con el fin de fortalecer de manera progresiva la seguridad de la información, la continuidad operativa y la capacidad de respuesta ante incidentes, asegurando la mejora continua del PDS. Y de igual forma, la evaluación futura de una certificación en seguridad sujeta a la decisión organizacional, recursos y madurez del sistema.

CAPÍTULO 5.

Diseño de un Sistema de Gestión de Riesgos Basado en la ISO 31000:2018 para Stratos Asesores S.A.S.

Organización: Stratos Asesores S.A.S.

Ubicación: Quito- Ecuador

En este capítulo se presenta el diseño del Sistema de Gestión de Riesgos (SGR) basado en ISO 31000:2018, adaptado a la realidad, tamaño y contexto operativo de Stratos Asesores S.A.S.

5.1. Objeto y Campo de Aplicación

La siguiente propuesta tiene como objetivo principal diseñar un Sistema de Gestión de Riesgos (SGR) para la organización Stratos Asesores S.A.S., basado en las directrices establecidas en la norma internacional ISO 31000:2018. Actualmente, la organización no cuenta con un SGR formal, por lo que la gestión de riesgos se realiza de manera no estructurada. En un contexto de prestación de servicios por proyectos, este escenario puede traducirse en retrasos, retrabajos, sobrecarga operativa y riesgos reputacionales, especialmente cuando se gestionan múltiples entregables y se maneja información sensible de clientes. En consecuencia, resulta necesario establecer un marco y un proceso sistemático que permita identificar, evaluar y tratar riesgos con criterios homogéneos, responsables definidos y seguimiento periódico.

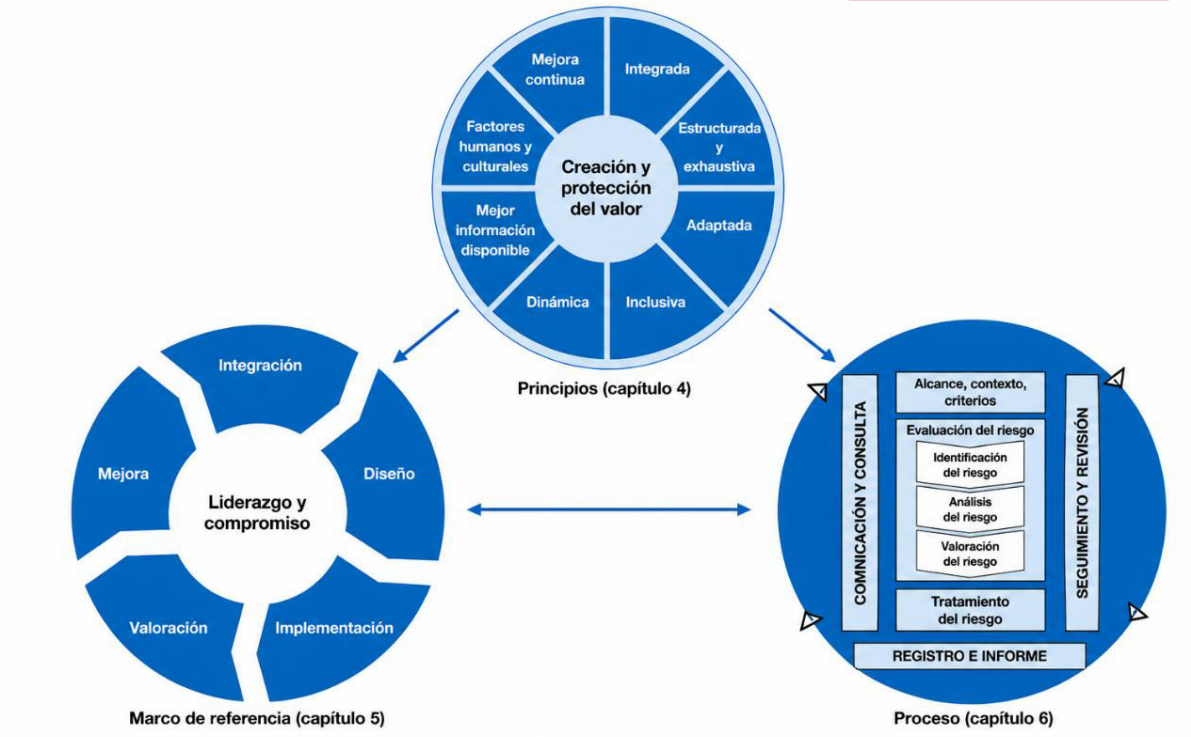
La finalidad del sistema es asegurar que la gestión del riesgo actúe como un soporte estratégico para el cumplimiento de los objetivos de Stratos Asesores S.A.S. Al alinear las directrices de la ISO 31000:2018 con las metas institucionales, se busca fortalecer la continuidad de los servicios de asesoría, optimizar la rentabilidad operativa asociada a proyectos y proteger la reputación de la firma ante incertidumbres internas y externas; de esta forma, la gestión de riesgos se convierte en una herramienta directa para la creación y protección de valor.

Respecto al campo de aplicación el Sistema de Gestión de Riesgos se diseñará para abarcar las dos áreas operativas de Stratos Asesores S.A.S.: Asesoría en Riesgos y Precios de Transferencia, considerando los procesos relacionados con la prestación de servicios por proyecto (comercial y contratación, planificación, ejecución, control de calidad/revisión, gestión documental y cierre). Adicionalmente, se incluirán los procesos de soporte administrativo y financiero (por ejemplo, facturación y cobranza) en la medida en que impactan la continuidad operativa y el cumplimiento de los proyectos, pese a que no constituyen una línea de servicio directa al cliente. La aplicación de la ISO 31000:2018 se realizará de manera adaptada y proporcional a la realidad de Stratos Asesores S.A.S., considerando su tamaño, estructura y contexto operativo, dado que la norma es aplicable a cualquier organización y puede ajustarse a sus necesidades.

Es importante mencionar que la norma ISO 31000:2018 no tiene carácter obligatorio ni certificable; está diseñada como una guía de directrices que puede integrarse con otros sistemas y prácticas de gestión existentes dentro de la organización(Organización Internacional de Normalización, 2018). De esta manera, en la Figura 8 se puede constatar que la articulación de sus componentes metodológicos esenciales permite estructurar una gestión sistemática del riesgo.

Figura 8

Principios, marcos de referencia y proceso basado en la ISO 31000:2018



Nota. Tomado de *Gestión del riesgo - Directrices (ISO 31000:2018),* por la Organización Internacional de Normalización, 2018.

La norma ISO 31000:2018 es aplicable a cualquier tipo de entidad, sin importar su tamaño, actividad o sector, ya que sus directrices pueden adaptarse al contexto organizacional. En este sentido, la presente propuesta se desarrolla con el fin de que Stratos Asesores S.A.S. cuente con lineamientos que permitan un manejo técnico, sistemático y proporcional de la gestión de riesgos, orientado a fortalecer la continuidad del servicio y la toma de decisiones.

El campo de aplicación de este sistema comprende de forma específica, los procesos y actividades de las siguientes áreas: Precios de Transferencia, Riesgos y Administración (soporte). La tabla 15 delimita las principales actividades por área y presenta los riesgos típicos asociados, con el propósito de establecer una base para la identificación, evaluación y tratamiento de riesgos dentro del Sistema de Gestión de Riesgos.

- Área de Precios de Transferencia.
- Area de Riesgos.
- Area de Administración (soporte).

Tabla 15

Actividades por área y riesgos típicos asociados

Área/Proceso	Descripción de actividades	Riesgos típicos asociados
Precios de transferencia	Recopilación y análisis de información del cliente; selección	Retrasos por información incompleta del cliente; errores

	y aplicación de criterios de comparabilidad; elaboración de informes técnicos y documentación de soporte para el cumplimiento normativo en operaciones con partes relacionadas.	metodológicos o de consistencia; retrabajo; confidencialidad de información financiera; riesgo reputacional por entregables con observaciones.
Riesgos	Ejecución de proyectos de consultoría y auditoría informática: planificación del trabajo, levantamiento y análisis de evidencias, evaluación de controles, elaboración y revisión de entregables (informes y papeles de trabajo) y comunicación de resultados al cliente.	Retrasos en entrega; hallazgos mal sustentados; pérdida/alteración de evidencias; errores por falta de estandarización; exposición de información del cliente; sobrecarga de capacidad y dependencia de personal clave.
Administración (soporte)	Procesos de soporte que impactan la continuidad y cumplimiento de los proyectos: facturación y cobranza, pagos y coordinación administrativa, gestión documental de soporte y apoyo en la asignación/seguimiento de recursos y cronogramas internos.	Retrasos por demoras en firmas/contratos; discrepancias contractuales (alcance/entregables); incumplimiento de NDA; atrasos de cobranza que afecten liquidez; fallas administrativas que impacten cronogramas o continuidad.

Nota. Alcance del Sistema de Gestión de Riesgos por áreas y procesos.

Considerando que la gestión del riesgo es un proceso dinámico, integrado y de mejora continua, el presente manual se propone como referencia para su aplicación sostenida en Stratos Asesores S.A.S. Su propósito es brindar a los responsables de cada área criterios y lineamientos para identificar, evaluar y tratar riesgos de manera sistemática, apoyando la toma de decisiones informadas, el cumplimiento de objetivos organizacionales y el fortalecimiento progresivo de los procesos internos.

5.2. Referencias Normativas

La gestión de riesgos debe considerar obligaciones externas e internas que influyen en la operación. Por ello, se identifican las autoridades competentes, la normativa legal aplicable, los compromisos contractuales y los lineamientos internos relevantes para Stratos Asesores S.A.S., los cuales servirán como base de referencia para la identificación, evaluación y tratamiento de riesgos dentro del Sistema de Gestión de Riesgos.

a) Autoridades competentes / entes reguladores

- Superintendencia de Compañías, Valores y Seguros (SCVS).
- Servicio de Rentas Internas (SRI).
- Ministerio de Trabajo.
- Instituto Ecuatoriano de Seguridad Social (IESS).
- Superintendencia de Protección de Datos Personales.
- Servicio Nacional de Derechos Intelectuales (SENADI).

b) Normas legales aplicables de forma general (Ecuador)

- Constitución de la República del Ecuador.
- Ley Orgánica de Protección de Datos Personales (LOPDP).
- Código Orgánico Penal (COIP).
- Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación.

- Ley de Compañías.
- Código de Comercio.
- Código Orgánico Administrativo (COA).
- Ley de Defensa Contra Incendios (reglamento aplicativo).
- Ley de Seguridad Pública y del Estado.
- Ley Orgánica de Servicio Público (LOSEP).
- Código Civil.
- Código del Trabajo (Codificación 17).
- Ley de Seguridad Social.
- Código Tributario.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos (apartado C).

c) Normas legales aplicables de forma específica (actividad de Stratos)

- Ley de Régimen Tributario Interno (LRTI) – Codificación 2004-026.
- Reglamento para la aplicación de la Ley de Régimen Tributario Interno (Decreto Ejecutivo 374).
- Contratos y acuerdos de confidencialidad (NDA).

d) Normas de régimen interno desarrolladas por la organización

- Manual de Políticas de Seguridad de la Información – Stratos.
- NTE INEN-ISO/IEC 27001 (Tecnología de la Información-Técnicas de Seguridad).
- NTE INEN-ISO 31000 (Gestión del Riesgo-Directores).

e) Buenas prácticas desarrolladas por la organización

- Uso de repositorios corporativos (OneDrive) con permisos para gestión documental por cliente/proyecto (Stratos Global Transfer Pricing S.A.S., 2025).
- Revisión por pares y control de calidad antes de la entrega de productos al cliente (Stratos Global Transfer Pricing S.A.S., 2025).
- Reuniones periódicas de seguimiento de proyectos y orden documental en repositorios corporativos (Stratos Global Transfer Pricing S.A.S., 2025).

5.3. Términos y Definiciones

Con la finalidad de garantizar la comprensión, a continuación, se describen los principales términos y definiciones utilizados en el marco de este proyecto. Estas definiciones se basan en la norma internacional ISO 31000:2018.

- **Riesgo:** efecto de la incertidumbre sobre los objetivos.
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- **Sistema de Gestión de Riesgos (SGR):** conjunto de elementos (marco, proceso, roles, herramientas y prácticas) que permiten gestionar riesgos de manera estructurada y sostenida.
- **Objetivo:** resultado o propósito que la organización busca alcanzar (estratégico, operativo, financiero, de cumplimiento o reputacional).
- **Contexto:** conjunto de condiciones internas y externas en las que la organización persigue sus objetivos (estructura, procesos, recursos, clientes, entorno regulatorio, mercado, etc.).
- **Parte interesada (stakeholder):** persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad.
- **Evento:** ocurrencia o cambio de circunstancias que puede influir en el logro de objetivos.
- **Amenaza**: evento o condición con potencial de causar daño a la organización.
- **Vulnerabilidad:** debilidad o condición que puede ser aprovechada por una amenaza, incrementando la posibilidad o el impacto de un evento adverso.
- **Consecuencia (impacto):** resultado de un evento que afecta el logro de objetivos (por ejemplo: retrasos, pérdidas económicas, incumplimientos, daño reputacional).

- **Probabilidad:** posibilidad de que ocurra un evento o se materialice un riesgo.
- **Nivel de riesgo:** magnitud del riesgo determinada a partir de la probabilidad y el impacto, conforme a los criterios definidos por la organización.
- **Criterios de riesgo:** reglas y referencias utilizadas para evaluar riesgos (escalas de probabilidad e impacto, niveles, apetito, tolerancia).
- **Apetito de riesgo:** cantidad y tipo de riesgo que la organización está dispuesta a asumir para alcanzar sus objetivos.
- **Tolerancia al riesgo:** límites aceptables de variación o nivel de riesgo permitido antes de requerir acciones de tratamiento o escalamiento.
- **Control:** medida que modifica el riesgo (reduce probabilidad, reduce impacto o ambos). Puede ser preventivo, detectivo o correctivo.
- **Riesgo inherente:** nivel de riesgo antes de considerar controles existentes.
- **Riesgo residual:** nivel de riesgo después de considerar controles existentes y/o acciones de tratamiento.
- **Tratamiento del riesgo:** proceso de selección e implementación de opciones para abordar el riesgo (evitar, reducir/mitigar, transferir/compartir, aceptar).

- **Monitoreo y revisión:** seguimiento periódico de riesgos, controles e iniciativas para asegurar vigencia, efectividad y mejora continua.
- **Registro de riesgos:** documento o repositorio donde se documentan riesgos identificados, su evaluación, responsables, controles, planes de tratamiento y estado de seguimiento.
- **Transferencia del riesgo:** opción de tratamiento mediante la cual la organización reduce su exposición trasladando o compartiendo parte del impacto con un tercero.

5.4. Principios

Bajo los lineamientos de la norma internacional ISO 31000:2018, los principios de la gestión del riesgo actúan como ejes rectores para asegurar que el sistema sea efectivo y aporte valor a la organización. La integración de estos fundamentos permite que la gestión del riesgo no se limite a un proceso aislado, sino que se consolide como un componente esencial de la dirección estratégica y de la operación diaria, orientado a crear y proteger valor mediante la toma de decisiones informadas y la priorización de acciones.

En el caso de Stratos Asesores S.A.S., la aplicación de estos principios busca fortalecer el cumplimiento de plazos y la calidad de los entregables en proyectos, reducir retrabajos y sobrecarga operativa, y proteger activos críticos como la información de clientes y la reputación corporativa. En consecuencia, los

principios que se detallan a continuación guiarán el diseño y aplicación del Sistema de Gestión de Riesgos en la organización.

Figura 9

Principios de la gestión del riesgo basados en la ISO 31000:2018

Nota. Tomado de *Gestión del riesgo - Directrices (ISO 31000:2018),* por la Organización Internacional de Normalización, 2018.

5.4.1. Integrada

La gestión del riesgo en Stratos Asesores S.A.S. se aplicará de forma integrada a la gestión y ejecución de sus servicios, de manera que no sea una actividad aislada, sino parte del trabajo cotidiano y de la toma de decisiones. En la práctica, esto implica incorporar la identificación y revisión de riesgos en los momentos clave del ciclo de un proyecto: definición de alcance y compromisos,

planificación, asignación de recursos, ejecución, control de calidad (revisión por pares) y entrega al cliente. Adicionalmente, la gestión de riesgos se integrará a las rutinas de seguimiento ya existentes en la organización, considerando que el equipo realiza reuniones semanales (lunes) para revisar avances, validar requerimientos y ajustar actividades, y que se mantienen reuniones quincenales con el cliente para comunicar avances y gestionar expectativas; en ambos espacios se identificarán riesgos emergentes y se definirán acciones de respuesta. Asimismo, los riesgos se registrarán y evaluarán con criterios homogéneos para facilitar su priorización, asignando responsables por área (Riesgos, Precios de Transferencia y soporte administrativo cuando corresponda) y asegurando seguimiento periódico. Este principio permite que el SGR contribuya directamente a prevenir retrasos, retrabajos y desorden operativo, al anticipar riesgos asociados a capacidad, calidad, manejo de información y cumplimiento contractual. Finalmente, al integrarse con prácticas existentes (repositorios documentales corporativos y controles internos), la gestión del riesgo se convierte en una herramienta práctica para mejorar el desempeño, proteger la reputación y sostener el crecimiento de la organización.

5.4.2. Estructurada y Exhaustiva

La gestión del riesgo en Stratos Asesores S.A.S. se desarrollará de manera estructurada y exhaustiva, asegurando consistencia en la forma de identificar, analizar, evaluar y tratar los riesgos en las distintas áreas y proyectos. Para ello,

el SGR utilizará una metodología común que incluya: definición del contexto, criterios de evaluación (probabilidad e impacto), registro de riesgos, determinación de responsables, controles existentes, planes de tratamiento y seguimiento periódico. Este enfoque evita que la gestión de riesgos dependa únicamente de criterios individuales o de respuestas improvisadas ante incidentes, y permite comparabilidad y trazabilidad en las decisiones.

La exhaustividad se logrará considerando riesgos a lo largo de todo el ciclo del servicio por proyecto, desde la contratación y planificación hasta la ejecución, control de calidad y entrega. En este marco, se incorporará la práctica existente de papeles de trabajo estándar en Excel, los cuales podrán variar según la norma o requerimiento del cliente, manteniendo un control mínimo de versiones y validaciones para asegurar coherencia. Asimismo, se reforzará el control de calidad como parte del sistema, considerando que todo informe pasa por revisión obligatoria del socio y del gerente de cada área antes de su entrega al cliente, lo cual se documentará como control existente dentro del registro de riesgos.

Adicionalmente, el sistema asegurará exhaustividad en la gestión documental, considerando que la organización almacena la información por cliente/proyecto en OneDrive, y que se implementará el almacenamiento de informes finales en el NAS como medida de respaldo y conservación. En consecuencia, este principio contribuye a reducir retrasos y retrabajos, al establecer un proceso

ordenado que identifica riesgos a tiempo, asigna acciones concretas y permite monitorear su efectividad.

5.4.3. Adaptada

El Sistema de Gestión de Riesgos (SGR) debe ajustarse al contexto de Stratos Asesores S.A.S., tomando en cuenta su tamaño, estructura, recursos, áreas de trabajo, herramientas tecnológicas, tipo de servicios, partes interesadas y objetivos organizacionales. Stratos cuenta con aproximadamente 17 colaboradores distribuidos entre las áreas de Riesgos, Precios de Transferencia y Administración. Su operación se coordina bajo modalidad de proyectos, con énfasis en la entrega de informes técnicos, el manejo de documentación del cliente y el uso de herramientas corporativas como Microsoft 365 (OneDrive, Outlook/correo corporativo y Teams), además de una herramienta especializada de apoyo para el área de Precios de Transferencia.

La adaptación también debe considerar el entorno interno y externo de la organización. Para ello, puede utilizarse una herramienta de análisis como PESTEL (Político, Económico, Social, Tecnológico, Ecológico y Legal), que permite revisar factores relacionados con la operación de Stratos y su exposición al riesgo. Esta revisión debe contemplar, entre otros, obligaciones de protección de datos personales, cambios tecnológicos, dependencia de proveedores, condiciones del mercado, capacidad operativa, recursos disponibles y compromisos asumidos con los clientes. La información obtenida orientará la

personalización de la gestión del riesgo (matrices y criterios de probabilidad e impacto), así como la definición de controles, responsables, plazos y revisiones, asegurando que el sistema sea proporcional a las capacidades de la organización y se mantenga alineado con objetivos de calidad del servicio, continuidad operativa, seguridad de la información, cumplimiento legal y confianza del cliente.

5.4.4. Inclusiva

La gestión del riesgo en Stratos Asesores S.A.S. se desarrollará de forma inclusiva, promoviendo la participación de las partes interesadas internas y externas pertinentes, con el fin de obtener una visión completa de los riesgos y fortalecer la aceptación de las decisiones. En el contexto de la organización, la inclusión implica considerar a la Dirección (socios), gerencias de área, consultores, personal administrativo y, cuando corresponda, a clientes y proveedores relevantes, debido a que su información y decisiones pueden influir en el alcance, plazos, calidad y continuidad de los proyectos.

En la práctica, este principio se aplicará integrando la gestión de riesgos en espacios de coordinación existentes: reuniones internas de avance (lunes) para identificar riesgos operativos y de capacidad, y reuniones quincenales con el cliente para validar requerimientos, gestionar cambios y anticipar riesgos asociados a disponibilidad de información, alcance y expectativas. Asimismo, se definirá un mecanismo claro para que cualquier miembro del equipo pueda

reportar riesgos o señales tempranas (por ejemplo, retrasos previstos, falta de insumos del cliente, conflictos de capacidad o incidentes de información), asegurando que estos se registren, asignen responsables y se les dé seguimiento. De esta forma, la inclusión contribuye a mejorar la comunicación, reducir la gestión reactiva y fortalecer la toma de decisiones informadas, alineadas con los objetivos y prioridades del negocio.

5.4.5. Dinámica

De acuerdo con la ISO 31000:2018, la gestión del riesgo debe caracterizarse por su naturaleza dinámica, lo que implica la capacidad de reconocer y responder oportunamente a cambios en el contexto interno y externo de la organización. En Stratos Asesores S.A.S., este principio se aplicará considerando que los riesgos pueden variar por cambios en proyectos, requerimientos del cliente, carga operativa, disponibilidad de información y evolución normativa y tecnológica.

- En el entorno externo, la gestión de riesgos se actualizará ante cambios normativos y requerimientos de entidades competentes. Para el área de Precios de Transferencia, esto incluye variaciones en normativa tributaria aplicable, requerimientos del Servicio de Rentas Internas (SRI) y lineamientos internacionales que puedan incidir en los análisis técnicos. Para el área de Riesgos, se considerarán cambios relevantes en el entorno tecnológico de los clientes, nuevas amenazas de ciberseguridad y requerimientos metodológicos asociados a servicios de

consultoría/auditoría. De manera transversal, se incorporarán cambios regulatorios relacionados con protección de datos personales y obligaciones contractuales con clientes.

- En el entorno interno, se revisarán riesgos y controles ante variaciones en la capacidad del equipo, cambios en la organización del trabajo por proyectos, rotación o ausencias, así como actualizaciones relevantes en herramientas corporativas (por ejemplo, Microsoft 365). En el caso del área Administrativa (soporte), se considerarán cambios en procesos que impactan el cumplimiento de proyectos, como gestión de contratos/NDA y coordinación de firmas, así como actividades de facturación y cobranza que pueden influir en continuidad operativa.

Para operacionalizar el dinamismo, el Sistema de Gestión de Riesgos incorporará revisiones periódicas en los espacios de coordinación ya existentes: la reunión semanal interna (lunes) para identificar desviaciones y riesgos emergentes, y las reuniones quincenales con el cliente para validar requerimientos, anticipar cambios de alcance y gestionar expectativas. Adicionalmente, como parte del diseño del SGR, se propone establecer un Sistema de Alerta Temprana (SAT) que permita activar acciones proporcionales al nivel de alerta, mejorando la respuesta ante desviaciones, incidentes o cambios relevantes, y manteniendo actualizado el registro de riesgos.

La Tabla 16 presenta una propuesta de Sistema de Alerta Temprana (SAT) que define niveles de alerta, criterios de activación y acciones dinámicas a ejecutar, con el fin de reforzar la capacidad de respuesta y la actualización oportuna del SGR.

Tabla 16

Sistema de Alerta Temprana (SAT)

Nivel	Estado	Criterio de activación	Acción dinámica
Bajo	Estable	Indicadores dentro de límites (avance del proyecto según cronograma, entregables en control, documentación completa y accesos sin novedades).	Mantenimiento y monitoreo pasivo (seguimiento en reunión del lunes y registro básico).
Medio	Preventivo	Desviación en tiempos de entrega, faltantes de información del cliente, sobrecarga del equipo o incidentes operativos (p. ej., permisos inadecuados o fallas de conectividad).	Activación de análisis de escenarios y plan de mitigación (ajuste de cronograma, reasignación de recursos y comunicación preventiva con el cliente).
Alto	Crítico	Incumplimiento contractual/ legal, exposición de información del cliente, incidente de seguridad relevante o interrupción que comprometa la entrega.	Respuesta rápida y escalamiento (contención, ajuste de estrategia, responsables definidos, registro del incidente y plan de recuperación).

La gestión de riesgos dinámica permite a Stratos Asesores S.A.S. anticipar y responder oportunamente a cambios del entorno tributario y tecnológico, fortaleciendo la continuidad del servicio, la calidad de los entregables y la reputación organizacional.

5.4.6. Mejor Información Disponible

La norma ISO 31000:2018 establece que la gestión del riesgo debe fundamentarse en la mejor información disponible, considerando datos históricos, información actual y, cuando corresponda, proyecciones futuras, así como las limitaciones e incertidumbres inherentes a dicha información. En este sentido, se reconoce que la eficacia de la gestión de riesgos depende directamente de la calidad, trazabilidad y pertinencia de los datos utilizados.

En Stratos Asesores S.A.S., la toma de decisiones para la gestión de riesgos se sustentará en información confiable y actualizada proveniente de fuentes internas y externas. Como fuentes internas, se considerarán los registros y evidencias de proyectos, avances revisados en la reunión semanal del equipo (lunes), observaciones y hallazgos derivados de la revisión por pares realizada por socios y gerentes antes de la entrega, así como la documentación organizada por cliente/proyecto en repositorio corporativo (OneDrive). Desde la perspectiva de áreas, se incluirán insumos propios de Precios de Transferencia (información técnica y documentación de soporte del cliente), del área de Riesgos (evidencias y resultados de consultorías/auditorías) y del área Administrativa (soporte) (contratos y acuerdos de confidencialidad (NDA), estado de firmas, facturación/cobranza y aspectos que afecten continuidad y cumplimiento de plazos).

Como fuentes externas, se considerarán los requisitos normativos aplicables (por ejemplo, disposiciones tributarias pertinentes, protección de datos personales) y las obligaciones contractuales con clientes (contratos y acuerdos de confidencialidad (NDA)), así como cambios del entorno tecnológico o del mercado que puedan influir en la operación. Asimismo, se documentarán las limitaciones de la información disponible (incompletitud o incertidumbre) y se actualizará el análisis cuando existan cambios relevantes o nueva evidencia, garantizando decisiones de riesgo consistentes y sustentadas.

Tabla 17

Estructura de información para la gestión de riesgos

Fuente de Información	**Uso en la Gestión de Riesgos de Stratos**	**Gestión de Limitaciones**
Datos Históricos	Análisis de proyectos previos, lecciones aprendidas, causas de retrasos/retrabajo y errores recurrentes.	Riesgo de obsolescencia por cambios normativos, tecnológicos o metodológicos; se mitiga actualizando criterios y revisando periódicamente.
Trazabilidad en repositorios corporativos (Microsoft 365)	Verificación de versiones, permisos y organización documental en OneDrive para evidencias y entregables.	Dependencia de infraestructura TI y configuración de accesos; se mitiga con controles mínimos y revisiones periódicas.
Juicio de expertos internos	Criterio técnico de socios y gerentes para validar metodología, decisiones y controles, especialmente en casos complejos.	Posibles sesgos subjetivos; se mitiga con revisión por pares, criterios documentados y evidencia de soporte.
Información contractual (contratos/NDA)	Definición de alcance, entregables, confidencialidad y	Riesgo de interpretaciones ambiguas; se mitiga con cláusulas claras y control de versiones/aprobaciones.

	responsabilidades; base para control de cambios.

Stratos Asesores S.A.S. operativiza este principio mediante el uso de herramientas corporativas de Microsoft 365 (OneDrive) como repositorio central para la gestión documental de proyectos, lo que permite fortalecer la trazabilidad, el control de versiones y la disponibilidad de evidencias. Como parte del diseño del SGR, se promoverá una cultura de comunicación transparente basada en datos, donde el equipo reporte avances, hallazgos y restricciones reales (por ejemplo, falta de insumos del cliente o desviaciones de cronograma), de modo que socios y gerentes dispongan de información confiable para la supervisión y toma de decisiones. Adicionalmente, el sistema incorporará la identificación de limitaciones y supuestos de la información utilizada en los análisis, registrando niveles de incertidumbre cuando corresponda, con el fin de que la dirección evalúe riesgos y tratamientos con conocimiento de los límites de la información disponible y del riesgo residual.

5.4.7. Factores Humanos y Culturales

La gestión de riesgos no depende únicamente de metodologías y controles, sino también de cómo las personas interpretan, comunican y aplican las decisiones en el trabajo diario. Por ello, los factores humanos y culturales influyen directamente en la identificación oportuna de riesgos, en la calidad de la

información utilizada y en la efectividad de los controles implementados dentro de la organización.

El comportamiento individual, la comunicación interna y la cultura organizacional pueden prevenir o incrementar la materialización de riesgos, especialmente en una organización que trabaja por proyectos y maneja información sensible de clientes. En Stratos Asesores S.A.S., este principio se alinea con el enfoque institucional de “Experiencia que Inspira”, entendiendo que la calidad del servicio y la confianza del cliente dependen tanto de la capacidad técnica como de prácticas consistentes de trabajo y responsabilidad en el manejo de la información.

Para aplicar eficazmente este principio, el Sistema de Gestión de Riesgos promoverá una cultura de reporte temprano y aprendizaje, incentivando que los equipos de Riesgos y Precios de Transferencia comuniquen oportunamente desviaciones o señales de riesgo (por ejemplo, falta de información del cliente, cambios de alcance, retrasos previstos o inconsistencias en papeles de trabajo). Estas alertas se revisarán en los espacios de coordinación ya existentes y, cuando corresponda, se registrarán en el sistema para su tratamiento y seguimiento. Adicionalmente, se fortalecerá la cultura de calidad mediante la revisión por pares y la validación de informes por socios y gerentes antes de su entrega, incorporando esta práctica como control existente dentro del sistema.

Finalmente, el SGR incorporará acciones de concientización y capacitación gradual en buenas prácticas de gestión documental, seguridad de la información y cumplimiento, buscando que la gestión del riesgo sea una responsabilidad compartida y sostenible, y que contribuya al equilibrio entre desempeño, calidad del entregable y bienestar del equipo.

5.4.8. Mejora Continua

La gestión del riesgo en Stratos Asesores S.A.S. se orientará a la mejora continua, asegurando que el Sistema de Gestión de Riesgos (SGR) se mantenga vigente, efectivo y alineado con los objetivos de la organización. Este principio implica que el SGR no se considere un elemento estático, sino un sistema que se revisa y fortalece de forma periódica a partir de resultados, lecciones aprendidas y cambios del entorno interno y externo.

Para operacionalizar este principio, el SGR se estructurará bajo un ciclo de mejora tipo Planificar–Ejecutar–Verificar–Actuar (PDCA). En la fase de Planificar, se define el contexto, los criterios de evaluación y el registro de riesgos prioritarios asociados a las áreas de Riesgos y Precios de Transferencia, así como los procesos de soporte del área Administrativa (por ejemplo, contratos/NDA, facturación y cobranza) cuando impacten el cumplimiento y continuidad de los proyectos. En la fase de Ejecutar, se aplican los controles y acciones definidos, integrando prácticas existentes como la gestión documental por cliente, el control de calidad mediante revisión por pares y la validación final

de informes por socios y gerentes, además de medidas preventivas para reducir retrasos y retrabajo.

En la fase de Verificar, se revisa la efectividad de las acciones mediante el seguimiento de avances y desviaciones en las reuniones internas semanales (lunes), la retroalimentación obtenida en reuniones quincenales con el cliente y los resultados de la revisión por pares. Asimismo, se considerarán eventos relevantes que afecten la seguridad y continuidad, incluyendo incidentes relacionados con el acceso o manejo de información, o condiciones de seguridad física del entorno de trabajo. En este punto, cuando aplique, se contemplará la coordinación con el edificio respecto a los sistemas de videovigilancia (cámaras pertenecientes al propietario del inmueble) a los que la organización tiene acceso, con el fin de apoyar la investigación de eventos sin que ello implique que la organización administre directamente dicha infraestructura.

Finalmente, en la fase de Actuar, se implementan ajustes y mejoras sobre controles, criterios, responsables y prácticas operativas, incorporando aprendizajes de cada proyecto (lecciones aprendidas) para fortalecer la estandarización progresiva, mejorar la planificación y reforzar la gestión documental y de accesos. En consecuencia, la mejora continua permitirá que el SGR evolucione junto con la organización, manteniendo actualizado el registro de riesgos y promoviendo una gestión preventiva, consistente y sostenible, orientada a proteger la reputación de la firma y apoyar su crecimiento ordenado.

Con lo anterior, se establecen los principios que guían el diseño del SGR en Stratos Asesores S.A.S., asegurando coherencia entre la norma ISO 31000:2018 y la realidad operativa de la organización.

5.5. Marco de Referencia

5.5.1. Generalidades

El marco de referencia establecido en la norma ISO 31000:2018 proporciona los lineamientos necesarios para integrar la gestión de riesgos dentro de la estructura, procesos y toma de decisiones de una organización. Su objetivo es asegurar que la gestión de riesgos se desarrolle de manera sistemática, alineada y estructurada con los objetivos de las organizaciones.

En el caso específico de Stratos Asesores S.A.S. la implementación de este marco de referencia permitirá fortalecer la identificación, evaluación y tratamiento de riesgos asociados a sus procesos estratégicos, administrativos y operativos. Esto promoverá una gestión más eficiente, con una mayor capacidad de respuesta y consolidará tanto el control interno como la mejora continua.

A continuación, se presenta el marco de referencia propuesto para la implementación del Sistema de Gestión de Riesgos en Stratos Asesores S.A.S. con base en los lineamientos establecidos en la norma ISO 31000:2018.

Figura 10

Gobernanza y objetivos estratégicos

Nota. Tomado de (Organización Internacional de Normalización, 2018).

5.5.2. Liderazgo y Compromiso

La implementación de la gestión de riesgos en Stratos Asesores S.A.S., con base en los lineamientos establecidos en la norma internacional ISO 31000:2018, requiere el compromiso permanente de los socios, de aquí en adelante denominado la alta dirección y la participación de todos los niveles de la organización. En este contexto, La alta dirección constituye un elemento clave para promover una cultura organizacional orientada a la gestión de riesgos, asegurando la asignación de responsabilidades, recursos y mecanismos de apoyo para la implementación del sistema.

En consecuencia, la presente propuesta establece que la alta dirección de Stratos Asesores S.A.S. deberá asumir el compromiso de promover una gestión integral

de riesgos orientada al cumplimiento de los objetivos organizacionales, fortalecer la continuidad de las operaciones y mejorar la capacidad de respuesta ante situaciones que puedan afectar el desarrollo de las actividades.

Con el propósito de garantizar una adecuada implementación del Sistema de Gestión de Riesgos, se propone que la alta dirección de Stratos Asesores S.A.S. adopte los siguientes compromisos, con base en los lineamientos establecidos en la norma internacional ISO 31000:2018.

Tabla 18

Compromisos para la implementación del Sistema de Gestión de Riesgos en Stratos Asesores S.A.S.

N.º	Compromiso	Aplicación Propuesta
1.	Liderazgo estratégico	La alta dirección deberá promover la gestión de riesgos como parte de la estrategia organizacional.
2.	Asignación de responsabilidades	Se deberán definir roles y responsabilidades para la gestión de riesgos en todos los niveles organizacionales.
3.	Disponibilidad de recursos	La organización deberá garantizar recursos humanos, tecnológicos y financieros para la implementación del Sistema de Gestión de Riesgos.
4.	Comunicación organizacional	Se deberá promover la difusión y comprensión de la gestión de riesgos en toda la organización.
5.	Cultura organizacional	La alta dirección deberá fomentar una cultura orientada a la prevención y control de riesgos.
6.	Participación de todo el personal	Se deberá incentivar la participación de los colaboradores en las actividades relacionadas con la gestión de riesgos.
7.	Mejora continua	La organización deberá promover mecanismos de seguimiento y mejora continua del Sistema de Gestión de Riesgos.

5.5.3. Integración

La integración de la gestión de riesgos en Stratos Asesores S.A.S. permitirá incorporar el análisis y tratamiento de los riesgos dentro de los procesos de la organización, facilitando una toma de decisiones más efectiva y orientada a la prevención de eventos que puedan afectar el cumplimiento de los objetivos de la organización.

Es entonces que la gestión de riesgos será considerada como parte de las actividades estratégicas, administrativas y operativas de la organización, facilitando la identificación oportuna de los riesgos, el control interno y la mejora continua de los procesos de la organización.

Tabla 19

Acciones para la integración de la gestión de riesgos en Stratos Asesores S.A.S.

N.º	Acción	Descripción
1.	Integración en los procesos organizacionales	Incorporar la gestión de riesgos en los procesos estratégicos, administrativos y operativos de la organización.
2.	Integración en la planificación estratégica	Considerar el análisis de riesgos en la formulación de objetivos, proyectos y toma de decisiones organizacionales.
3.	Articulación	Fortalecer la relación entre la gestión de riesgos y los mecanismos de control internos de la organización.
4.	Comunicación y sensibilización	Desarrollar programas de formación y capacitación relacionados con la gestión de riesgos y prevención organizacional.
5.	Monitoreo y Seguimiento	Implementar mecanismos de supervisión y evaluación continua para identificar oportunidades de mejora.

6.	Comunicación y reporte de riesgos	Promover canales internos de comunicación para el reporte oportuno y tratamiento de riesgos organizacionales.
7.	Actualización de los sistemas	Revisar y actualizar periódicamente el Sistema de Gestión de Riesgos de acuerdo con los cambios internos y externos.

5.5.4. Diseño

El diseño del marco de gestión de riesgos para Stratos Asesores S.A.S. se desarrolla conforme a los lineamientos establecidos en la norma ISO 31000:2018, considerando la naturaleza de la organización, su contexto operativo, sus objetivos estratégicos y los factores internos y externos que pueden influir en el cumplimiento de dichos objetivos.

De acuerdo con la ISO 31000:2018, el diseño del marco de gestión de riesgos debe permitir integrar la gestión del riesgo dentro de todas las actividades organizacionales, considerando el contexto interno y externo, las partes interesadas y el compromiso de la alta dirección.

5.5.4.1. Comprensión de la Organización y su Contexto

Propósito.

El propósito del presente análisis es comprender el contexto interno y externo de Stratos Asesores S.A.S., identificando los factores relevantes que pueden afectar el cumplimiento de sus objetivos organizacionales, operativos y estratégicos, con

el fin de establecer una base adecuada para el diseño del Sistema de Gestión de Riesgos basado en la ISO 31000:2018.

Este análisis permite identificar factores del entorno, necesidades de las partes interesadas y elementos críticos relacionados con la operación, seguridad de la información, cumplimiento normativo y sostenibilidad organizacional.

Contexto de Operación de la Organización.

Stratos Asesores S.A.S. es una firma ecuatoriana especializada en gestión de riesgos organizacionales y fiscalidad internacional, ubicada en Quito-Ecuador, que presta servicios profesionales bajo modalidades presencial, híbrida y remota.

La organización desarrolla sus actividades mediante un modelo operativo basado en proyectos, apoyándose en herramientas tecnológicas corporativas como Microsoft 365, OneDrive, Outlook y Teams para la gestión documental, coordinación de actividades y comunicación con clientes.

La operación de la organización depende significativamente del conocimiento técnico del personal, del cumplimiento de plazos contractuales, de la gestión adecuada de información confidencial y de la capacidad de coordinación entre las áreas de Riesgos, Precios de Transferencia y Administrativa.

Debido a la naturaleza de sus actividades, la organización se encuentra expuesta a riesgos operativos, tecnológicos, financieros, legales, reputacionales y de seguridad de la información, especialmente relacionados con:

- Retrasos en proyectos,

- Errores técnicos,
- Sobrecarga laboral,
- Incumplimiento contractual,
- Pérdida o fuga de información,
- Protección de datos personales,
- Continuidad operativa,
- Dependencia tecnológica.

Tabla 20

Partes interesadas internas

Parte interesada	Relación con la gestión del riesgo
CEO y socios	Definición de objetivos y apetito de riesgo
Gerencia	Supervisión operativa y control
Equipo consultor	Ejecución de proyectos y manejo de información
Área administrativa	Gestión financiera y soporte operativo

Tabla 21

Partes interesadas externas

Parte interesada	Relación con la gestión del riesgo
Clientes	Confidencialidad y calidad del servicio
Proveedores tecnológicos	Disponibilidad y seguridad tecnológica
Entidades regulatorias	Cumplimiento legal y normativo
Instituciones financieras	Obligaciones financieras
Mercado y competencia	Reputación y competitividad

Conforme a la ISO 31000:2018, las partes interesadas son personas u organizaciones que pueden afectar, verse afectadas, por las decisiones y actividades de la organización.

Tabla 22

Análisis PESTEL

Dimensión	Factores Clave Identificados
Político	Cambios regulatorios tributarios y organizacionales. Modificaciones en políticas económicas nacionales. Regulaciones relacionadas con protección de datos y seguridad de la información.
Económico	Inflación y variaciones económicas nacionales. Riesgos asociados a liquidez y recuperación de cartera. Alto nivel de endeudamiento financiero. Dependencia de contratos y proyectos.
Social	Creciente necesidad empresarial de gestión de riesgos. Incremento del trabajo híbrido y remoto. Importancia de la reputación y confianza organizacional.
Tecnológico	Dependencia de plataformas Microsoft 365 y OneDrive. Riesgos de ciberseguridad y accesos no autorizados. Necesidad de respaldo y control documental. Evolución constante de herramientas digitales.
Ecológico	Reducción de uso de papel mediante digitalización. Riesgos por interrupciones energéticas o eventos externos. Necesidad de continuidad operativa.
Legal	Cumplimiento de la Ley Orgánica de Protección de Datos Personales. Obligaciones contractuales y acuerdos de confidencialidad. Normativas tributarias y societarias aplicables.

5.5.4.2. Articulación del Compromiso con la Gestión del Riesgo.

Política de Gestión de Riesgos.

Stratos Asesores S.A.S. reconoce la importancia de la gestión de riesgos como un elemento fundamental para el cumplimiento de sus objetivos estratégicos, operativos, tecnológicos, legales, financieros y reputacionales.

En este sentido, la organización asume el compromiso de implementar y mantener un Sistema de Gestión de Riesgos basado en los lineamientos de la norma ISO 31000:2018, promoviendo una cultura orientada a la identificación, evaluación, tratamiento y monitoreo continuo de los riesgos que puedan afectar el desarrollo de sus actividades.

La organización se compromete a:

- Identificar, analizar, evaluar, tratar y monitorear los riesgos que puedan afectar el cumplimiento de sus objetivos estratégicos, operativos, tecnológicos, legales, financieros y reputacionales.
- Integrar la gestión de riesgos en todos los procesos organizacionales.
- Cumplir con los requisitos legales, regulatorios y contractuales aplicables.
- Asignar roles, responsabilidades y recursos necesarios para la implementación, mantenimiento y mejora del Sistema de Gestión de Riesgos.
- Fortalecer la toma de decisiones basada en riesgos.

- Promover la participación de la alta dirección, gerencias de cada área, colaboradores y personal de apoyo en la identificación, comunicación y tratamiento de los riesgos.
- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Comunicar y socializar la presente política a los colaboradores y partes interesadas, con el fin de fortalecer la cultura de gestión de riesgos dentro de la organización.
- Revisar periódicamente la matriz de riesgos, los planes de tratamiento y la presente política, con el fin de fortalecer la cultura de gestión de riesgos dentro de la organización.
- Promover la mejora continua del Sistema de Gestión de Riesgos.

La alta dirección será responsable de aprobar, supervisar y revisar la implementación de esta política de Riesgos dentro de la organización. La política deberá ser revisada al menos una vez al año o cuando existan cambios relevantes en la organización, sus procesos, servicios, normativa aplicable, tecnología o contexto interno y externo.

5.5.4.3. Asignación de Roles, Autoridades, Responsabilidades y Obligación de Rendir Cuentas en la Organización.

En la actualidad, Stratos Asesores no cuenta actualmente con un Sistema de Gestión de Riesgos formalmente establecido. Por esta razón, es fundamental

establecer un esquema que defina claramente las competencias, niveles de autoridad y tareas de cada participante. El propósito central es garantizar un manejo sistematizado de los riesgos, previniendo solapamientos de funciones, ausencia de monitoreo y falta de claridad sobre quién es responsable de cada riesgo detectado.

Dado que la organización cuenta con un equipo reducido de aproximadamente 17 colaboradores, es imprescindible que la distribución de funciones sea eficiente y acorde con su escala operativa. En lugar de diseñar una arquitectura elaborada, conviene integrar estas responsabilidades dentro de las posiciones y áreas ya existentes, particularmente en alta dirección, los líderes de las áreas de negocio, el responsable del Sistema de Gestión de Riesgos y los colaboradores. La asignación de roles permite establecer quién aprueba, quién coordina, quién ejecuta, quién reporta y quién debe mantenerse informado sobre los riesgos identificados. De esta manera, se fortalece la toma de decisiones, se mejora el seguimiento de los planes de tratamiento y se promueve una cultura organizacional orientada a la prevención y control de riesgos.

Tabla 23

Roles, responsabilidades, autoridad y rendición de cuentas

Rol	Responsabilidad	Autoridad	Rendición de cuentas
Alta dirección	Aprobar la política, metodología y prioridades del Sistema de Gestión de Riesgos.	Aprobar decisiones sobre riesgos críticos, recursos y planes de tratamiento.	Revisar informes de riesgos y tomar decisiones sobre riesgos relevantes.
Responsable del Sistema de Gestión de Riesgos	Coordinar la identificación, evaluación, tratamiento y seguimiento de riesgos.	Solicitar información a las áreas y proponer acciones de mejora.	Mantener actualizada la matriz de riesgos y reportar avances a la Alta Dirección.
Gerencia de Asesoría en Riesgos	Gestionar riesgos asociados a cumplimiento, auditoría, seguridad de la información, privacidad y continuidad.	Proponer controles y acciones para su línea de negocio.	Reportar riesgos, incidentes y avances de tratamiento de su área.

(Continua)

(Continuación)

Rol	Responsabilidad	Autoridad	Rendición de cuentas
Gerencia de Precios de Transferencia	Gestionar riesgos técnicos, normativos, documentales y reputacionales de su línea de servicio.	Proponer acciones para reducir errores, incumplimientos o afectaciones reputacionales.	Informar riesgos relevantes, controles pendientes y avances de su área.
Colaboradores	Cumplir controles internos y reportar eventos, debilidades o situaciones de riesgo.	Alertar oportunamente sobre situaciones que puedan afectar la operación o el servicio.	Responder por el cumplimiento de sus actividades y comunicar desviaciones.
Coordinadora Administrativa	Apoya con documentación, recursos, seguimiento, archivo de evidencias y coordinación operativa.	Gestionar documentos y registros de soporte del sistema.	Mantener actualizadas las evidencias relacionadas con la gestión de riesgos.

*Nota. C*on base en la información recopilada durante el desarrollo de la investigación.

La alta dirección debe encargarse de validar y aprobar los lineamientos de riesgos, revisar y avalar la metodología implementada, establecer prioridades en los riesgos críticos y destinar recursos adecuados para mantener el sistema funcional. Paralelamente, tiene el deber de fomentar un ambiente laboral que valore la mitigación, vigilancia continua y decisiones fundamentadas en análisis de riesgos.

El responsable del Sistema de Gestión de Riesgos asumirá la tarea de facilitar todo el ciclo del riesgo: desde su detección inicial, pasando por su valoración y planificación de controles, hasta su supervisión periódica. Sus funciones abarcan consolidar el registro integral de riesgos, supervisar la ejecución de planes correctivos y elaborar informes ejecutivos para la alta dirección.

Las gerencias de cada área de la organización serán responsables de identificar y controlar los riesgos específicos de sus áreas. En Asesoría de Riesgos, esto incluye vigilancia de normativa, resguardo de datos sensibles, protección de información personal, validación de procesos, planes de contingencia y garantía de eficiencia operacional. En el área de Precios de Transferencia, se contemplarán riesgos de índole técnica, legal, administrativa, reputacional y obligaciones hacia terceros e instituciones fiscales.

Los colaboradores tendrán la responsabilidad de cumplir las políticas, procedimientos y controles definidos, además de comunicar sin demoras cualquier circunstancia que signifique una amenaza potencial. Esto abarca

accidentes, deficiencias en mecanismos de control, fallas administrativas, incumplimientos normativos, atrasos, o cualquier acontecimiento que menoscabe la prestación del servicio, protección de confidencialidad o vínculos comerciales.

Para complementar la asignación de roles y responsabilidades, se propone utilizar una matriz RACI. Esta herramienta permite clarificar la participación de los actores en una actividad, identificando quién es responsable de ejecutar, quién aprueba, quién debe ser consultado y quién debe ser informado. Además, contribuye a reducir la confusión y la superposición de responsabilidades al establecer una propiedad clara de las tareas y las vías de comunicación entre los participantes (Atlassian, s. f.).

Tabla 24

Significado de la matriz RACI

Sigla	Significado	Descripción
R	Responsable	Persona o área que ejecuta la actividad.
A	Aprobador	Persona o área que toma la decisión final y responde por el resultado.
C	Consultado	Persona o área que aporta información, criterio o resultado de la actividad.
I	Informado	Persona o área que debe conocer el avance o resultado de la actividad.

Tabla 25

Matriz RACI

Actividad del Sistema de Gestión de Riesgos	Alta dirección	Responsable del SGR	Gerencia de Asesoría en Riesgos	Gerencia de Precios de Transferencia	Colaboradores	Administración
Aprobar la política de Gestión de Riesgos	A	R	C	C	I	I
Definir la metodología de Gestión de Riesgos	A	R	C	C	I	C
Identificar riesgos por proceso	I	C	R	R	C	C
Elaborar la matriz de riesgos	I	R	C	C	C	C
Evaluar probabilidad e impacto	I	R	C	C	C	I
Aprobar tratamiento de riesgos críticos	A	R	C	C	I	I

(Continua)

(Continuación)

Actividad del Sistema de Gestión de Riesgos	Alta dirección	Responsable del SGR	Gerencia de Asesoría en Riesgos	Gerencia de Precios de Transferencia	Colaboradores	Administración
Ejecutar planes de tratamiento	I	C	R	R	R	C
Dar seguimiento a los riesgos	I	R	C	C	I	C
Presentar informe de riesgos a la alta dirección	A	R	I	I	I	C
Actualizar la matriz de riesgos	I	R	C	C	C	C

Nota. La matriz RACI muestra la participación de los principales roles de Stratos Asesores en las actividades del Sistema de Gestión de Riesgos. Esta herramienta permite definir con mayor precisión quién ejecuta cada actividad, quién aprueba las decisiones, quién debe ser consultado y quién debe mantenerse informado. Su aplicación facilita el seguimiento, evita confusiones en la asignación de funciones y fortalece la obligación de rendir cuentas dentro de la organización.

La rendición de cuentas se realizará mediante reportes periódicos, reuniones de seguimiento, actualización de la matriz de riesgos y revisión de los planes de tratamiento. Cada responsable deberá informar el avance de las acciones asignadas, los controles implementados, las dificultades encontradas y los riesgos nuevos que puedan surgir en sus procesos.

Tabla 26

Mecanismos de rendición de cuentas

Actividad de rendición de cuentas	Responsable	Responsable del SGR	Frecuencia	Evidencia
Presentación del estado general de los riesgos	Responsable del Sistema de Gestión de Riesgos	Alta dirección	Trimestral	Informe de riesgos / acta de reunión
Reporte de avance de planes de tratamiento	Líderes responsables del tratamiento	Responsable del Sistema de Gestión de Riesgos	Mensual, hasta el cierre del plan	Matriz actualizada / registro de seguimiento
Comunicación de riesgos altos o críticos	Responsable del Sistema de Gestión de Riesgos	Alta dirección	Inmediata, una vez identificado el riesgo	Correo formal / reporte ejecutivo
Actualización de la matriz de riesgos	Responsable del Sistema de Gestión de Riesgos	Alta dirección y Gerencias de cada área	Trimestral o cuando exista un cambio relevante	Matriz de riesgos actualizada
Registro de evidencias del sistema	Administración	Responsable del Sistema de Gestión de Riesgos	Permanente	Actas, correos, reportes y documentos de soporte
Revisión de cumplimiento de responsabilidades	Alta dirección y responsable del Sistema de	Gerencias de cada área y colaboradores involucrados	Trimestral	Acta de revisión / compromisos definidos

De esta manera, la asignación de roles, autoridades y responsabilidades permite que el Sistema de Gestión de Riesgos no dependa únicamente de una persona, sino que se integre en la operación diaria de Stratos Asesores. Esto fortalece la cultura de riesgos, mejora el seguimiento de los controles y facilita la toma de decisiones basada en información clara y oportuna.

5.5.4.4. Asignación de Recursos.

La asignación de recursos constituye un elemento fundamental para el diseño del Sistema de Gestión de Riesgos basado en la Organización Internacional de Normalización (ISO) 31000, debido a que permite determinar los medios necesarios para que la gestión de riesgos pueda ser aplicada de forma realista dentro de Stratos Asesores. La norma ISO 31000 señala que las directrices para gestionar el riesgo pueden adaptarse a cada organización de acuerdo con su contexto, permitiendo que la asignación de recursos debe ser proporcional a la estructura, necesidades y objetivos de la organización (Organización Internacional de Normalización, 2018).

Stratos Asesores actualmente no tiene un Sistema de Gestión de Riesgos formal, por lo que es necesario definir qué recursos se requieren para implementarlo y mantenerlo funcionando: personal, tecnología, documentos, presupuesto y tiempo. Esta definición debe ser realista considerando que la organización tiene aproximadamente 17 colaboradores y opera en dos áreas principales: Asesoría en Riesgos y Precios de

Transferencia. El objetivo no es crear una estructura complicada o costosa, sino identificar los recursos mínimos indispensables para que la gestión de riesgos sea práctica, ordenada y sostenible en el día a día. De esta forma, el sistema no será solo un documento que queda guardado, sino un proceso activo que se pueda ejecutar, monitorear y mejorar continuamente.

Tabla 27

Recursos requeridos para el Sistema de Gestión de Riesgos

Tipo de recurso	Recurso requerido	Aplicación en Stratos Asesores
Recursos humanos	Alta dirección, Responsable del Sistema de Gestión de Riesgos, Gerencias de cada área, colaboradores y soporte administrativo.	Permiten coordinar, ejecutar, reportar y dar seguimiento a las actividades de gestión de riesgos.
Recursos tecnológicos críticos	Laptops corporativas, OneDrive, Outlook, red Ubiquiti, controlador UDM-Pro-Max y software Stratos Rate Company.	Soportan la operación principal, la comunicación, el almacenamiento de información, la conectividad y la prestación de servicios.
Recursos tecnológicos de apoyo	Teams, ESET Endpoint Security, Contifico, página web, celular corporativo, Bluetti AC70P y NAS Synology.	Apoyan la colaboración, seguridad, respaldo, continuidad, administración y presencia institucional.
Recursos documentales	Política de gestión de riesgos, matriz de riesgos, mapa de calor, planes de tratamiento, actas e informes.	Permiten documentar, evidenciar y dar trazabilidad a la gestión de riesgos.
Recursos de tiempo	Reuniones de identificación, revisión de matriz, seguimiento de planes y reportes a la alta dirección.	Permiten mantener el sistema actualizado y evitar que la gestión de riesgos sea solo documental.
Recursos de capacitación	Socialización de ISO 31000, metodología de riesgos, roles, responsabilidades y reporte de eventos.	Fortalecen la cultura de riesgos y la participación de los colaboradores.

Asignación de Recursos Humanos.

El factor humano es fundamental para que el Sistema de Gestión de Riesgos funcione. En Stratos Asesores no es necesario crear nuevos puestos de trabajo, sino distribuir las responsabilidades entre el personal actual de acuerdo con sus funciones existentes. Esto asegura que la gestión de riesgos sea acorde al tamaño de la organización y se incorpore naturalmente en el trabajo diario de cada colaborador. La Dirección será responsable de respaldar el sistema, autorizar los recursos necesarios y tomar decisiones sobre los riesgos más importantes. Habrá una persona encargada de coordinar todas las actividades del Sistema de Gestión de Riesgos, mientras que los jefes de cada área y todos los colaboradores serán responsables de identificar los riesgos, implementar controles y hacer seguimiento a su evolución.

Tabla 28

Asignación de recursos humanos

Rol	Recurso asignado	Función relacionada con la gestión de riesgos
Alta dirección	Tiempo para revisión, aprobación y toma de decisiones.	Aprobar la política, metodología, recursos y planes de tratamiento de riesgos críticos.
Responsable del Sistema de Gestión de Riesgos	Tiempo para coordinación, seguimiento y actualización del sistema.	Coordinar la matriz de riesgos, planes de tratamiento, reportes y reuniones de seguimiento.
Gerencia de Asesoría en Riesgos	Participación técnica en riesgos de su línea de negocio.	Identificar y tratar riesgos asociados a cumplimiento, auditoría, seguridad, privacidad y continuidad.
Gerencia de Precios de Transferencia	Participación técnica en riesgos normativos, tributarios y documentales.	Identificar y tratar riesgos relacionados con informes, anexos,

		consultas, procesos contenciosos y cumplimiento.
Colaboradores	Participación en reportes, controles y cumplimiento de actividades.	Reportar eventos, debilidades, incidentes o situaciones que puedan afectar la operación o calidad del servicio.
Administración	Apoyo documental y operativo.	Gestionar actas, registros, evidencias, comunicaciones y documentación del sistema.

Nota. Con base en la información recopilada durante el desarrollo de la investigación.

Asignación de Recursos Tecnológicos y Documentales.

La tecnología es vital para que Stratos Asesores pueda prestar sus servicios, ya que la organización la utiliza para guardar información, comunicarse con clientes, almacenar documentos y entregar sus trabajos. Por eso, contar con las herramientas y documentos adecuados es fundamental para mantener el Sistema de Gestión de Riesgos funcionando correctamente y disponible cuando se necesite. La organización utilizará plataformas como Microsoft 365, OneDrive, Teams y el correo corporativo para organizar toda la información del sistema en un solo lugar, facilitar la comunicación entre el equipo y guardar registros que demuestren qué se ha hecho y cuándo se ha hecho.

Tabla 29

Recursos tecnológicos y documentales

Recurso	Uso propuesto	Evidencia generada
OneDrive	Almacenamiento de política, matriz de riesgos, mapa de calor, planes de tratamiento y evidencias.	Documentos actualizados y controlados.

Outlook	Comunicación formal sobre riesgos, responsabilidades, planes de tratamiento, cambios relevantes y reportes.	Correos enviados y recibidos.
Teams	Reuniones de seguimiento, coordinación de actividades y consultas internas.	Convocatorias, actas o registros de reunión.
Laptops corporativas	Ejecución de actividades operativas, análisis de información y elaboración de entregables.	Registros de uso, documentos generados y evidencias de trabajo.
ESET Endpoint Security	Protección de equipos frente a virus, malware y amenazas digitales.	Reportes de seguridad o alertas generadas.
Infraestructura Ubiquiti y UDM-Pro-Max	Conectividad, segmentación y protección de la red corporativa.	Configuraciones, registros o reportes del proveedor tecnológico.
NAS Synology	Respaldo de información relevante para la organización.	Registros de respaldo o evidencia de almacenamiento.
Stratos Rate Company	Soporte especializado para análisis de comparación empresarial en precios de transferencia.	Resultados, reportes o análisis generados por la herramienta.
Matriz de riesgos y mapa de calor	Registro, análisis, evaluación y visualización de los riesgos identificados.	Matriz actualizada y mapa de calor vigente.
Planes de tratamiento	Definición de acciones, responsables, plazos y seguimiento.	Planes aprobados y registros de avance.
Actas e informes	Evidencia de decisiones, revisiones, compromisos y avances del sistema.	Actas firmadas o informes emitidos.

Asignación de Tiempo para la Gestión de Riesgos.

El Sistema de Gestión de Riesgos no puede ser solo un documento guardado en una carpeta; necesita tiempo real dedicado para funcionar. La organización debe reservar

tiempo regularmente para revisar los riesgos, analizarlos, darles seguimiento y actualizarlos, especialmente cuando aparezcan nuevos riesgos, cuando cambien las leyes, cuando haya problemas con la tecnología, cuando se modifiquen los procesos o cuando algo pueda afectar a los clientes. El tiempo dedicado debe ser realista y compatible con el trabajo diario de Stratos, por eso se establecerá un calendario de actividades regulares que permita que el sistema funcione continuamente. Los riesgos más graves o importantes recibirán mayor seguimiento y atención que los demás.

Tabla 30

Tiempo requerido para la gestión de riesgos

Actividad	Participantes	Frecuencia	Recurso de tiempo requerido
Socialización del Sistema de Gestión de Riesgos	Alta dirección, Responsable del Sistema de Gestión de Riesgos, Gerencias de cada área y colaboradores.	Al inicio de la implementación.	Una sesión inicial de inducción.
Identificación de riesgos por área	Responsable del Sistema de Gestión de Riesgos, Gerencias de cada área y colaboradores.	Trimestral o cuando existan cambios relevantes.	Reuniones de trabajo por área.
Actualización de la matriz de riesgos	Responsable del Sistema de Gestión de Riesgos y Gerencias de cada área.	Trimestral.	Tiempo para revisión, análisis y actualización documental.
Seguimiento de planes de tratamiento	Responsable del Sistema de Gestión de Riesgos y Gerencias responsables del tratamiento.	Mensual para riesgos altos y críticos.	Reuniones breves de seguimiento.
Reporte a la Alta dirección	Responsable del Sistema de Gestión de Riesgos.	Trimestral.	Preparación y presentación del informe de riesgos.

Revisión de recursos necesarios	Alta dirección y Responsable del Sistema de Gestión de Riesgos.	Semestral.	Evaluación de recursos humanos, tecnológicos, financieros y documentales.

Priorización de Recursos.

La organización debe decidir dónde invertir sus recursos considerando cuáles son los más importantes, qué tan grave sería si fallan o no funcionan, y cómo eso afectaría al negocio. Con esto en mente, Stratos debe enfocarse primero en proteger los recursos que son fundamentales: las herramientas necesarias para entregar sus servicios, la información confidencial que comparten los clientes, la capacidad de seguir trabajando si algo falla, la conexión a internet, el cumplimiento de las leyes y normas aplicables, y la calidad del trabajo que entrega a sus clientes.

Tabla 31

Criterios para priorizar la asignación de recursos

Criterio de priorización	Descripción	Aplicación en la organización
Criticidad del activo	Se priorizan los activos marcados como críticos.	Laptops, OneDrive, Outlook, red Ubiquiti, controlador UDM-Pro-Max y Stratos Rate Company.
Impacto en la operación	Se asignan recursos a elementos que soportan la prestación diaria de servicios.	Equipos, conectividad, plataformas de almacenamiento y herramientas de análisis.
Protección de información	Se priorizan recursos que resguardan información sensible de clientes.	OneDrive, Outlook, laptops corporativas, ESET y NAS Synology.
Continuidad del servicio	Se consideran recursos que permiten mantener la operación ante fallas o interrupciones.	Bluetti AC70P, NAS Synology, red Ubiquiti y plataformas en la nube.

Cumplimiento y reputación	Se priorizan recursos que reducen errores, incumplimientos o afectaciones a clientes.	Stratos Rate Company, Contifico, correo corporativo y documentación del sistema.
Disponibilidad presupuestaria	Se evalúa si los recursos actuales son suficientes antes de propones nuevas inversiones.	Uso de herramientas existentes antes de adquirir nuevas soluciones tecnológicas.

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

En resumen, Stratos Asesores debe asignar sus recursos de forma realista, práctica y acorde con su situación como organización de aproximadamente 17 colaboradores. El Sistema de Gestión de Riesgos no necesita ser complicado, sino distribuir bien el trabajo entre las personas, aprovechar la tecnología disponible, mantener documentos organizados, destinar presupuesto cuando sea necesario y reservar tiempo para que funcione. La tecnología es tan importante como las personas y los documentos: laptops, plataformas como Microsoft 365, conexión a internet, herramientas de seguridad, respaldos de información, sistemas administrativos y software especializado son recursos clave que permiten que el sistema funcione y que la organización pueda continuar sus operaciones, mantener la información de clientes protegida, entregar trabajos de calidad y ser confiable. Con una buena asignación de recursos, Stratos Asesores tendrá un Sistema de Gestión de Riesgos realista y sostenible que proteja lo más importante del negocio, mejore las decisiones que toma, resguarde la información confidencial y desarrolle una cultura en la que prevenir y gestionar riesgos es responsabilidad de todos.

5.5.4.5. Establecimiento de la comunicación y la consulta

De acuerdo con los principios transversales de la norma ISO 31000:2018, la comunicación y la consulta con las partes interesadas (tanto internas como externas) constituyen un pilar fundamental para garantizar que el Sistema de Gestión de Riesgos (SGR) sea dinámico e inclusivo y útil para la toma de decisiones. En Stratos Asesores S.A.S., este proceso se estructura considerando que la comunicación no debe limitarse a informar, sino que debe permitir escuchar, consultar y retroalimentar oportunamente a las partes interesadas.

Por lo cual, los mecanismos definidos para la comunicación y consulta deberán ser bidireccionales y oportunos. Esto implica que la Alta dirección, gerencias de cada área, colaboradores, clientes, proveedores tecnológicos y demás partes interesadas podrán acceder a información relevante, presentar observaciones, reportar incidentes o eventos ocurridos, realizar consultas y recibir retroalimentación sobre las medidas establecidas. Con lo cual se favorece una comunicación bidireccional, permitiendo que la información circule de manera efectiva y aporte a la identificación, análisis, tratamiento y monitoreo de los riesgos.

A continuación, se proponen los mecanismos de comunicación, consulta y retroalimentación dentro del Sistema de Gestión de Riesgos para la organización:

Tabla 32

Establecimiento de la comunicación

Información a comunicar	Alcance	Responsable de comunicar	Medio	Frecuencia	Evidencia
Política de gestión de riesgos	Todos los colaboradores	Alta dirección y el responsable del Sistema de Gestión de Riesgos	Correo electrónico y reuniones (Presencial/teams)	Al aprobarse o actualizarse	Política formalmente documentada/ Aprobada/ Correo electrónico enviado
Roles y responsabilidades (Matriz RACI)	Colaboradores y gerencias de cada área	Responsable del Sistema de Gestión de Riesgos	Reunión (Presencial/teams)	Inicio del proceso de implementación	Acta de reunión (Registro de asistencia)
Metodología de identificación y evaluación de riesgos	Gerencias de cada área	Responsable del Sistema de Gestión de Riesgos	Capacitación y o reunión (presencial o temas)	Inicio de la implementación y cuando se actualice	Presentación de la metodología y acta de reunión. (Registro de asistencia)
Riesgos críticos	Alta dirección	Responsable del Sistema de Gestión de Riesgos.	Reporte ejecutivo	Trimestral o inmediato cuando aplique	Informe de riesgo.

(Continua)

(Continuación)

Información a comunicar	Alcance	Responsable de comunicar	Medio	Frecuencia	Evidencia
Plan de tratamiento	Gerencias de cada área y propietario de riesgos	Responsable del Sistema de Gestión de Riesgos	Correo electrónico y reuniones (Presencial/teams)	Mensual y cuando exista un cambio relevante en el tratamiento de riesgos	Plan aprobado / matriz de riesgos actualizada
Avance de acciones correctivas o controles	Alta dirección y los Gerencias de cada área	Responsable del Sistema de Gestión de Riesgos	Reunión / Matriz de seguimiento	Con frecuencia trimestral	Acta de reunión / matriz actualizada
Cambios relevantes en los riesgos identificados	Alta dirección y gerencias de cada área relacionados con el riesgo	Responsable del Sistema de Gestión de Riesgos y el líder del área correspondiente	Correo electrónico/ reuniones (Presencial/ teams)	Una vez identificado, deberá reportarse en dos días laborales	Acta de reunión / Matriz actualizada y correo electrónico

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

El proceso de comunicación busca asegurar que la información relacionada con el Sistema de Gestión de Riesgos fluya de manera bidireccional. De manera que, la organización informa sobre las políticas aprobadas, responsabilidades asignadas, metodología establecida, riesgos relevantes, planes de tratamiento y avances alcanzados. Y así mismo, recopila observaciones, inquietudes, reportes de incidentes y retroalimentación por parte de los colaboradores, gerencias de cada área, clientes (encuestas de satisfacción por el servicio prestado) y demás partes interesadas. Promoviendo que la comunicación abarque la participación, oportunidad en la respuesta y el soporte para la adecuada toma de decisiones y no solo en transmitir información.

Tabla 33

Establecimiento de Consulta

Consulta a realizar	Participantes	Objetivo	Medio	Frecuencia	Evidencia
Consulta inicial por riesgo en cada área	Gerencia de cada área y colaboradores	Identificar el riesgo en cada proceso	Reunión	Inicio de proceso de implementación	Registro de riesgos identificados
Consulta sobre los controles existentes	Gerencia de cada área	Conocer los controles existentes y debilidades	Reunión	Trimestral	Acta de reunión / matriz actualizada
Consulta sobre incidentes o eventos ocurridos	Colaboradores	Detectar fallas, errores o problemas operativos	Correo electrónico / reunión	Cuanto ocurra un incidente o evento	Registro del evento
Consulta a clientes	Clientes seleccionados	Conocer las expectativas	Encuesta de	Al cierre de cada proyecto	Informe

		sobre calidad, cumplimiento, confidencialidad y servicio.	satisfacción / Reunión	y semestral para clientes recurrentes.	Consolidado Satisfacción de Clientes
Consulta sobre cambios normativos o tecnológicos	Gerencia de cada área.	Identificar nuevos riesgos por cambios externos e internos	Reunión técnica	Cuando exista un cambio relevante	Informe o acta de reunión.

El establecimiento de consulta está diseñado para la escucha activa y la recolección de retroalimentación tanto interna como externa, lo que alimenta y actualiza el sistema con datos de la realidad operativa. Este esquema permite que los colaboradores, gerencias de cada área y clientes aporten observaciones sobre riesgos, controles de incidentes y cambios relevantes. Asimismo, la inclusión de encuestas de satisfacción efectuadas a los clientes al finalizar cada proyecto permite evaluar la confidencialidad y calidad del servicio, junto al monitoreo de cambios normativos, demuestra que la organización no solo mira hacia adentro, sino que evalúa constantemente los riesgos del entorno exterior.

Este esquema permitirá que la comunicación y la consulta funcionen como procesos permanentes dentro del Sistema de Gestión de Riesgos. La información recibida en reuniones, correos, reportes, encuestas, registros de incidentes o matrices de seguimiento deberá ser revisada por los responsables correspondientes e incorporada

en la matriz de riesgos, los controles, los planes de tratamiento o las acciones de mejora.

Stratos Asesores S.A.S. asegurará que la comunicación no sea solo para informar decisiones o lineamientos, sino también para recibir observaciones, analizar necesidades y gestionar los riesgos de manera oportuna.

Tabla 34

Mecanismo bidireccional de comunicación y consulta

Mecanismo	Fuente de información	Responsable de analizar la información	Retroalimentación esperada	Evidencia
Reuniones con gerencias de cada área	Comentarios sobre riesgos, controles de incidentes y necesidades de cada área	Responsable del Sistema de Gestión de Riesgos y Gerencia correspondiente	Respuesta sobre acciones a tomar, actualización de matriz o modificación de controles	Acta de reunión y matriz actualizada
Correo electrónico	Reportes, consultas, observaciones o alertas relacionadas con riesgos	Responsable del Sistema de Gestión	Respuesta formal sobre la revisión realizada o acción definida	Correo enviado y respuesta a dicho correo
Microsoft Teams	Consultas, coordinación de actividades o reuniones.	Responsable del Sistema de Gestión de Riesgos y Gerencia correspondiente.	Confirmación, asignación de responsable o programación de reunión.	Acta o registro de conversación
Encuestas de satisfacción del servicio	Opiniones sobre calidad, confidencialidad y cumplimiento del servicio	Gerencia correspondiente y Responsable del Sistema de	Análisis de resultados y acciones a mejorar cuando aplique	Informe consolidado de satisfacción de clientes

		Gestión de Riesgos		
Registro de incidentes o eventos	Información sobre errores, retrasos, fallas de control o incidentes tecnológicos	Responsable del Sistema de Gestión de Riesgos y área involucrada	Definición de acciones correctivas o actualización de controles	Registro del evento y plan de acción

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

De esta manera, las partes interesadas no solo reciben información del Sistema de Gestión de Riesgos, sino que también pueden reportar, consultar, opinar y retroalimentar sobre riesgos, controles, incidentes o cambios relevantes. Las respuestas recibidas deberán ser analizadas y utilizadas para fortalecer la gestión de riesgos, dejando evidencia de las decisiones y acciones adoptadas.

Comunicación e Involucramiento Interno: Se implementan canales bidireccionales dinámicos para sensibilizar al factor humano y fortalecer la participación de los colaboradores. Los colaboradores y el personal administrativo no solo serán receptores de las políticas, procedimientos o lineamientos, sino que actuarán como una fuente activa de información para reportar riesgos, incidentes, debilidades de control y oportunidades de mejora.

Consulta y Relación con Partes Interesadas Externas: Dado que la organización maneja información tributaria, estratégica y de alta sensibilidad de sus clientes, la

consulta externa permitirá conocer expectativas relacionadas con calidad de servicio, confidencialidad, cumplimiento de plazos y continuidad. De igual manera, se tomará en cuenta el monitoreo de los requerimientos emitidos por las entidades de control, proveedores tecnológicos y actualizaciones de normativas que puedan originar nuevos riesgos o generar cambios en los riegos ya identificados.

Para facilitar la visualización y el despliegue estructurado de las interacciones institucionales, se resume la estrategia de comunicación y consulta en las siguientes tablas, diferenciando las acciones según su alcance interno o externo.

Tabla 35

Partes interesadas interno y externo

Parte Interesada	Tipo	Descripción
Alta dirección	Interno	Recibe reportes y toma decisiones sobre riesgos relevantes.
Responsable de gestión de riesgo	Interno	Coordina la comunicación la consulta y el seguimiento
Lideres de áreas	Interno	Informar riesgos de sus procesos y validan controles
Colaboradores	Interno	Reportan riesgos incidentes debilidades y oportunidades de mejora
Clientes	Externo	Comunican expectativas sobre calidad confidencialidad cumplimiento y continuidad de servicio
Proveedores tecnológicos	Externo	Intervienen cuando existan riesgos asociados a herramientas, soporte, hosting, respaldos o plataformas digitales.
Entidades de control	Externo	Se analizan considerando exposiciones frente a marcos legales, obligaciones tributarias, relaciones laborales, privacidad de la información, cumplimiento de la normativa.

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

En resumen, la comunicación y consulta en Stratos Asesores S.A.S. busca asegurar que la información vinculada con los riesgos sea transmitida, recibida, revisada y retroalimentada de forma oportuna. Bajo este enfoque, el Sistema de Gestión de Riesgos no se limitará a ser un proceso documental, sino que actuará como una herramienta participativa para detectar nuevos riesgos, verificar la efectividad de los controles, gestionar incidentes y reforzar la toma de decisiones con base a la información actualizada.

5.5.5. Implementación

La fase de implementación plantea la forma en que la organización debería poner en marcha el marco de referencia de la gestión del riesgo una vez que la Alta Dirección apruebe la implementación del sistema. De acuerdo con la norma ISO 31000:2018, para implementar el marco de gestión de riesgos es necesario contar con un plan que defina los plazos, recursos y responsables. Este plan debe permitir identificar cómo se toman las decisiones dentro de la organización, los procesos de toma de decisiones deben ser ajustados para incorporar la gestión del riesgo, procurando que las acciones definidas sean claras, comprendidas y aplicadas correctamente.

Por lo tanto, se plantea una implementación progresiva, estructurada en fases consecutivas, con el fin de que el equipo pueda familiarizarse con el sistema antes de aplicarlo de forma permanente. La primera ejecución completa del proceso de gestión

del riesgo, que comprende la identificación, análisis, evaluación y tratamiento de los riesgos, se desarrollará como un plan piloto. Sus resultados se presentarán en la sección 5.6 Proceso. A continuación, se muestra el cronograma propuesto para su implementación:

Tabla 36

Cronograma propuesto para la implementación del SGR

Fase	Actividades	Responsable Propuesto	Plazo Estimado
1	Aprobación de la política, metodología y los criterios de riesgo por parte de la Alta Dirección.	Alta Dirección	1 mes
2	Designación del Responsable del SGR, formalización de roles (matriz RACI) y creación del repositorio del SGR en OneDrive.	Alta Dirección y Responsable del SGR	1 mes
3	Socialización y capacitación al personal según el rol.	Responsable del SGR	2 meses
4	Integración de la gestión del riesgo en los puntos de decisión existentes.	Responsable del SGR y Gerencias de área	2 meses
5	Primera aplicación del proceso de gestión del riesgo por área (plan piloto)	Responsable del SGR y Gerencias de área.	3 meses
6	Revisión y ajuste del sistema con base en los resultados del plan piloto.	Alta Dirección y Responsable del SGR	3 meses
7	Operación regular, seguimiento y reporte periódico a la Alta Dirección.	Responsable del SGR	Permanente

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

La propuesta establece de manera clara dónde, cuándo, cómo y quién toma las decisiones relacionadas con la gestión del riesgo, considerando la estructura

organizacional y los espacios de coordinación que la organización ya utiliza en su operación diaria. Lo cual permite que las decisiones sobre los riesgos no se gestionen como una actividad aislada, sino como parte de los procesos habituales de planificación, seguimiento y control de las áreas involucradas.

La Tabla 37 presenta los principales puntos de decisión propuestos para la gestión del riesgo en la organización. Mediante la cual se identifican las decisiones clave, momento y espacio en que se tomarán, los responsables de su aprobación o ejecución, y la forma en que serán documentadas, permitiendo asegurar que las decisiones relacionadas con el riesgo sean claras, oportunas y debidamente respaldadas.

Tabla 37

Puntos de decisión propuestos para la gestión del riesgo

Decisión	Dónde y Cuándo	Quién Decide	Evidencia
Aprobar la política y los criterios de riesgo	Reunión de dirección, al inicio del sistema	Alta Dirección	Acta de reunión / Política aprobada
Identificar y registrar riesgos	Reunión semanal y trimestral por área	Gerencias de área y colaboradores	Registro en la matriz de riesgos
Aceptar riesgos bajos y moderados	Reunión de seguimiento	Responsable del SGR y Gerencias de área	Matriz de riesgos actualizada y acta de reunión
Aprobar el tratamiento de riesgos altos	Reunión mensual de seguimiento	Responsable del SGR y Gerencias de área	Plan de tratamiento aprobado
Aprobar o aceptar riesgos críticos	Reunión trimestral o extraordinaria	Alta Dirección	Acta de reunión o reporte ejecutivo
Gestionar cambios de alcance	Reunión quincenal con el cliente	Gerencias de área	Comunicación formal al cliente

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

La implementación debe incorporar actividades relacionadas con la gestión del riesgo por lo cual en la planificación de cada proyecto se incluirá una revisión inicial de los riesgos vinculados con el alcance, plazos y disponibilidad de información entregada por el cliente. Durante la ejecución, las reuniones semanales podrán incluir un espacio para comunicar nuevos riesgos en caso de existir, desviaciones o situaciones que requieran atención. De igual forma, debe existir una revisión por pares realizadas por la Alta Dirección y Gerencias para el control de calidad y podrán registrarse dentro de la matriz de riesgos. Finalmente, en la gestión con el cliente, las reuniones quincenales permitirán anticipar posibles cambios de alcance y alinear las expectativas.

De igual forma, se propone contemplar las siguientes acciones con el fin de que el Sistema de Gestión de Riesgos sea comprendido y aplicado por los distintos niveles de la organización.

- **Socialización inicial:** reunión dirigida a todo el personal de la organización para explicar el propósito del sistema, los principios de la ISO 31000 y la participación esperada de cada colaborador.
- **Capacitación diferenciada por rol:** dependiendo de cada rol asignado al personal de la organización se deberá crear un plan de capacitación propuesto, con contenidos y duración.
- **Manual y repositorio documental:** definir un repositorio digital en OneDrive para la política, metodología, matriz de riesgos y formatos con convenciones de nomenclatura y controles de versiones.

- **Comunicación continua:** definir los canales de comunicación tales como correo, Teams, grupos corporativos de WhatsApp para reportar riesgos, resolver dudas y retroalimentar al equipo.

  En definitiva, la implementación requerirá el compromiso permanente de la Alta Dirección, participación consciente de las partes interesadas y la asignación adecuada del tiempo y los recursos. De esta forma la organización podrá gestionar de manera más clara la incertidumbre asociada a sus decisiones e integrar la gestión del riesgo en sus actividades diarias. Esto permitirá establecer una base sólida para realizar el seguimiento, evaluación y la mejora continua del sistema.

5.5.6. Valoración

La valoración constituye una fase esencial dentro del marco de referencia del Sistema de Gestión de Riesgos (SGR), ya que permite determinar si los niveles de riesgo identificados y analizados son aceptables para la organización, considerando sus objetivos estratégicos, operativos, de cumplimiento y reputacionales. De acuerdo con la ISO 31000:2018, la valoración implica comparar los resultados del análisis de riesgos con los criterios previamente establecidos, con el fin de priorizar aquellos riesgos que requieren tratamiento y definir la respuesta más adecuada para cada caso.

En Stratos Asesores S.A.S., la valoración se realizará con base en los resultados obtenidos en la matriz de riesgos y en el mapa de calor, utilizando una escala de probabilidad e impacto de 1 a 5. El nivel de riesgo se obtiene multiplicando ambos valores, generando una clasificación de riesgo bajo, medio, alto o crítico. La

valoración permite revisar si el diseño propuesto responde a la realidad de la organización, a su tamaño, a sus recursos disponibles y a la naturaleza de sus servicios profesionales. En este sentido se evalúa si el sistema es funcional para una organización de aproximadamente 17 colaboradores y si puede integrarse en sus dos líneas principales de negocio Asesoría en Riesgos y Precios de Transferencia. Adicional, permite confirmar si los componentes desarrollados en el marco de referencia como por ejemplo la política de gestión de riesgos, la asignación de roles, la comunicación y consulta, la asignación de recursos, la matriz de riesgos, el mapa de calor y los planes de tratamiento están alineados entre sí y contribuyen a fortalecer la toma de decisiones de la organización.

Tabla 38

Criterios para valorar el Sistema de Gestión de Riesgos

Criterio de valoración	Aspecto evaluado	Aplicación en la organización
Pertinencia	Verifica si el sistema responde a las necesidades reales de la organización.	El sistema se enfoca en riesgos asociados a información de clientes, cumplimiento, continuidad, calidad de entregables y reputación.
Proporcionalidad	Evalúa si el sistema es adecuado al tamaño y recursos de la organización.	La propuesta evita una estructura compleja y se adapta a una organización de aproximadamente 17 colaboradores.
Integración	Revisa si la gestión de riesgos se incorpora en los procesos y decisiones.	El sistema se vincula con Asesoría en Riesgos, Precios de Transferencia, administración, tecnología y atención a clientes.
Claridad de responsabilidades	Verifica si los roles y autoridades están definidos.	Se asignan responsabilidades a la Alta dirección, Responsable del Sistema de Gestión de Riesgos, Gerencias de cada

		área, colaboradores y soporte administrativo.
Utilidad para la toma de decisiones	Evalúa si la información generada permite priorizar acciones.	La matriz de riesgos y el mapa de calor permiten identificar riesgos altos y críticos para definir tratamientos.
Capacidad de seguimiento	Verifica si existen mecanismos para revisar avances y actualizar información.	Se establecen reportes, reuniones, evidencias, seguimiento de planes y revisión periódica del sistema.

El Sistema de Gestión de Riesgos permite identificar los riesgos asociados a cada línea de servicio, establecer responsabilidades, recursos, mecanismos de comunicación, criterios de priorización y acciones de seguimiento. La efectividad del sistema dependerá de la actualización periódica de la matriz de riesgos, el seguimiento de los planes de tratamiento, la participación de las gerencias de cada área y el respaldo de la alta dirección en la toma de decisiones.

Los KPI son métricas que permiten la recopilación de información importante para las decisiones del proyecto, estos KPI ayudan a la identificación de las debilidades y fortalezas de la organización, y permiten definir el cumplimiento de los objetivos estratégicos planteados por la gerencia de tal manera que, sean la radiografía para las partes interesadas de cómo se encuentra la organización. (Acuña, 2025)

Para complementar la valoración del Sistema de Gestión de Riesgos se propone el uso de indicadores claves del desempeño (KPI) los cuales permitirán medir si el sistema está siendo aplicado de manera efectiva dentro de la organización, permitiendo evaluar

el funcionamiento del sistema, el cumplimiento de las actividades planificadas y la efectividad del seguimiento realizado.

Los KPIs permitirán identificar si los riesgos están siendo revisados oportunamente, si los planes de tratamiento se cumplen dentro de los plazos establecidos, si los colaboradores participan en la gestión de riesgos y si la información generada permite tomar decisiones preventivas.

Tabla 39

KPIs propuestos para valoración del Sistema de Gestión de Riesgos

Indicador clave de desempeño	¿Qué mide?	Forma de medición	Meta sugerida	Frecuencia
Revisión de la matriz de riesgos	Verifica si la matriz se revisa de forma periódica.	Matriz revisada dentro del período establecido.	1 revisión trimestral	Trimestral
Cumplimiento de planes de tratamiento	Mide si las acciones definidas para tratar los riesgos se cumplen.	Acciones cumplidas / acciones planificadas × 100	≥ 85%	Mensual
Riesgos altos y críticos con tratamiento	Verifica si los riesgos más importantes tienen acciones definidas.	Riesgos altos y críticos con plan de tratamiento / total de riesgos altos y críticos × 100	100%	Trimestral
Reportes presentados a la Alta dirección	Mide si la información de riesgos llega oportunamente a los Socios.	Reportes presentados / reportes planificados × 100	100%	Trimestral
Colaboradores capacitados	Verifica si el personal conoce la metodología y sus responsabilidades.	Colaboradores capacitados / total de colaboradores × 100	≥ 90%	Anual

Incidentes o eventos registrados	Mide si los eventos de riesgo son reportados y documentados	Número de incidentes o eventos registrados	Registro de todos los eventos conocidos	Cuando se presente un incidente o evento

Basándonos en los KPIs propuestos y su forma de medición es necesario explicar cómo se aplicará cada indicador dentro del Sistema de Gestión de Riesgos de Stratos Asesores. En otras palabras, los indicadores no son solo números que se registran, sino herramientas que permiten verificar si la gestión de riesgos realmente está funcionando: si se están ejecutando las actividades planeadas, si se está documentando lo que se hace y si se están revisando los resultados de forma correcta. Por lo cual es necesario mencionar lo siguiente:

En el caso de la revisión de la matriz de riesgos, la medición consiste en verificar si la matriz fue revisada dentro del período establecido. Por ejemplo, si la revisión debe hacerse trimestralmente, se comprobará que exista una matriz actualizada o un acta que evidencie dicha revisión.

Para el cumplimiento de planes de tratamiento, la medición se realiza comparando las acciones cumplidas frente a las acciones planificadas. Por ejemplo, si se planificaron 10 acciones de tratamiento y se cumplieron 8, el cumplimiento sería del 80%.

En el indicador de riesgos altos y críticos con tratamiento, se revisa si todos los riesgos clasificados como altos o críticos cuentan con un plan de tratamiento definido. Esto permite asegurar que los riesgos más relevantes no queden únicamente identificados, sino que tengan acciones concretas para gestionarlos.

En cuanto a los reportes presentados a los Socios, la medición consiste en comparar los reportes que efectivamente fueron presentados frente a los reportes que estaban planificados. Por ejemplo, si se estableció presentar un reporte trimestral, deberá existir evidencia del informe entregado o de la reunión realizada.

Para el indicador de colaboradores capacitados, se mide cuántos colaboradores recibieron capacitación sobre la gestión de riesgos en relación con el total de colaboradores de Stratos. Esto permite verificar si el personal conoce la metodología, sus responsabilidades y la forma de reportar eventos de riesgo.

Respecto al indicador de incidentes o eventos registrados, la medición consiste en verificar que los eventos de riesgo conocidos hayan sido documentados. Esto puede incluir errores, retrasos, incidentes tecnológicos, fallas de control, problemas con entregables o situaciones que puedan afectar la operación, la confidencialidad o la reputación de Stratos Asesores.

En conclusión, evaluar el Sistema de Gestión de Riesgos verifica que el modelo es adecuado para Stratos Asesores y funciona en la práctica. Los indicadores propuestos permiten medir el desempeño del sistema y facilitan la mejora continua.

5.5.7. Mejora

La mejora del Sistema de Gestión de Riesgos busca mantenerlo actualizado, útil y alineado con la realidad de la organización. Por lo cual, una vez realizada la valoración del sistema usando los criterios e indicadores definidos, los resultados obtenidos deben utilizarse para identificar que se puede mejorar, corregir lo que no está funcionando y

fortalecer la prevención de riesgos. La mejora es un proceso permanente que permite revisar si la política, los roles, los recursos, la comunicación, los riesgos identificados, los planes de acción y los controles siguen siendo apropiados.

Considerando que la organización está implementando su primer Sistema de Gestión de Riesgos y necesita desarrollar una cultura de riesgos practica y sostenible. La mejora del sistema se apoyará en la información obtenida de los reportes, reuniones de seguimiento, actualización de la matriz de riesgos, avance de los planes de tratamiento, registro de incidentes y resultados de los KPI. Cuando un indicador no alcance la meta establecida, el responsable del Sistema de Gestión de Riesgos en conjunto con las gerencias de cada área deberá analizar la causa, proponer acciones correctivas y reportar los avances a la alta dirección.

5.5.7.1. Adaptación.

La adaptación en Stratos Asesores S.A.S. permitirá que el Sistema de Gestión de Riesgos se mantenga actualizado frente a cambios internos o externos que puedan modificar la exposición de la organización al riesgo. La ISO 31000:2018 establece que el marco debe adaptarse según el contexto de la organización (Organización Internacional de Normalización, 2018). La organización deberá revisar periódicamente el marco y ajustarlo cuando sea necesario. Como Stratos trabaja por proyectos en sus distintas áreas de trabajo, esta revisión deberá considerar los cambios que puedan afectar la calidad del servicio, la continuidad operativa, el cumplimiento de los compromisos asumidos con los clientes o el manejo seguro de la información.

La revisión del marco se realizará una vez al año y también cuando ocurran cambios relevantes en la organización o en su entorno. Entre estos cambios se incluyen: modificaciones normativas, nuevos servicios o clientes, ajustes en herramientas tecnológicas, incidentes de seguridad, retrasos, cambios en contratos o acuerdos de confidencialidad, observaciones internas y variaciones en la capacidad operativa del equipo.

Tabla 40

Cambios y acciones para la adaptación del marco de gestión de riesgos en Stratos Asesores S.A.S.

Tipo de cambio	Descripción	Acción
Cambios normativos	Cambios en normas relacionadas con los servicios de la organización o con la protección de datos personales.	Identificar los riesgos relacionados y actualizar los documentos o controles que correspondan.
Cambios tecnológicos	Actualizaciones o cambios en Microsoft 365, OneDrive, Outlook, Teams, NAS, sitio web, Stratos Rate Company, plataformas tecnológicas o mecanismos de acceso.	Verificar permisos, respaldos, trazabilidad, control de versiones y medidas de seguridad de la información.
Cambios operativos	Ajustes en la planificación de proyectos, incorporación de nuevos servicios, cambios en los requerimientos del cliente o variaciones en los plazos de trabajo.	Actualizar los riesgos identificados, los controles de seguimiento, la comunicación con clientes y las prioridades de atención.
Cambios organizacionales	Incorporación de personal, rotación, ausencias, redistribución de funciones o aumento de carga laboral.	Ajustar roles, distribución de actividades, la capacidad operativa y necesidades de capacitación.
Incidentes u observaciones	Retrasos, retrabajos, errores técnicos, accesos indebidos, observaciones de clientes u observaciones internas.	Definir acciones correctivas o preventivas y actualizar controles cuando sea necesario.

Los cambios definidos a partir de estas revisiones deberán quedar documentados mediante actas, matrices, informes o cualquier documento interno que corresponda. Cuando el ajuste requiera recursos, cambios en funciones o decisiones de mayor alcance, deberá ser validado por la Alta Dirección o por las gerencias correspondientes. Con esto, el marco de gestión de riesgos podrá mantenerse útil para la organización y seguir apoyando la calidad del servicio, la continuidad operativa y la confianza de los clientes.

5.5.7.2. Mejora continua.

La mejora continua busca que el marco de Stratos Asesores S.A.S. se revise, se ajuste con base en sus resultados y se mantenga útil para identificar, tratar y dar seguimiento a los riesgos. Este proceso se apoyará en auditorías, revisiones periódicas, análisis de resultados y tratamiento de hallazgos. Su finalidad será mantener el marco actualizado, adecuado y efectivo, de modo que el sistema funcione como una herramienta de apoyo para la gestión, la prevención de errores y retrasos, el fortalecimiento de controles y la toma de decisiones.

Para aplicar este proceso, se establecen fases de seguimiento y mejora acordes con la forma de trabajo de Stratos Asesores S.A.S. En la Tabla 41 se detallan estas fases y las acciones previstas para su desarrollo:

Tabla 41

Fases para la mejora continua del marco de gestión de riesgos en Stratos Asesores S.A.S.

Fase	Actividad	Encargado	Frecuencia	Evidencia

Auditoría inicial	Realizar una revisión inicial del marco de gestión de riesgos mediante una lista de verificación, considerando los riesgos identificados, los controles, los roles y los mecanismos de seguimiento.	Responsable de Seguridad / Áreas involucradas	Una vez aprobado el marco	Informe de auditoría inicial con aspectos por mejorar.
Revisiones y auditorías periódicas	Revisar periódicamente el funcionamiento del marco de gestión de riesgos, considerando la ejecución de proyectos, los controles aplicados, los riesgos identificados, los incidentes, los cambios relevantes y las observaciones internas o de clientes.	Responsable de Seguridad / Áreas involucradas	Anual	Actas, reportes de revisión o informes de auditoría periódica.
Análisis de resultados y hallazgos	Analizar los resultados de las revisiones y auditorías para identificar causas, aspectos por mejorar y prioridades de atención.	Responsable de Seguridad / Áreas involucradas	Después de cada revisión o auditoría	Registro de hallazgos y aspectos por mejorar.
Acciones correctivas o preventivas	Definir acciones para corregir problemas identificados o prevenir que se repitan.	Área involucrada / Responsable de Seguridad	Según el hallazgo identificado	Plan de acción con actividades, plazos y evidencias.
Seguimiento y mejora	Verificar que las acciones hayan sido aplicadas y actualizar el marco cuando sea necesario.	Responsable de Seguridad / Área Involucrada / Alta Dirección (cuando aplique)	Hasta el cierre de las acciones	Evidencia de cierre, validación o actualización del marco.

La auditoría inicial servirá como primera referencia para conocer el estado del marco de gestión de riesgos y confirmar si sus elementos se ajustan a la realidad de Stratos

Asesores S.A.S. Luego, las revisiones y auditorías periódicas ayudarán a comprobar cómo funciona el marco en la práctica, especialmente frente a retrasos, retrabajos, incidentes, cambios relevantes u observaciones internas o de clientes. Los hallazgos que se obtengan deberán traducirse en acciones concretas, ya sea para corregir problemas identificados o para prevenir que vuelvan a presentarse. La ISO 31000:2018 también señala que, cuando se identifiquen oportunidades de mejora, deben definirse planes y tareas que fortalezcan la gestión del riesgo (Organización Internacional de Normalización, 2018).

La mejora continua se integrará al ciclo PHVA (Planificar–Hacer–Verificar–Actuar), como guía para ordenar la evolución del marco de gestión de riesgos. En la fase de Planificar, Stratos Asesores S.A.S. revisará los resultados obtenidos y definirá las acciones necesarias. En la fase de Hacer, aplicará las acciones correctivas o preventivas. En la fase de Verificar, comprobará si esas acciones fueron implementadas y si ayudaron a reducir los riesgos. Finalmente, en la fase de Actuar, incorporará los ajustes necesarios al marco, a los controles y a las prácticas internas de trabajo.

Figura 11

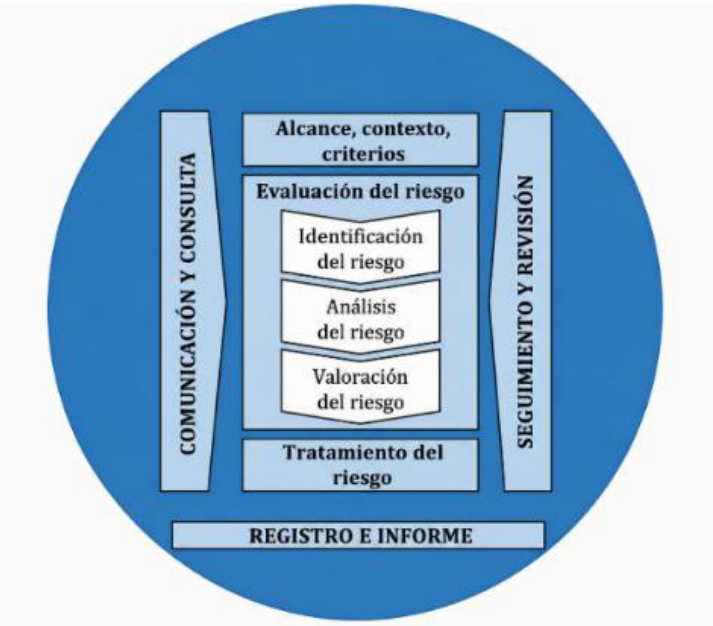
Ciclo PHVA para la mejora continua del marco de gestión de riesgos basado en la ISO 31000:2018

5.6. Proceso

El proceso del riesgo es el pilar fundamental de la normativa internacional ISO 31000:2018, y su aplicación deberá ser un proceso periódico y sistemático. Dicho proceso permitirá a la organización identificar, analizar, valorar, tratar, monitorear, revisar, registrar e informar los riesgos que puedan afectar el cumplimiento de sus objetivos estratégicos, operativos, legales, financieros, tecnológicos y reputacionales.

Figura 12

Sistema de Gestión de Riesgos.



Nota. Tomado de (Organización Internacional de Normalización, 2018).

De esta manera, los riesgos podrán ser gestionados antes de que afecten la calidad de los entregables, cumplimiento de plazos, confidencialidad de la información del cliente, continuidad del servicio o la reputación de la organización.

5.6.1. Generalidades

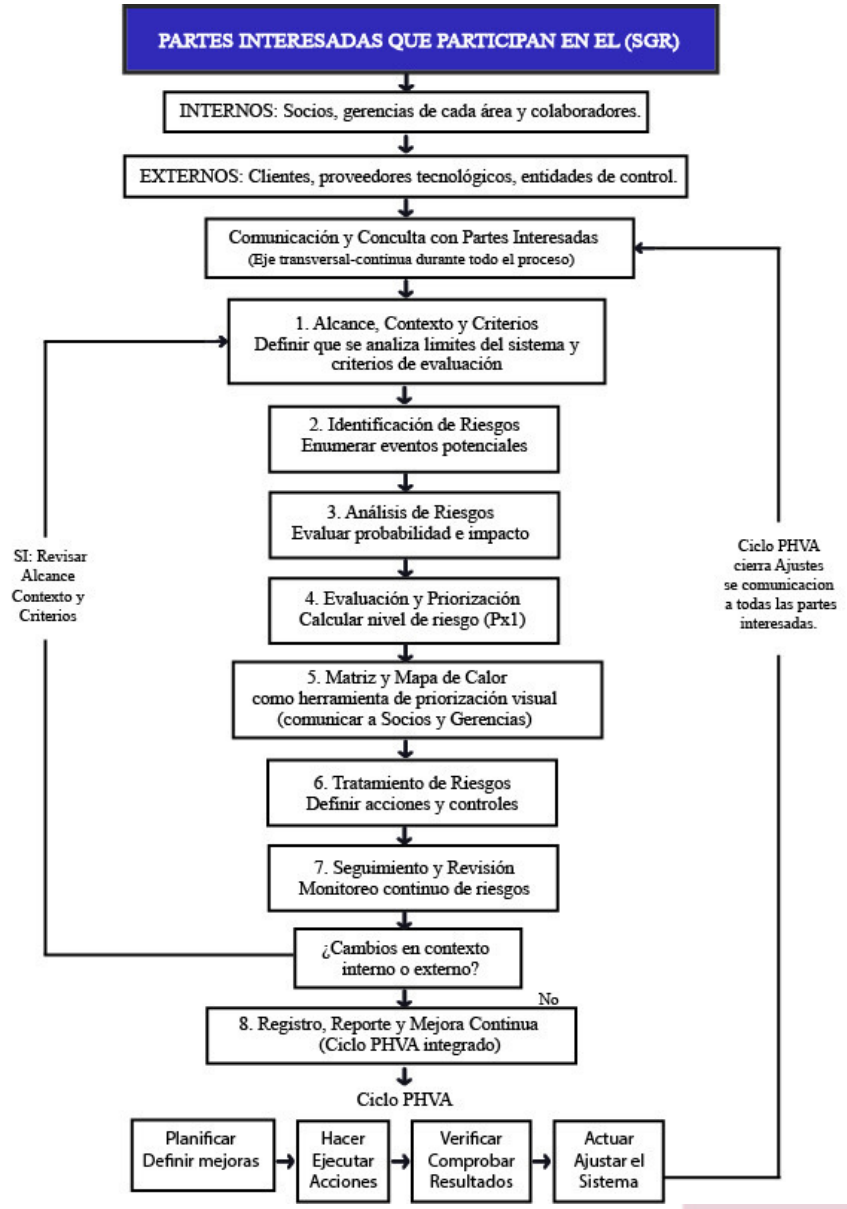
El Sistema de Gestión de Riesgos (SGR) se desarrollará bajo un enfoque sistemático, estructurado y continuo, alineado con los principios y directrices de la norma internacional ISO 31000:2018, considerando el contexto organizacional, la dimensión de la organización y las particularidades de su modelo de negocio basado en la

prestación de servicios profesionales. El sistema tiene como finalidad gestionar los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos y operativos, así como la calidad de los servicios brindados en las áreas de Asesoría en Riesgos y Precios de Transferencia. Para ello, incorpora actividades de comunicación, identificación, análisis, evaluación, tratamiento, seguimiento, revisión y retroalimentación.

El proceso de gestión del riesgo se organiza en etapas relacionadas entre sí, que se desarrollan de forma secuencial y, al mismo tiempo, permiten ajustes cuando sea necesario. Estas etapas comprenden el establecimiento del alcance, contexto y criterios; la identificación, análisis y valoración de los riesgos; el tratamiento de aquellos que requieren atención prioritaria; y las actividades de seguimiento y revisión. De manera transversal, todo el proceso se apoya en la comunicación y consulta con las partes interesadas. La Figura 13 muestra este flujo aplicado a Stratos Asesores S.A.S., con el fin de presentar de forma visual la secuencia operativa del sistema y facilitar su comprensión por parte del equipo.

Figura 13

Partes interesadas que participan en el SGR



Nota. Con base en el análisis realizado durante el desarrollo de la investigación.

Los principios de la norma ISO 31000:2018 orientan el diseño del Sistema de Gestión de Riesgos (SGR), procurando que este se integre a la operación diaria, considere información suficiente y promueva la participación de las áreas involucradas. Bajo este enfoque, el sistema no se limita a generar documentación, sino que busca apoyar la planificación de los proyectos, la asignación de recursos y la definición de controles adecuados.

Por ello, cuando se identifica un riesgo relevante, como retrasos en la entrega de servicios o pérdida de información, la respuesta no consiste únicamente en registrarlo en una matriz. También implica definir acciones concretas en las áreas de Asesoría en Riesgos y Precios de Transferencia, tales como ajustar cronogramas, revisar accesos a la documentación, reforzar controles o mejorar la validación de los entregables.

La gestión de riesgos en Stratos Asesores S.A.S. contribuirá a fortalecer la capacidad de la organización para anticiparse y responder ante eventos que puedan afectar su operación, situación financiera, tecnología, reputación, seguridad de la información o protección de datos personales. Asimismo, permitirá promover una cultura organizacional orientada a la prevención, el control y la mejora continua.

Un aspecto importante del Sistema de Gestión de Riesgos (SGR) es que no depende únicamente de la percepción de los socios o de las gerencias. También considera a los colaboradores, clientes y proveedores tecnológicos como fuentes relevantes para identificar riesgos emergentes. Por ejemplo, si un consultor identifica la falta de información crítica por parte de un cliente o advierte que los plazos de entrega podrían

verse afectados, esta situación debe reportarse mediante los canales definidos, como reuniones periódicas, comunicaciones internas o registros de incidentes, para que pueda ser analizada y tratada oportunamente.

De igual manera, el sistema permite atender cambios externos que puedan afectar a la organización, como reformas tributarias, actualizaciones en plataformas tecnológicas o nuevos requerimientos contractuales de los clientes. Para ello, se consideran mecanismos como el monitoreo mensual de la normativa, la revisión trimestral de la matriz de riesgos y las reuniones con clientes. Esta retroalimentación permite que la gestión del riesgo se mantenga actualizada, dinámica y alineada con la realidad operativa de Stratos Asesores S.A.S.

De esta manera, el sistema incorpora la gestión del riesgo en la toma de decisiones de Stratos Asesores S.A.S., procurando que las acciones definidas estén alineadas con sus objetivos estratégicos y operativos. Además, permite mantener un enfoque flexible y continuo, capaz de adaptarse a los cambios del entorno y a las necesidades de la organización.

El Sistema de Gestión de Riesgos servirá como base estructurada para:

- Mejorar la toma de decisiones.
- Reducir la incertidumbre en la ejecución de proyectos y prestación de servicios.
- Fortalecer el cumplimiento de los objetivos estratégicos y operativos.
- Resguardar la confidencialidad, integridad y disponibilidad de la información.
- Fortalecer la continuidad operativa y sostenibilidad de la organización.

- Mejorar la calidad de los entregables y la satisfacción de los clientes.
- Facilitar el cumplimiento de las obligaciones legales y regulatorias.

El Sistema de Gestión de Riesgos (SGR) será aplicable a los procesos y actividades vinculados con las líneas estratégicas de Asesoría en Riesgos y Precios de Transferencia. Su alcance incluye la planificación, ejecución, seguimiento, control documental y control operativo de dichas áreas. Asimismo, la gestión de riesgos se desarrollará como un proceso dinámico y adaptable, sujeto a revisión, seguimiento y mejora continua, de acuerdo con los cambios del entorno interno y externo de Stratos Asesores S.A.S.

5.6.2. Comunicación y Consulta

La comunicación y la consulta forman parte transversal del proceso de gestión del riesgo y se aplican de manera permanente en todas sus etapas. De acuerdo con la cláusula 6.2 de la norma ISO 31000:2018, estas actividades deben desarrollarse de forma bidireccional, continua y oportuna, involucrando a las partes interesadas para compartir información relevante sobre los riesgos y facilitar la comprensión de las decisiones tomadas.

En Stratos Asesores S.A.S., este componente se orienta a fortalecer la cultura de gestión de riesgos, apoyar la toma de decisiones y promover la participación activa de los responsables en la identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos.

Objetivo.

Establecer un canal estructurado de comunicación que permita el intercambio oportuno de información entre colaboradores, gerencias y Alta Dirección sobre los riesgos identificados en cada etapa del Sistema de Gestión de Riesgos. Este canal facilitará la claridad de responsabilidades en la identificación, análisis y tratamiento de los riesgos, conforme a los lineamientos de la norma ISO 31000:2018.

Responsabilidades en los procesos de comunicación.

Para que la comunicación y la consulta funcionen de manera efectiva, cada participante debe asumir un rol definido según su nivel de responsabilidad y su área de influencia:

- **Alta Dirección (socios):** aprueba los lineamientos de comunicación, autoriza la escalación de riesgos críticos y toma decisiones sobre los tratamientos que impliquen recursos adicionales o cambios operativos relevantes.
- **Gerencias de Asesoría en Riesgos y Precios de Transferencia:** comunican oportunamente los riesgos identificados en sus equipos, validan la información reportada por los consultores, coordinan la aplicación de los controles y presentan los avances al Responsable del Sistema de Gestión de Riesgos (SGR).
- **Responsable del Sistema de Gestión de Riesgos (SGR):** consolida y documenta los riesgos comunicados por las áreas, mantiene actualizado el registro de incidentes, coordina la comunicación entre los distintos niveles de la organización

y presenta los reportes correspondientes a la Alta Dirección.

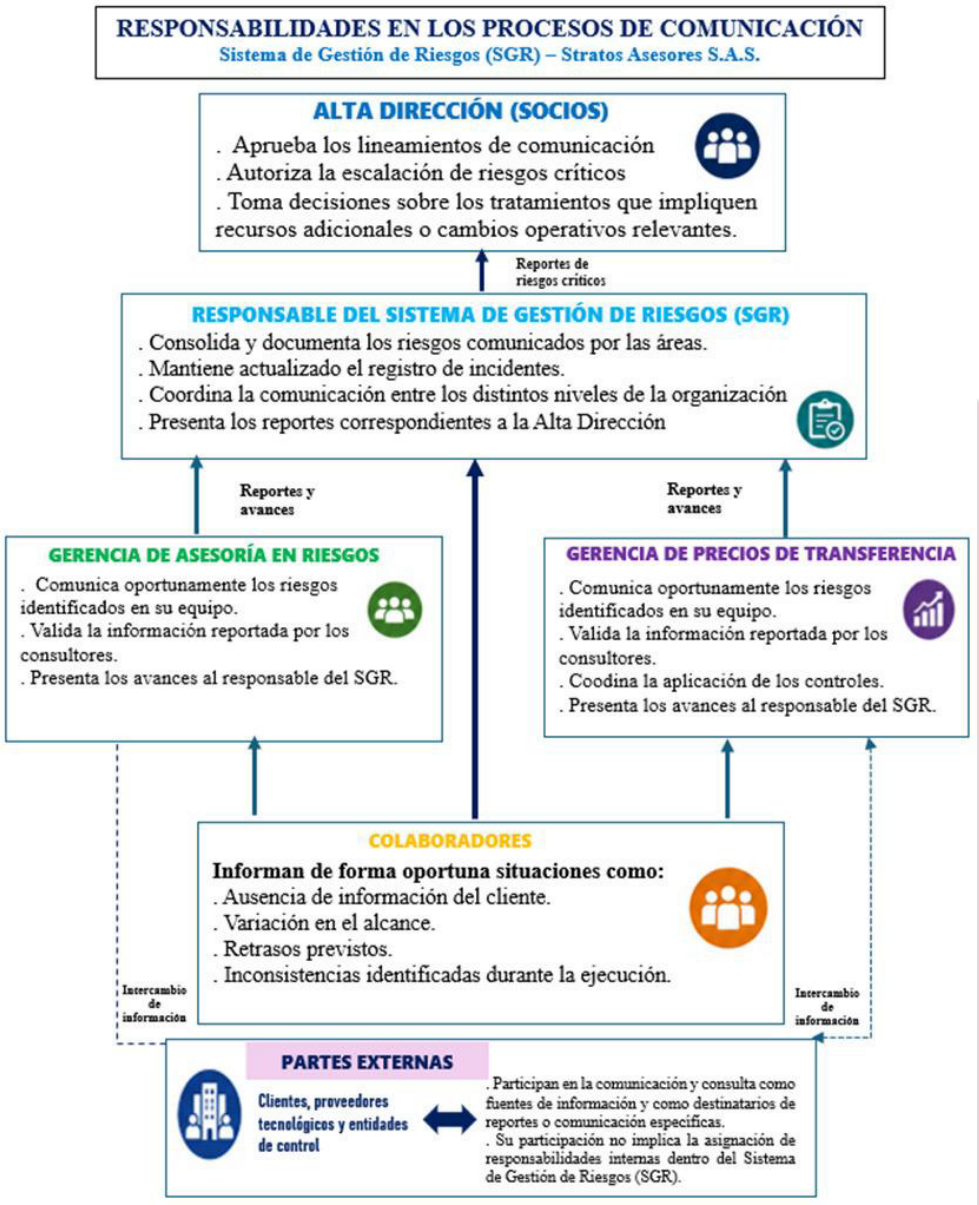
- **Colaboradores:** informan de forma oportuna situaciones como la ausencia de información del cliente, variaciones en el alcance, retrasos previstos o inconsistencias identificadas durante la ejecución.

Las partes externas, como clientes, proveedores tecnológicos y entidades de control participan en la comunicación y consulta como fuentes de información y como destinatarios de reportes o comunicaciones específicas. Sin embargo, su participación no implica la asignación de responsabilidades internas dentro del Sistema de Gestión de Riesgos (SGR).

La Figura 14 presenta el flujo de comunicación y consulta entre las partes interesadas, mostrando los canales previstos para compartir, reportar y retroalimentar información relacionada con los riesgos.

Figura 14

Flujo de comunicación y consulta



Nota. Con base en el análisis realizado durante el desarrollo de la investigación.

Matriz de comunicación de riesgos.

Para ordenar el flujo de información sobre los riesgos, se establece una matriz de comunicación que define qué información debe comunicarse, quién la genera, quien la recibe, el canal utilizado, la frecuencia y el propósito de cada comunicación. Esta matriz complementa los medios que la organización ya utiliza, como correo electrónico, Microsoft Teams y reuniones internas, permitiendo una gestión más clara y estructurada de los riesgos prioritarios. La Tabla 42 presenta la matriz propuesta.

Tabla 42

Matriz de comunicación de riesgos

Tipo de información	Emisor	Receptor	Canal	Frecuencia	Objetivo
Riesgos identificados	Colaboradores / Gerencias de área	Responsable del SGR	Reuniones de seguimiento (Teams o presencial)	Semanal	Mantener actualizada la matriz de riesgos
Brecha o incidente de seguridad de la información	Colaboradores / Gerencia de Asesoría en Riesgos	Responsable del SGR y Alta Dirección	Correo corporativo / alerta	Inmediato	Activar el protocolo ante incidentes
Incidente o interrupción tecnológica (Microsoft 365) o NAS	Colaboradores / Gerencia de área	Responsable del SGR	Correo corporativo / alerta	Inmediato	Activar el plan de contingencia y continuidad con el proveedor de TI
Desviación de plazos en entregables (IIPT/AOPR)	Colaboradores / Gerencia de Precios de Transferencia	Gerencia de área / Responsable del SGR	Teams o correo corporativo	Semanal	Evitar retrasos en las entregas al cliente

Cambios normativos del SRI	Gerencia de Precios de Transferencia	Colaboradores de Precios de Transferencia y Alta Dirección	Reunión técnica (Teams o presencial)	Mensual o al detectarse	Garantizar el cumplimiento normativo y la consistencia técnica
Indicadores de riesgo (KPIs)	Responsable del SGR	Alta Dirección	Informe ejecutivo	Mensual	Apoyar a la toma de decisiones
Avance de los planes de tratamiento	Gerencias de área	Responsable del SGR	Reunión de seguimiento	Mensual	Verificar el cumplimiento de las acciones correctivas
Riesgo alto o critico identificado	Responsable del SGR	Ata Dirección	Reporte / reunión	Inmediato	Escalar el riesgo y aprobar su tratamiento
Resultados de auditoría interna	Responsable del SGR	Alta Dirección y Gerencias de área	Informe formal	Semestral / anual	Identificar oportunidades de mejora
Capacitación en gestión de riesgos	Responsable del SGR	Todos los colaboradores	Capacitaciones presenciales o virtuales	Semestral	Fortalecer la cultura de gestión de riesgos

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

Comunicación según las fases del proceso de gestión de riesgos.

La comunicación forma parte integral de la gestión del riesgo, desarrollándose de manera continua y adaptándose a cada una de sus fases:

Fase 1: Identificación de riesgos.

Durante esta fase, el responsable del Sistema de Gestión de Riesgos convoca a reuniones trimestrales por área, en las que gerentes y consultores comparten los

riesgos detectados en sus proyectos. El flujo de comunicación es ascendente; el equipo técnico reporta mediante correos, reuniones de seguimiento y registros de incidentes, y las gerencias consolidan esta información para incorporarla en la matriz de riesgos, asegurándose que ningún riesgo relevante quede sin registro.

Fase 2: Análisis y evaluación.

Una vez identificados los riesgos, el responsable del Sistema de Gestión de Riesgos y las gerencias de área realizan la evaluación de probabilidad e impacto. En esta fase, la comunicación es bidireccional, ya que se revisa y valida cada calificación asignada, se aclara dudas sobre la definición de los riesgos y se asegura la coherencia en los criterios aplicados. Las decisiones adoptadas se documentan, junto con las actas que evidencian la participación.

Fase 3: Tratamiento y monitoreo.

Una vez establecidos los planes de tratamiento para los riesgos altos y críticos, la comunicación se centra en el seguimiento mensual. Los gerentes responsables reportan al responsable del Sistema de Gestión de Riesgos el avance de las acciones correctivas, incluyendo su cumplimiento en los plazos establecidos, dificultades y ajustes requeridos. Esta información es consolidad por el responsable del Sistema de Gestión de Riesgos, quien comunica de manera oportuna a los Socios cualquier situación que comprometa el tratamiento de los riesgos o requiera su intervención.

Ejemplo de comunicación ante cambios normativos en el área de precios de transferencia.

El área de Precios de Transferencia debe sostener una comunicación continua con el responsable del Sistema de Gestión de Riesgos sobre eventuales cambios en la normativa tributaria. Por ejemplo, si el Servicio de Rentas Internas (SRI) emite una resolución que modifica los criterios de comparabilidad en operaciones con partes relacionadas puede dar lugar a la aparición de nuevos riesgos o aumentar la probabilidad de uno ya identificado, como errores técnicos en informes o incumplimientos normativos.

Para este ejemplo, el flujo de comunicación funciona de la siguiente manera:

Tabla 43

Procedimientos de gestión de riesgos por cambios regulatorios tributarios

Etapas	Descripción resumida
Identificación del cambio	El área de Precios de Transferencia detecta cambios en la normativa tributaria emitidos por el SRI.
Comunicación inicial	La gerencia o colaboradores informan al responsable del Sistema de Gestión de Riesgos en máximo dos días laborables mediante correo o reunión.
Análisis del impacto	El responsable de Riesgos evalúa la incidencia en riesgos identificados, proyectos, metodologías y exposición con clientes.
Reunión extraordinaria	Si el impacto es significativo, la Coordinadora Administrativa convoca a socios, gerencia y responsable de Riesgos para definir acciones.
Medidas definidas	Se establecen acciones como revisión de proyectos, comunicación a clientes y controles adicionales.
Documentación y actualización	Las decisiones se registran en actas, se actualiza la matriz de riesgos y se incorpora el plan de tratamiento.
Acciones de tratamiento	Incluye capacitación del equipo, actualización de papeles de trabajo y revisión de informes en ejecución.
Seguimiento	El responsable del Sistema de Gestión de Riesgos realiza seguimiento mensual y reporta avances trimestralmente a los socios.

Mecanismos de comunicación estructurados.

La comunicación bidireccional se formaliza a través de:

- **Reuniones semanales de avance:** para que los consultores reporten incidentes, retrasos o cambios que impacten la ejecución de proyectos
- **Reuniones trimestrales de riesgos por área:** la Coordinadora Administrativa convoca al responsable del Sistema de Gestión de Riesgos y partes interesadas para revisar la matriz, validar calificaciones de riesgos y aprobar planes de tratamiento.
- **Comunicación inmediata por riesgos críticos:** se lo realiza mediante correo formal o reunión urgente virtual o presencial cuando se identifique un riesgo critico o se haya materializado un evento de alto impacto
- **Reporte de incidentes:** registro formal de errores técnicos, retrasos, incidentes de seguridad de la información u otros eventos susceptibles de causar nuevos riesgos o modificar los existentes.

De este modo, la comunicación no sea centrada solo en la difusión de políticas, sino que se desarrolle en ambos sentidos, facilitando que la información del equipo técnico alimente de forma continua la evaluación y el tratamiento de los riesgos.

Propuesta de implementación del proceso de comunicación y consulta

Para aplicar de manera práctica la comunicación y consulta, se plantea un plan específico para este componente, articulado con el plan general del marco descrito en

la sección 5.5.5. La Tabla 44 presenta las actividades previstas, los responsables asignados y los resultados esperados en cada fase.

Tabla 44

Plan de implementación del proceso de comunicación y consulta de riesgos

Fase	Actividades	Responsable	Resultado esperado
Preparación	Establecer los roles y responsables, documentar los canales y procedimientos de comunicación, y difundir los lineamientos de comunicación y consulta dentro de la organización	Responsable del SGR	Reuniones de seguimiento (Teams o presencial)
Configuración	Habilitar los canales de comunicación definidos, establecer los formatos para reportes y consultas, y precisar las frecuencias y mecanismos de seguimiento aplicables	Responsable del SGR y proveedor de TI	Canales habilitados y formatos estandarizados
Ejecución	Aplicar el proceso de comunicación y consulta, facilitando la participación de las partes interesadas y el intercambio oportuno de información sobre riesgos	Gerencias de área y Responsable del SGR	Flujo de información continuo y bidireccional en operación
Seguimiento y control	Dar seguimiento a los flujos de información y atender posibles fallas en el cumplimiento de canales y frecuencias de comunicación	Responsable del SGR	Control y trazabilidad de las comunicaciones
Mejora continua	Revisar la efectividad del modelo y aplicar mejoras en procedimientos, formatos y herramientas	Alta Dirección y Responsable del SGR	Fortalecimiento continuo del proceso de comunicación

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

La propuesta se estructura en cinco fases: preparación, configuración, ejecución, seguimiento y control, y mejora continua. Estas fases buscan definir responsabilidades, establecer canales de comunicación, promover la participación de las partes interesadas y asegurar la revisión periódica de la información. De esta manera, Stratos Asesores S.A.S. contará con un proceso de comunicación sistemático, oportuno y alineado con los objetivos del Sistema de Gestión de Riesgos (SGR).

De esta manera, la comunicación no se limita únicamente a transmitir políticas o lineamientos, sino que funciona en ambos sentidos. Esto permite que la información generada por el equipo técnico contribuya de forma continua a la evaluación y tratamiento de los riesgos, fortaleciendo así la cultura de gestión de riesgos dentro de la organización.

5.6.3. Alcance, Contexto y Criterios

La definición clara del alcance establece qué procesos, actividades y servicios serán objeto de evaluación, delimitando así el perímetro de responsabilidad del Sistema de Gestión de Riesgos. El análisis del contexto, tanto externo como interno, identifica los factores del entorno y de la organización que influyen en la exposición al riesgo y condicionan la forma en que la gestión de riesgos debe ser implementada. Finalmente, la definición de criterios de riesgo especifica qué es aceptable y qué no lo es para la organización, estableciendo parámetros de evaluación que permitan priorizar riesgos y tomar decisiones fundamentadas sobre su tratamiento (Organización Internacional de Normalización, 2018).

Para Stratos Asesores S.A.S., que se especializa en asesoría en gestión de riesgos organizacionales y precios de transferencia, estos elementos son especialmente críticos. Los servicios ofrecidos por la organización tienen el objetivo de asesorar a clientes corporativos sobre gestión integral de riesgos y cumplimiento normativo, por lo cual deben mantener coherencia entre los riesgos que identifican en sus clientes y los que la organización gestiona internamente. Esta alineación es fundamental para mantener credibilidad, confianza y consistencia con su misión declarada.

A continuación, se presenta el desarrollo de esta sección, estructurada según los lineamientos de ISO 31000:2018.

5.6.3.1. Generalidades.

El establecimiento del alcance, el contexto y los criterios constituye la fase fundacional y estratégica de todo el proceso de gestión de riesgos basado en la norma ISO 31000:2018 dentro de Stratos Asesores S.A.S. Esta etapa es la base operativa indispensable para garantizar que las fases posteriores de identificación, análisis y valoración de los riesgos se ejecuten con un enfoque unificado y estructurado.

La importancia crítica de este apartado radica en que permite alinear la gestión de riesgos con los objetivos del negocio. De este modo, se evita la dispersión de esfuerzos organizacionales y la sobrecarga de controles en áreas de baja relevancia. Además, asegura que las medidas de mitigación se diseñen a la medida exacta de una firma de servicios profesionales en crecimiento.

El desarrollo estructurado de esta fase persigue tres objetivos metodológicos fundamentales:

- **Identificar límites:** Fijar las fronteras operativas, organizacionales y temporales aplicables al sistema.
- **Analizar el contexto:** Evaluar las interacciones internas y las regulaciones externas del entorno ecuatoriano.
- **Definir criterios específicos:** Estructurar las escalas de medición de probabilidad e impacto para la toma de decisiones.

5.6.3.2. Definición del Alcance.

El alcance del Sistema de Gestión de Riesgos de Stratos Asesores S.A.S. comprende la evaluación de riesgos asociados a las dos líneas principales de negocio: Asesoría en Riesgos y Precios de Transferencia.

Línea de Asesoría en Riesgos:

Comprende servicios especializados que incluyen cumplimiento normativo, seguridad de la información, privacidad de datos, anticorrupción y antisoborno, auditoría interna, aseguramiento de procesos, auditoría de sistemas y resiliencia empresarial. La evaluación de riesgos se realiza a lo largo de todo el ciclo del proyecto, incluyendo la planificación, obtención de evidencias, análisis de hallazgos y la emisión de los informes.

Línea de Precios de Transferencia:

Incluye servicios como la elaboración del Informe Integral de Precios de Transferencia (IIPT), Anexos de Operaciones con Partes Relacionadas (AOPR), la asesoría en litigios tributarios y las Consultas de Valoración Previa (CVP). Los riesgos evaluados incluyen aspectos técnicos, regulatorios, documentales y reputacionales desde la recopilación de información del cliente hasta la presentación ante las autoridades fiscales.

Procesos excluidos del alcance:

El Sistema de Gestión de Riesgos no abarca la gestión de recursos humanos tales como contratación, desvinculación y compensaciones, los riesgos financieros asociados a inversiones o endeudamiento que excedan las operaciones normales. Asimismo, se excluyen los cambios estratégicos de largo plazo (más de tres años) y los eventos externos no controlables, como desastres naturales o pandemias.

Límites temporales:

La vigencia del Sistema de Gestión de Riesgos se estructura en ciclos anuales con revisiones continuas. En particular:

- Período de vigencia: La evaluación abarca la operación de Stratos Asesores S.A.S. en el año calendario vigente. Los proyectos en ejecución se analizan de acuerdo con su cronograma, mientras que los proyectos finalizados aportan información histórica para la identificación de riesgos recurrentes.
- Frecuencia de revisión del sistema: La matriz de riesgos se somete a una revisión trimestral estructurada. Sin embargo, si se detectan cambios relevantes, como un ajuste

normativo, incidente critico o una variación operativa significativa, la matriz se actualiza de forma inmediata.

- Ciclo de monitoreo de riesgos altos y críticos: Los riesgos clasificados como altos y críticos se monitorean mensualmente, mientras que los riesgos de nivel moderado o bajo se evalúan trimestralmente dentro del proceso integral de evaluación del sistema.
- Auditoría integral del sistema: Se efectúa una revisión formal anual del Sistema de Gestión de Riesgos, idealmente en el cuarto trimestre, con el propósito de valorar su funcionamiento y establecer oportunidades de mejora para el periodo siguiente.

Límites geográficos:

El Sistema de Gestión de Riesgos aplica exclusivamente dentro del territorio ecuatoriano, considerando que:

- Stratos Asesores S.A.S. tiene su base operativa en Quito, Ecuador, desde donde presta servicios a clientes corporativos dentro del territorio ecuatoriano.
- Los servicios se brindan a través de modalidades presencial, híbrida y remota, conforme al marco normativo ecuatoriano.
- La evaluación de riesgos considera el entorno normativo y tributario vigente en Ecuador, comprendiendo las disposiciones emitidas por el Servicio de Rentas Internas (SRI), la Superintendencia de Compañías, Valores y Seguros (SCVS) y otras entidades regulatorios competentes.

Delimitación clara de los recursos necesarios para el Sistema de Gestión de Riesgos.

Es necesario distinguir entre los recursos destinados a la operación general de la organización y aquellos requeridos de manera específica para la implementación y funcionamiento del Sistema de Gestión de Riesgos.

Recursos operativos generales (excluidos del Sistema de Gestión de Riesgos).

La infraestructura tecnológica, que incluye laptops, antivirus ESET Endpoint Security, software contable Contifico o NAS Synology, forma parte de los recursos utilizados en la operación diaria de la organización. Si bien estos activos pueden estar vinculados a riesgos evaluados, no se consideran recursos propios del Sistema de Gestión de Riesgos.

Recursos específicos del Sistema de Gestión de Riesgos.

Para asegurar el adecuado funcionamiento del Sistema de Gestión de Riesgos, la organización cuenta con los siguientes recursos:

Tiempo dedicado del personal.

El responsable del Sistema de Gestión de Riesgos requiere una dedicación variable dependiendo de la fase operativa de la organización y la actividad del sistema. Por lo cual en la Tabla 45 se propone las actividades y tiempo requerido:

Tabla 45

Actividades y tiempo requerido para el responsable del SGR

Actividad	Frecuencia	Horas
Reunión trimestral de identificación de riesgos - Área Asesoría en Riesgos	1 vez por trimestre	3 horas
Reunión trimestral de identificación de riesgos - Área Precios de Transferencia	1 vez por trimestre	3 horas

Análisis y evaluación de riesgos reportados ad hoc por gerencias	Continuo	2-4 horas/mes
Seguimiento mensual a planes de tratamiento (riesgos altos y críticos)	Mensual	4 horas
Revisión y actualización trimestral de la matriz de riesgos	1 vez por trimestre	4 horas
Análisis de incidentes y eventos reportados	En el momento que ocurran	Variable
Preparación de informe trimestral a los Socios	1 vez por trimestre	3 horas
Comunicación con gerencias	Semanal	1 o 2 horas por semana
Actualización de documentación, actas de reuniones, registros de evidencia	En función de las reuniones efectuadas	2 o 3 horas por mes

Variabilidad según la Fase de Operación.

La asignación del tiempo varía a lo largo del año según la fase de operación, de acuerdo con la siguiente estimación:

- Fase 1: Implementación inicial (1-3 meses): Durante la etapa inicial del sistema, cuando se desarrolla la matriz inicial, se valida la metodología y se ejecutan procesos de capacitación, se estima una dedicación aproximada de 8 a 10 horas semanales. Esta fase contempla el diseño de procesos, formalización de formatos, ajustes continuos y reuniones de socialización.
- Fase 2: Operación normal: Una vez consolidado el sistema y sin la ocurrencia de eventos relevantes, la dedicación requerida disminuye a 4 a horas por semana.
- Fase 3: Trimestres de mayor actividad: Durante los trimestres en los que se realiza la revisión integral del Sistema de Gestión de Riesgos, se presentan

cambios normativos relevantes o incidentes críticos que demandan análisis, por lo cual la dedicación puede incrementarse entre 6 a 8 horas semanales.

Tomando en cuenta el tamaño de Stratos Asesores S.A.S. y sus dos líneas de negocio se requiere de la participación de todas las partes internas interesadas, ya que el tiempo estimado refleja que la gestión de riesgos no puede ser una responsabilidad compartida sin claridad, ni puede estar centralizada en una sola persona sin dedicación adecuada. De igual forma, la variabilidad en la dedicación es inherente al funcionamiento del sistema ya que en periodos de estabilidad se requiere un nivel menor de coordinación, mientras que en periodos de cambios la demanda de la gestión se incrementa. Como resultado de la capacidad del sistema para adaptarse a la realidad operativa de la organización.

Capacitación Especializada en ISO 31000 y Gestión de Riesgos.

La capacitación en el Sistema de Gestión de Riesgos debe ser diferenciada según el rol y responsabilidades de cada participante:

Tabla 46

Capacitación especializada en IDO 31000

Grupo	Contenido	Horas	Frecuencia
Alta dirección	Principios ISO 31000, decisiones sobre riesgos críticos	1-2	Sesión inicial + actualización anual (30 min)
Gerencias de área	Metodología ISO 31000, identificación y evaluación de riesgos en sus procesos	3-4	Sesión inicial (consultor externo) + refuerzo anual (1-1.5 h)
Colaboradores	Cómo reportar riesgos emergentes en proyectos, canales de reporte	1-2	Sesión inicial + inducción para nuevos colaboradores

Responsable del SGR	ISO 31000 en profundidad, facilitación de procesos, software especializado, gestión documental del SGR, archivo de evidencias, control de versiones	16-20	Antes o durante mes 1 de implementación / cuando existan cambios de procesos

Software Especializado para el Registro y Seguimiento de Riesgos.

Actualmente, la organización podría utilizar hojas de cálculo de Excel para gestionar su matriz de riesgos, sin embargo, esta herramienta presentaría limitaciones para el desarrollo sostenible del Sistema de Gestión de Riesgos tales como:

- No genera alertas automáticas ante el vencimiento de los plazos asociados a los planes de tratamiento.
- Limita la generación de reportes dinámicos y la elaboración de resúmenes ejecutivos
- No cuenta con una trazabilidad para conocer quién, cuando y por qué se efectuaron los cambios realizados.
- Dependería de la actualización manual por parte de una sola persona, generando cuellos de botella.

Tomando en cuenta lo antes menciona, se plantea la implementación de un software especializado de gestión de riesgos que disponga de las siguientes características:

- Módulo de identificación y registro de riesgos con campos estructurados (código, descripción, probabilidad, impacto, nivel de riesgo y responsable).
- Módulo de gestión de planes de tratamiento que permita asignar acciones,

responsables, fechas de vencimiento y seguimiento de avance.

- Dashboards ejecutivos que permita visualizar el estado general de los riesgos, matrices de calor, análisis de tendencias y seguimientos de riesgos vencidos.
- Registros de auditoria (logs) para tener trazabilidad de los cambios realizados, identificando quién los efectuó y en qué momento.

Documentación Formalizada del Sistema.

Si bien la organización actualmente utiliza OneDrive como repositorio corporativo, no dispone de una estructura dedicada al Sistema de Gestión de Riesgos, por lo cual es necesario la creación de una carpeta dedicada solo al Sistema de Gestión de Riesgos con subcarpetas organizadas de la siguiente forma:

- Políticas y lineamientos: Política de gestión de riesgos, matriz RACI, criterios de evaluación.
- Matrices y mapas: Matriz de riesgos actualizada, mapa de calor, matriz de evaluación.
- Planes de tratamiento: Documentos por riesgo con acciones, responsables, plazos, evidencias de cumplimiento.
- Reportes: Informes trimestrales a los Socios, reportes de seguimiento mensuales.
- Capacitaciones: Presentaciones de socialización, materiales de entrenamiento, registros de asistencia.
- Evidencias de reuniones: Actas firmadas de reuniones de identificación, grabaciones de reuniones virtuales, evaluación, tratamiento y seguimiento.
- Registro de incidentes: Reporte formal de cada evento, análisis causal, acciones

implementadas.

- Convenciones de nomenclatura: Por ejemplo, "Matriz_Riesgos_2026_v1" para identificar claramente el período y versión.
- Controles de versión: Cada documento importante debe indicar versión, fecha de actualización, responsable y cambios realizados.

Recursos actualmente no existentes en Stratos Asesores S.A.S. y Propuesta de Implementación.

Considerando que la organización actualmente no dispone de un Sistema de Gestión de Riesgos, se han identificado y se proponen los siguientes recursos necesarios para su implementación efectiva:

Tabla 47

Recursos no existentes

Recurso no existente	Justificación	Propuesta de implementación
Software especializado de gestión de riesgos	Las hojas de cálculo en Excel no permiten automatizar alertas, generar reportes dinámicos, ni mantener un registro auditable de cambios en la matriz de riesgos. Un software especializado mejora la trazabilidad y reduce el riesgo de errores manuales.	Evaluar herramientas como Caseware, LogicGate o similares que integren módulos de identificación, evaluación y monitoreo. Implementar en el primer semestre de vigencia del sistema con capacitación del responsable del SGR.
Tiempo dedicado de un responsable del SGR	Actualmente, nadie en la organización tiene asignada esta función de forma explícita. La gestión de riesgos requiere coordinación permanente, no puede ser una actividad secundaria.	Asignar a uno de los integrantes del equipo actual (preferiblemente con perfil técnico y conocimiento de procesos) como responsable del SGR con dedicación del 15% de su tiempo laboral semanal. Alternadamente, contratar a un profesional externo

		para la primera fase (implementación) y luego transferir responsabilidades internas.
Capacitación formalizada en ISO 31000	Los colaboradores no conocen la norma ni sus principios metodológicos. Una capacitación estructurada asegura que todos comprendan el propósito del sistema y sus responsabilidades.	Contratar una jornada de capacitación inicial (2-4 horas) impartida por consultor externo especializado en ISO 31000. Luego, capacitaciones anuales de refuerzo (1-2 horas) lideradas internamente por el responsable del SGR.
Repositorio formalizado de documentos del SGR	Aunque OneDrive existe, no hay una estructura de carpetas dedicada al Sistema de Gestión de Riesgos. Es necesario organizar de forma sistemática políticas, matrices, planes de tratamiento, actas e informes.	Crear una carpeta "Sistema Gestión de Riesgos" en OneDrive corporativo con subcarpetas por componente (Políticas, Matrices, Planes de Tratamiento, Reportes, Capacitaciones, Evidencias de Reuniones). Establecer convenciones de nomenclatura y control de versiones.

5.6.3.3. Contextos Externo e Interno.

El análisis de los contextos externo e interno permite establecer las condiciones que influyen en el proceso de gestión del riesgo de Stratos Asesores S.A.S. Según la ISO 31000:2018, este análisis debe considerar el entorno en el que opera la organización, ya que los factores externos e internos pueden influir en el cumplimiento de sus objetivos y convertirse en fuentes de riesgo (Organización Internacional de Normalización, 2018).

Contexto externo.

El contexto externo comprende los factores del entorno que pueden influir en las actividades de Stratos Asesores S.A.S., aunque no dependan directamente de la

organización. Para su análisis se toma como referencia el modelo PESTEL, ya que permite ordenar los factores políticos, económicos, sociales, tecnológicos, ambientales y legales que pueden afectar la operación de una organización y su toma de decisiones (Whittington et al., 2020).

Características de partes interesadas externas:

- **Clientes corporativos:** organizaciones ecuatorianas que contratan los servicios de Asesoría en Riesgos y Precios de Transferencia, cuyas expectativas en cuanto a confidencialidad, calidad de entregables y cumplimiento de plazos son críticos para la sostenibilidad de Stratos Asesores S.A.S.
- **Autoridades regulatorias y competentes:** incluyen el Servicio de Rentas Internas (SRI), Superintendencia de Compañías, Valores y Seguros (SCVS), Ministerio de Trabajo, Instituto Ecuatoriano de Seguridad Social (IESS) y Superintendencia de Protección de Datos Personales. Las normativas, disposiciones y criterios emitidos por estas entidades impactan directamente la metodología aplicada y la conformidad de los servicios que presta Stratos Asesores S.A.S.
- **Proveedores tecnológicos:** proveedores responsables del suministro de plataformas críticas, como servicios de nube, conectividad y herramientas tecnológicas, cuya disponibilidad y rendimiento condicionan la continuidad de las operaciones.
- **Competidores:** otras organizaciones de consultoría que brindan servicios

comparables, cuyo nivel de posicionamiento, innovación y reputación incidente en la competitividad de Stratos Asesores S.A.S. y en su reputación ante el mercado.

Herramientas y métodos concretos para el monitoreo del contexto externo:

- **Análisis PESTEL:** revisión periódica de los factores políticos, económicos, sociales, tecnológicos, ambientales y legales que pueden influir en la organización, con el fin de identificar cambios del entorno y posibles riesgos asociados.
- **Monitoreo legislativo y normativo:** revisión mensual de los cambios aplicables en materia tributaria, laboral y de protección de datos personales, así como de las disposiciones emitidas por las entidades competentes. Esta actividad estará a cargo de las gerencias, quienes deberán comunicar los cambios relevantes al Responsable del Sistema de Gestión de Riesgos (SGR).
- **Análisis de comunicaciones regulatorias:** seguimiento de circulares, resoluciones y pronunciamientos emitidos por el Servicio de Rentas Internas (SRI), la Superintendencia de Compañías, Valores y Seguros (SCVS) y otras autoridades competentes. Cuando se identifique un cambio que pueda afectar los servicios de la organización, se realizará un análisis de impacto documentado y, de ser necesario, se actualizará la matriz de riesgos.
- **Consultas directas con clientes:** aplicación de encuestas al cierre de cada proyecto y reuniones con clientes recurrentes para identificar expectativas, exigencias regulatorias y preocupaciones sobre confidencialidad o continuidad del servicio.

- **Monitoreo de proveedores tecnológicos:** revisión continua de cambios, alertas de disponibilidad y comunicaciones de proveedores relacionados con Microsoft 365, hosting, respaldos y herramientas especializadas.
- **Análisis de amenazas emergentes:** seguimiento de alertas de ciberseguridad y vulnerabilidades tecnológicas que puedan comprometer la disponibilidad de los servicios, la seguridad de la información o la continuidad operativa de la organización.

Integración del contexto externo en el Sistema de Gestión de Riesgos:

La información obtenida mediante estos métodos servirá como insumo para actualizar la matriz de riesgos desarrollada en la sección 5.6.4, correspondiente a la evaluación del riesgo. Por ejemplo, si la Superintendencia de Compañías, Valores y Seguros (SCVS) emite una disposición que incrementa los requisitos de cumplimiento normativo, esto podría generar nuevas exigencias para los servicios de Asesoría en Riesgos. En este caso, la gerencia del área deberá comunicar el cambio al Responsable del Sistema de Gestión de Riesgos (SGR), quien analizará si dicho cambio incrementa la probabilidad de riesgos previamente identificados o si da lugar a nuevos riesgos que deban incorporarse en la matriz.

Tabla 48

Caso de la SCVS

Elemento	Descripción
Cambio identificado	La Superintendencia de compañías, valores y seguro (SCVS) emite una nueva disposición que aumenta los requisitos de cumplimiento normativo.
Área impactada	Asesoría en Riesgos

Reporte del cambio	La Gerencia de Riesgos comunica la disposición al responsable del Sistema de Gestión de Riesgos.
Evaluación del riesgo	Se analiza si el cambio incrementa riesgos existentes, como errores técnicos en informes incumplimientos de plazos, o si genera nuevos riesgos.
Actualización del SGR	Se actualiza la matriz de riesgos conforme al nuevo contexto normativo.
Acciones por aplicar	Capacitar al equipo, actualizar metodologías y papeles de trabajo, y revisar proyectos en ejecución para alinearlos con la disposición de la SCVS.
Resultado esperado	Mantener los servicios de asesoría alineados con la normativa vigente y reducir posibles incumplimientos.

De igual manera, si un cliente expresa inquietudes relacionadas con la confidencialidad de sus datos, dicha observación deberá registrarse en el consolidado de encuestas de satisfacción. Posteriormente, esta información será analizada como una posible señal de debilidades en los controles de acceso a la información, evaluando su relación con el riesgo de pérdida o filtración de información confidencial.

Tabla 49

Caso reportado por cliente

Aspecto	Resumen
Situación Identificada	Un cliente reporta inquietudes sobre la confidencialidad de los datos.
Registro de la Observación	La Observación se documenta en un registro consolidado de encuestas de satisfacción.
Análisis realizado	Se analiza como un indicador de debilidades en los controles de acceso a la información.
Riesgo evaluado	Pérdida o filtración de información confidencial.
Actividad de mejora	Se proponen controles correctivos cuando sea necesario.

Asimismo, ante una interrupción de Microsoft 365, se activará el procedimiento de continuidad correspondiente y el evento será analizado como una posible materialización del riesgo crítico asociado a la dependencia tecnológica. Como parte de este análisis, se documentarán las lecciones aprendidas y se evaluarán mejoras en los controles de respaldo y recuperación.

Tabla 50

Caso de Microsoft 365

Elemento	Descripción
Riesgo crítico	Dependencia de plataformas tecnológicas
Evento	Interrupción del servicio de Microsoft 365
Gestión documental	Registro de documentación de la lección aprendida.
Mejora continua	Evaluación y fortalecimiento de controles y respaldo.
Objetivo	Garantizar la continuidad de las operaciones y minimizar impactos.

Contexto Interno.

El contexto interno permite identificar los aspectos propios de Stratos Asesores S.A.S. que pueden influir en la gestión del riesgo. La ISO 31000:2018 considera dentro de este análisis elementos como la estructura organizacional, los roles, la cultura, los recursos, los sistemas de información, los flujos de información y las interdependencias internas (Organización Internacional de Normalización, 2018). Stratos Asesores S.A.S. cuenta con aproximadamente 17 colaboradores distribuidos entre las áreas de Asesoría en Riesgos y Precios de Transferencia, con un soporte administrativo que asiste la gestión documental sin formar parte del alcance de la

evaluación de riesgos. Su operación se desarrolla por proyectos, por lo que la coordinación entre áreas resulta necesaria para mantener el orden documental, la revisión técnica de los informes y el cumplimiento de los plazos establecidos.

Tabla 51

Factores del contexto interno en Stratos Asesores S.A.S.

Factor Interno	Descripción
Cultura organizacional	Stratos prioriza la calidad del servicio, el cumplimiento de compromisos y la confianza del cliente. La formalización del Sistema de Gestión de Riesgos permitirá reforzar el reporte oportuno de incidentes, retrasos, errores o fallas en la gestión de proyectos.
Estructura organizacional	La organización cuenta con una estructura reducida, integrada por la Alta Dirección, gerencias de área, administración y colaboradores. Esto facilita la comunicación directa y hace necesario mantener claras las responsabilidades de cada área.
Recursos disponibles	La prestación del servicio depende del conocimiento técnico de los socios, gerentes y consultores. La operación también se apoya en herramientas como Microsoft 365, OneDrive, Outlook, Teams, NAS Synology, ESET Endpoint Security, Contifico y Stratos Rate Company.
Procesos y documentación	Stratos trabaja con contratos, acuerdos de confidencialidad, archivos, informes técnicos y carpetas digitales por cliente o proyecto. La falta de registros completos o versiones actualizadas puede generar retrabajos o pérdida de trazabilidad.
Estrategia y objetivos	Stratos busca mantener la continuidad de sus servicios de asesoría y atender proyectos de forma ordenada. Los riesgos deben analizarse según su efecto en la operación, el cumplimiento de compromisos con clientes y la calidad del servicio.

Herramientas y métodos para el monitoreo del contexto interno.

Con el fin de mantener actualizado el análisis del contexto interno, la organización aplicará los siguientes métodos:

- **Indicadores de desempeño (KPI):** revisión de indicadores relacionados con la carga de trabajo, el desempeño financiero y la capacidad operativa del equipo, con el fin de evaluar las condiciones internas de la organización. Los indicadores clave de riesgo (KRI), enfocados en el seguimiento del comportamiento de los riesgos, se abordan en la sección 5.6.6, correspondiente a seguimiento y revisión.
- **Entrevistas y reuniones de seguimiento:** espacios periódicos de revisión con socios, gerencias y colaboradores, orientados a identificar cambios internos, necesidades operativas y riesgos emergentes que puedan afectar el funcionamiento de la organización.
- **Lecciones aprendidas de los proyectos:** análisis de los resultados obtenidos al cierre de cada proyecto, considerando retrasos, reprocesos, desviaciones de alcance e incidencias relevantes, con el fin de identificar oportunidades de mejora.
- **Seguimiento de incidentes y no conformidades:** documentación de situaciones relevantes ocurridas durante la operación, relacionadas con procesos internos, herramientas tecnológicas, calidad del servicio o seguridad de la información, con el fin de analizarlas y definir acciones de mejora.

Los factores internos identificados evidencian que la gestión del riesgo en Stratos Asesores S.A.S. depende de la coordinación entre las áreas, la definición clara de responsabilidades y el manejo ordenado de la información. En este contexto, las áreas

de Asesoría en Riesgos y Precios de Transferencia requieren información completa, documentación actualizada y revisión técnica para cumplir adecuadamente con cada proyecto. Estas actividades se apoyan en el soporte administrativo, especialmente en la gestión documental relacionada con contratos, acuerdos de confidencialidad y archivo. Por su parte, la Alta Dirección y las gerencias de área participan cuando se presentan retrasos, incidentes o cambios que puedan afectar la continuidad del servicio, el cumplimiento de los compromisos asumidos o la calidad de los entregables.

Mecanismo de revisión periódica del contexto.

Para asegurar que el análisis del contexto se mantenga actualizado y no refleje únicamente una situación puntual, se establece un mecanismo de revisión periódica. Este mecanismo define, para cada aspecto y herramienta utilizada, la frecuencia de revisión, el responsable y el medio correspondiente. La Tabla 52 consolida esta información y permite dar seguimiento continuo a los contextos externo e interno, aportando insumos oportunos para la actualización de la matriz de riesgos.

Tabla 52

Mecanismo de revisión periódica del contexto

Contexto	Herramienta	Frecuencia	Responsable
Externo	Análisis PESTEL	Semestral	Responsable SGR
Externo	Revisión normativa y regulatoria (SRI, SCVS, protección de datos)	Mensual	Gerencias de área
Externo	Evaluación de proveedores tecnológicos (Microsoft 365, NAS)	Continuo / anual	Responsable del SGR / proveedor de TI
Externo	Expectativas y requerimientos de los clientes	Al cierre de cada proyecto	Gerencias de área

Externo	Alertas de ciberseguridad y amenazas emergentes	Continuo	Responsable del SGR
Interno	Indicadores de gestión (KPI) de condiciones internas	Mensual	Responsable del SGR y Gerencias de área
Interno	Entrevistas y reuniones de seguimiento	Semanal / trimestral	Gerencias de área
Interno	Lecciones aprendidas de los proyectos	Al cierre de cada proyecto	Gerencias de área
Interno	Registro de incidentes	Continuo	Responsable SGR

Nota. Los resultados de estas revisiones se consolidan y sirven de insumo para la actualización de la matriz de riesgos y la identificación de riesgos emergentes.

De esta manera, las herramientas descritas no se plantean como elementos aislados, sino como insumos para mantener actualizada la matriz de riesgos, desarrollada en la sección 5.6.4, y los criterios de evaluación definidos en la sección 5.6.3.4. Esto permite que los cambios del entorno o de las condiciones internas de la organización se reflejen oportunamente en la valoración de los riesgos y en las acciones de tratamiento correspondientes, conforme a la sección 5.6.5.

Es importante diferenciar este monitoreo del contexto, orientado a revisar el entorno externo y las condiciones internas, del seguimiento de los riesgos ya identificados, el cual se aborda en la sección 5.6.6.

5.6.3.4. Definición de los Criterios de Riesgo

De acuerdo con la norma ISO 31000:2018, los criterios de riesgo corresponden a los parámetros establecidos por la organización para determinar la relevancia de los riesgos identificados y facilitar la toma de decisiones relacionadas con su evaluación, tratamiento, aceptación y seguimiento. Para Stratos Asesores S.A.S., la definición de

criterios de riesgo se establece considerando el contexto organizacional, del modelo de prestación de servicios basado en proyectos, del tratamiento de información sensible y del cumplimiento de objetivos estratégicos y operativos.

Los criterios definidos serán aplicables a todos los procesos incluidos dentro del alcance del Sistema de Gestión de Riesgos y permitirán mantener consistencia metodológica durante la identificación, análisis, evaluación y tratamiento de riesgos.

La valoración del riesgo se realizará considerando:

- Probabilidad de ocurrencia del evento.
- Impacto sobre el cumplimiento de objetivos.
- Cumplimiento normativo y contractual.
- Seguridad de la información y protección de datos.
- Continuidad operativa.
- Impacto reputacional.

La escala de probabilidad mide la frecuencia o factibilidad de ocurrencia de cada evento en cinco niveles. Dado la organización opera con un equipo de aproximadamente 17 colaboradores bajo un modelo de trabajo basado en proyectos, riesgos operativos y sobrecarga laboral presentan una mayor probabilidad de ocurrencia en comparación con organizaciones de mayor tamaño. Por tal motivo, la escala considera que eventos clasificados con probabilidad “media” pueden materializarse entre una y dos veces al año, lo cual resulta consistente con la dinámica operativa de una organización del tamaño de Stratos Asesores S.A.S.

Tabla 53

Escala de probabilidad

Nivel	Probabilidad	Descripción	Frecuencia
1	Muy baja	Riesgo poco probable y solo ocurriría en circunstancias accesionales.	Menos de una vez cada 5 años
2	Baja	Riesgo podría ocurrir, pero no se espera que suceda con frecuencia.	Una vez cada 3 años
3	Media	El riesgo puede ocurrir en determinadas condiciones o situaciones normales de operación.	Una a dos veces al año
4	Alta	El riesgo tiene una posibilidad significativa de ocurrir.	Varias veces al año
5	Muy alta	El riesgo es muy probable o ya ha ocurrido en situaciones similares.	Continua o varios eventos al mes

La escala de impacto permite determinar la severidad de las consecuencias que podría enfrentar la organización en caso de que un riesgo llegue a materializarse. Esta escala no se limita a una valoración general, sino que considera diferentes dimensiones, como el efecto operativo, reputacional, legal, normativo y financiero. Este enfoque es adecuado para la organización, donde la confianza del cliente y la capacidad técnica representan activos esenciales. Cuando un riesgo se materialice puede generar efectos más directos y evidentes en su operación al ser una organización de menor tamaño. La Tabla 54 presenta los 5 niveles definidos para esta escala.

Tabla 54

Escala de impacto

Nivel	Descriptor	Descripción	Impacto Operativo	Impacto Reputacional	Impacto Legal/Normativo	Impacto Financiero
1	Insignificante	Impacto es mínimo y no afecta de forma relevante la operación	No afecta procesos; inconveniente menor que se resuelve internamente.	Sin efecto en confianza del cliente; se mantiene la relación.	Sin incumplimientos; sin exposición regulatoria.	Pérdida < USD 1,000; sin efecto en liquidez.
2	Menor	Genera afectaciones leves que pueden corregirse fácilmente	Afecta área específica; soluble en corto plazo (1-2 días).	Comentarios negativos aislados; cliente expresa preocupación, pero mantiene relación.	Incumplimiento menor; requiere corrección rápida sin sanciones.	Pérdida USD 1,000-5,000; impacto leve en flujo de caja (<1% de los ingresos anuales).
3	Moderado	Puede afectar procesos internos, tiempo de entrega o calidad de servicios	Afecta procesos internos o tiempos de entrega; requiere reasignación de recursos (3-5 días de retraso).	Afecta percepción de calidad; cliente requiere explicación formal; riesgo de no renovación de contrato.	Incumplimiento normativo que requiere notificación a autoridades; sin sanciones financieras inmediatas.	Pérdida USD 5,000-15,000; afecta presupuesto del trimestre (1-3% de los ingresos anuales).

(Continua)

(Continuación)

	Nivel	Descriptor	Descripción	Impacto Operativo	Impacto Reputacional	Impacto Legal/Normativo
4	Mayor	Puede generar afectaciones importantes en clientes, operación, cumplimiento o reputación	Afecta múltiples proyectos o líneas de negocio; requiere intervención de gerencia (1-2 semanas de impacto).	Daño a reputación; cliente cuestiona competencia técnica; riesgo de pérdida de cliente clave.	Incumplimiento contractual significativo; probable sanción financiera; requiere defensa legal.	Pérdida USD 15,000-30,000; consume gran parte del capital de trabajo (3-6% de los ingresos anuales)
5	Crítico	Puede comprometer gravemente la continuidad del servicio, la confianza del cliente o la sostenibilidad de la organización	Compromete la continuidad del servicio o la sostenibilidad de la operación (> 2 semanas).	Daño severo a reputación; pérdida de confianza del cliente; impacto en capacidad de atraer nuevos clientes; exposición mediática negativa.	Incumplimiento grave de normativa; exposición a sanciones severas, cierre de operaciones, antecedentes regulatorios.	Pérdida > USD 30,000; supera el patrimonio y el capital de trabajo; amenaza la solvencia y la liquidez.

Los umbrales financieros presentados en la Tabla 54 fueron definidos con base en la información financiera de Stratos Asesores S.A.S. con corte al 31 de diciembre de 2025. Para ello, se consideraron los ingresos anuales de $ 490.812,91, un patrimonio de $ 30.462,13 y un capital de trabajo de $ 28.064, 86.

Bajo este contexto, el nivel crítico se estableció para pérdidas superiores a $ 30.000, debido a que dicho valor supera tanto el patrimonio como el capital de trabajo de la organización, lo que podría afectar su liquidez y solvencia. Los niveles restantes se estructuraron de manera proporcional a los ingresos anuales, tomando como referencia aproximada el 1%, 3% y 6%.

Esta definición resulta adecuada para la realidad financiera de la organización, considerando que presenta un endeudamiento del 83, 42%, una relación deuda/patrimonio de 5,03, una liquidez corriente de 1,18 y un resultado neto negativo de $-6.862,11 en 2025. Estos indicadores muestran que la organización tiene capacidad limitada para absorber pérdidas significativas, por lo que se justifica el uso umbrales conservadores.

Con el fin de facilitar una aplicación homogénea de la escala, la Tabla 55 relaciona cada nivel de impacto con descriptores específicos aplicables a los servicios de consultoría de Stratos Asesores S.A.S.

De esta manera, se cuenta con criterios más claros y concretos al momento de calificar cada riesgo.

Tabla 55

Descriptores de impacto aplicados a los servicios de Stratos Asesores S.A.S.

Nivel de impacto	Descriptor aplicado a los servicios de consultoría
Crítico (5)	Brecha masiva de confidencialidad con filtración de bases de datos de clientes; demanda legal por incumplimiento de la LOPD; glosa millonaria al cliente por fallas en el AOPR.
Alto (4)	Ataque de ransomware en el NAS Synology; retraso de más de 72 horas en la entrega del IIPT generando multas del SRI al cliente.
Moderado (3)	Caída parcial de servidores OneDrive por más de 24 horas; retrabajo técnico significativo en informes financieros por cambios normativos no monitoreados.
Bajo (2)	Retraso menor a 4 horas en la comunicación de tiempos de entrega; fallas menores de formato en reportes SOC detectadas internamente antes de la entrega final.
Insignificante (1)	Error de formato o tipográfico puntual en un documento de trabajo, detectado y corregido internamente antes de la entrega; sin efecto para el cliente.

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

El nivel de riesgo se obtiene al relacionar la probabilidad con el impacto, aplicando la fórmula PxI, de acuerdo con la matriz presentada en la Tabla 56. A partir del resultado obtenido, cada riesgo se clasifica en uno de los cuatro niveles definidos en la leyenda de la matriz.

Tabla 56

Matriz de Evaluación de Riesgos

Probabilidad/ Impacto	1 Insignificante	2 Menor	3 Moderado	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

Leyenda de colores:
Color rojo: Crítico (16–25): Requiere acción inmediata, fuera del apetito de riesgo.
Color naranja: Alto (10–15): Requiere plan de mitigación y seguimiento frecuente.
Color amarillo: Moderado (5–9): Riesgo aceptable con control.
Color verde: Bajo (1–4): Riesgo asumible, dentro del apetito de riesgo.

Nota. Tomado de *Metodología para la gestión de riesgos* (p. 25), por Muñoz Cantizano y Villalobos Serrano, 2021.

La interpretación de los niveles de riesgo resultantes es la siguiente:

- **Riesgo Bajo (1-4)**: Aceptable; se mantiene monitoreo periódico.
- **Riesgo Moderado (5-9)**: Tolerable; requiere mantener controles existentes.
- **Riesgo Alto (10-15)**: Significativo; requiere plan de mitigación y seguimiento frecuente.
- **Riesgo Crítico (16-25)**: No aceptable; requiere intervención inmediata y escalamiento a Alta Dirección.

De acuerdo con los niveles definidos, el apetito de riesgo de Stratos Asesores S.A.S. establece que la organización puede aceptar riesgos bajos y moderados,

siempre que se mantengan bajo control. En cambio, los riesgos altos deberán contar con un plan de tratamiento aprobado y un seguimiento periódico. Por su parte, los riesgos críticos se consideran fuera del nivel de riesgo aceptable para la organización, por lo que requieren atención e intervención inmediata.

Tabla 57

Criterios de aceptación del riesgo

Nivel de riesgo	Criterio	Decisión
Bajo	Riesgo aceptable	Seguimiento periódico
Moderado	Riesgo tolerable	Mantener controles existentes
Alto	Riesgo significativo	Implementar tratamiento y seguimiento frecuente
Crítico	Riesgo no aceptable	Intervención inmediata y escalamiento

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

La aceptación del riesgo residual estará a cargo del Responsable del Sistema de Gestión de Riesgos (SGR), en coordinación con las gerencias de las áreas involucradas. Para ello, se establecen distintos niveles de autorización según la criticidad del riesgo. Los riesgos bajos y moderados podrán ser aceptados por el Responsable del SGR y la gerencia del área correspondiente. En el caso de los riesgos altos, será necesaria una aprobación formal por parte de ambas instancias. Por su parte, los riesgos críticos deberán ser revisados y aprobados por la Alta Dirección, representada por los socios. En todos los casos, la decisión

de aceptar un riesgo deberá quedar debidamente documentada, incluyendo la justificación correspondiente y los compromisos definidos para su seguimiento. Los criterios establecidos en esta sección sirven como base para las etapas posteriores de evaluación y tratamiento del riesgo. Su aplicación permite mantener consistencia, al evaluar todos los riesgos bajo los mismos parámetros; pertinencia, al considerar la realidad operativa, financiera y estratégica de Stratos Asesores S.A.S.; trazabilidad, al facilitar la justificación y revisión de cada calificación; y claridad, al permitir que las partes interesadas comprendan el nivel asignado a cada riesgo y las acciones que se deben aplicar.

5.6.4. Evaluación del Riesgo

5.6.4.1. Generalidades.

La evaluación del riesgo representa el elemento principal en el Sistema de Gestión de Riesgos (SGR) que integra la identificación, análisis y la valoración de los riesgos. En Stratos Asesores S.A.S. esta evaluación se llevó a cabo de manera ordenada, participativa y continua, considerando el conocimiento de los responsables de las áreas de Asesoría en Riesgos y Precios de Transferencia. Además, se tomó como base la información disponible sobre los procesos, activos y condiciones del entorno organizacional.

Para el análisis de los riesgos de la organización se utilizará una calificación cualitativa con valoración numérica como se muestra en las siguientes tablas:

Tabla 58

Valoración de Probabilidad del Riesgo

Nivel	Probabilidad
1	Muy baja
2	Baja
3	Media
4	Alta
5	Muy alta

Tabla 59

Valoración del Impacto del Riesgo

Nivel	Impacto
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Crítico

A continuación, se presentan las tres etapas que conforman esta evaluación.

5.6.4.2. Identificación del Riesgo.

En la identificación del riesgo lo principal es encontrar, reconocer y describir los riesgos que pueden afectar el logro de los objetivos de la organización. Para ello se revisaron de manera sistemática los procesos clave de las áreas operativas y se relacionaron los activos con posibles amenazas de carácter operativo. En este análisis se consideraron las fuentes de riesgo, sus causas, los eventos asociados, las amenazas y oportunidades, los cambios del entorno, así como la dependencia

del personal y de la tecnología. Como resultado se identificaron ocho eventos de riesgo, codificados del R1 al R15, los cuales se presentan en la Tabla 60:

Tabla 60

Identificación de los riesgos

Código	Riesgo identificado	Área o proceso relacionado
R1	Pérdida o filtración de información confidencial de clientes.	Transversal / Seguridad de la información / Privacidad de datos.
R2	Errores técnicos de informes	Asesoría en Riesgos y Precios de Transferencia.
R3	Incumplimiento de plazos acordados con el cliente.	Asesoría en Riesgos y Precios de Transferencia.
R4	Dependencia de plataforma tecnológicas (herramienta Microsoft 365)	Transversal / Tecnología y continuidad operativa.
R5	Falta de documentación formal de procesos internos.	Procesos internos de las áreas operativas.
R6	Perdida de personal clave con conocimiento técnico especializado de las áreas operativas.	Administrativa / Continuidad del servicio (áreas operativas).
R7	Cambios normativos que afecten los servicios prestados.	Asesoría en Riesgos y Precios de Transferencia.
R8	Afectación reputacional por errores de prestación de servicios.	Transversal / Reputación y relación con clientes.
R9	Incumplimiento de los plazos legales de presentación ante el SRI (Anexo de Operaciones con Partes Relacionadas e Informe Integral de Precios de Transferencia).	Precios de Transferencia.
R10	Errores metodológicos en la selección o aplicación de comparables que deriven en observaciones del SRI o ajustes del cliente.	Precios de Transferencia.
R11	Inconsistencias entre el informe de Precios de Transferencia y las declaraciones tributarias del cliente.	Precios de Transferencia.

R12	Hallazgos de auditoría o consultoría sin evidencia suficiente.	Asesoría en Riesgos
R13	Pérdida, alteración o manejo inadecuado de evidencias y papeles de trabajo.	Asesoría en Riesgos
R14	Desactualización metodológica frente a marcos de referencia o mejores prácticas.	Asesoría en Riesgos
R15	Pérdida de independencia u objetividad.	Asesoría en Riesgos

El inventario incluye riesgos que afectan de manera transversal a ambas áreas, como los relacionados con seguridad de la información, dependencia tecnológica, talento humano, entorno normativo y reputación, identificados en los riesgos R1, R4, R6, R7 y R8. También considera riesgos vinculados con la gestión interna de las áreas operativas, como el R5 y riesgos específicos de cada línea de servicio. En el caso de Precios de Transferencia, los riesgos se relacionan principalmente con el cumplimiento tributario ante el Servicio de Rentas Internas (SRI), aplicación de la metodología de comparables y la calidad de información proporcionada por el cliente, correspondientes a los riesgos R9 a R12. Por su parte, en Asesoría en Riesgos, los riesgos se asocian con la sustentación de hallazgos, el manejo de evidencias, la actualización metodológica y la independencia profesional, identificados en los riesgos R13 a R15.

5.6.4.3. Análisis del Riesgo.

El análisis del riesgo tiene como finalidad comprender las características de cada evento identificado y establecer su nivel de exposición. Considerando el tamaño de la organización y la información disponible, se optó por un enfoque cualitativo. Para ello, se utilizaron las escalas de probabilidad e impacto definidas en la sección 5.6.4.1 Generalidades y combinándolas mediante la fórmula de probabilidad por impacto (PxI). La Tabla 61 presenta la matriz utilizada para clasificar los niveles de riesgo, junto con su respectiva leyenda de colores.

Al aplicar esta matriz a los quince riesgos identificados se obtiene el nivel y la clasificación de cada uno, cuyos resultados se presentan a continuación:

Tabla 61

Evaluación y Priorización de Riesgos

Código	Riesgos identificados	Probabilidad	Impacto	Nivel de riesgo	clasificación
R1	Pérdida o filtración de información confidencial de clientes.	3	5	15	**Alto**
R2	Errores técnicos de informes	3	5	15	**Alto**
R3	Incumplimiento de plazos acordados con el cliente.	2	5	10	**Alto**

R4	Dependencia de plataforma tecnológicas (herramienta Microsoft 365)	5	4	20	**Crítico**
R5	Falta de documentación formal de procesos internos.	5	3	15	**Alto**
R6	Perdida de personal clave con conocimiento técnico especializado de las áreas operativas.	2	4	8	**Moderado**
R7	Cambios normativos que afecten los servicios prestados.	3	5	15	**Alto**
R8	Afectación reputacional por errores de prestación de servicios.	3	5	15	**Alto**
R9	Incumplimiento de los plazos legales de presentación ante el SRI.	2	5	10	**Alto**
R10	Errores metodológicos en la selección o aplicación de comparables que deriven en observaciones del SRI o ajustes del cliente.	3	4	12	**Alto**
R11	Inconsistencias entre el informe de Precios de Transferencia y las declaraciones	2	4	8	**Moderado**

	tributarias del cliente.				
R12	Hallazgos de auditoría o consultoría sin evidencia suficiente.	2	4	8	**Moderado**
R13	Pérdida, alteración o manejo inadecuado de evidencias y papeles de trabajo.	2	3	6	**Moderado**
R14	Desactualización metodológica frente a marcos de referencia o mejores prácticas.	3	3	9	**Moderado**
R15	Pérdida de independencia u objetividad.	2	4	8	**Moderado**

El análisis muestra un escenario operativo que requiere atención, debido a que 9 de los 15 riesgos identificados se encuentran en niveles alto o crítico. El riesgo R4, relacionado con la dependencia de Microsoft 365 es el único clasificado como crítico, con una valoración de 20. Dentro de los riesgos altos se encuentran R1, R2, R5, R7 y R8, con una calificación de 15, seguidos del riesgo R10 con calificación de 12, y R3 y R9 con una calificación de 10. Esto evidencia que las principales exposiciones de la organización se relacionan con la seguridad de la información, calidad del servicio, cumplimiento de plazos y las obligaciones tributarias ante el SRI. Asimismo, los riesgos moderados R6, R11, R12, R13,

R14 y R15 se asocian principalmente con aspectos de talento humano, sustentación de evidencias e independencia profesional. Aunque estos riesgos se mantienen en un nivel controlado, requieren seguimiento periódico para evitar que incrementen su exposición.

5.6.4.4. Valoración del Riesgo.

La valoración del riesgo tiene como finalidad facilitar la toma de decisiones, comparando los resultados obtenidos en el análisis de riesgos y los criterios de riesgo definidos en la sección 5.6.3.4. Esta comparación permite establecer qué riesgos requieren acciones de tratamiento y cuál debe ser su prioridad. De acuerdo con los criterios establecidos, los riesgos críticos se ubican fuera del apetito de riesgo de la organización y requieren intervención inmediata. Los riesgos altos necesitan un plan de tratamiento y seguimiento frecuente, los riesgos moderados pueden aceptarse siempre que se mantengan bajo control y los riesgos bajos pueden ser asumidos por la organización. La Tabla 62 presenta la valoración de los riesgos, su nivel de prioridad y la decisión propuesta para cada caso.

Tabla 62

Valoración y priorización de riesgos

Prioridad	Código	Nivel	Clasificación	Decisión propuesta
1	R4	20	Crítico	Intervención inmediata y escalamiento a la Alta Dirección

2	R1	15	Alto	Implementar tratamiento y seguimiento frecuente
3	R2	15	Alto	Implementar tratamiento y seguimiento frecuente
4	R5	15	Alto	Implementar tratamiento y seguimiento frecuente
5	R7	15	Alto	Implementar tratamiento y seguimiento frecuente
6	R8	15	Alto	Implementar tratamiento y seguimiento frecuente
7	R10	12	Alto	Implementar tratamiento y seguimiento frecuente
8	R11	3	Alto	Implementar tratamiento y seguimiento frecuente
9	R3	2	Alto	Implementar tratamiento y seguimiento frecuente
10	R9	3	Moderado	Mantener los controles existentes
11	R15	2	Moderado	Mantener los controles existentes
12	R6	2	Moderado	Mantener los controles existentes
13	R12	2	Moderado	Mantener los controles existentes
14	R13	3	Moderado	Mantener los controles existentes
15	R15	2	Moderado	Mantener los controles existentes

Los resultados de la valoración muestran un nivel exposición relevante para la organización, debido a que ninguno de los riesgos identificados se encuentra en un nivel bajo. De acuerdo, con la clasificación obtenida, el riesgo R4 se ubica como crítico. Los Riesgos R1, R2, R5, R7, R8, R10, R3 Y R9 se clasifican como altos. Mientras que los riesgos R15, R6, R12, R13, R16 y R14 se mantienen en un nivel moderado. Por lo cual, los riesgos clasificados como críticos y altos requieren acciones de tratamiento, mientras que los riesgos moderados pueden mantenerse bajo control mediante seguimiento periódico.

El riesgo R4 relacionado con la dependencia tecnológica de Microsoft 365 es el de mayor prioridad ya que se encuentra fuera del apetito de riesgo definido y requiere una atención inmediata. Seguidamente, los riesgos altos vinculados con la seguridad de la información de los clientes, la calidad técnica de los entregables, la documentación de los procesos internos, los cambios normativos y la reputación de la firma.

Los resultados obtenidos se deberán registrar en la matriz de riesgos, comunicarse a las gerencias de área y a la Alta Dirección, y validarse conforme a los niveles de autorización definidos en la sección 5.6.3.4. De esta manera, las decisiones relacionadas con la aceptación o tratamiento de los riesgos se adoptan con el nivel de responsabilidad correspondiente y quedan debidamente documentados.

5.6.5. Tratamiento del Riesgo

5.6.5.1. Generalidades.

El tratamiento del riesgo tiene como finalidad definir e implementar las acciones más adecuadas para abordar aquellos riesgos que, de acuerdo con la valoración realizada en la sección 5.6.4.4, requieren intervención. Según la norma ISO 31000:2018, esta etapa se desarrolla de manera iterativa, ya que implica identificar y seleccionar opciones de tratamiento, planificar su ejecución, implementarlas, evaluar su efectividad y determinar si el riesgo residual

resultante puede ser aceptado. En caso de que dicho riesgo residual no sea aceptable, será necesario establecer acciones adicionales.

En Stratos Asesores S.A.S., el tratamiento se orienta principalmente a los riesgos priorizados en la valoración, es decir, el riesgo critico R4 y los riesgos altos R1, R2, R5, R7, R8, R10, R3 y R9. Estos riesgos requieren atención debido a que se encuentran pro encima del nivel de riesgo aceptable para la organización. Por su parte, los riesgos moderados R6, R12, R13, R14, R15 y R16 serán gestionados mediante retención, lo que implica aceptarlos bajo los controles existentes y mantenerlos sujetos a seguimiento periódico, sin necesidad de un plan tratamiento específico, conforme a los criterios de aceptación establecidos.

Asimismo, se reconoce que la aplicación de cualquier tratamiento puede generar un riesgo residual e incluso originar nuevos riesgos, por lo que estos deberán ser identificados, evaluados y gestionados dentro del mismo proceso.

5.6.5.2. Selección de las Opciones para el Tratamiento del Riesgo.

La selección de las opciones de tratamiento se realizó considerando el equilibrio entre los beneficios esperados, los costos y el esfuerzo requerido para su implementación, tomando en cuenta los objetivos, recursos y contexto de Stratos Asesores S.A.S. De acuerdo con la norma ISO 31000:2018, el tratamiento del riesgo puede orientarse a evitar la actividad que lo genera, aceptar o incrementar el riesgo para aprovechar una oportunidad, eliminar su fuente, modificar su probabilidad de ocurrencia, reducir sus consecuencias, compartirlo mediante

mecanismos como contratos o seguros, o retenerlo a partir de una decisión informada.

Con base en estas alternativas, la Tabla 63 presenta la opción de tratamiento seleccionada para cada uno de los nueve riesgos que requieren intervención, junto con la justificación correspondiente.

Tabla 63

Opción de tratamiento seleccionada

Código	Riesgo	Opción de tratamiento (Enfoque ISO 31000)	Justificación / Enfoque del control
R4	Dependencia de plataformas tecnológicas (Microsoft 365)	Modificar la consecuencia / Retener el riesgo residual	Reducir el impacto operativo ante una interrupción del servicio principal mediante la implementación de planes de continuidad del negocio y redundancia de datos.
R1	Pérdida o filtración de información confidencial de clientes	Modificar la probabilidad y compartir	Reducir la posibilidad de ocurrencia mediante controles de seguridad de la información (ISO 27001) y transferir la responsabilidad legal/financiera mediante acuerdos de confidencialidad (NDA) o pólizas.
R2	Errores técnicos en los informes	Modificar la probabilidad	Reducir la tasa de fallos en el entregable final mediante la estandarización de controles de calidad y la obligatoriedad de la revisión por pares.
R5	Falta de documentación	Eliminar la fuente / modificar la probabilidad	Documentar formalmente los procesos para reducir la

	formal de los procesos internos		dependencia del conocimiento no registrado.
R7	Cambios normativos que afecten los servicios prestados	Modificar la consecuencia / Asumir el riesgo para buscar una oportunidad	Dado que la organización no puede cambiar la ley (no puede modificar la probabilidad), el enfoque es minimizar el impacto mediante el monitoreo regulatorio temprano y la actualización ágil de metodologías.
R8	Afectación reputacional por errores en la prestación	Modificar la consecuencia	El riesgo reputacional es un riesgo consecuencial (deriva de R2 o R3). El tratamiento se enfoca en la contención del daño mediante un protocolo de gestión de incidentes y comunicación de crisis.
R10	Errores metodológicos en la selección de comparables	Modificar la probabilidad	Reducir la posibilidad de fallos técnicos mediante el uso exclusivo de bases de datos indexadas confiables y un flujo de validación técnica.
R3	Incumplimiento de los plazos acordados con el cliente	Modificar la probabilidad	Mitigar la ocurrencia de retrasos comerciales mediante la planificación basada en hitos y herramientas de seguimiento de cronogramas.
R9	Incumplimiento de plazos legales ante el SRI (AOPR/IIPT)	Evitar el riesgo	Eliminar la posibilidad de sanción legal asegurando la ejecución prioritaria y obligatoria de las obligaciones tributarias mediante un calendario con alertas automatizadas.

La definición de estas opciones consideró no solo los aspectos económicos, sino también las obligaciones, compromisos y expectativas de las partes interesadas de la organización. Una vez implementado cada tratamiento, será necesario

evaluar el riesgo residual obtenido. Si este se mantiene dentro del nivel aceptable, continuará bajo seguimiento, caso contrario, se deberán definir e implementar acciones adicionales de tratamiento.

5.6.5.3. Preparación e Implantación de los Planes de Tratamiento del Riesgo.

Los planes de tratamiento establecen cómo se llevarán a cabo las opciones seleccionadas para abordar los riesgos prioritarios. Conforme a la norma ISO 31000:2018, cada plan debe incluir la justificación de la opción elegida, los responsables de su aprobación e implementación, las acciones a ejecutar, los recursos requeridos, los indicadores de desempeño, las posibles restricciones, los reportes necesarios y los plazos definidos. Para este caso, los recursos considerados corresponden a los señalados en la sección 5.5.4.4, relacionadas con talento humano, herramientas tecnológicas, capacitación y tiempo. La Tabla 64 presenta el plan de tratamiento propuesto para los riesgos priorizados.

Tabla 64

Planes de tratamiento de riesgo

Código	Acciones de tratamiento	Responsable	Plazo	Indicador de seguimiento
R4	Implementar respaldos redundantes (NAS Synology y copia en la nube), plan de contingencia ante caídas y energía de respaldo.	Responsable del SGR / Proveedor de TI	Primer mes desde la aprobación del plan de tratamiento	Respaldos verificados y prueba de restauración

R1	Fortalecer la protección de la información mediante cifrado, control de accesos, autenticación multifactor (MFA), antivirus (ESET), política de seguridad de la información y acuerdos de confidencialidad (NDA).	Responsable del SGR	Dentro de los 60 días posteriores a la aprobación del plan de tratamiento.	Verificación de MFA habilitado, antivirus activo y NDA firmados
R2	Aplicar revisión por partes, listas de verificación y formato estandarizado para el control de calidad.	Gerencia de área	En cada revisión previa a la entrega al cliente	Registro de revisiones realizada y observaciones corregidas.
R5	Documentar los procedimientos claves del SGR, manteniendo un control de versiones que permita asegurar su actualización y trazabilidad.	Responsable del SGR / Gerencias de área	Dentro de los primeros 90 días del plan de tratamiento.	Procedimientos documentados y versiones actualizadas en el repositorio.
R7	Realizar un monitoreo periódico de la normativa aplicable y actualizar las metodologías de trabajo del equipo conforme a los cambios emitidos por el SRI y entes de control.	Gerencias de Precios de Transferencia y Asesoría en Riesgos	Revisión mensual	Cambios normativos revisados y metodologías actualizadas.
R8	Definir un protocolo para la gestión de incidentes y la comunicación oportuna con las partes involucradas,	Alta Dirección y Gerencias de área	Segundo mes de ejecución del plan de tratamiento.	Registro de incidentes atendidos y resultados de encuestas de

	complementando con el seguimiento de la satisfacción del cliente y atención de quejas recibidas.			satisfacción del cliente.
R10	Aplicar una revisión metodológica independiente dentro del equipo y emplear fuentes confiables de comparables, documentando los criterios utilizados para sustentar el análisis.	Gerencia de Precios de Transferencia	Antes de la entrega final de cada estudio.	Estudios revisados con criterios documentados y sin observaciones metodológicas relevantes.
R3	Definir cronograma por proyecto, con actividades clave y seguimiento en las reuniones semanales, considerando la gestión adecuada de la carga de trabajo.	Gerencias de área	Seguimiento semanal por proyecto	Registro de avances revisados y entregas cumplidas dentro del plazo.
R9	Implementar un calendario tributario con alertas previas y responsables asignados, para facilitar la presentación anticipada del AOPR y del IIPT.	Gerencia de Precios de Transferencia	Conforme al calendario establecido por el SRI.	Obligaciones tributarias presentadas a tiempo.

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

Los planes de tratamiento se incorporan a los procesos de gestión de la organización y se ejecutan considerando la participación de las partes interesadas que correspondan. Tanto el avance de las acciones como el riesgo residual

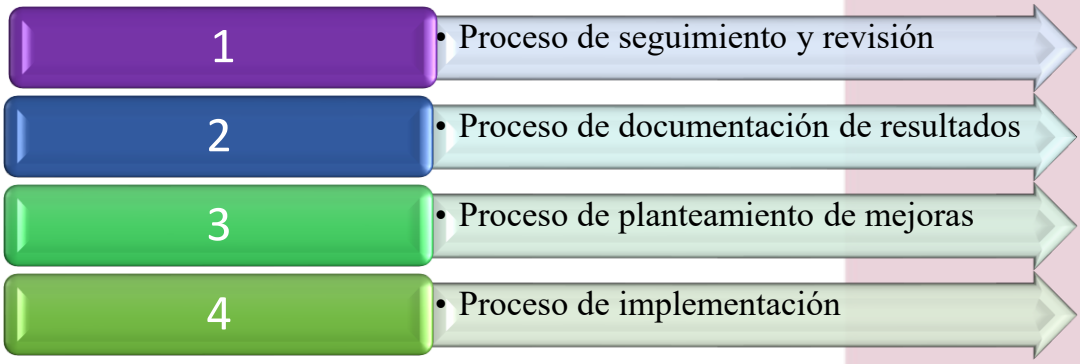
resultante deberán ser monitoreados y revisados de manera periódica, permitiendo verificar que las medidas implementadas sean efectivas y se mantengan adecuadas en el tiempo.

5.6.6. Seguimiento y revisión

El seguimiento y la revisión tiene como finalidad verificar y fortalecer la calidad, eficacia y resultados del proceso de gestión del riesgo. Considerando que el entorno de Stratos Asesores S.A.S. puede cambiar y que los riesgos pueden surgir, modificarse o dejar de ser relevantes, esta etapa plantea un monitoreo permanente de los controles y de los planes de tratamiento, acompañado de revisiones periódicas y responsabilidades asignadas.

Figura 15

Proceso de documentación de resultados de Stratos Asesores S.A.S.



Nota. Con base en la información proporcionada por la organización.

Estas actividades se aplican a lo largo de todo el proceso de gestión del riesgo e incluyen la planificación, recopilación y análisis de la información, el registro de resultados y la generación de retroalimentación. De esta forma, se puede

comprobar si las medidas de tratamiento continúan siendo efectivas, identificar cambios en el contexto organizacional y detectar riesgos emergentes que puedan afectar el cumplimiento de los objetivos de la organización.

Tabla 65

Seguimiento y Revisión área de operaciones y servicios Stratos Asesores S.A.S.

Encargado	Responsabilidad	Frecuencia
Alta Dirección	Revisa periódicamente el estado general de los riesgos y la eficacia del sistema y aprueba las acciones para los riesgos críticos y altos.	Trimestral
Responsable del Sistema de Gestión de Riesgos	Coordina el seguimiento continuo de los riesgos y de los planes de tratamiento, consolida la información, registra los resultados y reporta a la Alta Dirección.	Continuo / Mensual
Gerencias de área (Asesoría en Riesgos y Precios de Transferencia)	Revisan y validan los riesgos de su respectiva área, y verifican el cumplimiento de los controles y el avance de los planes de tratamiento.	Mensual
Colaboradores de cada área	Ejecutan los controles, reportan los riesgos emergentes y las desviaciones, y custodian las evidencias.	Continuo

Mecanismos de seguimiento.

El seguimiento se apoyará en los espacios de coordinación que la organización ya mantiene, con el fin de aprovechar las dinámicas existentes y evitar la creación de reuniones adicionales.

- Seguimiento continuo: reuniones semanales (lunes) se reportan los riesgos emergentes y el avance de los planes de tratamiento.
- Revisión mensual: el Responsable del SGR y las gerencias de área

revisan la matriz de riesgos y el estado de los controles.

- Revisión trimestral: la Alta Dirección evalúa el estado general de los riesgos y la eficacia del sistema.

Indicadores clave de riesgo (KRI)

Como parte del seguimiento, se establecen indicadores clave de riesgo, conocidos como KRI por sus siglas en inglés. Estos indicadores funcionan como señales de alerta temprana, ya que permiten identificar oportunamente si un riesgo está aumentando su probabilidad de ocurrencia o su nivel de impacto antes de que llegue a materializarse. A diferencia de los indicadores de gestión, conocidos como KPI, que se enfocan en medir el cumplimiento de objetivos, los KRI se orientan al monitoreo del comportamiento de los riesgos prioritarios de la organización.

Los indicadores clave de riesgo (KRI) de Stratos Asesores S.A.S. se construyen a partir de los indicadores de seguimiento definidos en los planes de tratamiento de la sección 5.6.5. Estos se consolidan en la Tabla 66, donde se identifica el riesgo asociado, el umbral o meta que genera una alerta, la frecuencia de medición y el responsable de su monitoreo.

Tabla 66

Esquema de indicadores clave de riesgo (KRI)

KRI	Riesgo	Criterio de alerta	Frecuencia	Responsable

Incidentes de seguridad de la información registrados	R1	Alerta cuando se registre al menos un incidente	Mensual	Responsable del SGR
Respaldos verificados con resultado satisfactorio	R4	Alerta cuando existan respaldos no verificados	Mensual	Responsable del SGR y proveedor de TI
Entregables revisados mediante revisión por pares	R2	Alerta cuando existan entregables sin revisión por pares	Por entregable	Gerencias de área
Procesos clave documentados y actualizados	R5	Alerta cuando el avance de documentación sea menor al 80 %	Trimestral	Responsable del SGR
Cambios normativos revisados y atendidos oportunamente	R7	Alerta cuando existan cambios normativos pendientes de atención	Mensual	Gerencias de área
Resultado de la medición de satisfacción del cliente	R8	Alerta cuando la satisfacción del cliente sea menor a 4 sobre 5	Trimestral	Alta Dirección y Gerencias de área
Estudios revisados sin observaciones metodológicas relevantes del SRI	R10	Alerta cuando se registre más de una observación relevante por estudio	Por estudio	Gerencia de Precios de Transferencia
Entregas cumplidas dentro del plazo acordado	R3	Alerta cuando las entregas dentro del plazo sean menores al 95 %	Mensual	Gerencias de área

Obligaciones tributarias presentadas oportunamente	R9	Alerta cuando exista al menos una obligación tributaria presentada fuera de plazo	Según calendario SRI	Gerencia de Precios de Transferencia

Nota. Con base en la información recopilada durante el desarrollo de la investigación.

El monitoreo de estos indicadores se incorpora a las actividades regulares de seguimiento definidas en esta sección. Sus resultados serán revisados en reuniones mensuales y trimestrales, y cuando alguno supere el criterio de alerta establecido, se activará la comunicación correspondiente y, si aplica, el ajuste del tratamiento definido en la sección 5.6.5. De esta manera, los indicadores clave de riesgo y las revisiones programadas permiten dar cumplimiento al objetivo específico de la investigación, orientado a establecer un esquema de seguimiento y mejora basado en indicadores y controles periódicos.

Herramienta de seguimiento

Como herramienta de apoyo al seguimiento, se propone el uso de una lista de verificación que permita revisar periódicamente el estado de cada riesgo. Esta propuesta de formato facilitará la comparación entre la situación actual del riesgo y su calificación previa, considerando las etapas de análisis, valoración y tratamiento, con el fin de determinar si las medidas aplicadas continúan siendo adecuadas o si requieren ajustes.

La siguiente Tabla 67 presenta la lista de verificación aplicada a los riesgos prioritarios aun también pudiendo utilizarse para los riesgos moderados. En cada ciclo de revisión, el responsable registrará el estado del control, utilizando las categorías Cumple, En proceso o No cumple, e incluirá las observaciones o acciones correctivas que correspondan.

Tabla 67

Seguimiento y revisión de riesgos

Código	Riesgo	Actividad	Frecuencia	Responsable	Estado	Observaciones
R4	Dependencia de plataformas tecnológicas (Microsoft 365)	Verificación de respaldos y prueba de restauración del servicio.	Mensual	Responsable del SGR y proveedor TI	Por evaluar	Cuando aplique
R1	Pérdida o filtración de información confidencial de clientes	Revisión de controles accesos, autenticación multifactor (MFA), antivirus activo y acuerdos de confidencialidad (NDA) firmados.	Mensual	Responsable del SGR	Por evaluar	Cuando aplique
R2	Errores técnicos en los informes	Revisión de entregables mediante revisión por pares, listas de verificación	Por entrega de informe de proyecto	Gerencias de área	Por evaluar	Cuando aplique

		y formatos de control de calidad.				
R5	Falta de documentación formal de los procesos internos	Verificación de procedimientos documentados y control de versiones aplicado en el repositorio del SGR.	Mensual	Responsable del SGR y Gerencias de área	Por evaluar	Cuando aplique
R7	Cambios normativos que afecten los servicios prestados	Revisión de cambios normativos identificados y actualizaciones metodológicas aplicadas.	Mensual	Gerencias de área	Por evaluar	Cuando aplique
R8	Afectación reputacional por errores en la prestación	Seguimiento de incidentes atendidos, quejas registradas y resultados de satisfacción del cliente.	Trimestral	Alta Dirección y Gerencias de área	Por evaluar	Cuando aplique
R10	Errores metodológicos en la selección de comparables	Revisión de estudios de comparables con criterios metodológicos documentados.	Por estudio	Gerencia de Precios de Transferencia	Por evaluar	Cuando aplique
R3	Incumplimiento de los plazos	Seguimiento de avances, carga de	Semanal	Gerencias de área	Por evaluar	Cuando aplique

	acordados con el cliente	trabajo y entregas cumplidas dentro del plazo acordado.				
R9	Incumplimiento de plazos legales ante el SRI (AOPR/IIPT)	Verificación del calendario tributario y de la presentación oportuna del AOPR y IIPT ante el SRI.	Antes de cada vencimiento tributario aplicable	Gerencia de Precios de Transferencia	Por evaluar	Cuando aplique

Los resultados del seguimiento y la revisión se documentarán de forma periódica, con una consolidación formal semestral a cargo del Responsable del Sistema de Gestión de Riesgos. Estos resultados serán presentados en las reuniones con la Alta Dirección y las gerencias de área, con el fin de informar el estado de los riesgos, evaluar la eficacia de los tratamientos aplicados, identificar riesgos emergentes y revisar el riesgo residual. Asimismo, estas revisiones permitirán definir oportunidades de mejora, especialmente en aquellos riesgos que, aun después de aplicar medidas de tratamiento, mantengan niveles relevantes de probabilidad o impacto.

El monitoreo de los controles permitirá identificar hallazgos, documentarlos y, posteriormente, definir mejoras o acciones correctivas. Una vez implementadas dichas acciones, el proceso continuará con nuevas actividades de seguimiento.

Este ciclo permite que las debilidades operativas o tecnológicas identificadas sean atendidas de manera ordenada y se conviertan en acciones correctivas sostenibles, conforme al enfoque de la norma ISO 31000:2018.

Finalmente, los resultados obtenidos se incorporarán a las actividades de medición, registro e informe de la organización.

5.6.7. Registro e informe

De acuerdo con la norma ISO 31000:2018, el registro e informe de la gestión de riesgos tiene como propósito documentar las actividades realizadas, comunicar los resultados obtenidos y proporcionar información para la toma de decisiones En Stratos Asesores S.A.S., estas actividades permiten informar sobre el desarrollo de la gestión del riesgo dentro de la organización, aportar información útil para la toma de decisiones, fortalecer el propio sistema y facilitar la comunicación con las partes interesadas.

Los principales documentos que formarán parte del registro del SGR son:

- Matriz de riesgos actualizada.
- Planes de tratamiento de riesgos.
- Listas de verificación de seguimiento
- Informes periódicos de desempeño
- Actas de reuniones de revisión

Estos registros se conservarán en el repositorio del Sistema de Gestión de Riesgos (SGR) en OneDrive, aplicando control de versiones y considerando el

uso, la sensibilidad de la información y el contexto interno y externo de la organización.

Para definir el contenido, la frecuencia y el medio de presentación de los informes, se considerarán las necesidades de información de las partes interesadas, la oportunidad y periodicidad del reporte, el canal más adecuado para cada destinatario y la utilidad de la información para los objetivos organizacionales y la toma de decisiones.

Tabla 68

Registros e informes del Sistema de Gestión de Riesgos

Documento	Descripción	Responsable
Matriz de riesgos	Registro de los riesgos identificados, evaluados y priorizados.	Responsable del SGR
Plan de tratamiento de riesgos	Contiene las acciones definidas para mitigar los riesgos.	Responsable del SGR y Gerencias
Informes periódicos de desempeño	Evidencian el estado de los riesgos y la efectividad de los controles.	Responsable del SGR
Actas de reuniones de revisión	Registran acuerdos y decisiones relacionadas con la gestión de riesgos.	Responsable designado

Nota. Con base en la información proporcionada por la organización y en el análisis realizado durante el desarrollo de la investigación.

Finalmente, los informes generados serán presentados periódicamente a la Alta Dirección para apoyar la toma de decisiones y asegurar la mejora continua del Sistema de Gestión de Riesgos.

5.6.7.1. Medios de comunicación

De acuerdo con la ISO 31000:2018, la comunicación y consulta constituyen actividades permanentes dentro del proceso de gestión de riesgos, ya que permiten compartir información relevante, apoyar la toma de decisiones y mantener informadas a las partes interesadas. Stratos Asesores S.A.S. define canales de comunicación diferenciados para que la información relacionada con la gestión del riesgo sea transmitida de forma clara, oportuna y segura a las partes interesadas. Los canales internos permiten sensibilizar al personal, reportar incidentes y coordinar acciones correctivas, mientras que los canales externos facilitan la comunicación con clientes, proveedores y organismos de control, procurando mantener el cumplimiento y proteger la reputación de la organización. La Tabla 69 presenta un resumen de estos medios de comunicación.

Tabla 69

Registros e informes del Sistema de Gestión de Riesgos

Medio	Uso	Objetivo	Destinatarios
Interno	Correo electrónico institucional	Notificación de alertas prioritarias y envío de los informes periódicos de desempeño.	Gerencias y Alta Dirección.
Interno	Reuniones de seguimiento (semanales y de revisión)	Revisar el avance del checklist de seguimiento y coordinar las acciones correctivas.	Responsable del SGR, Gerencias de área y colaboradores.
Interno	Microsoft Teams	Difusión de boletines, alertas de seguridad (p. ej., campañas	Todo el personal.

		contra phishing) y guías de uso de herramientas.	
Interno	Repositorio del SGR (OneDrive)	Disponibilidad de la matriz de riesgos, los planes y el estado de cumplimiento.	Responsable del SGR y Gerencias de área
Externo	Comunicados oficiales por correo o grupo corporativo de WhatsApp	Notificar actualizaciones de los acuerdos de confidencialidad (NDA), políticas de protección de datos y manejo de la información.	Clientes
Externo	Reuniones con clientes	Reportar cómo los controles protegen sus procesos de precios de transferencia y fiscalidad.	Clientes estratégicos
Externo	Página web y portal corporativo	Publicar el compromiso de la dirección y las políticas de privacidad y seguridad de la información.	Clientes, proveedores y terceros.
Externo	Informes a entes reguladores	Entrega de documentación y cumplimiento de la normativa vigente.	SRI y organismos de control.

Estos mecanismos permitirán mantener una comunicación bidireccional entre la Alta Dirección, las Gerencias de área, el Responsable del Sistema de Gestión de Riesgos, clientes, proveedores y los colaboradores, facilitando la detección temprana de riesgos y la adopción de acciones oportunas.

5.6.7.2. Cronograma de actividades para la implementación de procesos de mejora ante los riesgos detectados.

Una gestión del riesgo efectiva requiere organizar en el tiempo las acciones de tratamiento y mejora que se derivan de los riesgos identificados. En este sentido, la Tabla 70 presenta el cronograma propuesto para ejecutar los tratamientos

asociados a los riesgos prioritarios. Los plazos se plantean de forma relativa, a partir de la aprobación del sistema, para que puedan integrarse al plan de implementación del marco descrito en la sección 5.5.5, sin depender de fechas específicas.

Tabla 70

Cronograma de implementación de mejoras

Plazo	Actividad de mejora	Riesgos asociados	Responsables
Primer mes posterior a la aprobación del sistema	Aprobación y asignación de recursos para el tratamiento inmediato de la dependencia tecnológica, los respaldos redundantes y el plan de contingencia.	R4	Alta Dirección, Responsable del SGR, proveedor de TI.
Dentro de los dos primeros meses de ejecución	Implementación de controles de seguridad de la información y estandarización del control de calidad mediante revisión por pares y plantillas.	R1, R2	Responsable del SGR, Gerencias de área.
Entre el segundo y tercer mes de ejecución	Documentación de procesos internos, fortalecimiento del monitoreo normativo y actualización del calendario tributario con alertas.	R5, R7, R9	Responsable del SGR, Gerencia de Precios de Transferencia.
Durante el tercer mes de ejecución	Definición del protocolo de gestión de incidentes y reputación, revisión metodológica de comparables y seguimiento de cronogramas por proyecto.	R8, R10, R3	Alta Dirección, Gerencia de Precios de Transferencia
Entre el tercer y cuarto mes de ejecución	Capacitación y difusión de procedimientos y políticas al personal.	Todos los riesgos	Responsable del SGR.
Entre el cuarto y sexto mes de ejecución	Seguimiento de la eficacia de los tratamientos y primera revisión integral del sistema.	Todos los riesgos	Responsable del SGR, Alta Dirección.

El cronograma propuesto contempla un periodo de seis meses, estructurado en tres momentos principales. El primero corresponde a una etapa inicial, durante el primer mes, orientada a obtener el respaldo de la Alta Dirección y atender el riesgo crítico relacionado con la dependencia tecnológica. El segundo momento comprende la ejecución de acciones entre el segundo y cuarto mes, enfocadas en los riesgos altos vinculados con seguridad de la información, calidad, documentación, cumplimiento normativo y gestión de plazos. Finalmente, entre el cuarto y sexto mes se plantea una etapa de consolidación, destinada a verificar la eficacia de los tratamientos aplicados y fortalecer la mejora continua del sistema. Este despliegue se realizará procurando mantener la continuidad y calidad de los servicios de asesoría en riesgos y precios de transferencia.

La información documentada del sistema se conservará en el repositorio del Sistema de Gestión de Riesgos (SGR), considerando su uso y nivel de sensibilidad. Asimismo, los registros e informes generados servirán como insumo para la evaluación independiente de la eficacia del sistema, la cual se desarrollará mediante la auditoría interna descrita en la sección 5.6.8.

5.6.8. Auditoría interna

La auditoría interna del Sistema de Gestión de Riesgos de Stratos Asesores S.A.S. tendrá como propósito revisar si los controles y planes definidos para tratar los riesgos se aplican correctamente y si las responsabilidades asignadas se cumplen en las áreas de la organización. También permitirá comprobar si las

acciones adoptadas reducen los riesgos identificados y si el sistema se mantiene alineado con los objetivos organizacionales.

La auditoría se ajustará a la forma de trabajo de Stratos y revisará los procesos principales de la organización. Sus resultados permitirán identificar hallazgos, observaciones, no conformidades y oportunidades de mejora.

5.6.8.1. Objetivos de la Auditoría interna

- Verificar que el Sistema de Gestión de Riesgos funcione de acuerdo con los riesgos identificados, los controles definidos y los objetivos de la organización.
- Evaluar si los planes de tratamiento y las acciones aplicadas ayudan a reducir los riesgos priorizados en las áreas de la organización.
- Revisar la documentación, evidencias y registros relacionados con la matriz de riesgos, controles, responsables y seguimiento de acciones.
- Identificar hallazgos, observaciones, no conformidades y oportunidades de mejora que permitan fortalecer el Sistema de Gestión de Riesgos.

5.6.8.2. Procesos de la Auditoría interna

La auditoría interna cumplirá cuatro fases principales:

- **Planificación:** Se define el alcance de la auditoría, los criterios de revisión, el cronograma, el equipo auditor y los auditados. También se determinan los procesos de Stratos que serán evaluados, tomando como referencia la matriz de riesgos, los planes de tratamiento y los controles

definidos.

- **Ejecución:** Los auditores revisan documentos, registros y evidencias del Sistema de Gestión de Riesgos. En esta fase también se realizan consultas individuales a los responsables de las áreas auditadas para verificar si los controles se aplican correctamente y si las actividades se ejecutan según lo planificado.
- **Informe:** Se documentan los hallazgos, observaciones, no conformidades y oportunidades de mejora identificadas durante la auditoría. El informe debe ser claro, verificable y útil para la Alta Dirección y los responsables de las áreas auditadas.
- **Seguimiento:** Se verifica el cumplimiento de las acciones correctivas definidas en el informe. Esta fase permite comprobar si las acciones fueron aplicadas dentro del plazo establecido, si cuentan con evidencia suficiente y si corrigieron la desviación detectada.

Para aplicar estas fases, Stratos utilizará un plan de auditoría interna como se detalla en la Tabla 71:

Tabla 71

Plan de auditoría interna

Objetivos de la auditoría	1. Verificar y evaluar el funcionamiento del Sistema de Gestión de Riesgos de Stratos, según los riesgos identificados 2. Revisar la eficacia de los controles aplicados en los procesos auditados. 3. Incluir a la Alta Dirección, responsables de área y colaboradores en la actualización de la información del sistema.						
Alcance	Procesos principales de las áreas de Riesgos, Precios de Transferencia y Administración.						
Criterios	ISO 31000:2018. Matriz de riesgos. Procedimientos internos. Controles definidos. Requisitos legales aplicables.						
Fecha	**Hora**	**Encargado**	**Área**	**Procesos**	**Función**	**Auditado**	**N.C**
Dia 1	09h00 - 10h00	Auditor Designado	Alta Dirección	Dirección y seguimiento del SGR	Apertura de auditoría, revisión del objetivo, alcance y criterios	Alta Dirección y Responsable del SGR	Sí / No
Dia 1	10h00 - 12h00	Auditor Designado	Riesgos	Identificación, análisis, valoración y tratamiento de riesgos	Revisión de matriz de riesgos, planes de tratamiento, controles definidos, informes técnicos y documentación relacionada con las actividades del área	Responsable del área de Riesgos	Sí / No

(Continua)

(Continuación)

Fecha	Hora	Encargado	Área	Procesos	Función	Auditado	N.C
Dia 1	14h00 - 16h00	Auditor Designado	Precios de Transferencia	Planificación, ejecución técnica y revisión de estudios de precios de transferencia	Revisión de informes técnicos, validación técnica y documentación relacionada con las actividades del área	Responsable del área de Precios de Transferencia	Sí / No
Dia 2	09h00 - 11h00	Auditor Designado	Administración	Gestión contractual, facturación, cobranza y soporte administrativo	Revisión de contratos, acuerdos de confidencialidad, facturas, registros de cobranza y documentos administrativos	Responsable administrativo	Sí / No
Dia 2	11h00 - 12h30	Auditor Designado	Riesgos, Precios de Transferencia y Administración	Gestión documental y control de accesos	Revisión de carpetas de OneDrive, respaldos en NAS, permisos de acceso y organización documental por cliente o proceso	Responsables de área y Responsable del SGR	Sí / No
Dia 2	15h00 - 16h30	Auditor Designado	Alta Dirección y áreas auditadas	Resultados de auditoría	Reunión de cierre, presentación de hallazgos, observaciones, no conformidades y acciones requeridas	Alta Dirección y responsables auditados	Sí / No
	Nota: La duración de la auditoría podrá ajustarse según el alcance definido, la disponibilidad de las áreas auditadas y la cantidad de documentos o evidencias que deban revisarse.						

Al finalizar la auditoría se elaborará un informe con los hallazgos, observaciones, no conformidades y acciones requeridas. Este informe será comunicado a la Alta Dirección y a los responsables de las áreas auditadas. Cuando se definan acciones correctivas, se revisará posteriormente su cumplimiento y la evidencia presentada para cerrar la no conformidad o cualquier observación detectada.

5.6.8.3. No conformidades y acciones correctivas

Cuando en la auditoría interna se detecte una no conformidad, Stratos Asesores S.A.S., deberá registrarla y aplicar acciones correctivas para evitar que vuelva a repetirse. Estas no conformidades pueden originarse por incumplimientos en los controles, procedimientos o evidencias requeridas por el SGR.

El tratamiento de las no conformidades se realizará en tres etapas:"

- **Identificación de la causa raíz:** Se revisará el origen de la no conformidad para determinar qué falló y evitar que la corrección se limite al problema encontrado.
- **Acciones correctivas:** Identificada la causa, se definirán acciones para corregir la no conformidad y evitar que vuelva a presentarse. Estas acciones podrán incluir ajustes en procedimientos, refuerzo de controles, capacitación o reasignación de responsabilidades.
- **Verificación de la eficacia:** Después de aplicar las acciones correctivas, se revisará si fueron cumplidas y si corrigieron la causa identificada. Esta

verificación podrá realizarse mediante revisión documental, consulta al responsable del área o auditoría de seguimiento.

CAPÍTULO 6.

Conclusiones y Aplicaciones

6.1. Conclusiones Generales

Este trabajo presenta el diseño de un Sistema de Gestión de Riesgos basado en ISO 31000:2018 para Stratos Asesores S.A.S., considerando su tamaño, estructura, áreas principales de servicio y la forma en que desarrolla sus proyectos. La propuesta surge ante la falta de un esquema estructurado para gestionar riesgos. Su desarrollo incluye un marco de referencia, un proceso para gestionar los riesgos y herramientas ajustadas a las actividades de la organización. El análisis se centra en la operación, la seguridad de la información y la protección de datos personales.

El diseño propuesto ordena la gestión de riesgos a partir del contexto de la organización, los procesos clave y las responsabilidades de cada área. También permite contar con criterios comunes para identificar, valorar, documentar y tratar los riesgos, además de mecanismos de seguimiento y mejora continua. Esto le da a Stratos una base clara para anticipar situaciones que puedan afectar la calidad de sus servicios, los compromisos asumidos con los clientes, la continuidad operativa y el cumplimiento de sus objetivos.

6.2. Conclusiones Específicas

6.2.1. Análisis del Cumplimiento de los Objetivos de la Investigación

El trabajo de investigación cumple el objetivo general al diseñar un Sistema de Gestión de Riesgos basado en ISO 31000:2018 para Stratos Asesores S.A.S. La propuesta se estructura mediante el desarrollo del marco de referencia, del proceso para gestionar los riesgos y de las herramientas acordes con su tamaño, áreas de trabajo y forma de desarrollar proyectos. La gestión de riesgos se relaciona con la operación diaria, la seguridad de la información y la protección de datos personales.

El análisis del contexto interno y externo, junto con la revisión de los procesos clave, responde a los objetivos relacionados con la comprensión de la organización y su funcionamiento. Esta revisión permite ubicar dónde pueden originarse los riesgos, qué áreas participan en su gestión y qué responsabilidades deben quedar definidas. El marco propuesto incorpora la política, los roles y los mecanismos de reporte necesarios para ordenar la participación de las áreas involucradas.

La metodología propuesta permite cumplir los objetivos relacionados con la identificación, análisis y evaluación de riesgos, usando criterios de probabilidad e impacto. Estos criterios sirven para estructurar el registro de riesgos y priorizar los riesgos críticos en las áreas de Asesoría en Riesgos y Precios de Transferencia. Esa priorización permite plantear planes de tratamiento con acciones, responsables, plazos y evidencias. El seguimiento se apoya en indicadores de desempeño (KPI), indicadores clave de riesgo (KRI), revisiones periódicas y mejora continua, considerando los riesgos asociados con la seguridad de la información y la privacidad de los datos personales.

6.2.2. *Contribución a la Gestión Empresarial*

Diseñar un Sistema de Gestión de Riesgos basado en la ISO 31000:2018 constituye un aporte para la gestión empresarial de Stratos Asesores S.A.S., al proporcionar una estructura metodológica que permite abordar los riesgos de manera sistemática y alineada con los objetivos organizacionales. El marco, los procesos y las herramientas propuestas facilitan la identificación, análisis, evaluación y tratamiento de riesgos asociados a la operación, la seguridad de la información y la protección de datos personales, contribuyendo a fortalecer los mecanismos de control y la toma de decisiones dentro de la organización.

Además, dentro de la propuesta se definen responsabilidades claras, mecanismos de comunicación de riesgos y actividades de seguimiento para las acciones de tratamiento. Esto permite que la organización tenga una guía estructurada para gestionar los riesgos de manera más ordenada y preventiva. Aunque el sistema no se implementa como parte de este proyecto, el diseño propuesto establece las bases para que, en una futura aplicación, la empresa pueda integrar la gestión de riesgos en sus procesos y fortalecer la toma de decisiones orientadas al cumplimiento de sus objetivos.

6.2.3. *Contribución a Nivel Académico*

Desde una perspectiva académica, el presente proyecto permite aplicar de manera práctica los conocimientos adquiridos durante la Maestría en Gestión de Riesgos mediante el diseño de un Sistema de Gestión de Riesgos basado en la ISO 31000:2018

para Stratos Asesores S.A.S. Su desarrollo fortalece las competencias en análisis organizacional, identificación, evaluación y tratamiento de riesgos, así como en la estructuración de un marco de gestión alineado con estándares internacionales.

Además, el trabajo constituye una referencia académica para futuras investigaciones y proyectos relacionados con el diseño de sistemas de gestión de riesgos en organizaciones de servicios profesionales, evidenciando la aplicabilidad de la norma en empresas de tamaño pequeño y mediano.

6.2.4. Contribución a Nivel Personal

A nivel personal, esta investigación nos permite crecer profesional y técnicamente, porque llevamos a la práctica los lineamientos de la norma ISO 31000:2018 y la normativa de protección de datos en una organización real. Durante el desarrollo del trabajo, comprendemos mejor cómo se gestionan los riesgos dentro de una empresa y cómo estas decisiones se relacionan con la seguridad de la información, la confidencialidad y la continuidad de sus actividades.

El proceso también fortalece nuestra forma de analizar problemas, tomar decisiones y trabajar en equipo bajo plazos exigentes. La revisión de la realidad de Stratos Asesores S.A.S. nos hace más conscientes de la responsabilidad que implica manejar información sensible de clientes, empleados y terceros. Esta experiencia nos deja una visión más preventiva y ordenada de la gestión empresarial, y refuerza nuestro compromiso profesional para aportar soluciones responsables, técnicas y útiles dentro de una organización.

6.3. Limitaciones a la Investigación

Durante el desarrollo de la investigación, una de las principales limitaciones identificadas corresponde a la ausencia de documentación formal relacionada con la gestión de riesgos y la seguridad de la información en Stratos Asesores S.A.S. La organización no cuenta con un inventario consolidado de activos tecnológicos, procedimientos, políticas o registros que sirvan como referencia para el diseño del sistema propuesto. En consecuencia, resulta necesario llevar a cabo actividades de levantamiento de información y establecer una estructura de codificación documental que facilite la organización de las políticas y procedimientos desarrollados durante el proyecto.

De igual forma, la recopilación de información técnica sobre los equipos tecnológicos representa un reto, debido a la ausencia de un sistema centralizado de información y a la inexistencia de registros consolidados que especifiquen las características y configuraciones de los activos. Sin embargo, estos desafíos no afectan el cumplimiento de los objetivos planteados, permitiendo desarrollar las actividades previstas y alcanzar los resultados esperados del proyecto.

Bibliografía

Acuña, P. (2025). Análisis de indicadores Claves de Desempeño-KPI del Contrato de Concesión.

Estupiñán, G. (2011). Control interno y fraudes: con base en los ciclos transaccionales: análisis de informe COSO I y II. *Ecoe Ediciones.*

Muñoz Cantizano, F., y Villalobos Serrano, L.F. (2021). Diseño e implementación de un modelo de gestión de riesgo basado en la norma ISO 31000:2018.

Organización Internacional de Normalización. (2018). *Gestion de riesgo- Directrices (ISO 31000:2018).* Ginebra: ISO.

Whittington, R., Ragner, P., Angwin, D., Johnson, G., & Scholes, K. (2020). *Exploring Strategy.* Pearson.

Anexos

Anexo A

Procedimiento de elaboración de procedimientos normalizados de trabajo (PNT)

Procedimientos relacionados:

- Política Antisoborno Stratos Asesores
- Manual Políticas para la Gestión de Datos Personales
- Manual de Políticas de Seguridad de la Información

Índice

Redactado por	Revisado por	Aprobado por
Coordinadora Administrativa	Gerencia de Área	CEO

1. Objetivo

Establecer una forma estándar para identificar, crear, codificar, revisar, aprobar, publicar, actualizar y controlar los Procedimientos Normalizados de Trabajo que forman parte del Sistema de Gestión de Riesgos de Stratos Asesores. Este procedimiento busca que todos los documentos sobre gestión de riesgos sean elaborados de forma uniforme, clara y trazable, facilitando que los colaboradores los entiendan y puedan aplicarlos en su trabajo diario. Además, evita que existan documentos desactualizados, incompletos o creados sin seguir criterios comunes. De esta manera, los colaboradores de Stratos dispondrán de documentos consistentes, controlados y alineados con el diseño del Sistema de Gestión de Riesgos basado en la norma ISO 31000:2018.

2. Responsabilidad De Aplicación Y Alcance

2.1 Responsabilidad

La responsabilidad de aplicar este procedimiento recae en todas las personas de Stratos Asesores que intervengan en cualquier etapa de los Procedimientos Normalizados de Trabajo: desde su creación hasta su control y actualización.

Tabla A 1

Roles y responsabilidades para la gestión y control de procedimientos del Sistema de Gestión de Riesgos

Rol	Responsabilidad principal

Chief Executive Officer (CEO)	Aprobar los procedimientos que formen parte del SGR y asegurar que existan los recursos necesarios para su aplicación.
Gerencia de Área	Revisar que el contenido del procedimiento sea coherente con las actividades reales del área, los servicios prestados y los objetivos de la organización.
Coordinadora Administrativa	Coordinar la elaboración, actualización, codificación, publicación, comunicación y control de los procedimientos.
Responsable del proceso	Proporcionar información técnica sobre las actividades que serán documentadas y validar que la descripción refleje la realidad operativa.
Colaboradores	Aplicar los procedimientos aprobados, utilizar la versión vigente y comunicar oportunidades de mejora o cambios necesarios.

Nota. Con base en la estructura organizacional y las responsabilidades definidas para la gestión documental y operativa de Stratos Asesores.

2.2 Alcance

Este procedimiento se aplica a la creación de todos los Procedimientos Normalizados de Trabajo del Sistema de Gestión de Riesgos de Stratos Asesores, incluyendo los documentos sobre identificación, análisis, evaluación, control, monitoreo, comunicación y revisión de riesgos. El procedimiento también puede servir como guía para elaborar instructivos, manuales, formatos y otros documentos internos que necesiten estar controlados y seguir una estructura uniforme. Se aplica en todas las áreas de Stratos Asesores que trabajen en actividades de gestión de riesgos, como el área de Riesgos, Precios de Transferencia, Administración y cualquier otra área que se agregue al Sistema de Gestión de Riesgos en el futuro.

3. Definiciones

Chief Executive Officer (CEO): Persona que ocupa el cargo ejecutivo más alto dentro de una organización y tiene la responsabilidad principal de dirigir, tomar decisiones estratégicas y supervisar el cumplimiento de los objetivos institucionales.

Documento controlado: Documento sujeto a identificación, revisión, aprobación, distribución, actualización y control de cambios, con el fin de asegurar que se utilice únicamente la versión vigente.

Formato: Plantilla definida para registrar información de una actividad. Una vez completado, el formato se convierte en un registro.

Instructivo de Trabajo (IT): Documento que describe de manera detallada cómo realizar una actividad específica o una tarea puntual.

Procedimiento: Documento que establece qué se debe hacer, quién debe hacerlo, cuándo debe realizarse, cómo debe ejecutarse y qué evidencia debe generarse.

Procedimiento Normalizado de Trabajo (PNT): Documento escrito y aprobado que describe de forma específica, secuencial y detallada las operaciones a realizar en una tarea determinada, incorporando criterios de seguridad, calidad, eficiencia y control de riesgos.

Registro: Evidencia documental que demuestra que una actividad fue realizada. Puede ser físico o digital.

Revisión: Actividad mediante la cual se verifica que un documento sea adecuado, suficiente, coherente y aplicable antes de su aprobación o actualización.

Sistema de Gestión de Riesgos (SGR): Conjunto de lineamientos, responsabilidades, actividades, herramientas y documentos utilizados para gestionar los riesgos de la organización.

Coordinadora Administrativa: Persona encargada de coordinar las actividades administrativas de la organización y apoyar en la gestión de recursos, documentos y procesos internos.

Gerencia de área: Persona o unidad responsable de dirigir, coordinar y supervisar las actividades de un área específica de la organización, asegurando el cumplimiento de sus funciones y objetivos.

Colaboradores: Personas que forman parte de la organización y participan en la ejecución de sus actividades, funciones o procesos, de acuerdo con sus responsabilidades asignadas.

Responsable del proceso: Persona encargada de gestionar, supervisar y asegurar la correcta ejecución de un proceso específico dentro de la organización, verificando que las actividades se realicen conforme a los procedimientos establecidos.

Política: Lineamiento formal definido por la organización que establece criterios generales de actuación, responsabilidades y orientaciones para guiar la toma de decisiones y el cumplimiento de los objetivos institucionales.

Versión vigente: Última versión aprobada de un documento, autorizada para su uso dentro de la organización.

4. Descripción

Crear Procedimientos Normalizados de Trabajo permite organizar documentalmente las actividades importantes de Stratos Asesores, especialmente las que forman parte del Sistema de Gestión de Riesgos. Cada procedimiento debe ser fácil de entender, práctico y acorde con la forma en que la organización realmente trabaja. Estos procedimientos no deben ser solo documentos que se guardan en una carpeta, sino herramientas útiles que guíen a los colaboradores en la ejecución de sus actividades, ayuden a evitar errores, dejen clara la responsabilidad de cada persona y faciliten el monitoreo de los riesgos.

4.1. Tipos de documentos aplicables

Dentro del Sistema de Gestión de Riesgos de Stratos Asesores, se podrán utilizar los siguientes tipos de documentos:

Tabla A 2

Documentación del Sistema de Gestión de Riesgos

Tipo de documento	Descripción	Ejemplo
Procedimiento General (PG)	Documento que describe actividades transversales del SGR.	Procedimiento para la elaboración de PNT.
Procedimiento de Gestión de Riesgos (GR)	Documento que describe actividades específicas para gestionar riesgos.	Procedimiento para identificación y evaluación de riesgos.
Procedimiento Normalizado de Trabajo (PNT)	Documento que describe tareas rutinarias, operativas o técnicas que requieren ejecución uniforme.	PNT para protección de información de clientes.
Instructivo de Trabajo (IT)	Documento que explica de forma más detallada cómo ejecutar una tarea específica.	Instructivo para actualizar la matriz de riesgos.

Política (PO)	Documento que establece lineamientos generales para orientar la actuación de la organización.	Política de Privacidad de Datos
Formato (FT)	Plantilla que se utiliza para registrar información.	Formato de registro de riesgos.
Registro	Evidencia de una actividad ejecutada.	Matriz de riesgos completada y aprobada.

Nota. Se presentan los tipos de documentos que conforman la estructura documental del Sistema de Gestión de Riesgos, su descripción y ejemplos de aplicación en la organización.

4.2 Apartados de los Procedimientos Normalizados de Trabajo

Cada Procedimiento Normalizado de Trabajo que se elabore en Stratos Asesores debe incluir obligatoriamente los siguientes apartados, con el propósito de garantizar uniformidad, claridad y trazabilidad en la documentación:

Objetivo: Describir de manera simple y concisa el propósito del procedimiento. En este apartado se debe dejar claro cuál es la razón de existencia del procedimiento, es decir, qué se busca lograr con su aplicación.

Responsabilidad de aplicación y alcance: Especificar quién es responsable de ejecutar, validar, autorizar y seguir este procedimiento. También debe precisar en qué áreas, procesos, actividades o grupos de personas se aplica el procedimiento.

Definiciones: Explicar los términos, abreviaturas y conceptos importantes que se usan en el procedimiento para que cualquier persona lo pueda entender. Cuando se usen siglas, la primera vez que aparezcan deben escribirse completas.

Descripción: Explicar paso a paso cómo se ejecuta el procedimiento. Esta sección debe ser fácil de entender, estar bien organizada y ser práctica. Se pueden usar tablas, diagramas, flujogramas o listas numeradas para hacerlo más claro.

Registros: Listar todos los documentos o evidencias que se generan al aplicar el procedimiento. Si el procedimiento no produce registros, se debe escribir "No aplica".

Control de copias y registro de lectura: Documentar que el procedimiento fue comunicado al personal que lo necesita y que todos conocen cuál es la versión actual que deben usar.

Anexos: Incluir documentos adicionales necesarios para aplicar el procedimiento, como formatos para llenar, tablas de referencia, diagramas, instructivos paso a paso o cualquier otro material de apoyo.

Para facilitar la comprensión de las actividades y garantizar que todos los colaboradores entiendan correctamente el procedimiento, se recomienda utilizar la siguiente estructura en la sección de descripción del procedimiento:

Tabla A 3

Actividades para la elaboración, revisión, aprobación y publicación de procedimientos

N°	Actividad	Responsable	Descripción	Registro
1	Identificar la necesidad del procedimiento	Responsable del proceso	Determinar la actividad que requiere ser documentada.	Solicitud, correo o acta de reunión.
2	Elaborar el borrador	Coordinadora Administrativa	Redactar el procedimiento conforme a esta metodología.	Borrador del PNT.

3	Revisar el contenido	Gerencia de Área	Validar que el contenido sea aplicable y coherente.	Comentarios o versión revisada.
4	Aprobar el documento	CEO	Autorizar el uso del procedimiento.	Firma o aprobación formal.
5	Comunicar y publicar	Coordinadora Administrativa	Difundir el procedimiento aprobado.	Registro de comunicación o lectura.

Nota. La tabla describe las actividades, responsables, registros y controles requeridos para la gestión de procedimientos dentro del Sistema de Gestión de Riesgos.

4.3 Redacción de los procedimientos

Los Procedimientos Normalizados de Trabajo de Stratos Asesores deben elaborarse considerando los siguientes criterios:

Lenguaje claro y accesible: Utilizar un lenguaje sencillo y directo, evitando frases ambiguas o términos muy técnicos sin explicación.

Orden lógico y secuencial: Redactar las actividades en el mismo orden en que se ejecutan, de forma que sea fácil de seguir de inicio a fin.

Verbos de acción: Usar verbos precisos que describan qué se debe hacer, como: identificar, revisar, aprobar, registrar, actualizar, comunicar o archivar.

Estructura uniforme: Mantener el mismo formato y estructura en todos los procedimientos para facilitar su comprensión y uso.

Definición de siglas: Escribir completamente las siglas la primera vez que se utilizan. Ejemplo: Sistema de Gestión de Riesgos (SGR).

Información pertinente: Incluir solo la información necesaria y útil para aplicar el procedimiento, eliminando datos innecesarios.

Consistencia con otros documentos: Asegurar que el procedimiento no contradiga otros documentos del Sistema de Gestión de Riesgos.

Definición de responsables y evidencias: Especificar claramente quién es responsable de cada actividad y qué registros se generan.

Uso de "No aplica": Escribir "No aplica" en apartados que no correspondan, en lugar de eliminarlos, para mantener la estructura uniforme.

4.4 Codificación de documentos

Para asegurar la identificación clara y la trazabilidad de todos los Procedimientos Normalizados de Trabajo, es fundamental utilizar un sistema de codificación alfanumérica que permita identificar de forma única cada documento. Este sistema facilita la organización, el archivo, la búsqueda y el control de versiones de los procedimientos. La estructura de codificación propuesta será la siguiente:

STR-SGR-[TIPO]-[NÚMERO]-[VERSIÓN]

Tabla A 4

Elementos de la codificación documental

Elemento	Significado
STR	Stratos Asesores S.A.S.
SGR	Sistema de Gestión de Riesgos.
TIPO	Tipo de documento: PG, GR, PNT, IT o FT.
NÚMERO	Número consecutivo de tres dígitos.

VERSIÓN	Número de versión del documento.

Nota. La tabla detalla la estructura de codificación establecida para identificar y controlar los documentos del Sistema de Gestión de Riesgos mediante códigos normalizados.

A continuación, se presenta una tabla referencial con ejemplos de codificación documental que podrán utilizarse para identificar los procedimientos generados dentro del Sistema de Gestión de Riesgos (SGR) de Stratos Asesores S.A.S. Esta codificación permite diferenciar el tipo de documento, su número consecutivo y la versión correspondiente.

Tabla A 5

Codificación de documentos del Sistema de Gestión de Riesgos

Código	Significado
STR-SGR-PG-001-01	Primer Procedimiento General del SGR, versión 01.
STR-SGR-GR-002-01	Segundo Procedimiento de Gestión de Riesgos, versión 01.
STR-SGR-PNT-003-01	Tercer Procedimiento Normalizado de Trabajo del SGR, versión 01.
STR-SGR-IT-004-01	Cuarto Instructivo de Trabajo del SGR, versión 01.
STR-SGR-FT-005-01	Quinto Formato del SGR, versión 01.

4.5 Elaboración, revisión y aprobación

La elaboración de un PNT deberá seguir las siguientes etapas:

4.5.1 Identificación de la necesidad documental

La necesidad de elaborar un PNT podrá originarse por:

- Diseño o implementación del SGR.
- Identificación de riesgos que requieren controles documentados.
- Cambios en procesos internos.
- Recomendaciones de auditorías, revisiones o evaluaciones.
- Necesidad de estandarizar una actividad repetitiva.
- Cambios normativos, tecnológicos u organizacionales.
- Requerimientos de Socios, Gerencias o responsables de proceso.

4.5.2 Elaboración del borrador

La Coordinadora Administrativa, con apoyo del responsable del proceso, elaborará el borrador del procedimiento utilizando la estructura definida en este documento.

El borrador deberá describir las actividades reales de la organización y no actividades ideales que no puedan aplicarse en la práctica.

4.5.3 Revisión técnica

La Gerencia del área correspondiente revisará el contenido del PNT para verificar que:

- El procedimiento sea coherente con las actividades reales.
- Las responsabilidades estén correctamente asignadas.
- Las actividades sean comprensibles y aplicables.
- Los registros definidos sean adecuados.
- El documento no contradiga otros lineamientos del SGR.

4.5.4 Aprobación

Una vez revisado, el procedimiento será enviado al CEO para su aprobación.

La aprobación podrá realizarse mediante firma física, firma digital, correo electrónico formal o cualquier otro mecanismo definido por la organización.

Ningún PNT deberá considerarse vigente si no cuenta con aprobación formal.

4.6 Distribución, comunicación y publicación

Una vez aprobado, el PNT deberá ser comunicado al personal correspondiente. La comunicación podrá realizarse mediante:

- Correo electrónico institucional.
- Reunión interna.
- Carpeta compartida en OneDrive.
- Repositorio documental definido por la organización.
- Capacitación o inducción interna, cuando sea necesario.

La Coordinadora Administrativa deberá asegurar que el personal utilice únicamente la versión vigente del procedimiento.

Cuando el procedimiento sea aplicable a toda la organización, deberá comunicarse a todos los colaboradores. Cuando sea aplicable únicamente a un área o proceso, se comunicará al personal directamente involucrado.

4.7 Revisión y control de cambios

Los PNT deberán revisarse al menos una vez al año o cuando ocurra cualquiera de las siguientes situaciones:

- Cambios en la estructura organizacional.
- Cambios en procesos, actividades o responsabilidades.
- Identificación de nuevos riesgos o modificación de riesgos existentes.
- Resultados de auditorías, revisiones internas o incidentes.
- Cambios en herramientas tecnológicas utilizadas por la organización.
- Cambios normativos o contractuales aplicables.
- Observaciones realizadas por colaboradores, Gerencias o CEO.

Toda actualización deberá registrarse en el control de cambios del documento, indicando la versión, fecha, descripción del cambio, motivo y responsable.

Tabla A 6

Clasificación de cambios y control de versiones de los documentos

Tipo de cambio	Ejemplo	Acción sobre versión
Cambio menor	Corrección de redacción o formato sin afectar el contenido.	Puede mantenerse la versión o actualizarse.
Cambio relevante	Modificación de actividades, responsables, registros o controles.	Se debe generar una nueva versión.
Cambio crítico	Cambio que afecta la aplicación del procedimiento o el control de riesgos.	Se debe generar una nueva versión y comunicar formalmente al personal.

4.8 Control de documentos obsoletos

Cuando se apruebe una nueva versión de un PNT, la versión anterior deberá ser retirada de los puntos de uso o marcada como “Documento obsoleto”.

La Coordinadora Administrativa deberá conservar una copia histórica de las versiones anteriores, cuando sea necesario, para fines de trazabilidad, auditoría o consulta.

No se deberá utilizar un documento obsoleto para ejecutar actividades vigentes dentro del SGR.

5. Registros

Los registros derivados de este procedimiento son los siguientes:

Tabla A 7

Registros derivados

Código	Nombre del Registro	Responsable de archivo	Medio de conservación
STR-SGR-FT-001-01	Lista maestra de documentos del SGR	Coordinadora Administrativa	Digital
STR-SGR-FT-002-01	Registro de elaboración, revisión y aprobación	Coordinadora Administrativa	Digital o físico
STR-SGR-FT-003-01	Registro de comunicación y lectura de procedimientos	Coordinadora Administrativa	Digital o físico
STR-SGR-FT-004-01	Control de cambios documentales	Coordinadora Administrativa	Digital

Los registros deberán mantenerse disponibles para evidenciar la adecuada gestión documental del SGR.

6. Control de Copias y Registro de Lectura del Procedimiento

Esta sección permite evidenciar que el procedimiento fue distribuido o comunicado a las personas correspondientes.

Tabla A 8

Registro de comunicación y socialización de procedimientos

N°	Nombre del colaborador	Área	Medio de comunicación	Firma	Fecha
1					
2					
3					
4					

La confirmación podrá realizarse mediante firma física, correo electrónico, confirmación digital o registro de asistencia a una reunión de socialización.

Anexos

Anexo B

Control de revisión

Código del documento	Versión	Descripción del cambio	Motivo del cambio	Responsable	Fecha de aprobación
STR-SGR-PG-001-01	01	Emisión inicial del procedimiento.	Diseño del Sistema de Gestión de Riesgos de Stratos Asesores S.A.S.	Gerencia de Área	Mayo 2026

Anexo C

Lista maestra de documentos del SGR

Código	Nombre del documento	Tipo	Versión	Fecha de aprobación	Responsable	Estado
STR-SGR-PG-001-01	Procedimiento para la elaboración de Procedimientos Normalizados de Trabajo	PG	01	Mayo 2026	Gerencia de Área	Propuesto

Anexo D

Modelo de gestión de no conformidad

Tabla B 1

Estructura de la plantilla para el registro, análisis y control de no conformidades en Stratos Asesores S.A.S.

1. Datos generales

Organización	Stratos Asesores S.A.S.
Sistema	Sistema de Gestión de Riesgos basado en ISO 31000:2018
Código de no conformidad	[NC-STR-00X]
Fecha de detección	[dd/mm/aaaa]
Tipo de auditoría	[Interna / Documental / En sitio / Mixta]
Auditor designado	[Nombre y cargo]
Área auditada	[Riesgos / Precios de Transferencia / Administración]
Responsable del área auditada	[Nombre y cargo]

2. Registro de la no conformidad

Proceso revisado	[Indicar el proceso donde se detectó la no conformidad]
Criterio de referencia	[ISO 31000:2018, matriz de riesgos, procedimiento interno, control definido, requisito legal aplicable u otro criterio usado en la auditoría]
Descripción de la no conformidad	[Describir el incumplimiento detectado, indicando qué ocurrió, dónde se identificó y qué evidencia lo respalda]
Evidencia objetiva	[Documento, registro, correo, informe, carpeta, acta, captura, permiso de acceso u otra evidencia revisada]

Clasificación	[No conformidad mayor / No conformidad menor / Observación]
Impacto o riesgo asociado	[Indicar el posible efecto sobre el SGR, la confidencialidad, la continuidad del servicio, el cumplimiento contractual, la calidad del informe o la reputación de Stratos]

3. Identificación de la causa raíz

Causa raíz identificada	[Explicar la causa que originó la no conformidad]
Método utilizado para el análisis	[Revisión documental / consulta al responsable / análisis de los 5 porqués / entrevista / otro]
Responsable involucrado	[Nombre, cargo o área relacionada con la causa identificada]

4. Acciones correctivas

Acción correctiva definida	[Indicar la acción que se aplicará para corregir la no conformidad y evitar que vuelva a presentarse]
Acción preventiva, si aplica	[Indicar una acción adicional para evitar situaciones similares en otros procesos o áreas]
Responsable de ejecución	[Nombre, cargo o área responsable]
Fecha prevista de inicio	[dd/mm/aaaa]
Fecha prevista de finalización	[dd/mm/aaaa]
Evidencia esperada	[Documento, registro, informe, correo, acta, actualización de procedimiento, respaldo, capacitación u otra evidencia]
Estado de la acción	[Abierta / En proceso / Cerrada / Reprogramada]

5. Verificación de la eficacia

Responsable de la verificación	[Nombre y cargo]
Fecha prevista de verificación	[dd/mm/aaaa]
Método de verificación	[Revisión documental / consulta al responsable / revisión de permisos / auditoría de seguimiento / revisión de indicadores / otro]
Evidencias revisadas	[Indicar las evidencias revisadas para confirmar el cumplimiento de la acción]
Resultado de la verificación	[Eficaz / No eficaz / Requiere nueva acción]
Fecha de cierre	[dd/mm/aaaa]
Estado de la no conformidad	[Abierta / En seguimiento / Cerrada]
Observaciones finales	[Registrar comentarios sobre el cierre, nueva acción requerida o recomendaciones adicionales]

6. Firmas de validación

Responsable	Nombre y cargo	Firma	Fecha
Auditado	[Nombre y cargo]	[Firma]	[dd/mm/aaaa]
Auditor designado	[Nombre y cargo]	[Firma]	[dd/mm/aaaa]
Responsable de verificación	[Nombre y cargo]	[Firma]	[dd/mm/aaaa]

Stratos Asesores. (s.f.). *Logo de la organización Stratos Asesores S.A.S.*

[Logotipo].https://www.stratosasesores.com/

file:///C:/Users/HP/Downloads/Listado%20personal%20Activo%20Stratos%20Asesores.pdf

Teléfono: 09 83964548
Correo electrónico: administracion@stratos.ec
obravo@stratos.ec
Dirección: Av. 12 de Octubre y Coruña, Edif. Urban Plaza, Piso 12, Quito, Ecuador.

Google. (s. f.). *Choose your Safe Browsing protection level in Chrome*. Google Help.

Microsoft. (2025, abril 15). *Introducción a SmartScreen de Microsoft Defender*. Microsoft Learn.

Stratos Asesores S.A.S. (s. f.). Contratos y acuerdos de confidencialidad (NDA) [Documento interno no publicado].

Stratos Global Transfer Pricing S.A.S. (2025, 3 de marzo). Manual de Políticas de Seguridad de la Información (Versión 01) [Documento interno no publicado].

Stratos Global Transfer Pricing S.A.S. (2025, 3 de marzo). Manual de Políticas de Seguridad de la Información (Versión 01) [Documento interno no publicado].

Atlassian. (s. f.). Tabla RACI: qué es y cómo usarla. The Workstream. https://www.atlassian.com/es/work-management/project-management/raci-chart