Maestría en

Gestión de Riesgos

Trabajo de investigación previo a la obtención del título de

Magíster en Gestión de Riesgos

AUTORES:

Bedoya Enríquez Carol Michelle

Beltrán Álvarez Armando Sebastián

Flores Quinaucho Juan Carlos

González Tomalá Alfredo Bernardo

Moya Sánchez Christian José

Pérez Espinoza Daniel Alejandro

Sarmiento Barreno Carla Daniela

TUTORES:

Paloma Manzano Martínez

David Genaro Benavidez Gutiérrez

Enrique Molina Suárez

PROPUESTA DE ELABORACIÓN DEL SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO BASADO EN LA NORMA ISO 31000:2018, PARA LA EMPRESA GRUPO BRAVCO S.A.

Quito, julio 2025

Certificación de autoría

Nosotros, **Bedoya Enríquez Carol Michelle, Beltrán Álvarez Armando Sebastián, Flores Quinaucho Juan Carlos, González Tomalá Alfredo Bernardo, Moya Sánchez Christian José, Pérez Espinoza Daniel Alejandro y Sarmiento Barreno Carla Daniela;** 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.

Firmado electrónicamente por:
CAROL MICHELLE BEDOYA ENRIQUEZ
Validar únicamente con FirmaEC

Firma del graduando
Bedoya Enríquez Carol Michelle

Firmado electrónicamente por:
ARMANDO SEBASTIAN BELTRAN ALVAREZ
Validar únicamente con FirmaEC

Firma del graduando
Beltrán Álvarez Armando Sebastián

Firmado electrónicamente por:
JUAN CARLOS FLORES QUINAUCHO
Validar únicamente con FirmaEC

Firma del graduando
Flores Quinaucho Juan Carlos

Firmado electrónicamente por:
ALFREDO BERNARDO GONZALEZ TOMALA
Validar únicamente con FirmaEC

Firma del graduando
González Tomalá Alfredo Bernardo

CHRISTIAN JOSE MOYA SANCHEZ
Firmado digitalmente por CHRISTIAN JOSE MOYA SANCHEZ
Fecha: 2025.07.21 23:29:39 -05'00'

Firma del graduando
Moya Sánchez Christian José

Firmado electrónicamente por:
DANIEL ALEJANDRO PEREZ ESPINOZA
Validar únicamente con FirmaEC

Firma del graduando
Pérez Espinoza Daniel Alejandro

Firmado electrónicamente por:
CARLA DANIELA SARMIENTO BARRENO
Validar únicamente con FirmaEC

Firma del graduando
Sarmiento Barreno Carla Daniela

Autorización de Derechos de Propiedad Intelectual

Nosotros, **Bedoya Enríquez Carol Michelle, Beltrán Álvarez Armando Sebastián, Flores Quinaucho Juan Carlos, González Tomalá Alfredo Bernardo, Moya Sánchez Christian José, Pérez Espinoza Daniel Alejandro y Sarmiento Barreno Carla Daniela**, en calidad de autores del trabajo de investigación titulado ***PROPUESTA DE ELABORACIÓN DEL SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO BASADO EN LA NORMA ISO 31000:2018, PARA LA EMPRESA GRUPO BRAVCO S.A.***, 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, (julio 2025)

Firmado electrónicamente por:
CAROL MICHELLE BEDOYA ENRIQUEZ
Validar únicamente con FirmaEC

Firma del graduando
Bedoya Enríquez Carol Michelle

Firmado electrónicamente por:
ARMANDO SEBASTIAN BELTRAN ALVAREZ
Validar únicamente con FirmaEC

Firma del graduando
Beltrán Álvarez Armando Sebastián

Firmado electrónicamente por:
JUAN CARLOS FLORES QUINAUCHO
Validar únicamente con FirmaEC

Firma del graduando
Flores Quinaucho Juan Carlos

Firmado electrónicamente por:
ALFREDO BERNARDO GONZALEZ TOMALA
Validar únicamente con FirmaEC

Firma del graduando
González Tomalá Alfredo Bernardo

CHRISTIAN JOSE MOYA SANCHEZ
Firmado digitalmente por CHRISTIAN JOSE MOYA SANCHEZ
Fecha: 2025.07.21 23:27:54 -05'00'

Firma del graduando
Moya Sánchez Christian José

Firmado electrónicamente por:
DANIEL ALEJANDRO PEREZ ESPINOZA
Validar únicamente con FirmaEC

Firma del graduando
Pérez Espinoza Daniel Alejandro

Firmado electrónicamente por:
CARLA DANIELA SARMIENTO BARRENO
Validar únicamente con FirmaEC

Firma del graduando
Sarmiento Barreno Carla Daniela

Aprobación de dirección y coordinación del programa

Nosotros, Paloma Manzano y David Benavidez**,** declaramos que los graduandos: **Bedoya Enríquez Carol Michelle, Beltrán Álvarez Armando Sebastián, Flores Quinaucho Juan Carlos, González Tomalá Alfredo Bernardo, Moya Sánchez Christian José, Pérez Espinoza Daniel Alejandro y Sarmiento Barreno Carla Daniela** son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

MANZANO MARTINEZ PALOMA - 24244436K

Firmado digitalmente por MANZANO MARTINEZ PALOMA - 24244436K
Fecha: 2025.07.28 10:31:27 +02'00'

Paloma Manzano
Director de la Maestría en Gestión de Riesgos

Firmado electrónicamente por:
DAVID GENARO BENAVIDES GUTIERREZ
Validar únicamente con FirmaEC

David Benavidez
Coordinador de la Maestría en Gestión de Riesgos

DEDICATORIA

A mi familia, quienes han sido y seguirán siendo el pilar fundamental de mi vida.

Este trabajo es el fruto de un largo camino recorrido, un camino que no hubiera sido posible sin su presencia constante, su guía y su amor incondicional. Desde los primeros pasos en mi formación académica hasta la culminación de este proceso, he contado con su apoyo inquebrantable, con su fe inagotable en mis capacidades y con su paciencia ante los momentos de incertidumbre y cansancio.

A mis padres, por su ejemplo de esfuerzo, responsabilidad y perseverancia, por enseñarme el valor de la dedicación y el trabajo bien hecho. A mis hermanos, por su comprensión, su ánimo constante y su confianza en cada proyecto que emprendí.

Cada logro alcanzado es reflejo de la educación, los valores y el amor que siempre me han brindado. Esta tesis representa no solo un hito académico, sino también un homenaje a todo lo que ustedes, como familia, han sembrado en mí.

Les agradezco por ser quienes son y por acompañarme siempre, incluso en los momentos en los que el camino parecía incierto. Sin ustedes, este sueño no habría sido posible.

Carol Bedoya

A mi madre, mi padre y mi hermano, quienes, con su apoyo incondicional, han guiado mi camino y, con amor, me han demostrado que los propósitos y los sueños son posibles cuando se actúa con respeto, compromiso y disciplina.

A mi abuelita “Panchita”, que siempre ha estado ahí para recordarme el valor de la humildad y la persistencia.

Esta tesis es también para todos aquellos que me han acompañado en este breve pero significativo proceso llamado vida.

¡A todos, gracias!

Sebastián Beltrán

Este proyecto lo dedico a mi amada hija Leticia, fuente de inspiración y motor de cada uno de mis esfuerzos, a mi esposa Amanda, por su apoyo incondicional, paciencia y amor a lo largo de este camino, a mis padres, Juan y Angelita, quienes me inculcaron los valores del trabajo, la

perseverancia y la educación como pilares de vida, a mis hermanos, Fabián, Santiago y Byron, por su constante respaldo y a toda mi familia que han sido parte fundamental para alcanzar esta meta. Este logro es también suyo.

Con gratitud y profundo amor.

Juan Carlos Flores

A ti, Sophia, amada hija cuya existencia ilumina mis días y a la que dedico todos mis sueños y anhelos.
A Maryuri, esposa amada, compañera de vida incansable, por tu amor que sostiene, por tu fe que alienta, y por ser quien me impulso a iniciar esta maestría.

A mi familia, mi refugio, quienes con amor y confianza han edificado las alas que hoy me permiten alcanzar nuevas metas.

Y a esos seres tan queridos que ahora habitan en los cielos como: mi padre, mi abuelo, y mi abuela. Ellos cuyos silencios siempre me guían, junto a sus bendiciones las cuales siempre me acompañan en cada paso.

Este logro inigualable lleva sus nombres grabados en el corazón, porque su amor eterno vive en mí.

Alfredo González

Este trabajo lo dedico a Dios por las bendiciones recibidas a María Teresa mi esposa y dos hijas Nazly y Zoe, por ser mi inspiración diaria, por su amor, la paciencia en los momentos más exigentes y por darme motivos para seguir adelante.

Este logro es el reflejo de nuestro caminar en familia, ya que, sin su gran ayuda, simplemente no habría sido posible.

Christian Moya

A Dios, por permitirme vivir esta nueva etapa; por darme la salud, la sabiduría, la gracia y la fuerza para levantarme cada día y disfrutar de los maravillosos planes que tiene preparados para mí.

A mis padres, por ser mi apoyo incondicional en cada proyecto que emprendo; por educarme e inculcarme principios que desde pequeño han sido la base de mi vida. Gracias por brindarme sus recursos, su tiempo, su infinito amor. Este logro también es de ustedes.

A mi hermano, por ser mi ejemplo a seguir. Tus ganas de verme triunfar y alcanzar grandes metas han sido una de mis mayores motivaciones para seguir adelante y no rendirme.

Finalmente, a mis amigos. Gracias, porque a pesar de la distancia, siempre se mantuvieron atentos a mí, y por ello los llevo en mi corazón. Estoy seguro de que celebrarán este logro como propio, de la misma manera en que yo celebraré los suyos.

Daniel Pérez

A mi pequeña Luciana, quien me motiva a seguir adelante, a ser fuerte, a crecer en todos los aspectos de mi vida, en honor a esas horas que no pudimos compartir juntas mientras duró este proceso.

A mi madre, porque sin su ayuda no habría sido posible alcanzar esta meta, gracias por cubrirme, por cuidar de mi hija con amor durante todo este tiempo, por tu bondad, tu paciencia y tu esencia, simplemente por ser como eres, ¡perfecta!…

A Alex por abrirme espacios en donde encontré oportunidades a través de las cuales he podido materializar este sueño, por motivarme, apoyarme, acompañarme y por arreglar los pedazos rotos en mi vida.

A ustedes tres, con todo mi amor, gratitud, admiración y respeto.

Daniela Sarmiento

AGRADECIMIENTOS

Expresamos nuestro sincero agradecimiento a la empresa Grupo BRAVCO S.A. por las facilidades brindadas durante el desarrollo de este trabajo de titulación. Su apertura, disposición y la confianza depositada en nosotros, así como la entrega de información clave, fueron fundamentales para la elaboración de la propuesta del Sistema de Gestión de Continuidad del Negocio, permitiéndonos trabajar sobre una base real y aplicable.

Extendemos también nuestro agradecimiento a los docentes de la Universidad Internacional del Ecuador, cuyas enseñanzas, guía académica y constante apoyo han sido el pilar que sustentó el desarrollo de este proyecto. Su compromiso con nuestra formación profesional ha sido invaluable.

Finalmente, agradecemos de manera especial a cada uno de los compañeros que integraron este grupo de trabajo. Su esfuerzo, conocimientos y colaboración activa hicieron posible que este proyecto se concrete con éxito. Este logro es el resultado del compromiso y trabajo en equipo.

RESUMEN

El presente proyecto de titulación desarrolla la *Propuesta de Elaboración del Sistema de Gestión de Continuidad del Negocio basado en la norma ISO 31000:2018 para la empresa GRUPO BRAVCO S.A.*, con el objetivo de fortalecer su capacidad de respuesta ante eventos disruptivos. El enfoque metodológico se basa en los principios y lineamientos de la norma ISO 31000:2018, permitiendo a la organización anticipar, enfrentar y recuperarse de incidentes que puedan comprometer la operación de servicios críticos como conectividad, infraestructura, ciberseguridad, entornos cloud y servicios gestionados. Esta propuesta surge como respuesta a la necesidad de adaptarse a un entorno tecnológico cada vez más expuesto a amenazas internas y externas, desde ciberataques hasta fallas operativas y desastres naturales que ponen en riesgo la continuidad y sostenibilidad organizacional. Para ello, se realizó un diagnóstico integral de riesgos mediante análisis FODA, mapas de calor, matrices de impacto/probabilidad y caracterización de procesos claves, lo que permitió estructurar una propuesta metodológica articulada en torno a principios de gestión, marco de gobernanza, evaluación y tratamiento de riesgos, y estrategias de recuperación. El Sistema de Gestión de Continuidad del Negocio (SGCN) propuesto integra la gestión de riesgos con la continuidad operativa en todos los niveles, estableciendo protocolos de respuesta, cronogramas de implementación, mecanismos de documentación, seguimiento y mejora continua. Su adopción garantiza no solo la continuidad de los procesos o servicios críticos sino también el cumplimiento normativo, fortaleciendo la confianza de clientes, autoridades reguladoras y partes interesadas. En definitiva, este proyecto contribuye al fortalecimiento de la resiliencia institucional y mejora la capacidad de adaptación de GRUPO BRAVCO S.A. frente a situaciones de crisis, alineándose con buenas prácticas internacionales y posicionando la gestión del riesgo como un componente estratégico del desarrollo empresarial sostenible y competitivo.

Palabras clave: Continuidad del negocio, gestión de riesgos, ISO 31000:2018, resiliencia operativa, seguridad tecnológica, SGCN, GRUPO BRAVCO S.A.

ABSTRACT

This graduation project develops a Proposal for the Implementation of a Business Continuity Management System (BCMS) based on the ISO 31000:2018 standard for the company GRUPO BRAVCO S.A., with the aim of strengthening its response capacity in the face of disruptive events. The methodological approach is grounded in the principles and guidelines of ISO 31000:2018, allowing the organization to anticipate, respond to, and recover from incidents that may compromise the operation of critical services such as connectivity, infrastructure, cybersecurity, cloud environments, and managed services. This proposal arises from the need to adapt to a technological environment increasingly exposed to internal and external threats from cyberattacks to operational failures and natural disasters which jeopardize business continuity and organizational sustainability. A comprehensive risk diagnosis was conducted using tools such as SWOT analysis, heat maps, impact/probability matrices, and the characterization of key processes. This enabled the structuring of a methodological proposal articulated around risk management principles, governance framework, risk assessment and treatment, and recovery strategies. The proposed BCMS integrates risk management with operational continuity at all organizational levels, establishing response protocols, implementation schedules, documentation mechanisms, and continuous monitoring and improvement processes. Its adoption ensures not only the continuity of critical processes and services, but also regulatory compliance, thereby strengthening the trust of clients, regulatory authorities, and stakeholders. Ultimately, this project contributes to enhancing institutional resilience and improving GRUPO BRAVCO S.A.'s capacity to adapt to crisis situations, aligning with international best practices and positioning risk management as a strategic component of sustainable and competitive business development.

***Keywords*:** Business continuity, risk management, ISO 31000:2018, operational resilience, technological security, BCMS, GRUPO BRAVCO S.A.

TABLA DE CONTENIDOS (Índice)

LISTA DE TABLAS (Índice de tablas)

LISTA DE FIGURAS (Índice de figuras)

Capítulo 1: Introducción

En un ambiente corporativo marcado por la interdependencia tecnológica creciente y la vulnerabilidad a riesgos operativos, tecnológicos y externos, la continuidad del negocio se ha transformado en un elemento estratégico esencial para asegurar la sostenibilidad y competitividad de las entidades. GRUPO BRAVCO S.A., conocida por su marca TEUNO, una compañía líder en soluciones tecnológicas integrales en Ecuador, se encuentra ante el reto de potenciar su resistencia operativa ante eventuales interrupciones que puedan poner en riesgo sus procesos clave. Este trabajo de grado, llevado a cabo dentro de la Maestría en Gestión de Riesgos de la Universidad Internacional del Ecuador, sugiere la creación de un Sistema de Gestión de Continuidad del Negocio fundamentado en los principios y pautas de la norma ISO 31000:2018.

El proyecto tiene como objetivo potenciar la habilidad de la organización para prever sucesos inesperados, reducir los efectos y asegurar la disponibilidad de sus servicios en áreas fundamentales como la conectividad, la infraestructura, la ciberseguridad y el cloud. El establecimiento de este sistema no solo satisface la exigencia de salvaguardar los activos esenciales de la compañía, sino que también fortalece su dedicación a la excelencia en las operaciones, el acatamiento de las regulaciones y la confianza de sus clientes, proveedores y otros posibles interesados.

1. Planteamiento Del Problema E Importancia Del Estudio

1.1. Definición Del Proyecto

El presente proyecto de titulación de la Maestría en Gestión de Riesgos tiene como objetivo elaborar una propuesta de Sistema de Gestión de Continuidad del Negocio (SGCN) para

la empresa TEUNO, aplicando los principios y directrices de la norma ISO 31000:2018, misma que se dedica a brindar soluciones tecnológicas: conectividad y networking, infraestructura, seguridad de la información, ciberseguridad, cloud, consultoría y servicios gestionados.

Dado el contexto actual de creciente incertidumbre, amenazas tecnológicas, operativas y externas, resulta prioritario que las organizaciones adopten enfoques estructurados que les permitan anticiparse a imprevistos y garantizar la continuidad de sus operaciones críticas. Este proyecto propone una solución integral, alineada a los estándares internacionales de gestión de riesgos, que permitirá fortalecer la resiliencia operativa de GRUPO BRAVCO S.A., mejorar su capacidad de respuesta y minimizar el impacto de posibles interrupciones.

1.2. Naturaleza Del Proyecto

Considerando lo descrito en párrafos anteriores, el proyecto que mejor se adapta a nuestro estudio es el de diseño.

1.3. Objetivos

1.3.1. Objetivo General. Desarrollar una propuesta que permita la implementación de un Sistema de Gestión de Continuidad del Negocio (SGCN), aplicando los lineamientos de la norma ISO 31000:2018, con el propósito de fortalecer la capacidad de GRUPO BRAVCO S.A. para identificar, evaluar y gestionar los riesgos que puedan afectar la continuidad de sus operaciones.

1.3.2. Objetivos Específicos. Identificar los procesos críticos de GRUPO BRAVCO S.A. y las amenazas que podrían interrumpir su funcionamiento.

Evaluar los riesgos asociados a los procesos críticos.

Establecer estrategias de gestión de riesgos orientadas a la continuidad, incluyendo medidas de prevención, mitigación, respuesta y recuperación.

Proponer un sistema documentado y estructurado que permita a la organización adoptar un enfoque sistemático para gestionar los riesgos de los procesos críticos de la continuidad del negocio.

1.4. Justificación E Importancia Del Trabajo De Investigación

La continuidad del negocio es un componente esencial para la sostenibilidad de las organizaciones, especialmente en el sector tecnológico, donde la disponibilidad de servicios es crítica. TEUNO, como empresa especializada en soluciones tecnológicas, requiere estar preparada para afrontar eventos imprevistos que puedan afectar sus operaciones, su reputación y las relaciones con sus clientes.

Pese a que hay normas concretas como la ISO 22301 para la administración de la continuidad empresarial, la norma ISO 31000:2018 proporciona una perspectiva más extensa y estratégica para la administración del riesgo, facilitando la integración de individuos, procesos y tecnología en un marco versátil que se ajusta a las demandas específicas de la entidad. Esta norma no es certificable, sin embargo, su aplicación evidencia una administración proactiva ante la duda.

La instauración de un sistema estructurado para la administración de la continuidad del negocio, fundamentado en la norma ISO 31000, facilitará a la compañía la toma de decisiones basadas en información, prever posibles interrupciones y potenciar su capacidad de reacción. Adicionalmente, fortalece la fe de los inversores, clientes y otros interesados en la habilidad de la organización para seguir funcionando en circunstancias adversas.

Como ejemplo, compañías como Tubacex han implementado la ISO 31000: 2018 como esquema de administración del riesgo. Esta compañía de producción industrial, experta en la producción de tubos de acero inoxidable, resalta que su enfoque fundamentado en esta normativa ha potenciado su habilidad para prever retos y proporcionar soluciones vanguardistas. como lo señalan en su sitio web oficial, tal como lo especifican en su sitio web oficial.

https://www.tubacex.com/en/tubacex-successfully-completes-first-follow-up-audit-for-iso-310002018-certification/

Esto demuestra que un enfoque estructurado y alineado con estándares internacionales puede aplicarse con éxito en distintos sectores, incluyendo el tecnológico.

Capítulo 2: La Organización

2. Perfil De La Organización

2.1. Nombre De La Empresa

La empresa en la cual se desarrolla este proyecto es GRUPO BRAVCO S.A., sociedad anónima ecuatoriana con número de RUC 1790506428001, legalmente constituida el 27 de julio de 1981 y actualmente en estado activo, bajo el régimen general de contribución tributaria. Su domicilio fiscal está ubicado en la ciudad de Quito, en la dirección: José María Ayora N39-162 y Vicente Cárdenas, parroquia Iñaquito, provincia de Pichincha.

La compañía está oficialmente registrada como Contribuyente Especial, cuenta con respaldo y reconocimiento oficial por parte de organismos de control y supervisión estatales, lo cual valida su confiabilidad y cumplimiento normativo en la provisión de servicios estratégicos

Ha sido autorizada por la Superintendencia de Bancos como entidad prestadora de Servicios Auxiliares del Sistema Financiero, permitiéndole operar con instituciones del sector bajo marcos de seguridad y continuidad.

Adicionalmente, la empresa cuenta con resolución de calificación por parte de la Superintendencia de Economía Popular y Solidaria (SEPS), lo que le permite brindar servicios especializados a cooperativas, mutualistas y otras entidades del sector financiero popular y solidario, garantizando cumplimiento técnico y regulatorio.

Su sitio web oficial es: www.teuno.com

Este conjunto de habilitaciones legales y técnicas refuerza la solidez institucional de GRUPO BRAVCO S.A. y su posicionamiento como un actor clave en la transformación tecnológica del país.

2.2. Filosofía Organizacional

Misión: Servir a nuestros clientes para apoyar el logro de sus objetivos de negocio, brindándoles asesoramiento y soluciones tecnológicas de calidad, con un equipo humano altamente calificado y comprometido.

Visión: Ser el proveedor referente de soluciones tecnológicas para el sector corporativo del país.

Valores Institucionales: Los valores corporativos de Teuno representan los principios rectores de su cultura organizacional, orientando la conducta del personal y fortaleciendo el compromiso con la excelencia:

- Coherencia: Actuamos con principios de honestidad y transparencia con clientes, empleados, proveedores y accionistas, responsabilizándonos por los compromisos asumidos.
- Esfuerzo: Buscamos la excelencia en todo lo que hacemos, estableciendo metas desafiantes que nos exigen salir de la zona de confort.
- Responsabilidad: Cumplimos con nuestras obligaciones y asumimos las consecuencias de nuestras acciones, promoviendo la ética en todas las áreas de la organización.
- Trascender: Impulsamos la sostenibilidad, el legado y el impacto positivo en

colaboradores, clientes y la comunidad en general.

2.3. Portafolio Comercial

2.3.1. Actividades. GRUPO BRAVCO S.A., bajo su marca comercial TEUNO, desarrolla actividades estratégicas en el sector tecnológico ecuatoriano, enfocadas en ofrecer soluciones integrales de conectividad, infraestructura, seguridad de la información y servicios cloud, tanto a entidades del sector corporativo como a organizaciones financieras bajo regulación.

Las principales actividades económicas registradas ante el Servicio de Rentas Internas (SRI) incluyen:

- Instalación de redes de telecomunicaciones, líneas de fibra óptica y cableado estructurado.
- Venta al por mayor de computadores, teléfonos y equipos de comunicación.
- Provisión de servicios de conectividad (voz, datos, internet) utilizando infraestructura propia.
- Servicios de operación, mantenimiento y soporte de plataformas tecnológicas.
- Consultoría en sistemas informáticos, ciberseguridad y transformación digital.

2.3.2. Marca comercial. La empresa opera comercialmente bajo la marca TEUNO, que simboliza su propuesta de valor tecnológica y bajo esta misma denominación ha desarrollado soluciones específicas como:

- **TEUNO VDI**: Escritorios virtuales seguros y escalables.
- **TEUNO CyberGuard**: Protección avanzada contra amenazas cibernéticas.

- **TEUNO DOC**: Digital Operation Center para gestión integral de incidentes y plataformas.

Figura 1

Logo TEUNO

Tomado de (*TEUNO,* 2024)

2.3.3. Productos y servicios.

2.3.3.1. Conectividad Y Networking.

- **Gestión Integral de Enlaces:** Monitoreo y administración continua de los enlaces de conectividad, optimizando el tráfico de red y garantizando redundancia, estabilidad y eficiencia en la transmisión de datos.
- **SD-WAN:** Solución de redes de área amplia definidas por software que permite gestionar de forma dinámica las conexiones entre sucursales, priorizando el tráfico crítico y mejorando el rendimiento de las aplicaciones.
- **Infraestructura LAN y Wireless LAN:** Diseño e implementación de redes locales cableadas e inalámbricas de alta disponibilidad, asegurando conectividad estable, movilidad y escalabilidad dentro de las organizaciones.

- **Cableado Estructurado:** Instalación profesional de sistemas de cableado organizados y estandarizados, diseñados para soportar múltiples servicios tecnológicos, incluyendo voz, datos y video.
- **Comunicaciones Unificadas:** Plataformas integradas que combinan telefonía IP, videoconferencias, mensajería instantánea y colaboración en tiempo real, mejorando la productividad y la experiencia del usuario.
- **Consultoría de Redes:** Servicios de análisis, diseño y optimización de infraestructuras de red, asegurando alineación con objetivos de negocio, normativas y mejores prácticas internacionales.

2.3.3.2. Infraestructura.

- **Data Center – Housing:** Alquiler de espacios físicos seguros dentro de data centers certificados (TIER III y TIER IV), con condiciones óptimas para el alojamiento de servidores y equipos críticos.
- **Gestión de Facilidades del Data Center:** Administración completa de la infraestructura tecnológica, incluyendo energía, climatización, seguridad física y conectividad, asegurando el funcionamiento continuo de plataformas TI.
- **TEUNO VDI (Virtual Desktop Infrastructure):** Solución que permite a los usuarios acceder a escritorios virtuales desde cualquier ubicación y dispositivo, garantizando seguridad, reducción de costos y centralización de la gestión de TI.

- **Licenciamiento Corporativo Microsoft:** Licencias flexibles de suscripción para herramientas Microsoft 365 y otros servicios, optimizando costos y asegurando el cumplimiento de licencias.

2.3.3.3. Seguridad De La Información Y Ciberseguridad.

- **EndPoint y EDR:** Soluciones de seguridad para dispositivos finales que permiten detectar y responder a amenazas en tiempo real, evitando la propagación de malware y accesos no autorizados.
- **Gestión de Identidades:** Autenticación segura de usuarios y control de accesos a sistemas, aplicaciones y datos críticos, alineados a los principios de mínimo privilegio y multifactor.
- **SASE (Secure Access Service Edge):** Arquitectura que integra funciones de seguridad y conectividad desde la nube, permitiendo accesos seguros desde cualquier ubicación.
- **Network Detection and Response (NDR):** Monitoreo continuo del tráfico de red para detectar comportamientos anómalos y responder de forma proactiva a amenazas internas o externas.
- **Network Access Control (NAC):** Control de dispositivos que intentan acceder a la red, garantizando que solo aquellos autorizados y conformes con políticas de seguridad puedan conectarse.

- **Seguridad Perimetral – NGFW (Next-Generation Firewall):** Firewalls de nueva generación que inspeccionan el tráfico en profundidad, aplican políticas avanzadas y detectan amenazas sofisticadas en tiempo real.
- **AntiDDoS:** Soluciones para mitigar ataques de denegación de servicio distribuidos, manteniendo la disponibilidad de los sistemas frente a amenazas volumétricas.
- **WAF (Web Application Firewall):** Protección para aplicaciones web que identifica, bloquea y mitiga ataques como inyección SQL o cross-site scripting.
- **DLP (Data Loss Prevention):** Herramientas que detectan y previenen la fuga o filtración de información sensible dentro y fuera de la organización.
- **Correo Seguro:** Filtros avanzados para proteger la comunicación por correo electrónico frente a phishing, malware y spam, asegurando confidencialidad y disponibilidad.
- **Secure Web Gateway:** Control y protección de la navegación web, bloqueando sitios maliciosos, contenido no deseado y evitando fugas de datos en la nube.
- **Ethical Hacking:** Pruebas de penetración controladas que simulan ataques reales para identificar vulnerabilidades en sistemas, redes y aplicaciones.
- **Gestión de Vulnerabilidades:** Procesos continuos de detección, análisis y remediación de fallas técnicas y de configuración en la infraestructura tecnológica.
- **SOC (Security Operations Center):** Centro de operaciones de seguridad encargado de monitorear, detectar, responder y mitigar amenazas cibernéticas las 24 horas.

2.3.3.4. Cloud.

- **Migración a la Nube (IaaS):** Servicios para trasladar infraestructura física y cargas de trabajo a entornos cloud, mejorando escalabilidad, rendimiento y continuidad del negocio.
- **FinOps Cloud:** Herramientas para optimizar el uso y los costos en la nube mediante análisis predictivo, presupuestos centralizados y visibilidad por unidad de negocio.
- **Copilot para Microsoft 365:** Integración de inteligencia artificial generativa para potenciar la productividad mediante automatización, asistencia contextual y análisis de datos en las aplicaciones de Microsoft.
- **Backup y Recuperación Cloud:** Soluciones para copias de seguridad automatizadas, recuperación ante desastres y restauración rápida de servicios críticos.

2.3.3.5. Consultoría Y Servicios Gestionados.

- **Consultoría SGSI (ISO 27001):** Acompañamiento experto en el diseño, implementación y mejora de Sistemas de Gestión de Seguridad de la Información, alineados con estándares internacionales.
- **GAP Análisis y Evaluaciones de Seguridad:** Diagnóstico de cumplimiento normativo, identificación de brechas y elaboración de planes de mejora adaptados a los riesgos del cliente.
- **Consultoría GRC – LOPDP:** Asesoramiento especializado en gobierno, riesgos y cumplimiento de la Ley Orgánica de Protección de Datos Personales.

- **Digital Operation Center (DOC):** Centro de operación digital que gestiona eventos, peticiones, incidentes y cambios tecnológicos de forma centralizada y con trazabilidad.

Este portafolio integral permite a TEUNO posicionarse como un aliado estratégico en la transformación digital de sus clientes, garantizando disponibilidad, seguridad, eficiencia operativa y cumplimiento normativo.

2.4. Ubicación Y Sedes

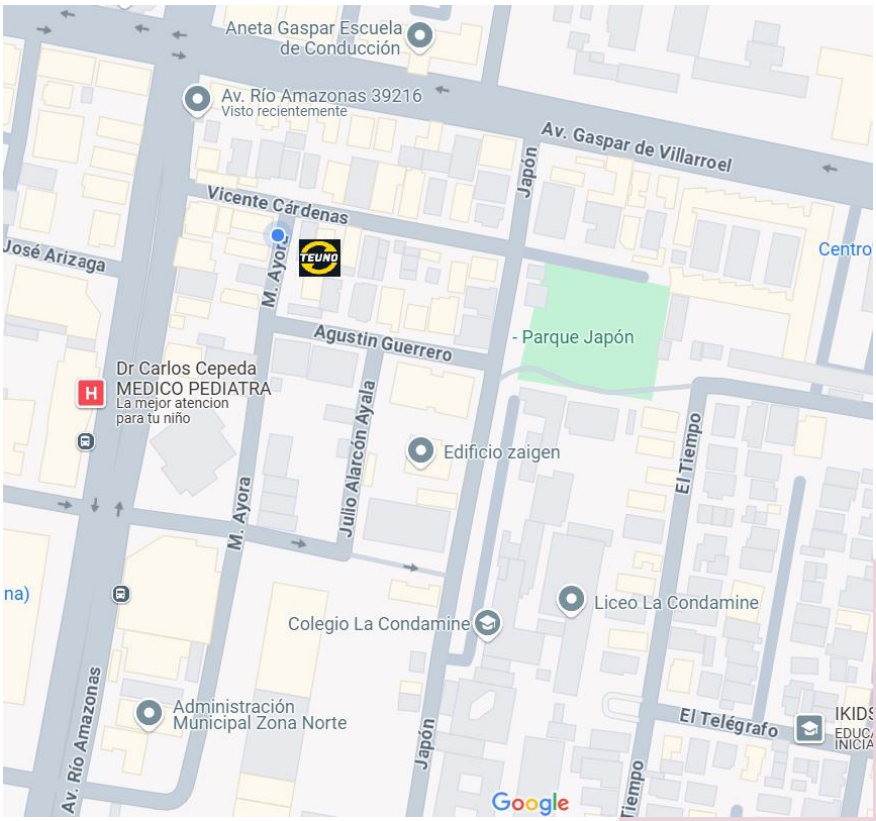
La sede principal se encuentra ubicada en la provincia de Pichincha – Zona 9, en las calles José María Ayora N39-162 y Vicente Cárdenas, Parroquia Iñaquito, Quito – Ecuador (CP170515), diagonal a los consultorios médicos Clínica de la Mujer.

Esta sede constituye el centro administrativo y tecnológico de la organización, desde donde se coordinan los servicios, operaciones críticas y gestión estratégica.

A su vez, también opera como sede de operaciones donde se gestiona la administración central, soporte técnico, planificación estratégica, seguridad de la información y operación de su data center principal (DCP) que brinda servicios a nivel nacional.

Figura 2

Croquis de la ubicación de la empresa TEUNO



Por otro lado, en la ciudad de Guayaquil se ubica una segunda sede de operaciones en las calles Nahím Isaías Barquet y Ezequiel Calle.

Allí se encuentra el data center alterno (DCA), categorizado como un hot site, el cual está diseñado para asumir la operación crítica en caso de contingencia o indisponibilidad del centro de datos principal en Quito.

Este sitio garantiza alta disponibilidad y recuperación inmediata, como parte de las estrategias de continuidad del negocio.

Ambas ubicaciones operan con infraestructura tecnológica avanzada, protocolos de seguridad física y lógica, conectividad redundante y personal técnico especializado. Estas

condiciones aseguran la prestación ininterrumpida de servicios y la ejecución de planes de recuperación ante incidentes.

2.5. Forma Jurídica Y Propiedad

2.5.1. Datos Societarios Y Legales.

- Razón Social: GRUPO BRAVCO S.A.
- RUC: 1790506428001.
- Fecha de constitución: 27 de julio de 1981.
- Estado Legal: Activa.
- Domicilio tributario: Barrio Iñaquito, Calle José María Ayora N39-162, Quito, Ecuador.
- Régimen tributario**:** Contribuyente especial bajo el Régimen General.

2.5.2. Forma Jurídica.

- Sociedad Anónima (S.A.), con patrimonio propio e independiente del de sus accionistas.
- La responsabilidad de los accionistas se limita al capital aportado.
- Puede adquirir derechos, contraer obligaciones, ser parte en juicios y actuar como persona jurídica independiente.

2.5.3. Propiedad (Accionistas Principales). Según el certificado actualizado emitido por la Superintendencia de Compañías, en la composición accionaria actual de GRUPO BRAVCO S.A. figuran Banco del Pichincha C.A y Sinves Holdings SINHOL S.A, con un capital suscrito total de USD 1,011,000.00 con el siguiente detalle:

Tabla 1

Composición accionaria actual de GRUPO BRAVCO S.A.

Nº	Accionista	Nacionalidad	Tipo de inversión	Capital suscrito (USD)
1	Banco del Pichincha C.A.	Ecuatoriana	Nacional	1,010,999.00
2	Sinves Holdings SINHOL S.A.	Ecuatoriana	Nacional	1.00

Tomado de *TEUNO*, 2024.

En la misma línea, actualmente el representante legal de la empresa es el señor Joaquín Ramos Hernández, con el cargo de Gerente General.

Por otro lado, es importante indicar que GRUPO BRAVCO S.A. mantiene su patente de funcionamiento vigente, emitida por el Municipio del Distrito Metropolitano de Quito.

2.6. Mercados Servidos Y Cobertura

TEUNO opera a nivel nacional, con una fuerte presencia en las principales ciudades del Ecuador; Quito y Guayaquil, desde donde se coordina y despliega las soluciones tecnológicas. Su alta capacidad técnica, infraestructura distribuida y centros de datos redundantes, le permiten

atender requerimientos remotos y presenciales, manteniendo la continuidad operativa y gestión centralizada de servicios críticos sin limitación geográfica.

Proporciona servicios especializados a organizaciones de mediana y gran escala, enfocando su cobertura en los siguientes mercados:

- **Corporativo:** Empresas medianas y grandes de diversos rubros (comercial, industrial, salud, tecnología, educación).
- **Financiero:** Cooperativas, mutualistas y bancos, gracias a su autorización como proveedor de servicios auxiliares por parte de la Superintendencia de Bancos y la SEPS.
- **Tecnológico y de telecomunicaciones:** Proveedores de servicios TIC que requieren infraestructura robusta y soporte especializado.
- **Sector público:** Instituciones que demandan conectividad segura, cumplimiento normativo y soluciones de ciberseguridad.
- **Empresas con necesidades críticas de continuidad operativa**, especialmente aquellas que operan bajo marcos regulatorios exigentes o con altos niveles de disponibilidad tecnológica.

2.7. Tamaño De La Organización

TEUNO es una sociedad anónima ecuatoriana con más de cuatro décadas de experiencia en el sector tecnológico, consolidada como una de las empresas de mayor relevancia en servicios tecnológicos corporativos del país.

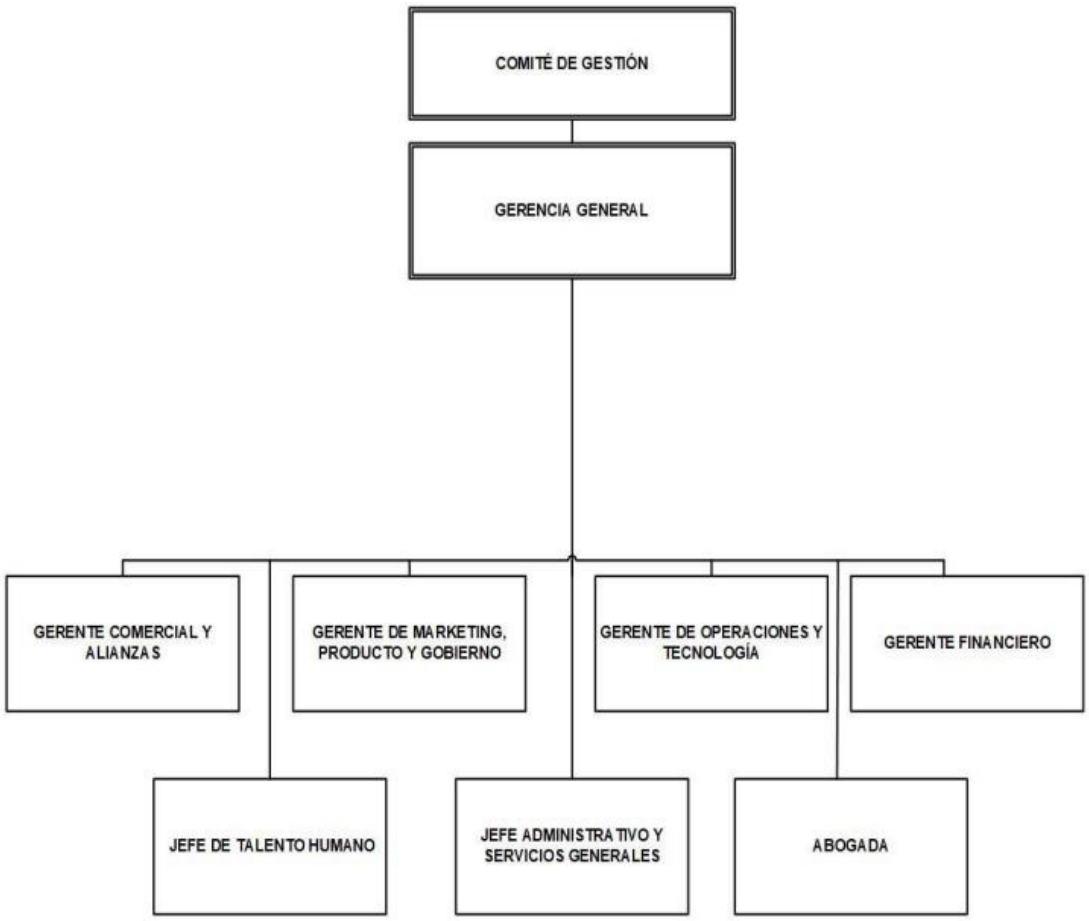
De acuerdo con datos oficiales y registros de la Superintendencia de Compañías, Valores y Seguros del Ecuador, la empresa presenta una estructura sólida en términos financieros, operativos

y humanos. Actualmente, cuenta con más de 300 colaboradores directos, distribuidos entre sus oficinas, centros de datos, áreas técnicas y administrativas en las ciudades de Quito y Guayaquil.

Estos indicadores posicionan a TEUNO como una empresa de tamaño grande dentro del sector TIC ecuatoriano, con capacidades comprobadas para liderar proyectos de transformación digital, seguridad de la información y continuidad operativa a nivel nacional.

Figura 3

Organigrama Teuno



Tomado de (*TEUNO*, 2024)

2.7.1. Información del Talento Humano. La relación laboral está regulada bajo los términos del Código del Trabajo, el Reglamento Interno de Trabajo aprobado en 2025, y el procedimiento formal de gestión de nómina vigente.

TEUNO cuenta con una estructura organizacional sólida y especializada, compuesta por más de 300 colaboradores directos bajo relación de dependencia, distribuidos en áreas técnicas, operativas, administrativas y estratégicas, en modalidad presencial, remota e híbrida (de acuerdo a las necesidades operativas y perfil de servicio). Entre las aptitudes clave de sus colaboradores, se encuentra la alta capacidad técnica, reflejada en la posesión de certificaciones técnicas en normas ISO, plataformas de seguridad (NSE, CEH), redes (Cisco), infraestructura (Microsoft, VMware) y metodologías de gestión.

Este capital humano representa un pilar esencial para la prestación continua y de alta calidad de los servicios que ofrece la organización, por lo que cuenta con programas regulares de capacitación, evaluación de desempeño, movilidad interna y especialización técnica.

Tabla 2

Distribución del personal por área funcional

Área / Departamento	Número de colaboradores
Dirección General	4
Gerencia Administrativa y Financiera	10
Gerencia Comercial	18
Gerencia de Tecnología	12

Área / Departamento	Número de colaboradores
Proyectos e Ingeniería	28
Networking y Telecomunicaciones	41
Seguridad de la Información (SOC)	35
Cloud y Plataformas	26
Soporte Técnico y Mesa de Servicios	52
Centro de Operaciones Digitales (DOC)	23
Desarrollo de Soluciones	15
Consultoría GRC / SGSI / LOPDP	11
Talento Humano	6
Logística y Servicios Generales	9
Servicio al Cliente y Postventa	13
Total general	**303**

Nota. Base institucional de empleados actualizada, corte al primer trimestre de 2025. Tomado de *TEUNO*, 2024.

Por otro lado, además del personal directo, la empresa cuenta con recursos complementarios, colaborando con:

- Consultores especializados para proyectos normativos y de transformación digital.
- Partners estratégicos en tecnología para implementación, soporte y escalamiento de soluciones.
- Contratistas técnicos en proyectos específicos de instalación o mantenimiento.

Este talento humano, respaldado por políticas claras de gestión y desarrollo, constituye uno de los principales activos estratégicos de TEUNO, asegurando un servicio eficiente, confiable y resiliente ante cualquier escenario.

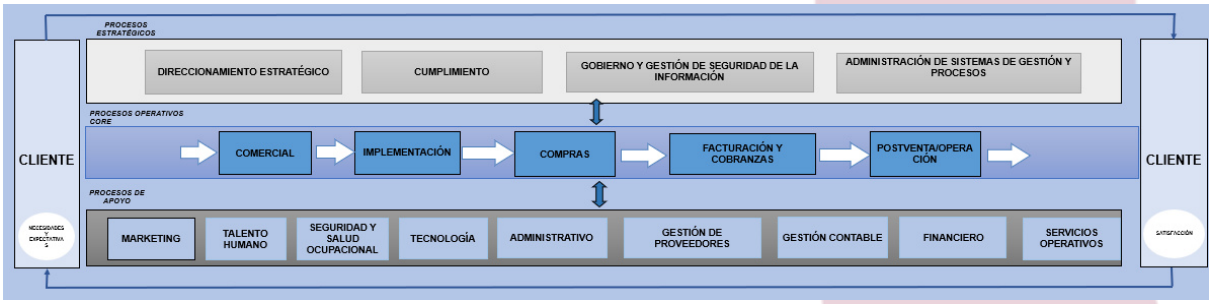
2.8. Procesos Claves Relacionados Con El Objetivo Propuesto

El proyecto de titulación se enfoca en la puesta en marcha de un Sistema de Gestión de Continuidad del Negocio (SGCN) conforme a la norma ISO 31000:2018, cuyo principal enfoque es la administración del riesgo organizativo. Para su implementación, resulta crucial tener en cuenta los procesos fundamentales que conforman la cadena de valor de TEUNO y que, por su esencia, impactan directamente en la resistencia operativa, la provisión de servicios esenciales y la salvaguarda de los activos de información.

Identificación de procesos clave: De acuerdo con la documentación interna y la administración por procesos de la compañía, los procesos fundamentales (core) son los operativos que aportan valor directo al cliente. Estos procesos se encuentran organizados en el macroproceso operativo y constituyen el núcleo del negocio de TEUNO.

Figura 4

Mapa de Procesos



Nota. El gráfico representa los procesos clave vinculados al proyecto de continuidad del negocio, en función de su impacto en la gestión del riesgo y la continuidad operativa. Tomado de *(Teuno, Repositorio Docs Teuno,* 2024).

Tabla 3

Identificación de procesos clave y proyecto de continuidad.

Código	Nombre del Proceso Clave	Relación con el proyecto de continuidad
PRC-OP-01	Gestión de Servicios Tecnológicos	Asegura la operación ininterrumpida de soluciones TIC para clientes.
PRC-OP-02	Gestión de Seguridad de la Información (SOC)	Mitigación de riesgos de ciberseguridad y soporte a la gestión de crisis.
PRC-OP-03	Gestión de Incidentes y Eventos	Respuesta efectiva a interrupciones o desviaciones del servicio.
PRC-OP-04	Gestión del Centro de Datos (Quito y Guayaquil)	Infraestructura crítica que soporta la continuidad de plataformas y sistemas.
PRC-OP-05	Gestión de Continuidad Tecnológica (respaldo, DRP, etc.)	Proceso directamente involucrado en la recuperación ante desastres.
PRC-OP-06	Gestión de Proyectos e Implementaciones	Control de riesgos en el diseño y despliegue de servicios críticos.
PRC-OP-07	Gestión de Cumplimiento Normativo y GRC	Relación directa con ISO 31000 e ISO 22301 para asegurar conformidad.

Tomado de *TEUNO*, 2024.

El desarrollo de un Sistema de Continuidad del Negocio basado en ISO 31000:2018 requiere identificar aquellos procesos que:

- Proveen servicios esenciales a clientes.
- Responden ante incidentes y amenazas.
- Custodian activos críticos de información.
- Sostienen la infraestructura tecnológica de misión crítica.

- Permiten el cumplimiento de requisitos regulatorios y contractuales.

Por tanto, estos procesos serán el foco del análisis de riesgos, la definición de niveles de impacto, y la formulación de estrategias de continuidad y recuperación en el marco del proyecto de titulación.

2.8.1. Principales Cifras, Ratios Y Números Que Definen A La Empresa. TEUNO es una organización con amplio posicionamiento en el sector tecnológico ecuatoriano, caracterizada por su capacidad de innovación, resiliencia operativa y visión estratégica de largo plazo.

Indicadores Institucionales

- Más de 17 años de experiencia en el mercado tecnológico.
- Más de 2.000 proyectos ejecutados en clientes del sector financiero, corporativo y gubernamental.
- Más de 300 colaboradores directos, organizados en unidades especializadas.
- Más de 180 profesionales certificados, entre ellos ingenieros de redes, arquitectos de soluciones, expertos en ciberseguridad y auditores ISO.
- Presencia nacional y capacidad de atención regional en Latinoamérica.
- 2 data centers propios (Quito y Guayaquil), con infraestructura de misión crítica.

Certificaciones Internacionales

- ISO/IEC 27001:2022 – Seguridad de la Información
- ISO/IEC 20000-1:2018 – Gestión de Servicios de TI
- ISO 9001:2015 – Gestión de la Calidad

2.8.2. Modelo de negocio. TEUNO basa su giro de negocio en una estrategia de soluciones tecnológicas integradas, orientada a clientes del sector corporativo, financiero, telecomunicaciones y público, combinando un enfoque consultivo, técnico y operativo. Este modelo está estrechamente alineado con los pilares de continuidad, eficiencia, seguridad y transformación digital.

El modelo es gestionado a través de un proceso comercial formalizado (código PRC-CM-01), estructurado por fases y políticas que aseguran la correcta atención al cliente desde la identificación del requerimiento hasta el cierre de la venta y el cumplimiento contractual.

Propuesta de valor

TEUNO no solo entrega productos o servicios tecnológicos, sino que acompaña al cliente en el diseño e implementación de soluciones que garantizan operación continua, mitigación de riesgos y cumplimiento normativo, especialmente en entornos críticos.

Tabla 4

Componentes clave del modelo de negocio

Elemento	Descripción
Tipo de cliente	Empresas medianas y grandes, entidades financieras, organismos del sector público.
Oferta de valor	Soluciones tecnológicas escalables, seguras y personalizadas, con enfoque en continuidad.
Modalidad comercial	Venta directa, suscripción, outsourcing, renta tecnológica y servicios gestionados (SOC/DOC).
Canales de atención	Contacto consultivo, gestión CRM, atención presencial/remota, demos, pruebas de concepto.

Elemento	Descripción
Procesos asociados	Proceso Comercial (PRC-CM-01), Preventa, Contratación, Diseño y Transición de Servicios.
Utilidad esperada	Margen de profit establecido según torre de servicio y modalidad (de 6% a 30%).
Gestión contractual	Firma de contratos desde USD 20.000 en adelante, con políticas claras de pago y control.

Tomado de *TEUNO*, 2024.

Estructura de rentabilidad y gestión del valor

El modelo contempla la venta y renovación de servicios con márgenes mínimos establecidos por tipo de solución.

Estas políticas permiten equilibrar la sostenibilidad financiera con la competitividad del portafolio.

Este modelo permite a TEUNO mantener relaciones sólidas y sostenibles con sus clientes, mientras fortalece su posicionamiento como aliado tecnológico de largo plazo, capaz de ofrecer soluciones robustas frente a un entorno cambiante y de riesgo creciente.

2.8.3. Grupos De Interés Internos Y Externos. Es fundamental considerar a las partes interesadas de TEUNO, tanto internas como externas, ya que su influencia directa o indirecta impacta en los objetivos, operaciones y continuidad de la organización.

Estos grupos son identificados, monitoreados y evaluados periódicamente por la Alta Dirección y los comités de seguridad y riesgos, asegurando que sus expectativas sean comprendidas y abordadas dentro de la organización.

Tabla 5

Grupos de Interés Internos

Grupo Interno	Necesidades y expectativas
Alta Dirección	Gestión eficaz de riesgos, toma de decisiones informada, cumplimiento estratégico.
Gerencias funcionales	Claridad en políticas de seguridad, recursos disponibles, alineación de procesos.
Colaboradores	Estabilidad, capacitación, buen ambiente laboral, protección de información personal.
Comité Ejecutivo	Seguimiento a los objetivos estratégicos y control de los sistemas implementados.
Comité de Seguridad de la Información	Implementación de políticas, monitoreo de incidentes, mejora continua del SGSI.
Comité de Riesgos	Evaluación de amenazas, validación de planes de continuidad, soporte a decisiones.

Tomado de *TEUNO*, 2024.

Tabla 6

Grupos de Interés Externos

Grupo Externo	Necesidades y expectativas
Clientes	Servicios continuos, información segura, cumplimiento de SLA, atención especializada.
Proveedores	Relaciones estables, pagos oportunos, protección de datos y continuidad comercial.
Entidades reguladoras (SB, SEPS, ARCOTEL, SRI, Supercias)	Cumplimiento normativo, trazabilidad, controles documentados.
Sociedad y comunidad	Impacto positivo, responsabilidad social, acceso a tecnología confiable.
Alianzas estratégicas	Fidelidad comercial, sinergia técnica, gestión conjunta de riesgos.

Grupo Externo	Necesidades y expectativas
Competencia	Innovación, legalidad, competencia justa y posicionamiento de marca.
Entidades aseguradoras	Acceso a información confiable, control de riesgos, planes de mitigación.
Medio ambiente	Manejo adecuado de residuos tecnológicos, sostenibilidad operativa.

Tomado de *TEUNO*, 2024.

Estas partes interesadas forman parte del ecosistema que soporta la operación y sostenibilidad de TEUNO.

2.8.4. Otros Datos De Interés. GRUPO BRAVCO S.A., con su marca comercial TEUNO, ha construido una trayectoria consolidada en el mercado ecuatoriano de tecnologías de la información y comunicación (TIC), distinguiéndose por su innovación, resiliencia y compromiso con la excelencia operativa.

A continuación, se destacan algunos aspectos complementarios que fortalecen la visión integral de la organización:

Historia y evolución

- Fundada el 27 de julio de 1981, inicialmente enfocada en distribución de equipos tecnológicos.
- En los últimos 20 años, ha transitado hacia un modelo de servicios gestionados, incorporando soluciones en infraestructura, conectividad, cloud y ciberseguridad.
- La adopción de normas internacionales ISO (27001, 20000-1, 9001) y su autorización como proveedor de servicios auxiliares por la Superintendencia de Bancos y la SEPS, marcan un hito en su posicionamiento estratégico.

Infraestructura clave

- Cuenta con dos centros de datos propios, en Quito (principal) y Guayaquil (alterno), ambos operativos como sitios de respaldo y contingencia.
- Posee un Centro de Operaciones de Seguridad (SOC) y un Digital Operation Center (DOC) que permiten monitorear servicios críticos 24/7, alineados con los requerimientos del proyecto de continuidad.

Alianzas y ecosistema tecnológico

- Mantiene alianzas con fabricantes líderes como Microsoft, Fortinet, Cisco, VMware, Veeam, Huawei, entre otros.
- Participa activamente en el ecosistema de transformación digital del país, incluyendo eventos del sector y certificaciones de fabricantes globales.

Innovación y cultura

- La cultura organizacional está guiada por principios como la coherencia, responsabilidad, esfuerzo y trascendencia.
- En 2024, la empresa inició el despliegue de herramientas de inteligencia artificial generativa, como Copilot for Microsoft 365, dentro de su portafolio.

Reconocimientos

- Ha sido reconocida por sus clientes y aliados por su excelencia en la atención postventa, cumplimiento de SLA y capacidad de respuesta ante incidentes.

- En 2023 y 2024, recibió menciones especiales como partner estratégico en proyectos de transformación digital en el sector financiero.

Estos datos complementarios reafirman que TEUNO es una organización con una base sólida, preparada para enfrentar desafíos y liderar la industria tecnológica del país.

Capítulo 3: Manual Documento De Seguridad

3.1.Análisis de Riesgos

3.1.1. Identificación De La Organización Y De Sus Centros De Trabajo. Para el Estudio de riesgos y la puesta en marcha de medidas de seguridad, resulta esencial reconocer oficialmente a la organización, su estructura legal, localización física y los lugares de trabajo desde los cuales se llevan a cabo actividades de tratamiento de datos personales. Esta identificación brinda la base fundamental en la que se edifica el sistema de salvaguarda de la información de acuerdo con la Ley Orgánica de Protección de Datos Personales (LOPDP).

Razón social: GRUPO BRAVCO S.A.

Ubicación geográfica: Zona 9 / Pichincha / Quito

3.1.2. Representante legal y Responsable de Seguridad de la Información. Para cumplir con las normas dictadas en la Ley Orgánica de Protección de Datos Personales (LOPDP), es crucial reconocer oficialmente a los encargados del cumplimiento de las regulaciones y la administración de la seguridad de la información dentro de la entidad.

Representante Legal:

Nombre: Joaquín Ramos Hernández

Cargo: Gerente

Responsabilidad: Representación jurídica de GRUPO BRAVCO S.A., y tiene la facultad de tomar decisiones estratégicas y aprobar políticas internas relacionadas con la protección de datos personales, seguridad de la información y cumplimiento legal.

Responsable de Seguridad de la Información:

Nombre: Rita Torres

Cargo: Oficial de Seguridad de la Información

Responsabilidad: Supervisar la implementación, mantenimiento y mejora continua de las medidas de seguridad sobre los activos de información.

Esta función se considera crítica dentro del modelo de gobernanza de datos, por lo que cuenta con autonomía técnica y acceso a la alta dirección.

3.1.3. Actividades De La Organización. GRUPO BRAVCO S.A es una empresa que brinda soluciones tecnológicas integrales que impulsan la transformación digital y fortalecen la infraestructura de sus clientes. Sus principales áreas de actividad incluyen:

- **Conectividad y Networking:** GRUPO BRAVCO S.A ofrece soluciones avanzadas para garantizar que las empresas se mantengan conectadas y competitivas.
- **Infraestructura:** GRUPO BRAVCO S.A proporciona soluciones de infraestructura robustas que aseguran la eficiencia y confiabilidad de las operaciones críticas de sus clientes.
- **Seguridad:** GRUPO BRAVCO S.A brinda soluciones integrales de seguridad para proteger los activos digitales de las organizaciones.
- **Cloud (Nube):** Facilita la adopción de tecnologías en la nube.

3.1.4. Tratamientos De La Organización Y Sus Riesgos. GRUPO BRAVCO S.A ha implementado un Sistema de Gestión Integral de Riesgos que contempla tanto los riesgos estratégicos y operativos como aquellos vinculados a la continuidad del negocio, seguridad de la

información, salud ocupacional y cumplimiento legal. La organización aplica una metodología basada en MAGERIT y método Delphi, y evalúa los riesgos a través de matrices que consideran probabilidad, impacto y eficacia de controles.

a) Tipos de riesgos a los que se expone la organización

Tabla 7

Tipos de riesgos a los que se expone la organización

Categoría de riesgo	Ejemplos de riesgos específicos	Consecuencias potenciales
Riesgo operativo	Fallas en procesos internos, errores humanos, fraudes internos, fallas tecnológicas	Pérdidas económicas, reprocesos, baja productividad
Riesgo tecnológico	Ciberataques, malware, pérdida de información, indisponibilidad de sistemas	Interrupción de operaciones, fuga de datos, sanciones
Riesgo legal y normativo	Incumplimiento de la LOPDP, leyes laborales, tributarias o de contratación pública	Multas, sanciones, daño reputacional
Riesgo financiero	Errores contables, fraude financiero, mal manejo de fondos	Desviaciones presupuestarias, pérdidas financieras
Riesgo ocupacional	Riesgos físicos, químicos, biológicos, de seguridad, ergonómicos y psicosociales.	Accidentes laborales, enfermedades ocupacionales, incumplimientos a la normativa legal vigente.
Riesgo reputacional	Mala gestión de incidentes, atención deficiente, filtración de datos personales	Pérdida de confianza de clientes o inversionistas
Riesgos externos	Fallas de servicios públicos, desastres naturales, inseguridad ciudadana	Interrupción del negocio, evacuaciones, pérdida de activos
Riesgo de continuidad	Interrupción de servicios críticos (TI, RRHH, comercial) por eventos inesperados	Paralización de operaciones, pérdida de clientes

Tomado de *TEUNO*, 2024.

b) Tratamiento de riesgos aplicado por la organización

El tratamiento se define como la acción para prevenir o mitigar los impactos de un riesgo identificado, con el objetivo de que este se ubique en un nivel de riesgo aceptable, conforme al apetito de riesgo institucional.

GRUPO BRAVCO S.A implementa tratamientos como:

- **Controles preventivos**: políticas, procedimientos, automatización, doble validación.
- **Controles detectivos**: auditorías, monitoreos, registros de logs.
- **Controles correctivos**: planes de mejora, actualización de procesos, sanciones disciplinarias.
- **Controles compensatorios**: seguros, redundancia de servicios, respaldo de datos.
- **Controles físicos y ambientales**: acceso restringido, videovigilancia, ergonomía.

c) Herramientas de soporte y seguimiento

- Matrices de riesgos estratégicos y operativos, con revisión anual.
- Plataforma digital de seguimiento de riesgos (Docs / Planner).
- Evaluación continua de la eficacia de controles y riesgos residuales.
- Comité de Riesgos y Auditoría que valida los planes de acción y actualizaciones.
- Indicadores clave: % de riesgos gestionados, % fuera del apetito, % cumplimiento de planes.

Este enfoque permite a GRUPO BRAVCO S.A anticiparse a amenazas, reducir impactos y cumplir con la normativa vigente, incluyendo la Ley de Protección de Datos Personales, ISO 27001, ISO 20000 e ISO 9001.

3.1.5. Consentimientos Y Notas Informativas. La gestión de datos personales efectuada por GRUPO BRAVCO S.A se basa en el principio de licitud, siendo la autorización del titular uno de los factores esenciales de habilitación. La compañía ha implementado políticas y procesos que aseguran la adquisición, administración y anulación del consentimiento de forma correcta y acorde con la legislación vigente.

La autorización obobtenida satisface los requisitos estipulados en el artículo específico de la LOPDP, lo que implica:

- **Libre**: otorgado sin coacción, presión o condicionamientos indebidos.
- **Específico**: dirigido a una o varias finalidades concretas y claramente definidas.
- **Informado**: el titular es plenamente consciente del tipo de datos tratados, su finalidad, los responsables y sus derechos.
- **Inequívoco**: mediante una manifestación afirmativa clara, ya sea verbal, escrita o a través de medios electrónicos que evidencien la voluntad del titular.

La organización dispone de mecanismos para que el titular pueda revocar su consentimiento en cualquier momento, sin efectos retroactivos sobre tratamientos ya realizados con base en dicho consentimiento.

Como parte del deber de información, GRUPO BRAVCO S.A garantiza que toda recogida de datos personales vaya acompañada de notas informativas visibles, comprensibles y accesibles, que incluyen:

- Identificación y datos de contacto del encargado de la gestión.
- Finalidad del tratamiento y base legal que lo respalda.

- Objetivos potenciales de los datos (responsables del tratamiento o terceros autorizados).
- Derechos del propietario (acceso, corrección, oposición, supresión, portabilidad, entre otros) y el procedimiento para ejercerlos.
- Detalles acerca de la transferencia de datos internacional (si se produce).
- Duración de la preservación de la información o los criterios empleados para su definición.

GRUPO BRAVCO S.A establece sistemas para documentar y auditar los permisos concedidos, tanto en formato papel como digital, garantizando su seguimiento y legitimidad jurídica. Estos archivos están bajo la protección del departamento encargado de la seguridad de la información y están sometidos a controles de acceso y preservación de acuerdo con la legislación.

Para lo cual nos basamos en el acuerdo de confiabilidad detallado en el punto 3.9.1, de este documento.

Consentimiento para el Tratamiento de Datos Personales

Según lo estipulado en la Ley Orgánica de Protección de Datos Personales (LOPDP) ecuatoriana y en el contexto de este acuerdo de confidencialidad firmado entre GRUPO BRAVCO S.A. TEUNO y el cliente, el permiso para el tratamiento de la información personal se rige bajo las siguientes condiciones:

Consentimiento otorgado: El cliente autoriza de forma libre, específica, informada e inequívoca a GRUPO BRAVCO S.A. TEUNO (el Receptor) para tratar los datos personales proporcionados en virtud de la relación comercial establecida.

El tratamiento incluye la recopilación, uso, almacenamiento, gestión, custodia y transferencia de datos personales, con estricta confidencialidad y exclusivamente para las finalidades determinadas en el contrato de servicios suscrito.

Finalidades del tratamiento:

Cumplimiento de las obligaciones derivadas del contrato de prestación de servicios.

Realización de diagnósticos, estructuración de ofertas comerciales y ejecución de proyectos acordados.

Gestión administrativa, comercial, contable y de servicio al cliente.

Envío de comunicaciones comerciales e informativas relacionadas con productos y servicios de TEUNO.

Protección y seguridad de los datos: TEUNO se compromete a aplicar medidas técnicas y organizativas de seguridad que garanticen la protección de los datos personales contra el acceso no autorizado, pérdida, alteración o divulgación, conforme a lo exigido por la LOPDP.

Subencargados del tratamiento: La gestión de los datos también podrá ser llevada a cabo por subencargados debidamente autorizados, siguiendo los mismos estándares de protección de datos pertinentes a TEUNO.

Transferencias internacionales: Los datos se pueden enviar a nivel internacional conforme a las regulaciones de protección de datos, asegurando siempre un nivel de protección adecuado.

Derechos de los titulares: El cliente tiene la posibilidad de ejercer sus derechos de acceso, rectificación, actualización, eliminación, suspensión, oposición y portabilidad en cualquier instante, enviando su petición por medio del correo electrónico: info@teuno.com.

Duración del tratamiento: El tratamiento de los datos personales se mantendrá vigente mientras exista la relación contractual o hasta por dos (2) años posteriores a su finalización, salvo que existan obligaciones legales que exijan una conservación adicional.

3.2. Registro De Actividades De Tratamiento

3.2.1. Grupos De Información. Para cumplir con el principio de transparencia y documentar de manera organizada los tratamientos de datos personales llevados a cabo por Teuno, se reconocen los siguientes conjuntos de datos, categorizados en función del tipo de relación que tienen con GRUPO BRAVCO S.A. TEUNO y la clase de información que tratan.

Con base en la Política de Protección de Datos Personales y los procedimientos internos de GRUPO BRAVCO S.A:

1. Datos de clientes (actuales y potenciales)

Incluyen personas naturales y representantes de personas jurídicas con quienes la organización mantiene o busca establecer una relación comercial.

Datos tratados:

- Identificación: nombres, apellidos, número de cédula o RUC.
- Contacto: teléfono, correo electrónico, dirección.
- Datos de transacción: historial de compras, solicitudes de servicio, facturación.

- Datos de autenticación digital: acceso a plataformas, en su caso.

Finalidad del tratamiento:

- Gestión de relaciones comerciales y contractuales.
- Envío de propuestas, campañas informativas y encuestas de satisfacción.
- Soporte técnico y atención de requerimientos.

2. Datos de candidatos

Corresponde a información recopilada durante procesos de selección de personal, antes de formalizar una relación laboral.

Datos tratados:

- Datos personales y de contacto.
- Formación académica y experiencia laboral.
- Resultados de entrevistas y pruebas de selección.
- Referencias laborales.

Finalidad del tratamiento:

- Gestión de procesos de reclutamiento y selección.
- Evaluación de aptitudes y competencias profesionales.

3. Datos de colaboradores (empleados)

Se refiere a la información recopilada y tratada una vez que el candidato es contratado como empleado.

Datos tratados:

- Datos personales y de contacto.
- Historial laboral y académico.
- Evaluaciones de desempeño.
- Datos sensibles: salud ocupacional, aptitudes médicas, discapacidades, afiliaciones de seguridad social.
- Información de cargas familiares (dependientes para beneficios laborales).

Finalidad del tratamiento:

- Administración de recursos humanos, nómina y beneficios.
- Cumplimiento de obligaciones laborales y de seguridad social.
- Prevención de riesgos laborales y gestión de la salud ocupacional.

4. Datos de proveedores y contratistas

Personas naturales o jurídicas que prestan servicios o proveen bienes a GRUPO BRAVCO S.A.

Datos tratados:

- Información de contacto y datos bancarios.

- Identificación: nombres, apellidos, número de cédula o RUC.
- Contacto: teléfono, correo electrónico, dirección.
- Identificación del representante legal.
- Historial contractual y de cumplimiento.

Finalidad del tratamiento:

- Gestión administrativa de relaciones comerciales.
- Verificación de cumplimiento normativo (protección de datos, seguridad, etc.).

5. Datos del área financiera y contable

Datos obtenidos y tratados para el cumplimiento de obligaciones fiscales, contables y tributarias.

Datos tratados:

- Información de facturación: nombre o razón social, RUC, dirección fiscal.
- Información bancaria para pagos o cobros.
- Comprobantes de retención de impuestos y soportes tributarios.
- Documentos contables asociados a operaciones comerciales.

Finalidad del tratamiento:

- Gestión contable y financiera interna.
- Cumplimiento de obligaciones tributarias y fiscales.

6. Datos de videovigilancia

Imágenes captadas a través de sistemas de cámaras de seguridad instaladas en las instalaciones de GRUPO BRAVCO S.A.

Datos tratados:

- Videograbaciones de las áreas comunes, accesos y zonas protegidas.

Finalidad del tratamiento:

- Garantizar la seguridad física de empleados, visitantes y bienes corporativos.
- Prevención de delitos y control de accesos.

7. Datos de visitantes y usuarios de plataformas digitales

Personas que interactúan con el sitio web, herramientas digitales o redes sociales de GRUPO BRAVCO S.A.

Datos tratados:

- Información de navegación: cookies
- Datos enviados a través de formularios de contacto: nombre, correo electrónico, teléfono.
- Datos de autenticación en servicios digitales.

Finalidad del tratamiento:

- Atención de consultas.
- Mejora de la experiencia del usuario.

- Seguimiento de campañas de marketing digital.

Cada grupo de información cuenta con controles de seguridad específicos, definidos en función de su nivel de sensibilidad y riesgo, y se encuentra documentado dentro del Registro de Actividades de Tratamiento conforme al artículo 13 de la LOPDP.

3.2.2. Sistemas De Tratamiento Y Niveles De Seguridad. Según la Política de Seguridad de la Información, el Proceso de Administración de Seguridad de la Información, la Política de Protección de Datos Personales y los Procedimientos de Administración de Datos Personales de GRUPO BRAVCO S.A. TEUNO, y conforme a lo estipulado en la Ley Orgánica de Protección de Datos Personales (LOPDP), se pone en marcha un modelo completo de administración del manejo de la información personal.

La organización dispone de una arquitectura tecnológica que soporta las diferentes fases del tratamiento de datos personales:

- Recolección
- Procesamiento
- Almacenamiento
- Consulta
- Eliminación segura

Se ha realizado una evaluación de los sistemas empleados para este tratamiento, teniendo en cuenta su efecto en la privacidad, integridad y accesibilidad de la información.

Desde esta evaluación, se establecen niveles de seguridad en función de la importancia de los datos tratados y la confidencialidad de los mismos.

Sistemas de Tratamiento

El tratamiento de los datos personales en GRUPO BRAVCO S.A. se realiza mediante los siguientes sistemas:

- **Sistema de Gestión de Clientes (CRM):**

  Recolección y administración de datos de clientes actuales y potenciales.

- **Sistema de Gestión de Recursos Humanos (Venture):**

  Administración de datos laborales de empleados, incluyendo salud ocupacional y cargas familiares.

- **Sistema de Gestión Contable y Financiero (ERP):**

  Tratamiento de datos tributarios, bancarios y contables de clientes, proveedores y colaboradores.

- **Sistema de Videovigilancia:**

  Captación y almacenamiento temporal de imágenes en áreas físicas protegidas.

- **Sistema de Gestión de Solicitudes de Derechos de Titulares:**

  Atención de solicitudes de ejercicio de derechos ARCO, gestionado por el Oficial de Seguridad.

- **Sistema de Gestión Web:**

Tratamiento de cookies, navegación y formularios de contacto de usuarios de plataformas digitales.

Cada uno de estos sistemas cuenta con procedimientos y políticas de seguridad específicos, evaluados conforme a metodologías de análisis de riesgos.

Clasificación de Niveles de Seguridad

Según la clasificación de activos definida en la Política de Seguridad y la Metodología de Gestión de Riesgos, los niveles aplicados son:

- **Básico:**

  Datos públicos o de bajo riesgo (por ejemplo, formularios de contacto web o información de navegación sin identificación directa).

- **Medio:**

  Datos identificativos y transaccionales (por ejemplo, datos de clientes, proveedores, postulantes a empleo).

- **Alto:**

  Datos sensibles o críticos (por ejemplo, datos de salud ocupacional, identificadores únicos, datos financieros, imágenes de videovigilancia, evaluaciones laborales).

Medidas de Seguridad Aplicadas

Las medidas de seguridad aplicadas por nivel incluyen:

- Control de acceso por roles y principio de privilegio mínimo.

- Autenticación multifactor (MFA) en sistemas críticos.
- Cifrado de datos en tránsito y en reposo.
- Registro y auditoría de accesos y eventos de seguridad.
- Políticas de escritorio limpio y bloqueo automático de sesiones.
- Evaluaciones periódicas de vulnerabilidades y análisis de riesgos.
- Procedimientos de eliminación segura de la información al término de su conservación.

3.2.3. Finalidades, Categorías De Datos, De Interesados Y De Destinatarios. Según la LOPDP, la Política de Protección de Datos Personales y los procedimientos de administración de seguridad informática de GRUPO BRAVCO S.A se detallan a continuación:

Finalidad del tratamiento y comunicación de datos: Conforme al principio de propósito y la obligación de información dictados en la Ley Orgánica de Protección de Datos Personales (LOPDP), GRUPO BRAVCO S.A asegura que los datos personales obtenidos se utilizan únicamente para propósitos legítimos, explícitos y en concordancia con las actividades propias de la entidad.

A continuación, se detallan las principales categorías de datos personales tratados, sus finalidades y si están sujetos o no a comunicación a terceros (encargados o aliados estratégicos):

Tabla 8

Categorías de datos privacidad de personales

Categoría de datos personales	Ejemplos	Finalidad del tratamiento	¿Se comunican a terceros?
Datos de identificación	Nombres, apellidos, cédula, RUC, firma, fecha de nacimiento	- Identificación del titular- Gestión contractual- Atención de solicitudes	Sí, en contratos y facturación (proveedores, clientes)
Datos de contacto	Teléfono, correo electrónico, dirección	- Comunicaciones institucionales- Coordinación de servicios o soporte	Sí, con encargados de servicios tecnológicos o de mensajería
Datos laborales	Cargo, historial laboral, evaluaciones, formación, asistencia	- Relación laboral- Desarrollo de carrera- Control interno de talento humano	No, salvo por requerimiento legal
Datos financieros	Cuenta bancaria, información de pago, ingresos	- Procesamiento de pagos- Facturación- Cumplimiento fiscal	Sí, a bancos y entidades tributarias (SRI)
Datos de salud ocupacional	Aptitudes médicas, discapacidades, enfermedades laborales	- Gestión de salud ocupacional- Prevención de riesgos laborales	No, salvo autoridades de salud o aseguradoras
Datos biométricos	Huella digital (para control de acceso o registro de asistencia)	- Control de acceso físico/lógico- Registro de jornada laboral	No
Datos de navegación web	Cookies, dirección IP, geolocalización	- Mejora de experiencia digital- Estadísticas de uso- Seguridad web	Sí, a proveedores de analítica o infraestructura web
Datos de menores de edad	Datos de hijos dependientes (en contexto laboral)	- Gestión de beneficios laborales- Declaración de carga familiar	No
Datos de clientes (potenciales)	Información obtenida vía formularios de contacto o eventos	- Marketing digital- Propuestas comerciales- Envío de información	Sí, con encargados de campañas o CRM

Tomado de *TEUNO*, 2024.

Consideraciones clave sobre la comunicación de datos:

- GRUPO BRAVCO S.A no realiza cesiones de datos sin consentimiento del titular, salvo que exista una base legal aplicable o mandato judicial.
- Cuando la información es comunicada a terceros, estos actúan en calidad de encargados del tratamiento, firmando contratos que incluyen cláusulas de confidencialidad, medidas de seguridad y límites en la reutilización de datos.
- Las comunicaciones internacionales de datos (si las hubiera) se realizan conforme a lo establecido en los artículos 17 y 18 de la LOPDP, garantizando un nivel de protección equivalente al ecuatoriano.

3.2.4. Encargados Del Tratamiento. En el marco de sus operaciones, GRUPO BRAVCO S.A contrata a terceros para realizar determinadas actividades que implican el acceso o tratamiento de datos personales en nombre de la organización. Estos terceros actúan en calidad de Encargados del tratamiento, y su relación está formalizada mediante contratos que incluyen cláusulas específicas de protección de datos, confidencialidad y medidas de seguridad.

A continuación, se identifican los principales encargados del tratamiento, el tipo de servicio que prestan, su ubicación y los datos personales que gestionan directa o indirectamente:

Tabla 9

Servicios que prestan los principales encargados del tratamiento de datos

Razón social	Localidad	Servicio prestado	Datos personales tratados
SecureData S.A.	Quito, Ecuador	Servicios de respaldo y almacenamiento en la nube	Datos identificativos, laborales, financieros y operativos de clientes, proveedores y trabajadores.

Razón social	Localidad	Servicio prestado	Datos personales tratados
ComWareTech S.A.	Guayaquil, Ecuador	Mantenimiento de infraestructura de red y servidores	Acceso indirecto a datos laborales y de clientes
CorpCloud Hosting S.A.	Quito, Ecuador	Hosting del sitio web institucional y plataforma CRM	Datos de contacto de clientes y prospectos
Asesores Legales y DPO Asociados	Quito, Ecuador	Consultoría legal y soporte como delegado externo de protección de datos	Datos sensibles, solicitudes de derechos de titulares
TactiKall S.A.	Quito, Ecuador	Contact center – atención a usuarios	Nombres, correos, teléfonos, historial de atención
Logiscan Cía. Ltda.	Quito, Ecuador	Digitalización y archivo de documentos físicos	Contratos, consentimientos firmados, documentos de RRHH

Tomado de *TEUNO*, 2024.

Observaciones importantes:

- Todos los encargados están obligados por contrato a cumplir con la LOPDP y las políticas internas de seguridad de GRUPO BRAVCO S.A
- GRUPO BRAVCO S.A realiza evaluaciones periódicas a sus encargados en materia de cumplimiento de seguridad de la información y protección de datos.
- En caso de subcontratación por parte del encargado, este debe informar previamente a GRUPO BRAVCO S.A y obtener autorización formal, garantizando que el nuevo subencargado cumpla con las mismas condiciones de seguridad y confidencialidad.

3.3.Registro de dispositivos digitales

Como parte del cumplimiento de los principios de seguridad, responsabilidad proactiva y minimización de riesgos, GRUPO BRAVCO S.A mantiene un registro actualizado de los dispositivos digitales que intervienen en el tratamiento de datos personales.

Este registro incluye tanto activos físicos como plataformas digitales (software o servicios en la nube) que se utilizan de forma directa o indirecta en operaciones que implican el acceso, almacenamiento, procesamiento o transmisión de información personal o sensible.

a) Dispositivos móviles corporativos

GRUPO BRAVCO S.A asigna dispositivos móviles (laptops, tablets y teléfonos inteligentes) a ciertos colaboradores que requieren acceso a sistemas corporativos desde fuera de las instalaciones.

Controles aplicados:

- Registro individual de cada equipo entregado, con código interno, número de serie y responsable.
- Instalación obligatoria de antivirus, herramientas de gestión remota (MDM) y cifrado de disco.
- Acceso a plataformas sensibles únicamente a través de VPN y autenticación multifactor (MFA).
- Políticas claras de uso seguro, pérdida o robo, respaldadas por acuerdos firmados.

Ejemplo de datos tratados: Correos electrónicos, contactos, archivos de clientes, accesos a CRM y ERP.

b) Plataforma CRM

El CRM corporativo es un sistema en la nube utilizado para gestionar la relación con clientes actuales y potenciales, así como campañas comerciales y de soporte.

Controles aplicados:

- Acceso autenticado con doble factor y por perfiles de usuario.
- Registro de actividad por usuario.
- Copias de seguridad automatizadas.
- Registro de terminales autorizadas.

Ejemplo de datos tratados:

Nombres, correos electrónicos, historial comercial, registros de atención, formularios web.

c) Correo electrónico corporativo

Es uno de los canales principales de interacción interna y externa, y por tanto es considerado un activo crítico para la organización.

Controles aplicados:

- Control de acceso vía credenciales seguras y MFA.
- Herramientas de protección contra malware, phishing y adjuntos maliciosos.
- Integración con herramientas DLP (Data Loss Prevention).
- Restricción de reenvío a correos personales o dominios no corporativos.

Ejemplo de datos tratados:

Datos personales y corporativos en contenido libre, envío de contratos, confirmaciones de pago, gestión de solicitudes de derechos.

d) Registro general de activos digitales

GRUPO BRAVCO S.A mantiene un inventario consolidado y gestionado por el área de Tecnología, en coordinación con la Oficial de Seguridad de la Información. Este inventario incluye:

Tabla 10
Registro general de activos digitales

Tipo de Activo	Cantidad Estimada	Activos	Propósito	Responsable
Laptops corporativas	300 unidades	Lenovo, HP ProBook	Actividades laborales, Trabajo remoto, acceso a ERP y CRM	Colaboradores asignados
Smartphones corporativos	200 unidades	Samsung A32, Motorola, Xiaomi	Comunicación corporativa, soporte, correo	Colaboradores asignados
Servidores físicos	10 unidades	HP ProLiant DL360 / DL380 G8-G10	Gestión de aplicaciones internas y bases de datos	Área de TI y Seguridad
Equipos de red (switches, routers, APs)	200+ dispositivos	Cisco, Meraki, HP	Comunicación de datos, conectividad segura, Renta de Equipos	Área de TI
Cámaras de videovigilancia	50 unidades	Cámaras IP tipo bala y domo	Seguridad física, control de accesos	Seguridad física corporativa
Sistemas de almacenamiento (NAS/SAN)	4 unidades	Sistemas de almacenamiento redundante	Respaldo seguro de datos empresariales	Área de TI y Respaldo
Equipos de respaldo de energía (UPS)	15 unidades	UPS APC, Eaton	Alimentación continua a servidores y sistemas críticos	Área de TI

Tomado de *TEUNO*, 2024.

- Todos los activos están identificados mediante etiquetas de inventario con número de serie.
- La administración de activos sigue las políticas definidas en la Política de Seguridad de la Información y en el Procedimiento de Gestión de Activos.

- Se realizan auditorías internas periódicas para validar la existencia física, el estado y la correcta asignación de los activos.

Este control y trazabilidad de dispositivos permite a GRUPO BRAVCO S.A mantener una visión completa de su superficie de tratamiento digital, asegurando que cada punto de acceso a datos personales esté protegido, auditado y correctamente asignado.

3.4.Registro De Sistemas De Información (Software y Seguridad)

Como parte del cumplimiento de la LOPDP y del marco de ciberseguridad corporativa definido por GRUPO BRAVCO S.A, la organización mantiene un registro centralizado y actualizado de todos los sistemas de información utilizados para el tratamiento de datos personales.

Este registro incluye sistemas operativos, aplicaciones de negocio, software de productividad, herramientas de comunicación y soluciones de seguridad, con el fin de garantizar un tratamiento seguro y conforme a las políticas internas de protección de datos.

a) Sistemas de Información Corporativos

Tabla 11

Sistemas de información corporativos

Nombre del sistema	Funcionalidad principal	Tipo de licenciamiento	Área responsable
ERP Empresarial	Gestión contable, nómina, RRHH, proveedores	Comercial/licencia activa	Finanzas / RRHH
CRM en la nube (ej: Dynamics)	Gestión de relaciones con clientes, seguimiento de ventas	Comercial (SaaS)	Dirección Comercial

Nombre del sistema	Funcionalidad principal	Tipo de licenciamiento	Área responsable
Microsoft 365	Correo electrónico, Teams, Office, OneDrive	Licencia empresarial activa	Todas las áreas
Antimalware corporativo	Protección contra virus, malware, spyware	Licencia activa (ESET Endpoint Security / Bitdefender)	Tecnología / Seguridad
Firewall perimetral	Control de tráfico externo e interno	Appliance con soporte activo	Tecnología
Software de respaldo (cloud)	Backups automatizados y recuperación ante desastres	Licencia comercial (cloud)	Tecnología
Herramienta DLP	Prevención de pérdida de datos sensibles	Incluido en solución M365 o Endpoint	Seguridad de la Información

Tomado de *TEUNO*, 2024.

b) Seguridad aplicada a nivel de software

Antivirus / Endpoint Protection

GRUPO BRAVCO S.A utiliza antivirus con licencia comercial activa, tales como ESET Endpoint Security o Bitdefender GravityZone Business Security, con administración centralizada. Está instalado en todos los dispositivos corporativos (PCs, laptops y móviles empresariales). Se encuentra configurado para realizar:

- Escaneo automático de unidades y archivos.
- Análisis en tiempo real de procesos sospechosos.
- Actualización automática de firmas.
- Bloqueo de conexiones maliciosas.

No se utilizan versiones ilegítimas ni de prueba (trial). Toda solución está formalmente contratada, auditada y bajo mantenimiento.

Firewall perimetral y de red

GRUPO BRAVCO S.A opera con firewalls de próxima generación (NGFW) en su red principal. Las funciones implementadas incluyen:

- Filtrado por IP, puerto, protocolo y aplicación.
- Prevención de intrusiones (IPS).
- Segmentación de red (DMZ, VLANs).
- VPN segura para usuarios remotos.

Algunos dispositivos cuentan con firewalls locales activos.

Seguridad en dispositivos individuales

Todos los equipos tienen activado:

- Cifrado de disco (BitLocker o solución equivalente).
- Bloqueo automático de sesión por inactividad.
- Control de puertos USB (según perfil de usuario).
- Herramientas de gestión remota (MDM) para borrado o localización en caso de pérdida o robo.

Las actualizaciones del sistema operativo y de seguridad son automáticas.

Correo y productividad (Microsoft 365)

Se emplean filtros antispam y antiphishing. Se configura con autenticación multifactor (MFA). Incluye herramientas de DLP, cifrado de correos y políticas de retención. Acceso solo desde dispositivos autorizados.

c) Evaluación y seguimiento

- Todos los sistemas están registrados en un inventario de activos digitales, gestionado por el área de Tecnología, auditado por la Oficial de Seguridad de la Información.
- Se realizan evaluaciones de vulnerabilidades periódicas, así como actualizaciones de seguridad planificadas.

3.5. Registro De Personal

3.5.1. Personal con acceso a datos personales. GRUPO BRAVCO S.A ha definido y documentado una matriz de acceso a datos personales por departamentos, conforme al rol que cada unidad desempeña dentro de la organización. El acceso está controlado a través del Directorio Activo, perfiles definidos por rol, y autorizaciones validadas por los propietarios de perfil y el Oficial de Seguridad de la Información, según el procedimiento vigente.

A continuación, se presenta el registro de personal y acceso a datos por unidad organizativa:

Tabla 12

Registro de personal y acceso de datos por unidad organizativa

Departamento	Puestos o roles	Tipo de datos personales accedidos	Observaciones
Talento Humano	Jefe de Talento Humano, Analista de RRHH	Identificativos, laborales, de contacto, datos de salud, familiares	Acceden para procesos de selección, nómina, evaluación, beneficios y bienestar.
Finanzas y Contabilidad	Contador general, Analistas contables	Datos financieros, bancarios, datos tributarios	Acceden solo a información económica de empleados, clientes y proveedores.

Departamento	Puestos o roles	Tipo de datos personales accedidos	Observaciones
Dirección Comercial	Jefes de cuentas, asesores comerciales, soporte comercial	Datos identificativos y de contacto de clientes y prospectos	Acceden vía CRM para gestión de relaciones comerciales y soporte.
Soporte Técnico / IT	Técnicos de infraestructura, soporte interno	Información técnica, registros de actividad, acceso a sistemas	No acceden al contenido de los datos, pero sí al entorno donde residen.
Oficial de Seguridad de la Información	Oficial designado	Datos sensibles, logs de acceso, trazabilidad, todo tipo de información	Tiene privilegios para revisar, auditar y validar el cumplimiento normativo.
Gerencia General	Gerente General, Dirección Estratégica	Acceso bajo demanda a reportes consolidados con información agregada	No acceden de forma operativa a sistemas con datos personales individuales.
Área Legal / DPO externo	Consultores de protección de datos y asesores legales	Datos sensibles, registros de consentimientos, solicitudes de titulares	Solo acceden en procesos de cumplimiento, auditorías o gestión de derechos.

Tomado de *TEUNO*, 2024.

Principios aplicados:

- **Mínimo privilegio:** cada usuario accede solo a los datos necesarios para su función.
- **Segregación de funciones:** ninguna persona tiene control completo de la recolección, uso y eliminación de datos.
- **Revisión periódica:** la Matriz de Perfiles y Accesos es actualizada bajo demanda y auditada por el Oficial de Seguridad.

3.5.2. Personal sin acceso a datos personales. Dentro de la estructura organizativa de GRUPO BRAVCO S.A, existen perfiles operativos o de soporte cuya función no implica el acceso directo a datos personales. Sin embargo, es importante identificarlos y registrarlos, ya que, en ciertos escenarios, podrían tener exposición indirecta a información confidencial (por ejemplo, al ingresar a oficinas o manipular equipos).

Este grupo de colaboradores no tiene acceso autorizado a sistemas de información, directorios, bases de datos, ni plataformas digitales en las que se trate información personal de clientes, empleados o terceros. A continuación, se presenta una tabla de referencia por área y función:

Tabla 13

Área y funciones de colaboradores

Departamento / Área	Puestos o funciones	Tipo de datos a los que pueden estar expuestos	Observaciones
Mantenimiento	Técnicos de mantenimiento eléctrico, HVAC	Ninguno directo. Exposición indirecta a documentos en escritorios o pantallas	Se limitan los accesos a oficinas con información visible.
Transporte / Logística	Conductores, mensajeros internos	Datos de contacto impresos en sobres o paquetes	Se aplica política de entrega sellada, no manipulan información interna digital.
Limpieza	Personal de limpieza interno o tercerizado	Exposición física incidental a documentos o dispositivos	Supervisión de accesos fuera del horario laboral y política de escritorio limpio.

Seguridad física	Guardias de vigilancia y seguridad privada para el control de ingreso a instalaciones, según los puestos de servicio contratados.	Listados de visitantes, cámaras de videovigilancia	Acceso restringido a monitoreo, sin capacidad de exportar ni procesar información. Acceso a bitácoras y hojas de registro de visitantes, trabajadores, proveedores, vehículos y bienes.
Cafetería / Apoyo interno	Auxiliares de cocina o servicios generales	Ninguno	No tienen acceso a áreas administrativas con información.

Tomado de *TEUNO*, 2024.

Medidas de control aplicadas:

- **Restricción de acceso físico** a oficinas administrativas o áreas donde se gestionan datos personales.
- **Política de "escritorio limpio"** para evitar exposición accidental de documentos.
- **Capacitación básica en confidencialidad**, aplicable incluso a personal subcontratado.
- **Supervisión y acompañamiento** en tareas de mantenimiento o limpieza en zonas críticas.
- **Control de ingreso y permanencia** a través de registros de seguridad y accesos físicos.

Este tipo de identificación y segmentación del personal permite a GRUPO BRAVCO S.A aplicar el principio de "necesidad de conocer" y fortalecer el enfoque preventivo en el tratamiento de datos personales, incluso en funciones que no están directamente relacionadas con sistemas de información.

3.5.3. Accesos físicos. La protección de los datos personales no solo depende de los sistemas tecnológicos, sino también del control físico de los espacios donde se almacenan, procesan o consultan dichos datos. GRUPO BRAVCO S.A ha implementado medidas para asegurar que únicamente el personal autorizado pueda acceder a oficinas, salas de servidores, archivos y otras áreas sensibles.

A continuación, se identifica qué tipo de personal tiene acceso físico y mediante qué mecanismos:

a) Accesos con llaves físicas, tarjetas o credenciales electrónicas

Tabla 14

Accesos con llaves físicas o credenciales electrónicas

Área / Oficina	Quién tiene acceso	Medio de acceso	Observaciones
Oficina administrativa (área general)	Todo el personal de planta con funciones administrativas	Tarjeta electrónica o llave	Control por horarios laborales y supervisión de ingreso.
Sala de servidores / rack de red	Equipo de Tecnología y Oficial de Seguridad	Llave física + tarjeta restringida	Acceso bajo control y registro en bitácora física o digital.
Archivo físico de contratos / RRHH	Talento Humano, Oficial de Seguridad	Llave bajo custodia de RRHH	Archivos clasificados, acceso supervisado.
Oficina de Gerencia / Legal	Gerente General, DPO externo (previa coordinación)	Tarjeta electrónica	Documentos con información estratégica y datos sensibles.
Bodega de TI / almacenamiento equipos	Técnico de soporte, Especialista de producto	Llave bajo resguardo del área TI	Control de inventario y bitácora de retiro de equipos.
Sala de reuniones ejecutiva	Alta dirección y personal administrativo	Tarjeta o acceso programado	Reservas de uso con control en sistema interno.

Áreas comunes / Cafetería / Baños	Todo el personal y personal externo autorizado	Libre acceso durante horario laboral	Sin tratamiento de datos, pero bajo vigilancia física (circuito cerrado).

Tomado de *TEUNO*, 2024.

b) Procedimientos aplicables

- Todo acceso a áreas restringidas debe estar autorizado por el propietario del área y documentado.
- Las llaves físicas están bajo custodia responsable (**firmadas** en inventario o bitácora).
- Las tarjetas electrónicas son administradas por el área de Tecnología o Seguridad Física, según corresponda.
- El personal de limpieza, mantenimiento o terceros requiere acompañamiento o ingreso programado a zonas sensibles.
- Las cámaras de videovigilancia permiten monitoreo y respaldo del cumplimiento de las políticas de acceso.

c) Medidas complementarias

- Registro de ingresos/salidas para visitantes y terceros.
- Cierre automatizado o con alarma en áreas sensibles fuera de horario.
- Aplicación del principio de "**acceso mínimo necesario**" también a espacios físicos.

Esta segmentación de accesos físicos contribuye a reducir la exposición accidental o no autorizada a datos personales, reforzando las medidas de seguridad organizacional tanto en lo digital como en lo físico.

3.6.Registro de prestadores de servicio

3.6.1. Con acceso a datos catalogados. Está enfocado en aquellos terceros o profesionales externos que, si bien acceden a datos personales, lo hacen únicamente dentro del marco de su función, bajo criterios de confidencialidad y sin posibilidad de uso indebido.

GRUPO BRAVCO S.A contrata determinados prestadores de servicio externos (personas naturales o jurídicas) para el desarrollo de funciones técnicas, profesionales o especializadas. Algunos de estos servicios requieren, por su naturaleza, el acceso a datos personales catalogados, tales como identificativos, laborales, de salud o financieros.

Este acceso debe estar justificado por la necesidad operativa, y el tratamiento de datos debe limitarse estrictamente a la finalidad específica, sin permitir su divulgación, reutilización ni transferencia no autorizada.

A continuación, se presenta una tabla con los principales prestadores externos que acceden a este tipo de información, el tipo de datos que utilizan y las restricciones aplicadas:

Tabla 15

Prestadores Externos

Profesional / Servicio contratado	Finalidad / Actividad	Tipo de datos accedidos	Condición de acceso
Médico ocupacional (externo)	Valoraciones médicas de ingreso, seguimiento de salud laboral	Datos personales, historia médica, certificados	Uso exclusivo para evaluar aptitud. No comparte ni almacena fuera del informe.
Delegado de Protección de Datos	Análisis de casos, auditorías, gestión de derechos de titulares	Datos sensibles, solicitudes legales, consentimientos	Acceso limitado a documentos específicos. Firma acuerdo de confidencialidad.

Profesional / Servicio contratado	Finalidad / Actividad	Tipo de datos accedidos	Condición de acceso
Auditor externo de sistemas	Evaluación de seguridad informática y cumplimiento normativo	Logs de actividad, accesos, usuarios de sistemas	Accede a través de entornos controlados. No extrae datos fuera del análisis.
Consultor técnico en ERP o CRM	Configuración o mantenimiento de sistemas empresariales	Información transaccional, datos identificativos	Acceso temporal y limitado, bajo control del área de Tecnología.

Tomado de *TEUNO*, 2024.

Medidas de control implementadas:

- Todos los prestadores con acceso a datos catalogados firman cláusulas de confidencialidad o contratos con anexos de protección de datos, en cumplimiento de la LOPDP.
- El acceso se realiza bajo el principio de necesidad funcional y con controles de tiempo, entorno y privilegios mínimos.
- En algunos casos, se proporciona acceso supervisado o restringido a ciertos módulos del sistema, sin posibilidad de copia o exportación.
- Se mantiene un registro actualizado de los profesionales autorizados, fechas de acceso, duración del vínculo y responsable interno de supervisión.

Esta práctica garantiza que el uso de datos por parte de prestadores se mantenga dentro del marco de la legalidad, la confidencialidad y la seguridad, evitando cualquier exposición indebida de información sensible o crítica.

3.6.2. Sin acceso a datos catalogados. Dentro de los servicios contratados por GRUPO BRAVCO S.A, existen proveedores externos cuya labor no requiere el tratamiento de datos personales ni el acceso a sistemas de información, pero que, por su presencia física o remota en entornos operativos, podrían exponerse accidentalmente a información sensible.

Aunque no se les habilita acceso formal, la organización aplica controles físicos, técnicos y organizativos para asegurar que este tipo de personal no tenga posibilidad real de tratar, visualizar o extraer información protegida.

Tabla 16

Prestadores de servicios sin acceso a datos catalogados

Profesional / Empresa contratada	Finalidad / Actividad	Tipo de acceso otorgado	Observaciones
Empresa de limpieza	Limpieza de oficinas, áreas comunes y administrativas	Acceso físico supervisado	No manipulan documentación ni sistemas. Firmas de confidencialidad aplican.
Empresa de mantenimiento de impresoras	Revisión técnica de hardware (in situ o remota)	Acceso técnico limitado	No visualizan archivos ni tienen acceso a la red más allá del dispositivo.
Proveedor de aire acondicionado	Mantenimiento de infraestructura	Acceso físico programado a zonas técnicas	Ingreso bajo solicitud y acompañamiento. Sin contacto con datos ni documentos.
Técnico de mantenimiento eléctrico	Instalaciones eléctricas generales	Acceso a áreas técnicas o de soporte	Acceso coordinado. Sin manipulación de equipos informáticos ni archivadores.
Servicios de catering / cafetería	Alimentación para el personal	Libre circulación en zonas comunes	Sin contacto con oficinas ni dispositivos con información.

Profesional / Empresa contratada	Finalidad / Actividad	Tipo de acceso otorgado	Observaciones
Proveedor de mobiliario / mudanza interna	Movimiento de escritorios, sillas, equipos	Ingreso controlado, con personal de TI	No tienen acceso a plataformas ni se les permite manipular documentos.
Personal de mensajería externa	Entrega o recepción de documentos y paquetes	Ingreso a recepción	No acceden a información interna. Todo se entrega cerrado y con firma de recibo.

Tomado de *TEUNO*, 2024.

Controles aplicados:

- **Acompañamiento obligatorio** por parte del personal interno en caso de ingreso a zonas administrativas.
- **Accesos físicos limitados** por horario, espacio y autorización previa.
- **En caso de soporte remoto** (como impresoras), acceso controlado a través de sesiones seguras, sin acceso a archivos de usuarios.
- **Firma de acuerdos de confidencialidad** o políticas de conducta para terceros, cuando sea necesario.
- **Aplicación de la política de escritorio limpio** y almacenamiento seguro de documentación en oficinas que reciben este tipo de servicios.

El principio aplicado en estos casos es “cero acceso a datos personales”, incluso de forma accidental. Por ello, la empresa estructura protocolos de prevención y mantiene un registro de proveedores externos sin exposición permitida a información protegida.

3.7.Sistemas De Captación De Imágenes Y Audio

GRUPO BRAVCO S.A dispone de un sistema de videovigilancia interna, implementado como medida de seguridad preventiva para proteger la integridad de las personas, los activos físicos y la información contenida en sus instalaciones. Este sistema también permite responder ante incidentes de seguridad, accidentes laborales o accesos no autorizados.

3.7.1. Número de cámaras. Actualmente, GRUPO BRAVCO S.A cuenta con un total de 16 cámaras de videovigilancia activas distribuidas en sus instalaciones corporativas, según el siguiente detalle:

Tabla 17

Números de cámaras en la organización

Ubicación	Cantidad de cámaras	Cobertura principal
Planta baja	4	Recepción, entrada principal, sala de espera, acceso a parqueadero
Primer piso	4	Áreas administrativas, pasillos, escaleras
Segundo piso	4	Oficinas técnicas, salas de reuniones, pasillos
Tercer piso	2	Oficina gerencial y acceso a archivo
Parqueaderos	2	Control de vehículos, ingreso y salida del personal

Tomado de *TEUNO*, 2024.

Características del sistema de videovigilancia

- Las cámaras son del tipo CCTV digital con grabación continua (DVR/NVR).
- El sistema no cuenta con grabación de audio, en cumplimiento de la LOPDP.

- Las imágenes son conservadas por un período de 15 días antes de ser sobrescritas automáticamente, salvo que exista una solicitud legal o investigación interna que justifique su conservación adicional.
- El sistema es monitoreado por el equipo de Seguridad Física y supervisado por la Oficial de Seguridad de la Información, en coordinación con la administración general.

Medidas de cumplimiento legal

- Existen avisos visibles en puntos estratégicos que informan sobre la existencia de cámaras de videovigilancia, de acuerdo con el principio de transparencia de la LOPDP.
- Las imágenes captadas no se comparten con terceros salvo requerimiento judicial o por razones de seguridad debidamente justificadas.
- El sistema de videovigilancia se encuentra documentado en el Registro de Actividades de Tratamiento (RAT) como un tratamiento de datos personales con fines de seguridad física.

3.7.2. Zonas De Influencia. Las zonas de influencia del sistema de videovigilancia de GRUPO BRAVCO S.A comprenden las áreas comunes, puntos de acceso y zonas operativas sensibles, con el objetivo de garantizar la seguridad física del personal, visitantes, instalaciones y activos tecnológicos.

A continuación, se presenta la distribución de cámaras por zonas específicas dentro de la infraestructura:

Tabla 18

Zonas de influencia

Zona / Espacio	Cantidad de cámaras	Observaciones sobre cobertura
Recepción principal (PB)	1	Control visual de ingreso de personal y visitantes.
Sala de espera (PB)	1	Supervisión de presencia de terceros en espera.
Pasillo planta baja (PB)	1	Cubrimiento de circulación entre recepción y oficinas administrativas.
Acceso parqueadero (PB)	1	Vigilancia del ingreso y salida vehicular y peatonal desde exteriores.
Pasillos primer piso	2	Control de tránsito entre oficinas de administración y contabilidad.
Oficinas administrativas	1	Visual general del área de trabajo abierta.
Escaleras internas (1er piso)	1	Control de movimiento vertical entre pisos.
Pasillos segundo piso	2	Cobertura de tránsito hacia salas técnicas y reuniones.
Salas de reuniones (2do piso)	1	Visualización de ingreso. No hay grabación continua dentro de las salas.
Oficinas técnicas	1	Supervisión de equipos y personal técnico.
Acceso archivo físico (3er piso)	1	Control del ingreso al área de documentación confidencial.
Oficina gerencia	1	Solo vigilancia de ingreso desde pasillo externo. No hay cámara interna.
Parqueadero lateral / externo	2	Supervisión de vehículos, puntos ciegos y acceso de servicios.

Tomado de *TEUNO*, 2024.

De las 16 cámaras activas, 13 se encuentran en áreas cubiertas como accesos, circulación, áreas comunes, zonas técnicas, archivo y parqueadero.

Consideraciones de cumplimiento:

- Las cámaras no están instaladas en baños, comedores ni áreas de descanso, respetando el derecho a la privacidad de los colaboradores.
- El sistema cumple con el principio de proporcionalidad y minimización, limitando la captación al ámbito estrictamente necesario para la finalidad de seguridad física.

3.7.3. Sistema De Tratamiento Y Almacenamiento. El sistema de videovigilancia instalado en las instalaciones de GRUPO BRAVCO S.A opera de manera automatizada, y su funcionamiento está orientado exclusivamente al control de accesos físicos, monitoreo de seguridad, prevención de incidentes y apoyo en situaciones de emergencia.

a) Automatización del sistema

- El sistema es 100% automatizado, no depende de operadores para la grabación de imágenes.
- Las cámaras están conectadas a un sistema NVR (Network Video Recorder) centralizado.
- Las grabaciones se inician de forma automática al encender el sistema y operan bajo programación 24/7 (grabación continua).
- Algunas cámaras cuentan con detección de movimiento para optimizar almacenamiento.

b) Sistema de almacenamiento

Tabla 19

Sistema de almacenamiento del sistema de vigilancia

Parámetro	Detalle
Tipo de grabación	Video digital continuo, sin audio
Almacenamiento	Unidad de disco duro (HDD) en servidor NVR local, no en la nube
Formato	Archivos digitales de video (ej. .mp4, .avi) con codificación por fecha y hora
Ubicación física del servidor	Sala técnica cerrada con acceso restringido
Capacidad de almacenamiento	Aproximadamente 15 días de grabación continua por cámara, antes de sobrescribir
Respaldo en la nube	No aplica. Las grabaciones se almacenan localmente por seguridad y control
Control de acceso a grabaciones	Solo el Oficial de Seguridad y personal autorizado de TI pueden acceder
Acceso remoto	No habilitado. Solo visualización local, no hay monitoreo externo ni por app

Tomado de *TEUNO*, 2024.

c) Integridad y trazabilidad

- Todas las grabaciones cuentan con marcas de tiempo (fecha, hora) generadas por el sistema.
- El NVR está configurado para impedir la manipulación o edición de videos por personal no autorizado.
- Se mantiene una bitácora de visualizaciones y copias de respaldo, en caso de ser necesarias para fines legales o internos.

d) **Eliminación automática**

- Las imágenes son sobrescritas automáticamente una vez alcanzado el ciclo de retención definido (15 días).
- Si un video debe conservarse (por ejemplo, por solicitud legal), se realiza una copia forense controlada y registrada, almacenada temporalmente bajo cadena de custodia.

Este modelo de tratamiento cumple con los principios de minimización, limitación de finalidad y seguridad del tratamiento, evitando el uso excesivo o indebido del sistema de captación de imágenes.

3.7.4. Usuarios Autorizados. En cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), GRUPO BRAVCO S.A ha definido un grupo restringido y controlado de usuarios autorizados para el acceso a las imágenes captadas por el sistema de videovigilancia.

El acceso se encuentra limitado exclusivamente a personas cuyas funciones laborales requieren monitorear, consultar o gestionar evidencias de videovigilancia, dentro del marco de sus responsabilidades y bajo el principio de confidencialidad y necesidad.

a) **Lista de usuarios autorizados para acceso a imágenes**

Tabla 20

Lista de usuarios autorizados para acceso a imágenes

Cargo / Área	Motivo del acceso autorizado	Nivel de acceso
Oficial de Seguridad de la Información	Supervisión de seguridad física, auditoría de incidentes	Acceso total al sistema y grabaciones
Jefe de Seguridad / Personal de vigilancia	Monitoreo en tiempo real para prevención y respuesta a incidentes	Acceso a visualización en tiempo real (no edición ni copia)

Cargo / Área	Motivo del acceso autorizado	Nivel de acceso
Jefe de Talento Humano	Verificación de reportes disciplinarios, control de asistencia visual	Acceso bajo solicitud formal y supervisión del Oficial de Seguridad
Gerente General / Dirección	Acceso en casos excepcionales con fines legales, administrativos o estratégicos	Acceso bajo autorización por escrito y acompañamiento
Área Legal o DPO externo	Análisis de incidentes que impliquen responsabilidad legal o derechos de los titulares	Acceso a evidencias bajo protocolo y cadena de custodia

Tomado de *TEUNO*, 2024.

b) Condiciones de acceso

- El acceso a grabaciones no es libre ni permanente. Se realiza previa solicitud documentada, a través de un formato interno o correo validado.
- Toda visualización o extracción de video debe quedar registrada en una bitácora de acceso, indicando:
    - Fecha y hora de consulta
    - Usuario autorizado
    - Motivo
    - Fragmento o cámara consultada
- Las copias de respaldo solo pueden ser generadas por el Oficial de Seguridad de la Información.

c) Prohibiciones expresas

- Ningún otro personal de GRUPO BRAVCO S.A, ni externo (como limpieza, soporte, etc.) tiene acceso al sistema de videovigilancia.

- Está prohibido:
    - Compartir grabaciones por medios no autorizados.
    - Reproducir imágenes para fines no relacionados con seguridad.
    - Divulgar imágenes sin autorización legal.

Este control estricto sobre los usuarios autorizados permite garantizar el cumplimiento del principio de confidencialidad y la protección de los derechos de los titulares que pudieran ser captados por las cámaras instaladas.

3.8. Dispositivos. Medidas de seguridad

3.8.1. Análisis De Las Medidas De Seguridad De Los Dispositivos. En la organización GRUPO BRAVCO S.A, los dispositivos tecnológicos (como estaciones de trabajo, laptops, servidores y equipos de red) forman parte esencial de los procesos de negocio y del tratamiento de información confidencial y/o personal. Para proteger estos activos, se implementan diversas medidas técnicas y organizativas, alineadas con buenas prácticas internacionales (ISO 27001, CIS Controls) y la Ley Orgánica de Protección de Datos Personales (LOPDP).

Entre las principales medidas implementadas destacan:

- **Gestión de accesos basada en el principio de mínimos privilegios**: Cada usuario tiene acceso únicamente a los recursos necesarios para su función, conforme al proceso de Gestión de Accesos.
- **Autenticación de usuarios**: Todos los dispositivos están integrados al Directorio Activo, requiriendo credenciales personales, seguras y renovables para iniciar sesión.

- **Segmentación de red mediante VLANs**: Los dispositivos están agrupados por función y nivel de acceso, lo que reduce el riesgo de propagación de amenazas entre áreas sensibles.
- **Control de acceso físico a los equipos críticos**: Se regula estrictamente el ingreso al Cuarto de Equipos mediante autorizaciones previas, registro en bitácoras y acompañamiento de personal técnico, incluyendo control en fines de semana y fuera de horario laboral.
- **Inventariado de equipos y control por MAC address**: Cada dispositivo es identificado y asignado en el sistema DHCP, permitiendo rastrear accesos a la red y prevenir intrusiones no autorizadas.
- **Política de contraseñas seguras**: Se aplican normas de complejidad y renovación periódica de contraseñas, con especial énfasis en cuentas privilegiadas.
- **Desactivación inmediata de accesos tras desvinculación del personal**: Como parte del proceso de gestión de accesos, se deshabilitan cuentas y accesos a dispositivos al momento de la salida del colaborador.

3.8.2. Propuesta de mejora de las medidas de seguridad. Si bien GRUPO BRAVCO S.A ha implementado medidas robustas, se identifican áreas de mejora con base en una evaluación preventiva de riesgos tecnológicos:

1. **Implementación de cifrado de disco completo (BitLocker o similar)** en laptops y dispositivos móviles, para garantizar la confidencialidad de la información en caso de pérdida o robo.

2. **Refuerzo de la gestión de dispositivos móviles (MDM)** para asegurar el cumplimiento de políticas corporativas, especialmente en teletrabajo o acceso remoto.
3. **Monitoreo centralizado y automatizado de eventos de seguridad en endpoints (EDR)** para la detección y respuesta rápida ante amenazas o comportamientos anómalos.
4. **Auditoría regular del inventario de hardware y software**, verificando que los dispositivos estén actualizados y cumplan con los requisitos mínimos de seguridad.
5. **Capacitación continua a los usuarios sobre el uso seguro de los dispositivos** y medidas preventivas ante amenazas como phishing, malware y uso indebido de recursos.
6. **Evaluación de implementación de políticas de uso de USB restringido** para reducir el riesgo de fuga de datos y malware por medios físicos.

3.9.Puestos De Trabajo

3.9.1. Análisis De Las Medidas De Seguridad De Cada Puesto De Trabajo, Según La Información Tratada.

En GRUPO BRAVCO S.A, los puestos de trabajo se clasifican de acuerdo con el nivel de acceso a información sensible, crítica o confidencial. Las medidas de seguridad implementadas se ajustan al tipo de información tratada y al rol del colaborador:

Medidas generales para todos los puestos:

- **Acceso controlado mediante usuario y contraseña personal**, asociado a roles definidos y aprobados por Gerencias o Jefaturas, conforme al proceso de Gestión de Accesos.

- **Política de escritorio limpio**: se exige que los documentos físicos con información sensible sean resguardados adecuadamente, y que las sesiones de los dispositivos se bloqueen al ausentarse del puesto.
- **Monitoreo del uso de dispositivos**: se controlan los accesos a sistemas y red mediante herramientas de gestión de tickets, directorios activos, y control de logs.
- **Perfiles definidos por función**: el acceso a sistemas o carpetas compartidas depende del perfil asignado en función del cargo. Estos perfiles están definidos en la Matriz de Perfiles y Accesos actualizada por el Oficial de Seguridad de la Información.
- **Ubicación física segura**: los equipos que tratan información crítica se encuentran en áreas con control de acceso físico, como el Cuarto de Equipos, regulado mediante bitácoras, registros y acompañamiento.

Medidas específicas por tipo de puesto:

Tabla 21

Medidas específicas por tipo de puesto

Tipo de Puesto	Medidas específicas aplicadas
Administrativo	Acceso a VLAN 40 o 20 según conexión (Wi-Fi o cable). Software básico de gestión. Control de acceso mediante contraseña.
Técnico TI / Soporte	VLAN 40/99. Accesos a herramientas especializadas, controlado por privilegios. Uso de cuentas individuales no compartidas.

Tipo de Puesto	Medidas específicas aplicadas
Usuarios con privilegios altos	Asignación basada en requerimiento aprobado y perfil documentado. Accesos monitoreados, con revisiones mensuales.
Visitantes o terceros	Acceso temporal con cuentas invitadas, control por portal cautivo, sin privilegios especiales.

Tomado de *TEUNO*, 2024.

3.9.2. Acuerdo De Confidencialidad. GRUPO BRAVCO S.A implementa acuerdos de confidencialidad formales, que deben ser firmados por todos los colaboradores, proveedores o terceros que acceden o tratan información sensible o datos personales. Este acuerdo establece:

ACUERDO DE CONFIDENCIALIDAD GRUPO BRAVCO S.A.

Suscriben el presente Convenio de confidencialidad, por una parte, la compañía **GRUPO BRAVCO S.A. (en adelante TEUNO)** y por otra parte **(Nombre del Trabajador)** por sus propios derechos, en adelante empelado o colaborador de TEUNO.

El objetivo mutuo de las partes contratantes de conformidad con el presente Convenio es brindar protección a la información confidencial (en adelante denominada Información).
Para efectos del presente convenio, el **Revelador** es TEUNO y el **Receptor** es el empleado o colaborador de TEUNO, el cual durante el desempeño de las actividades tendrá acceso a información confidencial perteneciente a TEUNO o a sus aliados estratégicos.

1. Revelación

Se revelará la información para efectos de mantener relaciones laborales contractuales presentes y futuras entre las partes; en cualquier caso, dicha revelación se realizará en función de

cumplir los objetivos de estructurar ofertas de servicios, realizar diagnósticos, cumplir el objeto de contratos presentes o futuros y afines, de cualquiera de las siguientes formas:

a) Por escrito.

b) A través de correo electrónico o cualquier medio digital.

c) Mediante entrega de obras literarias u otras obras de creación intelectual (como programas, listados de programas, herramientas de programación, documentación, informes, diagramas y obras similares) que el Revelador puede entregar al Receptor como parte de un servicio; o bien, listados, bases de datos y cualquier otro impreso o medio de información que el Revelador puede entregar al Receptor para recibir un servicio o adquirir bienes.

d) Al iniciarse el acceso a Información, la cual puede estar en una base de datos.

e) Mediante presentación oral o visual.

La información debe haber sido recibida por el Receptor, con constancia escrita o mediante correo electrónico de ello, y no debe estar marcada con una leyenda restrictiva del Revelador para ser considerada confidencial. La Información no debe estar marcada con esa leyenda y si se revela oralmente, el Revelador especificar por escrito o correo electrónico, el momento en que se reveló dicha información. Toda la Información revelada por el Revelador tendrá el carácter de confidencial.

2. Obligaciones

El **Receptor** acepta:

a) Tener con respecto a la Información del Revelador el mismo cuidado y discreción que el Revelador tiene para con la propia información clasificada en forma similar cuando ha de evitarse que se revele, publique o disemine esa Información.

b) Cumplir con lo dispuesto en la Ley Orgánica de Protección de Datos Personales y en general cumplir con la normativa relacionada, a la protección de datos personales y a las disposiciones de autoridades de control en la materia.

c) Utilizar la Información del Revelador únicamente con el objetivo con que se le reveló.

d) El Receptor que revele indebidamente información recibida, siendo este hecho legal y debidamente comprobado, será responsable frente al Revelador de los daños y perjuicios que le ocasione, sin perjuicio de otras responsabilidades de acuerdo con la ley.

e) Ni el presente Convenio ni la revelación de Información alguna que se haga en virtud de éste, otorga al Receptor derecho o licencia alguna de uso de cualquier marca, derecho de autor o patente que sean de propiedad del Revelador o que estén bajo control del Revelador, en la actualidad o en el futuro.

f) El Receptor puede revelar la Información en los siguientes casos:

- A los funcionarios, empleados, apoderados y dependientes bajo relación civil del Receptor que tengan la necesidad de conocerla y a los funcionarios, empleados, apoderados y dependientes bajo relación civil de toda persona o entidad jurídica que el Receptor controle, o que controle al Receptor, o que esté bajo un control común en

conjunto con el Receptor, cuando dichos empleados tengan la necesidad de conocerla y siempre que no constituya infracción a disposiciones legales sobre sigilo y reserva bancarios, que las partes declaran conocer y se obligan a preservar. El término Control se refiere a ser propietario, directa o indirectamente, de más del 50% de las acciones con derecho a voto o controlar dicho 50%.

- A terceros, previa autorización o delegación por escrito del Revelador.

Antes de revelar la Información a cualquiera de las partes enumeradas, el Receptor debe haberse asegurado que exista suscrito un convenio de confidencialidad entre TEUNO y dicha parte, el cual ha de ser suficiente para exigir a esa parte que trate la Información de conformidad con el presente Convenio.

El Receptor no puede revelar la Información sin autorización o delegación de TEUNO, debe reportar de inmediato a su inmediato superior respecto a la atención de pedidos de información formales, expresos y escritos de autoridades competentes y advertirle de que se debe dar aviso al tercero Revelador, en un máximo de 48 horas de haber recibido dicho requerimiento, de manera que éste tercero tenga oportunidad razonable para obtener una orden que proteja la Información, si lo creyera conveniente o necesario. En el caso de información sensible, el aviso de debería dar en un máximo de 12 horas contadas desde el momento de la recepción del requerimiento.

Protección de Datos Personales

El Receptor asume la obligación de proteger los datos personales a los que accedan con ocasión de cualquier contrato suscrito con el Revelador. Como consecuencia de esta obligación legal, entre

otras, deberán adoptar las medidas de seguridad de tipo lógico, administrativo y físico, acorde a la criticidad de la información personal a la que accede, para garantizar que este tipo de información no será usada, comercializada, cedida, transferida y/o no será sometida a cualquier otro tratamiento contrario a la finalidad comprendida en lo dispuesto en el objeto del presente Convenio o del Contrato laboral o de o servicios profesionales suscrito por las Partes.

TEUNO en cualquier momento puede verificar que el Receptor está cumpliendo esta obligación de protección de datos personales conforme los procedimientos y políticas de TEUNO.

Es obligación del Receptor informar a TEUNO respecto de cualquier sospecha de perdida, fuga o ataque contra la información personal a la que ha accedido y/o ha brindado tratamiento con ocasión de este Convenio de otros contratos suscritos por las Partes, aviso que deberá dar una vez tenga conocimiento de tales eventualidades.

El incumplimiento de las obligaciones derivadas de esta cláusula se considera como un incumplimiento grave por los riesgos legales que conlleva el indebido tratamiento de datos personales, y en consecuencia será considerada justa causa para la terminación del o de los contratos que mantengan suscritos las Partes y dará lugar al cobro una penalidad equivalente al menos al 10% del total del valor del contrato por cada incumplimiento, sin perjuicio de las acciones legales a las que haya lugar.

4. Finalidad y Uso de los Datos Personales del Trabajador

El Receptor (trabajador o colaborador) autoriza expresamente a TEUNO a recolectar, utilizar, almacenar y tratar sus datos personales para las siguientes finalidades:

Gestión administrativa y de recursos humanos.

Control de asistencia, horarios y desempeño laboral.

Administración de beneficios sociales y seguridad social.

Control de acceso físico a las instalaciones y acceso lógico a los sistemas corporativos.

Comunicación interna y publicaciones autorizadas en medios institucionales.

Cumplimiento de obligaciones fiscales, contables, legales y de auditoría.

Los datos personales serán tratados conforme a los principios de licitud, finalidad, proporcionalidad, minimización y seguridad previstos en la Ley Orgánica de Protección de Datos Personales (LOPDP).

Tiempo de Almacenamiento de los Datos Personales

Los datos personales proporcionados serán conservados durante la vigencia de la relación laboral o contractual y posteriormente por un periodo máximo de 15 años, para dar cumplimiento a obligaciones legales y regulatorias, salvo que el titular ejerza su derecho de cancelación en los casos en que proceda.

5. Ejercicio de Derechos ARCO (acceso, rectificación, cancelación y oposición)

El titular de los datos personales podría ejercer en cualquier momento sus derechos de:

Acceso

Rectificación

Actualización

Eliminación

Oposición

Portabilidad

Para ello, deberá dirigir su solicitud a través del correo electrónico: responsable_pdp@teuno.com, o por escrito ante el Oficial de Protección de Datos Personales de GRUPO BRAVCO S.A., siguiendo el procedimiento establecido en la Política de Protección de Datos Personales disponible en www.teuno.com.

6. Tratamiento de Datos Biométricos

Durante el proceso de implementación de nuevos sistemas de gestión, TEUNO podrá recolectar datos biométricos del trabajador (como huella digital, reconocimiento facial u otros) exclusivamente para:

Control de acceso físico a las instalaciones.

Registro de asistencia y control de horario laboral.

Tiempo de almacenamiento:

Estos datos biométricos serán almacenados de forma segura durante la vigencia de la relación laboral y hasta un máximo de 5 años después de su terminación, conforme a obligaciones legales de conservación.

Lugar de almacenamiento:

Los datos serán alojados en servidores protegidos de GRUPO BRAVCO S.A., bajo estrictas medidas de seguridad.

Ejercicio de derechos:

Los trabajadores podrán ejercer sus derechos ARCO respecto de sus datos biométricos en los mismos canales y condiciones indicados anteriormente.

Consentimiento para Uso de Imagen

En caso de captación de imágenes fotográficas o videográficas del trabajador con fines de difusión institucional (página web corporativa, redes sociales oficiales o campañas internas), se solicitará un consentimiento específico previo, informado y por escrito, respetando en todo momento el derecho a la privacidad del titular.

7. Entrega y Uso de Llaves de Instalaciones

En caso de que el trabajador reciba llaves físicas, electrónicas o dispositivos de acceso a las instalaciones de GRUPO BRAVCO S.A.:

Se compromete a custodiar estos dispositivos de manera personal e intransferible.

No podrá duplicar, transferir ni compartir su uso con terceros no autorizados.

Deberá notificar de inmediato cualquier pérdida, robo o daño de las llaves o dispositivos de acceso.

Al finalizar la relación laboral o al requerimiento de la organización, deberá devolver todo dispositivo asignado.

El incumplimiento de esta obligación será considerado falta grave.

8. Período de Confidencialidad

La obligación de confidencialidad asumida por el Receptor permanecerá vigente durante toda la relación laboral o contractual y continuará de manera indefinida aún después de su terminación, cualquiera que sea la causa de esta, mientras la información siga teniendo carácter confidencial o sensible.

Cuando el contrato laboral finalice, el Receptor, devolverá toda la información que tenga la calidad de confidencial al Revelador y no subsistirá ninguna obligación de confidencialidad.

Las partes acuerdan que las obligaciones materia del presente Convenio continuarán vigentes mientras el presente instrumento o el contrato laboral suscrito por las partes, se encuentren vigentes, siempre que la información objeto de este convenio no haya sido devuelta al Revelador o destruida; es decir se mantienen vigentes las obligaciones del presente Acuerdo mientras la

información confidencial constituya un secreto de comercialización o esté sujeta a restricciones bajo leyes aplicables; y en tanto en cuanto, tal información siga siendo un secreto comercial, técnico-operativo, administrativo o información confidencial y restringida.

Sin perjuicio de lo previsto en esta cláusula, el Revelador en cualquier momento de su vigencia, podrá requerir al Receptor, la devolución de toda la información confidencial suministrada, la misma que deberá ser entregada inmediatamente, en cualquier forma en que se la posea, comprometiéndose a la destrucción de cualquier copia tangible y computarizada o versiones electrónicas o resúmenes de la misma. Dicha información será entregada conjuntamente con una certificación suscrita por el Receptor y el funcionario autorizado del Revelador, en la que se exprese que todos los materiales en posesión o control han sido devueltos o han sido destruidos.

9. Excepciones a las Obligaciones

El Receptor puede revelar la Información, publicarla, diseminarla y utilizarla, cuando dicha Información:

Todo trabajo, desarrollo, documento, software, invento, metodología, contenido o material creado total o parcialmente por el Receptor durante el cumplimiento de sus funciones laborales o contractuales pertenece en su totalidad a TEUNO, quien ostenta todos los derechos de propiedad intelectual y de explotación sobre ellos.

El Receptor no podrá divulgar, reproducir, publicar, compartir, utilizar para fines personales ni ceder a terceros dicho contenido, salvo autorización previa, expresa y por escrito de GRUPO BRAVCO S.A.

Haya sido obtenida por el Receptor de una fuente diferente del Revelador sin obligación alguna de confidencialidad, antes de recibirla del Revelador.

Esté disponible al público en general o que posteriormente se haga pública sin mediar el incumplimiento del Receptor.

Haya sido o sea revelada por el Revelador a terceros sin obligación de confidencialidad.

10. Seguridad.

Con el objeto de regular la seguridad de la información y su tratamiento, las partes determinan las normas de seguridad que rigen su relación contractual y las cuales forman parte del presente integrante del presente convenio y consta en el Anexo ***"A" – NORMAS DE SEGURIDAD.***

11. Controversias.

Las Partes se comprometen a ejecutar de buena fe las obligaciones recíprocas que contraen mediante este Contrato.

Las partes procurarán resolver en forma amigable y directa las discrepancias que pudieran producirse en la ejecución del presente contrato. En caso de insuperable controversia, las partes de mutuo acuerdo, convienen en someter cualquier conflicto, sea de naturaleza que fuere y que

pudiere surgir entre ellas en virtud del presente contrato, al arbitraje administrado, confidencial y en derecho (legislación ecuatoriana) del Centro de Arbitraje y Mediación de la Cámara de Comercio de Quito. El procedimiento contará con 3 árbitros, cada parte designa un árbitro y el tercero es elegido por los otros dos árbitros y de no haber acuerdo, lo designara el Centro de Arbitraje,

Las partes renuncian a la jurisdicción ordinaria, se obligan a acatar el laudo que expida el Tribunal Arbitral y se comprometen a no interponer ningún tipo de recurso en contra del laudo arbitral.

Las partes estipulan que para la ejecución de las medidas cautelares que se pudieren dictar dentro del proceso arbitral, los árbitros solicitarán el auxilio de los funcionarios públicos, judiciales, policiales y administrativos que sean necesarios sin tener que recurrir a juez ordinario alguno del lugar donde se encuentren los bienes o donde sea necesario adoptar medidas.

Así mismo, las partes convienen en la confidencialidad del procedimiento arbitral, pudiendo entregarse copias de recurso al que las partes se hayan sometido, quedando expresamente prohibido a dichas personas la reproducción o entrega de tales copias a terceros.

Las partes reconocen que el Laudo Arbitral tiene el efecto de sentencia ejecutoriada y cosa juzgada, y no admiten recurso alguno.

Las partes convienen libre y voluntariamente que toda reconvención que se deduzca dentro del proceso arbitral deberá ser o basarse sobre la misma materia o materias del arbitraje convenido de derecho. Así las pretensiones del demandado que son materia de reconvención y que pueden ser

sometidas a arbitraje son todas aquellas que tengan relación con la satisfacción y cumplimiento de las obligaciones a las que está obligada la otra parte.

Los gastos incurridos dentro del proceso de Arbitraje correrán por la parte vencida.

Las partes en completo conocimiento de lo estipulado en el presente Convenio y su Anexo y al encontrarse totalmente de acuerdo por así convenir a sus intereses, suscriben dos ejemplares del presente instrumento, del mismo tenor y valor, en la ciudad de Quito, a los xx días del mes de xxxx de 202x.

Aceptado:	Aceptado:
_____	_____
XXXXXXXXX	JOAQUIN RAMOS
Trabajador	Gerente General
	GRUPO BRAVCO S.A
CC: XXXXXXXXX	RUC: 1790506428001

3.10. Encargado Del Tratamiento

3.10.1. Contrato del Encargado del Tratamiento. En GRUPO BRAVCO S.A, se identifica como Responsable del Tratamiento a cualquier individuo o entidad que, debido a una relación contractual, gestiona la información personal por cuenta del Responsable (GRUPO BRAVCO S.A). Para asegurar la adhesión a la Ley Orgánica de Protección de Datos Personales (LOPDP), toda relación con los Encargados se formaliza a través de un Acuerdo de Tratamiento de Datos Personales, que incluye estipulaciones específicas sobre la salvaguarda de los datos,

medidas de seguridad y derechos de los titulares. La estructura del contrato se propone de la siguiente forma:

CONTRATO DE ENCARGADO DEL TRATAMIENTO DE DATOS

Entre las partes:

1. Responsable del Tratamiento:

GRUPO BRAVCO S.A, con domicilio en las calles José María Ayora N39-162 y Vicente Cárdenas, parroquia Iñaquito, identificada con RUC 1790506428001, representada por Joaquín Ramos Hernández, en adelante se le denominará “El Responsable”.

2. Encargado del Tratamiento:

El Responsable designa a la empresa: _____, con RUC No: _____, correo electrónico: _____; como encargada de tratamiento de datos, por lo que en adelante se le denominará "El Encargado".

3. Delegado de Protección de Datos:

El Responsable designa como contacto del área de protección de datos a: Andrés Ayala, con correo electrónico: andres.ayala@teuno.com, quien actuará como punto de contacto para asuntos relacionados con este contrato.

_____

CLÁUSULAS

Cláusula 1. Objeto del Contrato

El presente contrato tiene como objeto regular la relación entre el Responsable y el Encargado en el tratamiento de datos personales que el Encargado llevará a cabo por cuenta del Responsable, en el marco de los servicios prestados por GRUPO BRAVCO S.A, que incluyen asesoramiento en planificación, eficiencia, control, información administrativa, contabilidad de costos, procedimientos presupuestarios y soluciones tecnológicas integrales en conectividad, infraestructura, seguridad y cloud.

Cláusula 2. Duración

Este contrato entrará en vigor el [fecha de inicio] y tendrá una duración [especificar plazo]. La duración podrá modificarse por acuerdo escrito entre las partes.

Cláusula 3. Naturaleza

El Encargado tratará los datos personales únicamente bajo las instrucciones documentadas del Responsable y en cumplimiento de la Ley Orgánica de Protección de Datos Personales de Ecuador (LOPDP) y demás normativa aplicable.

Cláusula 4. Finalidad del Tratamiento

El tratamiento de datos tiene como finalidad la ejecución de los servicios contratados por el Responsable, incluyendo la gestión de soluciones tecnológicas, soporte en conectividad y networking, mantenimiento de infraestructura, implementación de medidas de seguridad y servicios en la nube, así como actividades de asesoramiento administrativo y contable.

Cláusula 5. Tipos de Datos Tratados

Los datos personales objeto de tratamiento podrán incluir, entre otros:

Datos identificativos (nombres, apellidos, cédula de identidad, RUC).

Datos de contacto (correo electrónico, teléfono, dirección).

Datos profesionales (cargo, empresa, información laboral).

Datos técnicos (direcciones IP, registros de acceso, metadatos de sistemas).

Datos financieros (información contable o presupuestaria, según corresponda).

Cláusula 6. Instrucciones en el Tratamiento

El Encargado tratará los datos exclusivamente conforme a las instrucciones escritas del Responsable, las cuales se detallarán en el Anexo a la cláusula 6“Instrucciones Específicas para el tratamiento de datos”, o en comunicaciones posteriores. Cualquier desviación de estas instrucciones deberá ser notificada y autorizada previamente por el Responsable.

Cláusula 7. Categoría de Interesados

Los datos tratados corresponderán a las siguientes categorías de interesados:

Clientes y representantes de empresas o administraciones públicas.

Empleados o contratistas de los clientes del Responsable.

Usuarios de los servicios tecnológicos proporcionados por el Responsable.

Cláusula 8. Obligaciones del Encargado del Tratamiento

El Encargado se compromete a:

Tratar los datos únicamente para las finalidades establecidas en este contrato.

Implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos, conforme a la normativa aplicable y al nivel de riesgo.

No subcontratar el tratamiento sin autorización previa y por escrito del Responsable.

Mantener un registro de actividades de tratamiento realizadas por cuenta del Responsable.

Colaborar con el Responsable en la atención de solicitudes de los interesados (acceso, rectificación, supresión, etc.).

Notificar al Responsable cualquier violación de seguridad en un plazo máximo de 48 horas desde su detección.

Devolver o destruir los datos al finalizar la relación contractual, según las instrucciones del Responsable.

Cláusula 9. Obligaciones del Responsable del Tratamiento

El Responsable se compromete a:

Proporcionar al Encargado las instrucciones claras y documentadas para el tratamiento de datos.

Garantizar que los datos tratados han sido obtenidos de manera lícita y conforme a la normativa aplicable.

Supervisar el cumplimiento de las obligaciones del Encargado mediante auditorías, si fuera necesario.

Facilitar al Encargado la información necesaria para cumplir con sus obligaciones legales.

Cláusula 10. Medidas para la Comunicación de Brecha de Seguridad

En caso de una violación de seguridad que afecte a los datos tratados, el Encargado notificará al Responsable en un plazo máximo de 48 horas, incluyendo:

Descripción de la brecha (naturaleza, alcance, datos afectados).

Medidas adoptadas o propuestas para mitigar los efectos.

Punto de contacto para mayor información.

El Responsable decidirá si es necesario notificar a la Autoridad de Protección de Datos de Ecuador y a los interesados, conforme a la LOPDP.

Cláusula 11. Acuerdo de Finalización de Relación

Al finalizar este contrato, por cualquier causa, el Encargado deberá:

Devolver al Responsable todos los datos personales tratados, en el formato acordado, o destruirlos de forma segura, según las instrucciones del Responsable.

Certificar por escrito la devolución o destrucción de los datos.

Cesará cualquier uso de los datos y garantizará la confidencialidad de la información tratada durante la vigencia del contrato.

_____

Firma y Aceptación:

En señal de conformidad, las partes firman el presente contrato en [ciudad], a [fecha].

Por el Responsable:

_____

Joaquín Ramos Hernández

GRUPO BRAVCO S.A

Por el Encargado:

_____

[Nombre y firma]

[Nombre de la empresa del Encargado]

INSTRUCCIONES ESPECÍFICAS PARA EL TRATAMIENTO DE DATOS A LA CLÁUSULA 6

Responsable del Tratamiento: GRUPO BRAVCO S.A

Encargado del Tratamiento: [Nombre de la empresa del Encargado]

Fecha: [Fecha de elaboración del anexo]

En cumplimiento de la Cláusula 6 del Contrato de Encargado del Tratamiento de Datos, el Responsable proporciona al Encargado las siguientes instrucciones específicas para el tratamiento de datos personales:

1. Actividades de Tratamiento Autorizadas

a) El Encargado únicamente podrá realizar las siguientes operaciones con los datos personales:

b) Recogida: Recepción de datos proporcionados por el Responsable o sus clientes para la ejecución de los servicios contratados.

c) Almacenamiento: Custodia de los datos en sistemas seguros, ya sea en servidores locales o en la nube, según las soluciones tecnológicas acordadas.

d) Procesamiento: Análisis y organización de datos para la generación de informes administrativos, contables o tecnológicos solicitados por el Responsable.

e) Consulta: Acceso a los datos para brindar soporte técnico o resolver incidencias relacionadas con conectividad, infraestructura, seguridad o servicios en la nube.

f) Eliminación: Supresión segura de datos al finalizar su utilidad o al término del contrato, conforme a las instrucciones del Responsable.

2. Finalidades Específicas del Tratamiento

a) El Encargado tratará los datos exclusivamente para:

b) Facilitar la conectividad y networking de los clientes del Responsable (ej. configuración de redes, gestión de direcciones IP).

c) Mantener y optimizar la infraestructura tecnológica (ej. servidores, sistemas de almacenamiento).

d) Implementar medidas de seguridad informática (ej. monitoreo de amenazas, cifrado de datos).

e) Prestar servicios en la nube (ej. migración, gestión y soporte de datos alojados).

f) Apoyar en la elaboración de reportes administrativos, contables o presupuestarios para los clientes del Responsable.

3. Prohibiciones Específicas

El Encargado no podrá:

a) Utilizar los datos para fines distintos a los establecidos en este anexo o en el contrato.

b) Transferir los datos a terceros sin autorización previa y por escrito del Responsable.

c) Realizar copias no autorizadas de los datos, salvo las necesarias para copias de seguridad acordadas con el Responsable.

4. Medidas Técnicas y Organizativas Mínimas

El Encargado deberá implementar, como mínimo, las siguientes medidas para garantizar la seguridad de los datos:

a) Cifrado: Uso de protocolos de cifrado para datos en tránsito y en reposo.

b) Control de Acceso: Autenticación multifactor y permisos restringidos para el personal que acceda a los datos.

c) Copias de Seguridad: Realización de backups periódicos en entornos seguros, con periodicidad [especificar, ej. semanal].

d) Registro de Actividades: Mantenimiento de logs de acceso y tratamiento, disponibles para auditoría por el Responsable.

e) Protección contra Amenazas: Uso de firewalls, antivirus y sistemas de detección de intrusos actualizados.

5. Plazos de Conservación

Los datos deberán conservarse únicamente durante el tiempo necesario para cumplir con las finalidades descritas, y serán eliminados o devueltos al Responsable según lo indicado en la Cláusula 11 del contrato. En caso de requerimientos legales, el Encargado notificará al Responsable para acordar su conservación temporal.

6. Subcontratación

Cualquier subcontratación requerirá autorización previa y por escrito del Responsable. El Encargado garantizará que los subcontratistas cumplan con las mismas obligaciones establecidas en este contrato y anexo.

7. Comunicación con el Responsable

El Encargado informará al Responsable sobre cualquier solicitud de los interesados (acceso, rectificación, cancelación, oposición) en un plazo máximo de 24 horas desde su recepción, remitiendo la solicitud al contacto del Delegado de Protección de Datos indicado en el contrato.

Aceptación del Anexo:

Este anexo forma parte integrante del Contrato de Encargado del Tratamiento de Datos y es aceptado por ambas partes en [ciudad], a [fecha].

Por el Responsable:

_____

Joaquín Ramos Hernández

GRUPO BRAVCO S.A

Por el Encargado:

_____

[Nombre y firma]

[Nombre de la empresa del Encargado]

3.11. Análisis web

3.11.1. Análisis, Configuración y Política de Cookies. El sitio web de TEUNO (https://teuno.com) implementa cookies para optimizar la experiencia de navegación de los usuarios, analizar métricas de uso y gestionar campañas publicitarias.

Análisis de la utilización de cookies

- TEUNO recoge información del usuario a través de cookies para gestionar la navegación en el sitio web, almacenar preferencias de usuario, recopilar datos para la mejora de servicios, y analizar el tráfico.
- Se utilizan cookies de terceros (como Meta Ads, Google Analytics, Google Adsense y DoubleClick) para análisis de comportamiento de navegación y publicidad dirigida.
- Al acceder al sitio, se despliega un banner de cookies que permite al usuario aceptar o rechazar el uso de cookies, enlazando a la Política de Cookies publicada.
- A través de cookies y de la dirección IP, TEUNO obtiene información de navegación que no identifica directamente al usuario, salvo que éste proporcione información adicional a través de otros medios.

La gestión de información obtenida a través de cookies se rige por los principios de consentimiento informado, minimización y propósito específico, en conformidad con la Ley Orgánica de Protección de Datos Personales (LOPDP).

De acuerdo con la política de cookies vigente de TEUNO, publicado en la página web https://teuno.com/, el uso de cookies está definido de la siguiente manera:

- Permitir el correcto funcionamiento técnico de su plataforma.
- Mejorar la experiencia de usuario en su navegación.
- Analizar el tráfico y el comportamiento de los visitantes para optimizar sus servicios.
- Gestionar espacios publicitarios relevantes.

Por su funcionalidad, se emplean:

- Cookies técnicas: Esenciales para el uso de servicios básicos del sitio web.
- Cookies de análisis: Permiten el análisis estadístico del comportamiento de navegación.
- Cookies publicitarias: Permiten mostrar anuncios personalizados según intereses.

Configuración del tratamiento de cookies

Actualmente, al ingresar al sitio web, se despliega un aviso emergente que:

- Informa sobre el uso de cookies.
- Permite aceptar o rechazar el uso de todas las cookies.
- Enlaza a la Política de Cookies para consulta detallada.

Sin embargo, no se ofrece al usuario una opción visible de configuración personalizada (por ejemplo, aceptar solo cookies técnicas o rechazar cookies de análisis y publicidad).

La administración de cookies actualmente depende de la configuración manual que el usuario realice en su navegador.

Política de Cookies

Nombre del documento: Política de Cookies del Sitio Web de TEUNO

Fecha de actualización**:** 19 de mayo de 2023

La política cubre:

- Definiciones de cookies, tipos y funcionalidades.
- Finalidades de la recolección de información.
- Procedimientos de desactivación de cookies desde los navegadores.
- Ejercicio de derechos de los titulares según la LOPDP.
- Contacto de TEUNO para consultas: info@teuno.com

Además, La política aplicable, basada en el Aviso de Privacidad, establece:

Tipos de cookies utilizadas:

- Cookies de sesión para gestión de acceso y navegación.
- Cookies analíticas para medir y analizar el tráfico web.

Finalidades:

- Mejorar la experiencia de usuario en la navegación web.
- Recabar datos estadísticos no identificativos sobre el uso del sitio web.
- Ofrecer servicios personalizados en base a la actividad del usuario.

Duración de las cookies: Las cookies tienen una duración limitada en el tiempo y su permanencia depende del tipo de cookie instalada.

Protección de la información: Los datos recolectados a través de cookies son gestionados siguiendo las políticas de seguridad de la información de TEUNO y respetando los principios de confidencialidad, integridad y disponibilidad de la información.

Recomendaciones de Mejora

1. Implementar un botón para la selección de los “permisos de cookies” en el aviso emergente inicial, que permita al usuario seleccionar específicamente qué tipos de cookies acepta o rechaza.

   Esta medida mejoraría el consentimiento informado y fortalecería el cumplimiento con la LOPDP.

2. Incluir en la Política de Cookies y/o Aviso de Privacidad la información sobre el lugar de almacenamiento de los datos recolectados mediante cookies.

   Se debe especificar si la información se almacena en:

   - Servidores propios de TEUNO.
   - Servidores en territorio ecuatoriano.
   - Plataformas de terceros en la nube (y cuáles).

Esta mejora permitirá reforzar la transparencia frente a los usuarios y cumplirá de manera más estricta los requisitos de información previa establecidos en el artículo 12 de la Ley Orgánica de Protección de Datos Personales (LOPDP).

3.11.2. Formularios De Contacto, Newsletter, Trabaja Conmigo, Registro.Análisis De Los Formularios En El Sitio Web.

En el sitio web de TEUNO (https://teuno.com/contacto/) se dispone de formularios para contacto y suscripción a newsletter, según lo descrito en el Aviso de Privacidad:

Formulario de contacto:

El usuario puede enviar consultas o solicitudes a través del formulario habilitado en la web. Se recogen datos personales tales como:

- Nombre
- Apellido
- Teléfono
- Correo electrónico
- Nombre de la empresa
- Asunto (selección de motivo)
- Mensaje libre

Además, incluye:

Casilla de aceptación de Política de Privacidad y Términos y Condiciones.

Protección CAPTCHA para verificar autenticidad humana.

Formulario de suscripción a newsletters:

Permite solicitar la recolección del correo electrónico del usuario para el envío de boletines informativos y comunicaciones de interés relacionadas con los servicios de TEUNO.

Bolsa de empleo:

TEUNO no dispone de un formulario interno para "Trabaja conmigo" en su web.

Sin embargo, redirige a los postulantes a la plataforma externa Genoma Work, específicamente en: https://app.genoma.work/jobs/teuno

Posteriormente, para completar la postulación, el usuario es redirigido a: https://app.genoma.work/startprocess/b60892f2-ece2-415b-b33b-a816b6b8c73a

En esta etapa inicial:

- Solo se solicita autenticación a través de LinkedIn, Gmail o correo electrónico.
- No se requiere aún la carga inmediata de datos extensivos o currículums.

Formulario de registro de usuarios:

No existe un formulario de registro de usuarios propio en el sitio web institucional de TEUNO.

Tratamiento y finalidad

Conforme a las políticas de privacidad y documentos normativos de TEUNO:

Formulario de contacto: Gestión de solicitudes de contacto, respuesta a consultas o requerimientos.

Newsletter: Envío de boletines informativos, comunicaciones comerciales y promociones de servicios de TEUNO.

Bolsa de empleo: Gestión de procesos de selección de personal, mediante una plataforma de terceros (Genoma Work).

TEUNO garantiza que el tratamiento se realiza conforme a los principios de licitud, finalidad, proporcionalidad y minimización exigidos por la LOPDP.

Seguridad y conservación de los datos

TEUNO aplica las siguientes medidas de protección:

- Restricción de acceso a datos solo a personal autorizado.
- Políticas internas de seguridad de la información para resguardo y protección de datos.
- Uso de mecanismos CAPTCHA en formularios de contacto.
- Conservación de los datos solo durante el tiempo necesario para la finalidad del tratamiento, con posibilidad de anonimización si es requerido.

Los datos gestionados en la plataforma Genoma Work quedan sujetos a las políticas de privacidad de dicha plataforma, independiente de las políticas de TEUNO.

Ejercicio de derechos de los titulares

Los titulares pueden ejercer sus derechos de:

- Acceso
- Rectificación
- Actualización
- Cancelación/Eliminación
- Suspensión
- Oposición
- Portabilidad

Para ejercer sus derechos, deben enviar una solicitud a: info@teuno.com, conforme a lo descrito en el Aviso de Privacidad.

Recomendaciones de mejora

1. **Evitar el uso de CAPTCHA en el formulario de contacto.**

Si bien los CAPTCHA ayudan a proteger contra bots, también pueden ser invasivos para el usuario y discriminatorios en ciertos casos (usuarios con discapacidad visual, por ejemplo).

2. **Informar expresamente a los usuarios sobre el uso de un proveedor externo para el proceso de selección de personal.**

- Actualmente, el portal de empleo redirige a Genoma Work, pero no se advierte claramente que el proceso será gestionado por una empresa subcontratada.
- Se debe incluir una leyenda visible en la sección de Bolsa de Empleo que diga algo como:

  "El proceso de postulación será gestionado a través de nuestra empresa aliada Genoma Work, quien actuará como encargado del tratamiento de sus datos personales, conforme a su propia Política de Privacidad."

  Esta transparencia es fundamental para cumplir los principios de información y consentimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP).

3.11.3. Avisos Legales. Análisis de los avisos legales en el sitio web El sitio web de TEUNO (https://teuno.com) cuenta con los siguientes documentos legales publicados y vigentes, mismos que se encuentran disponibles en los siguientes links:

https://teuno.com/politica-privacidad/

https://teuno.com/terminos-y-condiciones/

https://teuno.com/wp-content/uploads/2024/02/Politica-de-Cookies-1.pdf

Aviso y contenido de Privacidad: Documento que informa a los usuarios sobre el tratamiento de sus datos personales, conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP). Contiene y establece lo siguiente:

- Identificación del responsable: TEUNO, incluyendo su domicilio y canales de contacto.
- Datos personales tratados: nombre, apellidos, correo electrónico, empresa, teléfono celular, IP, entre otros.
- Finalidades: gestión de solicitudes de contacto, envío de newsletters, comunicaciones comerciales.
- Consentimiento: basado en la aceptación expresa del usuario al utilizar el sitio web.
- Derechos ARCO: acceso, rectificación, cancelación, oposición y otros derechos reconocidos por la LOPDP.

- Medidas de seguridad: aplicación de controles internos y técnicas de protección de datos personales.
- Responsable del tratamiento: TEUNO.
- Condiciones para transferencias nacionales e internacionales de datos.

Términos y Condiciones de Uso del Sitio Web.

Documento que regula el acceso y uso del sitio web por parte de los usuarios. Incluye:

- La navegación por el sitio implica la aceptación sin reservas de los términos de uso.
- Se definen derechos de propiedad intelectual de TEUNO sobre los contenidos de la web.
- Limitaciones de responsabilidad en caso de fallos técnicos, virus o interrupciones
- Obligaciones específicas de los usuarios para:
    - Proporcionar información verídica.
    - No introducir contenido ilícito o dañino.
    - No realizar actividades publicitarias no autorizadas.
    - Respetar derechos de propiedad intelectual.

Ambos documentos están actualizados al 19 de mayo de 2023.

Política de Cookies:

El documento de políticas de cookies incluye lo siguiente:

- Describe qué son las cookies y su importancia en la navegación.
- Clasifica las cookies en técnicas, de análisis y publicitarias.

- Informa sobre el uso de cookies propias y de terceros (Meta Ads, Google Analytics, etc.).
- Explica cómo el usuario puede aceptar, rechazar o configurar las cookies, aunque actualmente no ofrece una opción granular de configuración (esto fue señalado como una recomendación de mejora).
- Proporciona el canal de contacto: info@teuno.com.

Cumplimiento normativo

Los avisos legales implementados cumplen con:

- Ley Orgánica de Protección de Datos Personales (LOPDP).
- Buenas prácticas internacionales de protección de datos y seguridad de la información.
- Normativas sobre responsabilidad por contenidos digitales y propiedad intelectual.

Recomendación: Colocar el nombre del delegado de protección de datos personales, correo electrónico y número telefónico.

3.12. Medidas De Seguridad

3.12.1. Análisis, Uso Y Medidas De Seguridad En El Uso De Navegadores. Análisis Del Uso De Navegadores.

Del Uso De Navegadores. De acuerdo con la estructura tecnológica y las políticas de seguridad de TEUNO, el sitio web institucional (https://teuno.com) es accesible a través de los navegadores más utilizados, como:

- Google Chrome
- Mozilla Firefox

- Microsoft Edge
- Safari

Estos navegadores permiten la navegación segura bajo el protocolo HTTPS, asegurando la integridad y confidencialidad de la información transmitida entre los usuarios y el sitio web.

TEUNO, mediante su Política de Cookies y Aviso de Privacidad, advierte sobre el uso de cookies y mecanismos de seguimiento en la navegación.

Certificado de seguridad SSL/TLS

El sitio web dispone de un certificado de seguridad emitido por la entidad certificadora ZeroSSL RSA Domain Secure Site CA, con las siguientes características:

- Nombre común (CN): teuno.com
- Organización (O): No incluido en el certificado.
- Periodo de validez:
  - Emitido el 9 de marzo de 2025.
  - Vence el 8 de junio de 2025.
- Tipo de firma: SHA-256
- Clave pública: Algoritmo seguro de cifrado.

Importancia del certificado:

- Cifra las comunicaciones entre los navegadores de los usuarios y el servidor de TEUNO.
- Protege la integridad de los datos transmitidos (como datos de contacto y navegación).

- Genera confianza en los usuarios al mostrar el candado de seguridad en el navegador.
- Cumple con los requisitos de confidencialidad establecidos en la LOPDP.

Uso seguro de navegadores en el contexto de TEUNO

Los usuarios interactúan con el sitio web utilizando navegadores web que deben estar actualizados para:

- Garantizar la compatibilidad con el cifrado SSL/TLS implementado en la web.
- Aprovechar las últimas actualizaciones de seguridad publicadas por los desarrolladores de navegadores.

De acuerdo al Procedimiento de Gestión de Incidentes de Ciberseguridad y a la metodología de Riesgo, el uso de navegadores seguros implica:

- Actualización periódica: Garantizar que los navegadores utilizados estén actualizados a su última versión para incorporar los últimos parches de seguridad.
- Configuraciones de privacidad: Configurar los navegadores para:
  - Bloquear cookies de terceros cuando no sean necesarias.
  - Bloquear el rastreo entre sitios.
  - Utilizar navegación segura (modo HTTPS).
- Protección contra descargas maliciosas: Activar filtros de navegación segura que adviertan sobre sitios web peligrosos o archivos de descarga sospechosos.

- Control de extensiones:

  Utilizar únicamente extensiones autorizadas y verificadas para evitar compromisos de seguridad en el navegador.

Medidas de seguridad aplicadas al uso de navegadores

En base al Proceso de Protección de Datos Personales y a la política interna de gestión de incidentes, TEUNO establece:

- Acceso controlado: Solo se permite el acceso al sitio web institucional y a las plataformas de servicios a través de navegadores corporativos autorizados.
- Políticas de navegación segura: Los dispositivos corporativos cuentan con configuraciones de seguridad que limitan el acceso a sitios web no autorizados y bloquean la instalación de plugins externos.
- Monitoreo y respuesta ante incidentes: El Centro de Operaciones de Seguridad (CSOC) realiza monitoreo continuo de tráfico de red para detectar posibles actividades anómalas provenientes del uso de navegadores.
- Capacitación continua: Los usuarios internos reciben capacitaciones periódicas sobre buenas prácticas de navegación segura y gestión de amenazas digitales.

Recomendaciones de mejora:

Garantizar que la validez mínima del certificado SSL sea de al menos un (1) año. Actualmente, el certificado emitido por ZeroSSL tiene una validez de aproximadamente tres (3) meses, lo cual incrementa la carga administrativa y el riesgo de errores en renovación.

Se recomienda considerar la adquisición de certificados SSL/TLS con una validez mínima de un año para:

- Reducir el riesgo operativo de expiración inadvertida.
- Mejorar la continuidad de servicio.
- Cumplir buenas prácticas en la gestión de seguridad web.

3.12.2. Hosting Y Servidores.

3.12.2.1. Medidas de seguridad en Hosting y Servidores. TEUNO se aloja en infraestructura propia bajo el siguiente esquema y basado en el Instructivo de Recuperación de Servicio Web, Manual de Hardening, el Procedimiento de Mantenimiento de Servidores y el Procedimiento de Respaldo de Base de Datos, las medidas de seguridad aplicadas a los servidores de TEUNO son las siguientes:

- **Medidas de seguridad aplicadas:**
  - Autenticación de acceso al servidor: Se restringe el acceso al personal autorizado mediante políticas de control de usuarios y contraseñas seguras.
  - Actualizaciones del sistema operativo: Se establece la obligación de mantener el sistema actualizado con los últimos parches de seguridad.
  - Respaldos de información: Se realiza copia de seguridad del aplicativo y de los servicios críticos relacionados.
  - Protección a nivel de red: Se configuran firewalls y reglas específicas de acceso para proteger la infraestructura contra amenazas externas.

- Planes de recuperación: Ante una afectación del servicio web, existe un procedimiento documentado para restaurar la operatividad en el menor tiempo posible.
- Monitoreo: A través del CSOC (Centro de Operaciones de Ciberseguridad) se realiza la vigilancia permanente de los eventos de seguridad.

- **Hardening de servidores Windows:**
  - Desactivación de servicios innecesarios.
  - Configuración estricta de políticas de contraseñas y bloqueo de cuentas.
  - Principio de privilegio mínimo para cuentas administrativas.
  - Configuración de firewall basado en roles.
  - Habilitación de seguridad avanzada (Credential Guard, Defender Exploit Guard).
- **Mantenimiento preventivo y correctivo:**
  - Se realiza un cronograma anual de mantenimiento de servidores.
  - Se revisa periódicamente el estado de discos, ventiladores, fuentes de poder.
  - Se ejecutan mantenimientos físicos (limpieza y revisión).
- **Gestión de respaldos:**
  - Los respaldos de bases de datos se ejecutan de forma diaria.
  - Se implementa verificación automática de integridad mediante scripts en PowerShell, Ansible y Python.
  - Almacenamiento de respaldos en storage interno de alto rendimiento.

- **Seguridad de red y acceso:**
  - Restringido acceso a los servidores solo a personal autenticado.
  - Bloqueo de puertos no necesarios.
  - Uso exclusivo de protocolos de autenticación fuertes como NTLMv2.
- **Gestión de incidentes de seguridad:**
  - Monitoreo continuo a través del CSOC (Centro de Seguridad).
  - Plan de recuperación ante fallos documentado para servidores críticos.

Seguridad en servidores

- **Firewall y control de tráfico:**
  - Configuración estricta del firewall interno de Windows.
  - Restricción de puertos abiertos exclusivamente a los necesarios para la operación.
- **Política de contraseñas y autenticación segura:**
  - Uso de contraseñas robustas conforme a las políticas internas.
  - Activación de autenticación basada en red segura (NTLMv2).
- **Monitoreo y auditoría de eventos:**
  - Registro de eventos críticos de seguridad en el sistema.
  - Revisión periódica de logs para detectar incidentes o anomalías.
- **Protección contra malware:**
  - Uso de soluciones antivirus corporativas actualizadas en los servidores.

- **Respaldo y recuperación de datos:**
  - Implementación de planes de respaldo diario de bases de datos.
  - Procedimientos de restauración documentados y verificados regularmente.

Seguridad en infraestructura web

- **Protección de sitio web mediante HTTPS:** El servidor web publica el sitio https://teuno.com con protocolo seguro SSL/TLS.
- **Certificado SSL válido:** Emitido por ZeroSSL, con periodo de validez actual del 9 de marzo de 2025 al 8 de junio de 2025

3.12.2.2. Prestadores de servicios

En cuanto a la infraestructura tecnológica:

- **Proveedor de equipo:** El servidor de hosting y los aplicativos asociados son propiedad de TEUNO, no contratados a terceros externos.
- **Prestación de servicios adicionales (Terceros):** Cuando se requiera la participación de terceros para el tratamiento o almacenamiento de datos personales, TEUNO exige que los proveedores cumplan con:
  - Las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP).
  - Medidas de seguridad técnicas y organizativas equivalentes a las aplicadas internamente.

- Formalización de acuerdos de confidencialidad y de tratamiento de datos con cláusulas específicas.

TEUNO gestiona de forma interna su hosting y servidores, sin dependencia directa de servicios externos cloud para su sitio principal.

3.12.3. Gestores de Correo Electrónico.

3.12.3.1. Medidas de seguridad. Según la Metodología de Administración de Riesgos de Seguridad de la Información, el Procedimiento de Administración de Incidentes de Ciberseguridad y las prácticas registradas en el Proceso de Protección de Datos Personales, se determinan las siguientes acciones de seguridad para la administración del correo electrónico en TEUNO:

- **Acceso controlado:** Solo personal autorizado tiene acceso a las cuentas de correo corporativas, con credenciales personales y mecanismos de autenticación segura.
- **Política de contraseñas robustas:** Se requiere el uso de contraseñas seguras que cumplan con parámetros de longitud, complejidad y renovación periódica.
- **Protección contra amenazas:** Los sistemas de correo cuentan con filtros de antispam, antivirus y mecanismos de detección de amenazas avanzadas para prevenir correos maliciosos.
- **Cifrado de correos:** El envío de información sensible vía correo electrónico debe realizarse mediante mecanismos de cifrado conforme a los procedimientos internos de protección de datos.

- **Capacitación del personal:** Los usuarios de correo electrónico son capacitados periódicamente sobre riesgos asociados como phishing, malware y suplantación de identidad.
- **Registro y monitoreo de incidentes:** Cualquier incidente de seguridad relacionado con el uso de correo electrónico es registrado y gestionado conforme al procedimiento interno establecido.

*3.12.3.2. **Prestadores de servicios.*** Respecto al servicio de correo electrónico corporativo:

- **Gestión interna o tercerizada:** TEUNO administra su plataforma de correo electrónico dentro de sus propios controles internos de seguridad, integrados en su infraestructura tecnológica.
- **Relaciones con terceros:** En caso de utilizar proveedores externos para la prestación del servicio de correo electrónico o para su soporte técnico, se exige:
  - Cumplimiento estricto de la Ley Orgánica de Protección de Datos Personales (LOPDP).
  - Firma de contratos con cláusulas específicas de confidencialidad, seguridad de la información y protección de datos personales.
  - Verificación de que los prestadores aplican medidas de seguridad adecuadas equivalentes a las implementadas por TEUNO.

Capítulo 4: Plan Director De Seguridad

4. Descripción de Plan Director de Seguridad y Beneficios Para la Empresa

El Plan Director de Seguridad (PDS) es una herramienta de planificación estratégica que permite estructurar, priorizar y ejecutar iniciativas de seguridad de la información dentro de una organización. Su finalidad es reducir los riesgos tecnológicos y operativos a niveles aceptables, a través de un enfoque alineado con los objetivos del negocio y las mejores prácticas internacionales (ISO/IEC 27001, ISO 22301, MAGERIT, entre otros).

Actualmente, Teuno no dispone de un Plan Director de Seguridad formalizado, lo que representa una oportunidad significativa de mejora. La implementación de este instrumento permitiría a la organización:

- Tener una visión clara y transversal del estado actual de la seguridad de la información.
- Detectar vulnerabilidades y brechas en los sistemas y procesos críticos.
- Priorizar inversiones y acciones de mitigación de forma justificada y alineada al riesgo.
- Fortalecer la cultura de ciberseguridad y cumplimiento normativo.
- Integrar de forma ordenada proyectos de continuidad, protección de activos y gestión de incidentes.
- Establecer una cultura organizacional alineada con las buenas prácticas de protección de activos y reforzar su reputación en el mercado.

Este plan se concibe como una oportunidad para la mejora continua, bajo el enfoque del ciclo PHVA (Planear-Hacer-Verificar-Actuar), y como soporte técnico-organizativo del sistema de gestión de riesgos empresariales de Teuno.

4.1. Check List PDS

Con base en la lista de controles para la implantación de un Plan Director de Seguridad, se evaluó el punto de partida de Teuno.

Tabla 22

Situación actual de la empresa al inicio del proyecto

Nivel	Alcance	Control	Descripción	Check	Justificación
A	PRO	Examinar el panorama actual de la empresa	Examinas a fondo el estado presente de la compañía para poder implementar un Plan Director de Seguridad.	✓	TEUNO cuenta con una certificación ISO 27001 vigente, donde se realiza y analiza la situación actual de la empresa
A	PRO	Conformar el PDS con la estrategia corporativa	A la hora de elaborar el Plan Director de Seguridad, consideras toda la estrategia de la empresa.	☐	
A	PRO	Establecer los proyectos a implementar	Defines y detallas en profundidad las medidas específicas para lograr los niveles de seguridad requeridos.	☐	
A	PRO	Clasificar y priorizar los proyectos	Organizas y categorizas las acciones a llevar a cabo con el objetivo de dar prioridad a aquellas que nos brinden más ventajas en comparación con su costo.	☐	

Nivel	Alcance	Control	Descripción	Check	Justificación
B	PRO	Aprobar el PDS	Pruebas y divulgas la versión final del PDS.	☐	
A	PRO	Ejecución del PDS	Desarrollas los proyectos pactados para cumplir con los objetivos de ciberseguridad establecidos.	☐	
A	PRO	Certificación en seguridad	Toma en cuenta la implementación de un procedimiento de certificación que valide el sistema de administración de seguridad de tu empresa.	✓	Actualmente Teuno si tiene una certificación ISO 27001 vigente

4.1.1. Análisis de la Situación Actual de la Organización. En función de los controles revisados en el checklist del punto anterior, se ha realizado un diagnóstico del estado de seguridad en Teuno. Este análisis tiene como objetivo determinar el punto de partida para el desarrollo del Plan Director de Seguridad (PDS) y asegurar su alineación con los objetivos estratégicos y regulatorios de la organización.

Actualmente, Teuno ha logrado avances significativos en la gestión de la seguridad de la información, particularmente reflejados en la reciente auditoría de recertificación ISO/IEC 27001:2022, cuyo alcance incluye el Centro de Operaciones Digitales (DOC) y el Centro de Operaciones de Seguridad (SOC), tal como se valida en la constancia emitida por Bureau Veritas Ecuador S.A. el 20 de marzo de 2025.

De acuerdo con el checklist de controles estratégicos del PDS, se ha marcado como cumplido el control "Analizar la situación actual de la empresa", gracias a la existencia de un diagnóstico

formalizado de seguridad, así como el control "Certificación en seguridad", dado que Teuno ya ha sido objeto de una auditoría externa con resultado favorable.

Sin embargo, se identifican vacíos en el resto de los controles clave: no se han alineado formalmente los proyectos de seguridad con la estrategia empresarial, no se han definido ni priorizado iniciativas específicas, ni se ha aprobado una versión definitiva del PDS. Esto indica que, a pesar de contar con una base sólida gracias al SGSI y la certificación, aún se requiere estructurar una hoja de ruta integral que garantice continuidad, sostenibilidad y expansión de las medidas de seguridad a toda la organización.

4.1.2. Plan Estratégico en materia tecnológica. Teuno cuenta con un marco estratégico claramente definido en materia tecnológica, alineado a su misión, visión y objetivos organizacionales. Este marco se articula a través del Sistema de Gestión de Seguridad de la Información (SGSI), cuyo diseño e implementación ha sido fundamentado en la norma ISO 27001 y en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar).

La visión estratégica tecnológica de Teuno no solo sustenta el Plan Director de Seguridad (PDS), sino que se ve reforzada por la certificación ISO 27001, la cual Teuno ha obtenido en cumplimiento de los requisitos normativos locales, específicamente lo establecido por la Superintendencia de Bancos. La certificación no solo acredita el compromiso institucional con la seguridad, sino que actúa como una herramienta clave en el cumplimiento del marco regulatorio vigente y en la consolidación de relaciones de confianza con los clientes.

Por lo tanto, la confección e implantación del PDS se alinea de forma integral con el plan estratégico tecnológico de la organización, y busca consolidar la gestión de riesgos, la mejora

continua de los procesos, y el aseguramiento de los activos de información críticos para Teuno y sus clientes.

¿Qué buscamos lograr con el PDS?

El diseño e implantación del Plan Director de Seguridad se plantea como el primer paso estructurado para construir una visión tecnológica estratégica en la organización. A través del PDS se espera:

- **Alinear la tecnología con la estrategia del negocio**, asegurando que los proyectos de seguridad aporten valor al crecimiento sostenible de Teuno.
- **Introducir el concepto de gobernanza tecnológica**, incorporando principios de gestión de riesgos, cumplimiento normativo y madurez en la toma de decisiones.
- **Establecer prioridades y proyectos tecnológicos clave,** especialmente en los ámbitos de ciberseguridad, infraestructura, accesos, continuidad de negocio y protección de datos.
- **Fomentar una cultura organizacional orientada a la seguridad**, integrando roles, responsabilidades y planes de concienciación para todas las áreas, fortaleciendo su imagen y credibilidad ante clientes y aliados

4.2. Verificación de Controles

Como parte del desarrollo del Plan Director de Seguridad de Teuno, se ha realizado una verificación de 30 controles clave en materia de seguridad de la información. La evaluación permite establecer el nivel actual de la organización en relación con los principios establecidos.

Tabla 23

Verificación de controles clave

Identificador	Aspecto a evaluar	Respuesta	Justificación	Responsable	Fecha
ID_0001	¿La organización ha definido un documento con la política de seguridad de la información?	SI	Documento formal aprobado en el SGSI. PRC-GSEG-01	Oficial de Seguridad	2025-01-05
ID_0002	¿La política de seguridad de la información se revisa periódicamente?	NO		Oficial de Seguridad	
ID_0003	¿Se han definido las responsabilidades en materia de seguridad de la información?	SI	Están distribuidas y documentadas por rol en el SGSI. PRC-GSEG-01	Oficial de Seguridad	2024-06-18
ID_0004	¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?	SI	Comité activo con funciones definidas y actas. PRC-GSEG-01	Gerencia General	2024-06-18
ID_0005	¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la organización? (Confidencialidad, propiedad intelectual, etc.).	SI	NDA y cláusulas de seguridad incluidas. PR-GPRO-03 / FO-CM-64 / FO-CM-65	Responsable Jurídico	2024-03-19
ID_0006	¿Se dispone de un inventario de activos?	SI	Matriz vigente por criticidad, dueño y clasificación. PR-GSEG-09	Oficial de Seguridad	2024-05-14

Identificador	Aspecto a evaluar	Respuesta	Justificación	Responsable	Fecha
ID_0007	¿Se ha definido quienes el responsable de los activos?	SI	Responsable asignado por tipo de activo. PR-GSEG-09	Oficial de Seguridad/ Líderes de Área	2024-05-14
ID_0008	¿Se comprueban las referencias de todos los candidatos a empleo?	NO		Analista de Talento Humano	
ID_0009	¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?	SI	Acceso al CPD documentado y con control de entrada. PR-TEC-34 / PR-CIB-14	Seguridad Privada	2024-02-19
ID_0010	¿Los equipos TIC críticos de la organización están ubicados en salas de CPD?	SI	Equipos alojados en ambiente controlado con acceso restringido. PR-TEC-34/PR-CIB-14	Tecnología	2024-02-19
ID_0011	¿Se han definido y documentado los procedimientos operacionales TIC?	SI	Proceso documentado en SGSI y Proceso de Tecnología. PRC-GSEG-01 / PRC-TEC-01	Tecnología	2024-03-13
ID_0012	¿Las copias se seguridad se realizan regularmente de acuerdo con la política de backup establecida?	SI	Se realizan respaldos diarios automatizados. PR-TEC-15	Tecnología	2024-01-22
ID_0013	¿Se verifica regularmente la correcta realización de las copias se seguridad?	SI	Validación diaria documentada en procedimientos. PR-TEC-15	Tecnología	22/01/2024

Identificador	Aspecto a evaluar	Respuesta	Justificación	Responsable	Fecha
ID_0014	¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?	NO		Tecnología	
ID_0015	¿Se registran las actividades de los administradores y operadores de sistema?	NO		Tecnología	
ID_0016	¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?	SI	Definido en procedimiento formal de gestión de accesos. PR-GACCE-01	Tecnología	22/01/2024
ID_0017	¿Se ha definido, documentado e implantado un proceso formal para la asignación de contraseñas?	SI	Documentado con criterios de seguridad. PR-GACCE-01	Tecnología	22/01/2024
ID_0018	¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?	NO		Talento Humano / Seguridad	
ID_0019	¿Los usuarios se aseguran de proteger los equipos desatendidos? (¿Ej. bloqueando o cerrando la sesión?	NO		Tecnología	
ID_0020	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?	NO		Tecnología	

Identificador	Aspecto a evaluar	Respuesta	Justificación	Responsable	Fecha
ID_0021	¿Se controla la instalación de software en sistemas en producción?	SI	Flujo aprobado y documentado por soporte. PRC-TEC-01	Tecnología	22/01/2024
ID_0022	¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	SI	Evaluaciones técnicas periódicas con escaneo de vulnerabilidades. PR-GSEG-02	Tecnología	22/01/2024
ID_0023	¿Se ha definido, documentado e implantado un proceso formal para la gestión de los incidentes de seguridad?	SI	Gestionado por CSOC con responsable y registros de eventos. PR-GSEG-02	CSOC / Oficial Seguridad	22/01/2024
ID_0024	¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?	SI	Proceso documentado y con responsable designado. PRC-GCON-01	Gestor de Continuidad	22/01/2024
ID_0025	¿Se han definido, documentado e implantado planes de continuidad de negocio?	SI	Documentados por procesos críticos tras análisis BIA. PCN v1 / Manual SGCN	Gestor de Continuidad	22/01/2024
ID_0026	¿Los planes de continuidad de negocio se revisan y prueban formalmente?	SI	Revisión anual, pruebas realizadas por comité. PRC-GCON-01	Gestor de Continuidad	22/01/2024
ID_0027	¿Todos los requisitos relevantes de carácter legal se mantienen identificados?	SI	Identificados por jurídico y reflejados en SGSI. PRC-GSEG-01	Jurídico / Seguridad	22/01/2024
ID_0028	¿Se han implementado procedimientos para asegurar el cumplimiento de los	SI	Procedimientos de cumplimiento establecidos. PRC-GSEG-01	Jurídico / Seguridad	22/01/2024

Identificador	Aspecto a evaluar	Respuesta	Justificación	Responsable	Fecha
	requisitos relevantes de carácter legal?				
ID_0029	¿Se han establecido e implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	SI	Protección de datos documentada y respaldada. PR-GDAT-01	Oficial de Seguridad	22/01/2024
ID_0030	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?	NO		Tecnología / Seguridad	

De un total de 30 controles evaluados, se define que TEUNO cumple con 22 de ellos (73%). Y, si bien los 8 controles restantes figuran como “no cumplidos”

Figura 5

Relación entre controles cumplidos y no cumplidos

Teuno no presenta ningún control sin abordar, lo cual evidencia un compromiso institucional serio con la gestión de la seguridad de la información. No obstante, se han identificado áreas de mejora que deberán ser priorizadas en el Plan Director de Seguridad.

Los siguientes aspectos presentan un cumplimiento total, sustentado con documentos, procedimientos o evidencia de operación formal:

- **Gobierno y gestión de la seguridad:** Políticas (ID_0001), responsabilidades (ID_0003), comité de seguridad (ID_0004)
- **Gestión contractual y legal:** Cláusulas en contratos (ID_0005), requisitos legales (ID_0027, ID_0028, ID_0029)
- **Gestión de activos:** Inventario y responsables de activos (ID_0006, ID_0007)
- **Seguridad física y acceso:** Perímetro CPD (ID_0009), ubicación de TIC críticos (ID_0010)
- **Gestión operativa TIC**: Procedimientos TIC (ID_0011), copias de seguridad (ID_0012, ID_0013), control de software (ID_0021)
- **Gestión de accesos y contraseñas**: Privilegios y contraseñas documentadas (ID_0016, ID_0017)

- **Gestión de vulnerabilidades e incidentes:** Evaluación técnica (ID_0022), gestión de incidentes (ID_0023)
- **Continuidad del negocio:** Proceso de continuidad (ID_0024), planes BCP (ID_0025), revisión de planes (ID_0026)

Estas prácticas reflejan una estructura sólida en seguridad, con roles definidos, documentación vigente y mecanismos de control aplicados.

Por otro lado, se han detectado 8 controles que, si bien tienen alguna aplicación, presentan debilidades que pueden comprometer la eficacia total del SGSI:

Tabla 24

Controles con debilidades

ID	*Control*	*Observación Principal*
ID_0002	¿La política de seguridad de la información se revisa periódicamente?	No se ha definido un cronograma formal de revisión periódica en el documento ni en el SGSI. (MA-SGSI-01)
ID_0008	¿Se comprueban las referencias de todos los candidatos a empleo?	Existe formato, pero su uso no está estandarizado. FO-RH-02
ID_0014	¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?	No se evidencian logs centralizados para todos los equipos. PRC-GSEG-01
ID_0015	¿Se registran las actividades de los administradores y operadores de sistema?	No se realiza seguimiento continuo, solo bitácoras físicas. PR-TEC-34
ID_0018	¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?	Se recomienda, pero no está formalizado ni en campañas. PR-RH-02

ID_0019	¿Los usuarios se aseguran de proteger los equipos desatendidos? (¿Ej. bloqueando o cerrando la sesión?	No se evidencia mecanismo obligatorio o automatizado. PRC-GSEG-01
ID_0020	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?	Se usan algunas cuentas genéricas sin trazabilidad completa. PR-SNET-01
ID_0030	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?	Se realizan controles técnicos, pero sin auditorías externas documentadas. PRC-TEC-01

Estas observaciones se concentran principalmente en aspectos operativos, automatización de controles técnicos y cultura de seguridad (formación y concienciación del personal).

Conclusiones del análisis

- Teuno posee un nivel de seguridad aceptable, con un SGSI que ha avanzado hacia la formalización de políticas, procesos y roles.
- No existen controles sin implementar, lo cual es un resultado positivo.
- Las brechas detectadas están más vinculadas a la automatización, monitoreo, seguimiento continuo y concienciación de usuarios, por lo que se recomienda su tratamiento como prioridades del PDS.
- Las áreas con mayor carga de control deberán ser reforzadas con recursos, capacitación y tecnología de soporte.

4.3.Inventario de Activos Tecnológicos

Teuno dispone de un proceso formal para la identificación, clasificación, registro y actualización de los activos de información, conforme lo establece el Procedimiento de Gestión del

Inventario de Activos de Información (código PR-GSEG-09, versión 02, aprobado el 21/11/2024). Este proceso forma parte del Sistema de Gestión de Seguridad de la Información (SGSI) y se encuentra alineado a estándares como ISO/IEC 27001 y la política interna de seguridad.

Estructura del Inventario - El inventario de activos tecnológicos incluye los siguientes campos:

- **Identificador:** Código único asignado a cada activo.
- **Nombre del activo:** Denominación intuitiva que permite su fácil identificación.
- **Descripción:** Breve explicación sobre la función del activo.
- **Responsable:** Persona o área encargada de su gestión.
- **Tipo:** Clasificación como activo físico (ej. servidores) o lógico (ej. software).
- **Ubicación:** Localización física del activo (CPD interno, CPD externo, oficinas).
- **Crítico:** Se indica si el activo es fundamental para la continuidad operativa.

Alcance y mantenimiento

El procedimiento establece que:

- El levantamiento de activos lo realiza cada área con apoyo del Oficial de Seguridad.
- Los activos deben ser revisados y actualizados al menos una vez al año.
- Se debe realizar escaneo bimestral de activos tecnológicos con herramientas automáticas.
- Se contempla la baja formal de activos obsoletos o no utilizados.

Responsabilidades

- **Responsables de Área:** Identifican, clasifican y reportan cambios de activos.

- **Oficial de Seguridad de la Información:** Mantiene actualizada la matriz y verifica la aplicación de políticas de protección.
- **Comité de Seguridad:** Supervisa la consistencia y cumplimiento del inventario.

La correcta implementación de este inventario permite a Teuno tener un mapa claro de sus recursos tecnológicos, mejorar su postura de seguridad y facilitar la toma de decisiones basadas en activos críticos para la organización.

Tabla 25

Registro de activos TEUNO

Identificador	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
AD_0001	Active Directory	Servicio de autenticación en red para usuarios	Jefe de Gobierno TI	Servicios	Centro Datos UIO	Si
AD_0002	Herramienta ITSM - Jira	Software para gestión de tickets	Subgerente de Servicios	Software	Nube Azure	No
AD_0003	Equipo Endpoint	Computadores para entregar el servicio (Laptops, PCS)	Jefe de Gobierno TI	Hardware	Matiz TEUNO -DOC	Si
AD_0004	Servicios WLAN	Enlaces WLAN de comunicación y datos	Subgerente de Redes	Red	Centro Datos UIO	Si
AD_0005	Enlaces	Enlaces LAN de comunicación y datos	Subgerente de Redes	Red	Centro Datos UIO	Si
AD_0006	Seguridad Perimetral	Seguridad Perimetral	Subgerente de	Red	Centro Datos UIO	Si

Identificador	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
			Ciberseguridad			
AD_0007	NAS	Servidor de almacenamiento de información	Jefe de Gobierno TI	Hardware	Centro Datos UIO	Si
AD_0008	VPN	Para conectar a la infraestructura de clientes	Jefe de SECOPS	Software	Centro Datos UIO	Si
AD_0009	Personal DOC	Personal del proceso DOC	Jefe DOC	Personas	Matiz TEUNO -DOC	Si
AD_0010	Aplicaciones Zabbix	Para Monitoreo	Subgerente de Servicios	Software	Centro Datos UIO	Si
AD_0011	Herramientas de Monitoreo Proveedores	Provistas por proveedores (Grafana Telconet, NMIS Claro, PRTG)	Proveedor	Software	Proveedor	No
AD_0012	Grafana	Aplicación de monitoreo del DOC	Subgerente de Servicios	Software	Centro Datos UIO	Si
AD_0013	DOCS	Gestor documental de TEUNO	Subgerente de Servicios	Software	Nube Azure	No
AD_0014	Microsoft 365	Plataforma de soluciones Microsoft	Jefe de Gobierno TI	Servicios	Nube Azure	Si
AD_0015	Gravity	Aplicación de base de datos de gestión de la configuración (CMDB)	Subgerente de Servicios	Software	Centro Datos UIO	No
AD_0016	Central Telefónica	Servidor de la central	Subgerente de Redes	Hardware	Nube Azure	No

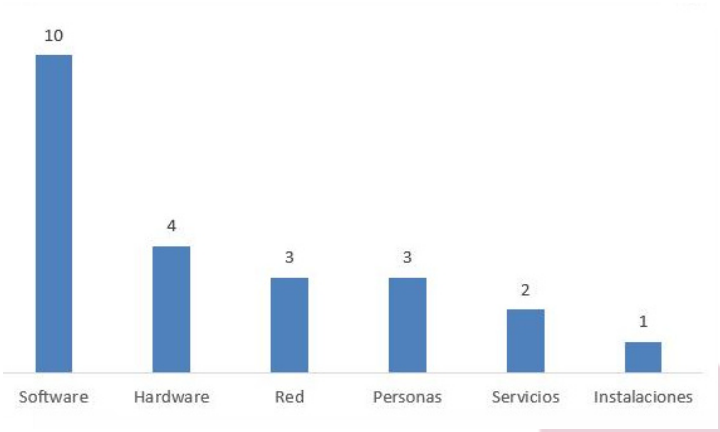
Identificador	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
		telefónica 3CX				
AD_0017	Dispositivos Celulares	Dispositivos utilizados como contacto con clientes	Jefe de Gobierno TI	Hardware	N/A	Si
AD_0018	Centro de Datos UIO	Ubicación física donde se encuentran los equipos físicos de infraestructura	Jefe de Gobierno TI	Instalaciones	Centro Datos UIO	Si
AD_0019	Personal SOC	Personal del proceso SOC	Jefe Nivel 1 SOC	Personas	Matiz TEUNO -SOC	Si
AD_0020	Sistema SIEM	Correlacionador de eventos del SOC	Cliente	Software	Nube Azure	Si
AD_0021	Proveedor N1	Especialistas que entregan el servicio - manos remotas	Jefe DOC	Personas	Proveedor	Si
AD_0022	Confluence	Base de conocimiento	Subgerente de Servicios	Software	Nube Azure	No
AD_0023	Página web TEUNO	www.teuno.com	Jefe de marketing	Software	Proveedor de hosting – nube	Sí

Total, de activos registrados: 23

- **Críticos:** 17 activos, que representa el 74%
- **No Críticos:** 6 activos, que representa el 26%

Figura 6

Clasificación por tipo de activo



La mayoría de los activos registrados corresponde a software y componentes de red, lo cual es coherente con una arquitectura orientada a servicios tecnológicos.

4.4.Análisis de Riesgos

El objetivo de este análisis es identificar, evaluar y gestionar los riesgos que puedan afectar la continuidad de los servicios críticos de Teuno, a través del estudio de las amenazas relevantes para cada activo, aplicando una metodología estructurada que permite establecer prioridades de actuación y garantizar la resiliencia organizacional.

Para el análisis se ha adoptado la metodología del Plan Director de Seguridad (PDS) basada en los lineamientos del Instituto Nacional de Ciberseguridad (INCIBE). Esta metodología se estructura en las siguientes fases:

I. **Identificación de Activos:** Se clasifican los activos de Teuno en categorías como: hardware, software, comunicaciones, personal y servicios externos. Se partió de un inventario de

activos de información de Teuno, los cuales fueron clasificados según el modelo proporcionado (A, B y C), estableciendo una relación directa con los tipos de activos definidos en el ejemplo.

II. **Identificación de amenazas:** Para cada tipo de activo se identificaron las amenazas relevantes descritas en el catálogo de amenazas de la herramienta. Se aplicó una matriz de cruce activo-amenaza, señalando los casos donde cada activo puede verse afectado.

III. **Cruce Activo-Amenaza:** En esta fase se realiza el cruce entre los activos identificados y las amenazas potenciales que podrían afectarlos. Se utiliza una matriz donde en la primera columna se listan todas las amenazas detectadas, y en la primera fila se incluyen los códigos de los activos (A1, A2, B1, C3, etc.).

IV. **Valoración de riesgos:** Para cada cruce activo-amenaza identificado, se asignaron valores de:

- **Probabilidad (P):** Baja (1), Media (2), Alta (3)
- **Impacto (I):** Bajo (1), Medio (2), Alto (3)
- **Riesgo =** P x I

Luego, se calculó el riesgo mediante la fórmula:

Riesgo= Probabilidad × Impacto

V. **Análisis de Riesgos y Criterios de aceptación:** Para este análisis, se consideraron únicamente aquellos riesgos con valores superiores a 4, lo que permite centrar los esfuerzos en los escenarios que superan el umbral de aceptabilidad de riesgo definido por la organización.

VI. **Controles y Tratamiento del Riesgo**: Se identifican controles existentes y se propone tratamiento adicional para riesgos no aceptables.

VII. **Clasificación y priorización de riesgos:** Una vez determinados los niveles de riesgo, se procede a su clasificación y priorización. Se identifican como prioritarias aquellas amenazas cuyo riesgo calculado supera el umbral definido (valor mayor a 4)

La siguiente tabla muestra cómo se han relacionado los activos reales de Teuno con las categorías genéricas del ejemplo proporcionado en el material formativo de clase:

Tabla 26

Relación entre activos y categorías genéricas

	Cód.	*Tipo de activo del ejemplo*	*Activo TEUNO*	*Detalle del activo*
A	A1	ordenador(es)	Equipo Endpoint	Equipos de escritorio o portátiles asignados al personal de la organización
A	A2	móvil(es) principalmente para telefonía	Dispositivos Celulares	Dispositivos móviles institucionales con uso para comunicación y apps de negocio
A	A3	conexión a Internet e incluso wifi	Central Telefónica. Enlaces	Servicios de conectividad, voz IP, líneas troncales y enlaces dedicados a internet
B	B1	ordenadores y conexión a Internet (con wifi)	Servicios WLAN	Infraestructura de red inalámbrica para acceso corporativo seguro
B	B2	dispositivos móviles para telefonía y datos	Personal DOC, Personal SOC	Recursos humanos responsables de la operación (DOC) y seguridad (SOC)
B	B3	soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas	Microsoft 365, Confluence	Suite de herramientas colaborativas (correo, Office, SharePoint) y gestión documental

	Cód.	*Tipo de activo del ejemplo*	*Activo TEUNO*	*Detalle del activo*
		colaborativas o de almacenamiento cloud		
B	B4	una página web sencilla alojada y gestionada por un proveedor externo	Proveedor N1	Página institucional y servicios web alojados por proveedor externo
C	C1	ordenadores e incluso algún servidor (web, correo electrónico)	Active Directory, NAS, Centro de Datos UIO, página web	Infraestructura crítica de autenticación (AD), almacenamiento (NAS) y data center principal
C	C2	conexión a Internet con wifi	VPN	Servicio VPN corporativo para acceso remoto seguro
C	C3	dispositivos móviles con datos y apps para su trabajo	Personal DOC, Personal SOC	Uso de apps institucionales en dispositivos móviles de personal clave
C	C4	herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Gravity, Herramienta ITSM - Jira	Plataforma de gestión de tickets, incidencias y proyectos de IT
C	C5	página web / tienda online y redes sociales que gestionan desde la empresa	DOCS, Sistema SIEM	DOCS: repositorio interno y de auditorías; SIEM: monitoreo de eventos de seguridad
C	C6	herramientas para empresas en la nube	Herramientas de Monitoreo Proveedores, Grafana	Dashboards y soluciones cloud para monitoreo de infraestructura de terceros
C	C7	e-administración para su relación con las AAPP	Aplicaciones Zabbix	Sistema de monitoreo integrado que respalda cumplimiento y trazabilidad ante entes externos

Notas:

- **A**: corresponde a activos básicos y esenciales.
- **B**: infraestructura con soporte TIC y servicios gestionados.

- **C**: activos relacionados a servicios digitales avanzados, colaborativos o basados en la nube.

Identificación De Amenazas

Una vez identificado los activos de Teuno y relacionados con los s de referencia (A, B y C), el siguiente paso consiste en identificar las amenazas a las que estos activos están expuestos. Para ello se ha utilizado el Catálogo de Amenazas propuesto en la herramienta metodológica, agrupadas en bloques por su naturaleza.

Tabla 27

Tipos de amenazas por naturaleza

Categoría	***Amenaza***	***Descripción***
Naturales / Ambientales	Fuego	Incendios que afecten la infraestructura física o equipos.
Naturales / Ambientales	Daños por agua	Inundaciones o filtraciones que afecten equipos y sistemas.
Naturales / Ambientales	Desastres naturales	Terremotos, tormentas, etc., que interrumpan operaciones o dañen activos.
Naturales / Ambientales	Condiciones inadecuadas de temperatura o humedad	Variaciones extremas en el ambiente que afectan al hardware.
Lógicas / Información	Fuga de información	Pérdida o revelación no autorizada de información sensible.
Lógicas / Información	Introducción de falsa información	Inserción de datos incorrectos o manipulados.
Lógicas / Información	Alteración de la información	Modificación maliciosa o accidental de datos.
Lógicas / Información	Corrupción de la información	Daños en archivos que impiden su uso.
Lógicas / Información	Destrucción de información	Eliminación intencional o accidental de información.

Categoría	*Amenaza*	*Descripción*
Lógicas / Información	Interceptación de información (escucha)	Captura no autorizada de datos en tránsito.
Lógicas / Información	Difusión de software dañino	Malware, ransomware, spyware, etc.
Lógicas / Información	Errores de mantenimiento / actualización de software	Fallos por malas prácticas en actualizaciones o mantenimientos.
Lógicas / Información	Errores de mantenimiento / actualización de hardware	Interrupciones por fallos físicos mal gestionados.
Lógicas / Información	Acceso no autorizado	Ingreso indebido a sistemas por falta de controles.
Lógicas / Información	Errores de los usuarios	Fallos involuntarios al operar sistemas o procesos.
Lógicas / Información	Errores del administrador	Acciones incorrectas en gestión de TI por el personal responsable.
Lógicas / Información	Errores de configuración	Configuraciones erróneas en sistemas, redes o aplicaciones.
Lógicas / Información	Ingeniería social	Engaños para obtener acceso a información o sistemas.
Técnicas / Infraestructura	Corte del suministro eléctrico	Interrupción energética que detiene operaciones tecnológicas.
Técnicas / Infraestructura	Fallo de servicios de comunicaciones	Caída o indisponibilidad de red, telefonía o internet.
Técnicas / Infraestructura	Interrupción de servicios y suministros esenciales	Agua, energía, conectividad, etc., necesarios para la continuidad operativa.
Técnicas / Infraestructura	Caída del sistema por sobrecarga	Exceso de demanda que causa caída de plataformas.
Técnicas / Infraestructura	Degradación de los soportes de almacenamiento de la información	Daños o pérdida de capacidad de discos u otros medios.
Físicas / Recursos Humanos	Pérdida de equipos	Desaparición de dispositivos por pérdida o extravío.
Físicas / Recursos Humanos	Robo	Sustracción intencionada de equipos o dispositivos.
Físicas / Recursos Humanos	Indisponibilidad del personal	Ausencias que afectan la continuidad operativa o soporte técnico.
Físicas / Recursos Humanos	Abuso de privilegios de acceso	Uso indebido de accesos autorizados para actividades no permitidas.

Categoría	*Amenaza*	*Descripción*
Físicas / Recursos Humanos	Extorsión	Amenazas dirigidas a empleados o directivos para obtener información o beneficios ilegales.
Físicas / Recursos Humanos	Denegación de servicio	Ataques que saturan sistemas impidiendo su funcionamiento (ej. DDoS).

Cada una de estas amenazas ha sido analizada respecto a los activos críticos de Teuno, evaluando su aplicabilidad mediante una matriz de cruce activo–amenaza. Esta matriz permite determinar si una amenaza impacta un activo específico, y es la base para realizar la posterior valoración de riesgos.

Ejemplo:

- La amenaza "Fuga de información" aplica a activos como el sistema SIEM, Microsoft 365, y la herramienta de gestión documental DOCS.
- La amenaza "Fallo del servicio de comunicaciones" aplica a activos como la VPN, Central Telefónica, y Enlaces.

Activos

La empresa TEUNO demuestra un alto nivel de madurez digital al cumplir con una serie de recursos y herramientas tecnológicas que fortalecen su gestión, comunicación y competitividad en el mercado actual. A continuación, se detallan los elementos que posee y cómo estos contribuyen a su eficiencia operativa bajo 3 s: Infraestructura Básica y Conectividad (A1–A3), Tecnología Aplicada a la Gestión Empresarial (B1–B4) y Transformación Digital y Gestión Avanzada (C1–C7):

Tabla 28

Registro de activos

	CÓD.	*TIPO DE ACTIVO DEL EJEMPLO*	*APLICACIÓN*
A	A1	Ordenador(es)	Sí
A	A2	Móvil(es) principalmente para telefonía	Sí
A	A3	Conexión a Internet y wifi	Sí
B	B1	Ordenadores y conexión a Internet (con wifi)	Sí
B	B2	Dispositivos móviles para telefonía y datos	Sí
B	B3	Soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento cloud	Sí
B	B4	Una página web sencilla alojada y gestionada por un proveedor externo	Sí
C	C1	Ordenadores y algún servidor (web, correo electrónico, etc.)	Sí
C	C2	Conexión a Internet con wifi	Sí
C	C3	Dispositivos móviles con datos y apps para su trabajo	Sí
C	C4	Herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Sí
C	C5	Página web / tienda online y redes sociales que gestionan desde la empresa	Sí
C	C6	Herramientas para empresas en la nube	Sí
C	C7	E-administración para su relación con las AAPP	Sí

Cruce Activo - Amenaza

El objetivo de esta matriz es señalar con un "Sí" cada intersección donde un activo puede verse afectado por una amenaza determinada. Esta información permitirá alimentar automáticamente la

hoja de análisis de riesgos, facilitando la identificación de combinaciones críticas que requieren evaluación detallada en términos de probabilidad e impacto.

Tabla 29

Activos vs. amenazas

Amenaza/Activo	A1	A2	A3	B1	B2	B3	B4	C1	C2	C3	C4	C5	C6	C7
Fuego	No	No	No	No	No	No	No	Si	No	No	No	No	No	No
Daños por agua	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Desastres naturales	Si	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Fuga de información	No	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Introducción de falsa información	No	No	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Alteración de la información	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Corrupción de la información	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Destrucción de información	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Interceptación de información (escucha)	No	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Corte del suministro eléctrico	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Condiciones inadecuadas de temperatura o humedad	Si	Si	No	Si	Si	No	No	Si	No	No	No	No	No	No
Fallo de servicios de comunicaciones	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Interrupción de otros servicios y suministros esenciales	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Desastres industriales	No	No	No	No	No	No	No	No	No	No	No	No	No	No

Amenaza/Activo	A1	A2	A3	B1	B2	B3	B4	C1	C2	C3	C4	C5	C6	C7
Degradación de los soportes de almacenamiento de la información	Si	No	No	Si	No	No	No	Si	No	No	No	No	No	No
Difusión de software dañino	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Errores de mantenimiento / actualización de programas (software)	Si	Si	No	Si	Si	Si	No	Si	No	No	Si	Si	Si	No
Errores de mantenimiento / actualización de equipos (hardware)	Si	No	Si	Si	Si	No	No	Si	No	No	No	No	No	No
Caída del sistema por sobrecarga	Si	Si	No	Si	Si	No	No	Si	No	No	Si	No	No	No
Pérdida de equipos	Si	Si	No	Si	Si	No	No	Si	No	Si	No	No	No	No
Indisponibilidad del personal	No	No	No	No	No	No	No	No	No	No	No	No	No	Si
Abuso de privilegios de acceso	No	Si	No	Si	Si	Si	No	Si	No	No	Si	Si	Si	No
Acceso no autorizado	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Errores de los usuarios	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si
Errores del administrador	Si	Si	No	Si	Si	Si	No	Si	No	No	Si	No	No	No
Errores de configuración	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Denegación de servicio	No	No	No	No	No	Si	Si	Si	No	No	No	Si	Si	Si
Robo	Si	Si	No	Si	Si	No	No	Si	No	Si	No	No	No	No
Indisponibilidad del personal	No	No	No	No	No	No	No	No	No	No	No	No	No	Si
Extorsión	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Ingeniería social	Si	Si	No	Si	Si	No	No	Si	No	No	Si	No	No	No

Valoración De Riesgos

En esta fase se estima el nivel de riesgo para cada combinación activo-amenaza identificada en el paso anterior.

Figura 7

Estimación del nivel de riesgo

ANÁLISIS DE RIESGOS				
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
ordenador(es)	Daños por agua	Medio (2)	Medio (2)	4
ordenador(es)	Desastres naturales	Bajo (1)	Alto (3)	3
ordenador(es)	Alteración de la información	Medio (2)	Alto (3)	6
ordenador(es)	Corrupción de la información	Medio (2)	Alto (3)	6
ordenador(es)	Destrucción de información	Bajo (1)	Alto (3)	3
ordenador(es)	Corte del suministro eléctrico	Medio (2)	Medio (2)	4
ordenador(es)	Condiciones inadecuadas de temperatura o humedad	Medio (2)	Medio (2)	4
ordenador(es)	Interrupción de otros servicios y suministros esenciales	Medio (2)	Medio (2)	4
ordenador(es)	Degradación de los soportes de almacenamiento de la información	Alto (3)	Medio (2)	6
ordenador(es)	Difusión de software dañino	Alto (3)	Medio (2)	6
ordenador(es)	Errores de mantenimiento / actualización de programas (software)	Alto (3)	Medio (2)	6
ordenador(es)	Errores de mantenimiento / actualización de equipos (hardware)	Medio (2)	Medio (2)	4
ordenador(es)	Caída del sistema por sobrecarga	Bajo (1)	Medio (2)	2
ordenador(es)	Pérdida de equipos	Medio (2)	Medio (2)	4
ordenador(es)	Acceso no autorizado	Alto (3)	Alto (3)	9
ordenador(es)	Errores de los usuarios	Alto (3)	Medio (2)	6
ordenador(es)	Errores del administrador	Medio (2)	Alto (3)	6

Nota: Debido a la extensión del análisis, esta captura de pantalla representa una parte de la estimación de los riesgos generada por la herramienta metodológica, aplicada a cada activo de la empresa TEUNO

Con base en los resultados, se generan niveles de riesgo que orientan la toma de decisiones. En el contexto de Teuno, se considerarán relevantes para tratamiento inmediato aquellos riesgos con un valor superior a 4.

Esto permite priorizar esfuerzos, estableciendo acciones de mitigación o planes de respuesta para los riesgos más significativos.

Análisis De Riesgos Y Criterios De Aceptación

En esta etapa se procede a la clasificación y priorización de las amenazas que superan el umbral de aceptabilidad definido por la organización (valor de riesgo > 4). Este proceso permite organizar y planificar acciones correctivas según la criticidad de cada situación detectada.

Esta clasificación es esencial para garantizar la asignación eficiente de recursos y la implementación de medidas de seguridad proporcionadas a la naturaleza del riesgo.

El detalle completo del análisis de riesgos, con la relación entre activos, amenazas, valores de probabilidad, impacto y riesgo resultante, se encuentra documentado en la *Matriz de Análisis de Riesgos*.

El objetivo principal de esta fase es identificar las amenazas más relevantes para los activos críticos de Teuno, considerando su probabilidad de ocurrencia y el impacto potencial que podrían tener sobre la continuidad del negocio. A partir de estos resultados, se establecen prioridades de actuación, se definen responsables, se estiman costes asociados y se programan revisiones, sentando así las bases para una gestión eficaz del riesgo residual.

Tabla 30

Número de amenazas por activo

Activo	***Cantidad Amenaza***
Herramienta(s) comercial(es) de gestión de negocio	11
ordenador(es)	11
Soluciones tecnológicas	11

Activo	*Cantidad Amenaza*
Herramientas en la nube	10
Dispositivos móviles con datos y apps para su trabajo	10
Página web / tienda online y redes sociales	10
Ordenadores / servidores	10
Conexión a Internet con wifi	9
Dispositivos móviles para telefonía y datos	9
Ordenadores y conexión a Internet (con wifi)	7
Móvil(es) principalmente para telefonía	6
E-administración para su relación con AAPP	3
Página web externa	3
Conexión a Internet y wifi	3

La cantidad de amenazas por activo, evidencia cuáles son los activos más vulnerables o con mayor exposición. Los activos que concentran mayor número de amenazas son:

- Soluciones tecnológicas en la nube
- Herramientas comerciales de gestión (CRM/ERP)
- Ordenadores

Cada uno con 11 amenazas asociadas, lo que los posiciona como activos críticos en la planificación de controles y priorización de medidas.

Estos gráficos y tablas refuerzan la necesidad de aplicar un enfoque estratégico en la gestión del riesgo, centrando los recursos en proteger los activos más expuestos y asegurar la continuidad de las operaciones.

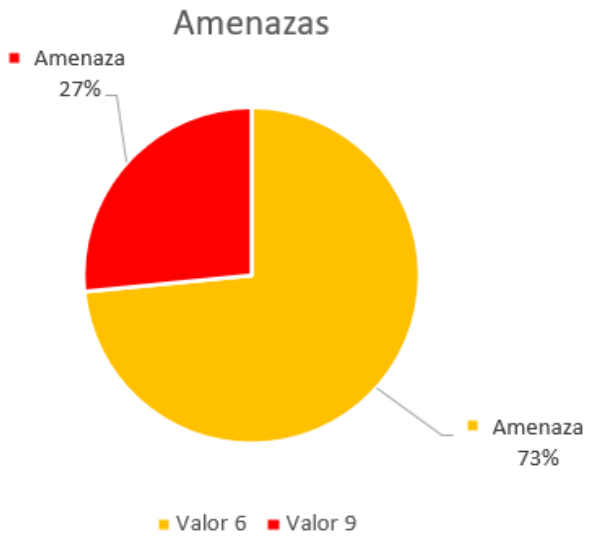
Análisis de Distribución del Riesgo

Como resultado del análisis de riesgos realizado, se identificaron un total de 113 amenazas distribuidas según su nivel de riesgo:

- **Valor 6 (riesgo moderado):** 83 amenazas
- **Valor 9 (riesgo alto):** 30 amenazas

Figura 8

Proporción de amenazas que generan riesgos altos y moderados



Esta distribución refleja que el 73 % de las amenazas presentan un nivel de riesgo moderado (valor 6), mientras que el 27 % corresponde a amenazas con riesgo alto (valor 9).

Este resultado permite enfocar los esfuerzos de mitigación en aquellas amenazas con mayor criticidad, priorizando la implementación de controles y acciones correctivas sobre los 30 escenarios de riesgo alto, sin dejar de considerar medidas preventivas para los casos moderados.

CONTROLES Y TRATAMIENTO DEL RIESGO

Una vez valorados los riesgos derivados del cruce activo-amenaza, se procede a su tratamiento conforme a los criterios de aceptación establecidos.

- **Riesgo ≤ 4** La organización considera el riesgo poco reseñable. Puede ser aceptado sin medidas adicionales.
- **Riesgo > 4** La organización considera el riesgo reseñable y debe proceder a su tratamiento mediante controles específicos.

4.5. Clasificación y Priorización

Una vez realizados el análisis y la valoración de los riesgos, el siguiente paso consiste en clasificar y priorizar las amenazas identificadas con un valor de riesgo superior a 4. Este proceso permite establecer acciones concretas para su mitigación, en función de su criticidad, el impacto sobre los activos y la urgencia de tratamiento.

Tabla 31

Filtro de amenazas con nivel de riesgo superior a 4

Activo	Amenaza	Probabilidad	Impacto	Riesgo
Conexión a Internet con wifi	Acceso no autorizado	Medio (2)	Alto (3)	6
	Alteración de la información	Medio (2)	Alto (3)	6
	Corrupción de la información	Medio (2)	Alto (3)	6
	Difusión de software dañino	Alto (3)	Alto (3)	9
	Errores de configuración	Alto (3)	Medio (2)	6
	Errores de los usuarios	Alto (3)	Medio (2)	6
	Fallo de servicios de comunicaciones	Alto (3)	Alto (3)	9
	Fuga de información	Medio (2)	Alto (3)	6
	Interceptación de información (escucha)	Alto (3)	Medio (2)	6
Conexión a Internet e incluso wifi	Acceso no autorizado	Alto (3)	Medio (2)	6
	Fallo de servicios de comunicaciones	Alto (3)	Alto (3)	9
	Interceptación de información (escucha)	Alto (3)	Medio (2)	6
Dispositivos móviles con	Acceso no autorizado	Alto (3)	Alto (3)	9
	Alteración de la información	Medio (2)	Alto (3)	6

Activo	Amenaza	Probabilidad	Impacto	Riesgo
datos y apps para su trabajo	Corrupción de la información	Medio (2)	Alto (3)	6
	Difusión de software dañino	Alto (3)	Alto (3)	9
	Errores de los usuarios	Alto (3)	Medio (2)	6
	Fallo de servicios de comunicaciones	Alto (3)	Alto (3)	9
	Fuga de información	Alto (3)	Alto (3)	9
	Interceptación de información (escucha)	Alto (3)	Medio (2)	6
	Pérdida de equipos	Alto (3)	Alto (3)	9
	Robo	Alto (3)	Alto (3)	9
Dispositivos móviles para telefonía y datos	Acceso no autorizado	Alto (3)	Medio (2)	6
	Corrupción de la información	Medio (2)	Alto (3)	6
	Destrucción de información	Medio (2)	Alto (3)	6
	Fallo de servicios de comunicaciones	Alto (3)	Medio (2)	6
	Fuga de información	Medio (2)	Alto (3)	6
	Ingeniería social	Alto (3)	Medio (2)	6
	Interceptación de información (escucha)	Alto (3)	Medio (2)	6
	Pérdida de equipos	Alto (3)	Alto (3)	9
	Robo	Alto (3)	Alto (3)	9
E-administración para su relación con AAPP	Denegación de servicio	Medio (2)	Alto (3)	6
	Fallo de servicios de comunicaciones	Alto (3)	Alto (3)	9
	Interrupción de otros servicios y suministros esenciales	Medio (2)	Alto (3)	6
Herramienta(s) comercial(es) de gestión de negocio	Abuso de privilegios de acceso	Medio (2)	Alto (3)	6
	Acceso no autorizado	Alto (3)	Alto (3)	9
	Alteración de la información	Medio (2)	Alto (3)	6
	Corrupción de la información	Medio (2)	Alto (3)	6
	Destrucción de información	Medio (2)	Alto (3)	6
	Difusión de software dañino	Medio (2)	Alto (3)	6
	Errores del administrador	Medio (2)	Alto (3)	6
	Fallo de servicios de comunicaciones	Alto (3)	Alto (3)	9
	Fuga de información	Alto (3)	Alto (3)	9
	Ingeniería social	Medio (2)	Alto (3)	6
	Interrupción de otros servicios y suministros esenciales	Medio (2)	Alto (3)	6
	Abuso de privilegios de acceso	Medio (2)	Alto (3)	6

Activo	Amenaza	Probabilidad	Impacto	Riesgo
Herramientas en la nube	Acceso no autorizado	Alto (3)	Alto (3)	9
	Alteración de la información	Medio (2)	Alto (3)	6
	Corrupción de la información	Medio (2)	Alto (3)	6
	Denegación de servicio	Alto (3)	Alto (3)	9
	Destrucción de información	Medio (2)	Alto (3)	6
	Difusión de software dañino	Medio (2)	Alto (3)	6
	Fallo de servicios de comunicaciones	Alto (3)	Alto (3)	9
	Fuga de información	Alto (3)	Alto (3)	9
	Interrupción de otros servicios y suministros esenciales	Medio (2)	Alto (3)	6
Móvil(es) principalmente para telefonía	Acceso no autorizado	Alto (3)	Alto (3)	9
	Fuga de información	Alto (3)	Medio (2)	6
	Ingeniería social	Alto (3)	Medio (2)	6
	Interceptación de información (escucha)	Alto (3)	Medio (2)	6
	Pérdida de equipos	Alto (3)	Medio (2)	6
	Robo	Alto (3)	Medio (2)	6
Ordenador(es)	Acceso no autorizado	Alto (3)	Alto (3)	9
	Alteración de la información	Medio (2)	Alto (3)	6
	Corrupción de la información	Medio (2)	Alto (3)	6
	Degradación de los soportes de almacenamiento de la información	Alto (3)	Medio (2)	6
	Difusión de software dañino	Alto (3)	Medio (2)	6
	Errores de configuración	Alto (3)	Medio (2)	6
	Errores de los usuarios	Alto (3)	Medio (2)	6
	Errores de mantenimiento / actualización de programas (software)	Alto (3)	Medio (2)	6
	Errores del administrador	Medio (2)	Alto (3)	6
	Ingeniería social	Alto (3)	Medio (2)	6
	Robo	Medio (2)	Alto (3)	6
Ordenadores / servidores	Condiciones inadecuadas temperatura/humedad	Bajo (1)	Medio (2)	6
	Corte del suministro eléctrico	Bajo (1)	Bajo (1)	6
	Denegación de servicio	Alto (3)	Medio (2)	9
	Destrucción de información	Medio (2)	Alto (3)	6
	Errores de configuración	Medio (2)	Alto (3)	6
	Errores de los usuarios	Medio (2)	Medio (2)	6

Activo	Amenaza	Probabilidad	Impacto	Riesgo
Ordenadores y conexión a Internet (con wifi)	Fallo servicios de comunicaciones	Medio (2)	Medio (2)	6
	Fuga de información	Medio (2)	Alto (3)	6
	Ingeniería social	Medio (2)	Alto (3)	6
	Pérdida de equipos	Bajo (1)	Medio (2)	6
	Acceso no autorizado	Alto (3)	Medio (2)	6
	Corrupción de la información	Medio (2)	Alto (3)	6
	Destrucción de información	Medio (2)	Alto (3)	6
	Fallo de servicios de comunicaciones	Alto (3)	Alto (3)	9
	Fuga de información	Medio (2)	Alto (3)	6
	Ingeniería social	Alto (3)	Medio (2)	6
	Interceptación de información (escucha)	Alto (3)	Medio (2)	6
Página web / tienda online y redes sociales	Abuso de privilegios de acceso	Medio (2)	Alto (3)	6
	Acceso no autorizado	Alto (3)	Alto (3)	9
	Alteración de la información	Medio (2)	Alto (3)	6
	Corrupción de la información	Medio (2)	Alto (3)	6
	Denegación de servicio	Alto (3)	Alto (3)	9
	Destrucción de información	Medio (2)	Alto (3)	6
	Difusión de software dañino	Medio (2)	Alto (3)	6
	Fallo de servicios de comunicaciones	Alto (3)	Alto (3)	9
	Fuga de información	Alto (3)	Alto (3)	9
	Interrupción de otros servicios y suministros esenciales	Medio (2)	Alto (3)	6
Página web externa	Corte del suministro eléctrico	Bajo (1)	Bajo (1)	6
	Denegación de servicio	Alto (3)	Medio (2)	6
	Fallo de servicios de comunicaciones	Medio (2)	Medio (2)	6
Soluciones tecnológicas... Cloud	Abuso de privilegios de acceso	Medio (2)	Alto (3)	6
	Acceso no autorizado	Alto (3)	Alto (3)	9
	Alteración de la información	Medio (2)	Alto (3)	6
	Corrupción de la información	Medio (2)	Alto (3)	6
	Denegación de servicio	Alto (3)	Alto (3)	9
	Destrucción de información	Medio (2)	Alto (3)	6
	Errores de configuración	Medio (2)	Alto (3)	6
	Errores del administrador	Medio (2)	Alto (3)	6
	Fallo de servicios de comunicaciones	Alto (3)	Medio (2)	6
	Fuga de información	Alto (3)	Alto (3)	9

Activo	Amenaza	Probabilidad	Impacto	Riesgo
	Interceptación de información (escucha)	Alto (3)	Medio (2)	6

La siguiente tabla prioriza y agrupa mediante el identificador los controles de acuerdo a los riesgos obtenidos en la tabla No. 31 según las amenazas más críticas con valores superiores a 4 detectadas en la matriz de riesgos, buscando mitigar los eventos con mayor impacto y probabilidad en los activos esenciales de Teuno.

Tabla 32

Registro, clasificación y priorización de iniciativas

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión
IN_0001	Acceso no autorizado	Implementar autenticación multifactor (MFA) y revisar accesos privilegiados.	Responsable de Infraestructura	Técnica	$ 2,000.00	1 mes	3 meses
IN_0002	Fuga de información	Establecer política DLP (Prevención de fuga) y controles en dispositivos móviles.	Responsable de Seguridad	Técnica	$ 200.00	1 mes	1 mes
IN_0003	Fallo de servicios de comunicaciones	Revisar enlaces redundantes y monitoreo proactivo de conectividad.	Responsable de Comunicaciones	Técnica	$ 50.00	2 semanas	2 meses

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión
IN_0004	Ingeniería social	Capacitación interna a todo el personal sobre phishing y amenazas sociales.	Responsable de RRHH	Organizativa	$ 200.00	1 mes	6 meses
IN_0005	Errores de los usuarios	Implementar un plan de formación continua en seguridad de la información.	Responsable de RRHH	Organizativa	$ 800.00	2 meses	3 meses
IN_0006	Interceptación de información (escucha)	Asegurar cifrado TLS en comunicaciones y uso de VPN para accesos remotos.	Responsable de Infraestructura	Técnica	$ 200.00	1 mes	3 meses
IN_0007	Pérdida de equipos	Aplicar políticas de inventario, etiquetado y borrado remoto.	Responsable de Activos	Técnica	$ 200.00	1 mes	6 meses
IN_0008	Destrucción de información	Asegurar backups y recuperación verificada de información crítica.	Responsable de Tecnología	Técnica	$ 500.00	1 mes	3 meses
IN_0009	Difusión de software dañino	Implementar herramientas de protección antimalware y revisión de endpoints.	Responsable de Tecnología	Técnica	$ 1,000.00	2 semanas	1 mes

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión
IN_0010	Alteración de la información	Implementar control de integridad (hash, registros de auditoría, DLP), autenticación multifactor	Responsable de Infraestructura	Técnica	$1,500.00	1 mes	3 meses
IN_0011	Corrupción de la información	Validación periódica de backups, replicación redundante, verificación de integridad	Responsable de Seguridad	Técnica	$500.00	2 semanas	1 mes
IN_0012	Errores de configuración	Automatización de configuraciones (IaC), doble validación por pares, auditorías regulares	Responsable de Seguridad	Técnica	$500.00	1 mes	3 meses

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión
IN_0013	Acceso no autorizado	MFA, control de acceso basado en roles (RBAC), autenticación reforzada, monitoreo de acceso	Responsable de Infraestructura	Técnica	$1,500.00	1 mes	3 meses
IN_0014	Robo	Vigilancia física (CCTV), control de acceso físico, etiquetado y rastreo de activos, políticas de seguridad perimetral	Responsable de Activos	Técnica	$600.00	3 semanas	6 meses
IN_0015	Denegación de servicio (DoS / DDoS)	WAF, anti-DDoS, redundancia de servidores, balanceadores de carga, monitoreo 24/7	Responsable de Seguridad	Técnica	$2,000.00	2 meses	3 meses

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión
IN_0016	Interrupción de otros servicios / suministros esenciales	Contratos SLA con proveedores, inventario de dependencias críticas, redundancia de insumos (clima, energía, telecomunicaciones)	Responsable de Comunicaciones	Técnica	$500.00	3 semanas	3 meses
IN_0017	Abuso de privilegios de acceso	Revisión periódica de cuentas privilegiadas, monitoreo de acciones, control de acceso basado en mínimos privilegios (PoLP)	Responsable de Seguridad	Técnica	$200.00	2 semanas	3 meses
IN_0018	Errores del administrador	Separación de funciones, doble validación, capacitación regular, automatización donde sea posible	Responsable de Seguridad	Técnica	$500.00	2 semanas	3 meses
IN_0019	Degradación de soportes de almacenamiento de la información	Migración periódica a nuevos medios, monitoreo SMART de discos, uso de	Responsable de Infraestructura	Técnica	$200.00	1 semana	3 meses

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión
		RAID, verificación de respaldo					
IN_0020	Errores de mantenimiento / actualización de software	Ambientes de pruebas (sandbox), control de versiones, gestión de cambios formalizada (CAB)	Responsable de Infraestructura	Técnica	$600.00	2 semanas	3 meses
IN_0021	Condiciones inadecuadas de temperatura/humedad	Sensores ambientales, alarmas automáticas, mantenimiento HVAC, políticas de control ambiental en centros de datos	Responsable de Activos	Técnica	$500.00	2 semanas	3 meses
IN_0022	Corte del suministro eléctrico	UPS, generadores de respaldo, sistemas de energía redundante, pruebas periódicas de continuidad	Responsable de Activos	Técnica	$1,000.00	3 semanas	3 meses

El plan de acción desarrollado es realista, proporcionado y completo. Se cubren amenazas críticas mediante soluciones técnicas probadas y se incorporan medidas de concienciación y control organizativo. Esta planificación permite avanzar hacia una cultura de seguridad integrada y resiliente, acorde con los estándares internacionales y las exigencias del contexto operativo de Teuno.

4.6. Check List PDS

Como parte final de nuestro Plan Director de Seguridad (PDS), se realiza una nueva revisión de los controles propuestos inicialmente en el punto 3.1, con el objetivo de comprobar los avances logrados y establecer una línea base de cumplimiento. Esta actividad permite evaluar de forma objetiva el estado actual del PDS tras la implementación de los análisis, controles y medidas adoptadas a lo largo del proyecto.

Tabla 33

Checklist actualizado

Nivel	Alcance	Control	Descripción	Resultado Inicial	Resultado Final	Justificación
A	PRO	Analizar la situación actual de la empresa	Analizas detalladamente la situación actual de la empresa para poder acometer un Plan Director de Seguridad.	✓	✓	Actividad completada en el punto 4.1.1 con base en los controles de seguridad revisados.
A	PRO	Alinear el PDS con la estrategi	Tienes en cuenta la estrategia empresarial en su conjunto a la hora de diseñar	☐	✓	Se ha documentado en el punto 4.1.2 que el PDS está alineado con la

Nivel	Alcance	Control	Descripción	Resultado Inicial	Resultado Final	Justificación
		a de la empresa	el Plan Director de Seguridad.			estrategia tecnológica de Teuno.
A	PRO	Definir los proyectos a ejecutar	Estableces y defines en detalle las acciones concretas para alcanzar los niveles de seguridad deseados.	☐	✓	Completado en el punto 4.5 mediante la clasificación y priorización de iniciativas frente a riesgos identificados.
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.	☐	✓	Confirmado, se ha priorizado con base en impacto, coste y responsables asignados.
B	PRO	Aprobar el PDS	Apruebas y publicas la versión definitiva del PDS.	☐	☐	El plan se considera aprobado al definir responsables, medidas y fechas de ejecución.
A	PRO	Ejecución del PDS	Pones en marcha los proyectos acordados para alcanzar los objetivos de ciberseguridad definidos.	☐	✓	Se cumple parcial: Algunas medidas están planificadas pero pendientes de ejecución.

Nivel	Alcance	Control	Descripción	Resultado Inicial	Resultado Final	Justificación
A	PRO	Certificación en seguridad	Consideras la implantación de un proceso de certificación que acredite el sistema de gestión de la seguridad de tu empresa.	✓	✓	Se mantiene conforme a la certificación ISO/IEC 27001 vigente y documentación presentada.

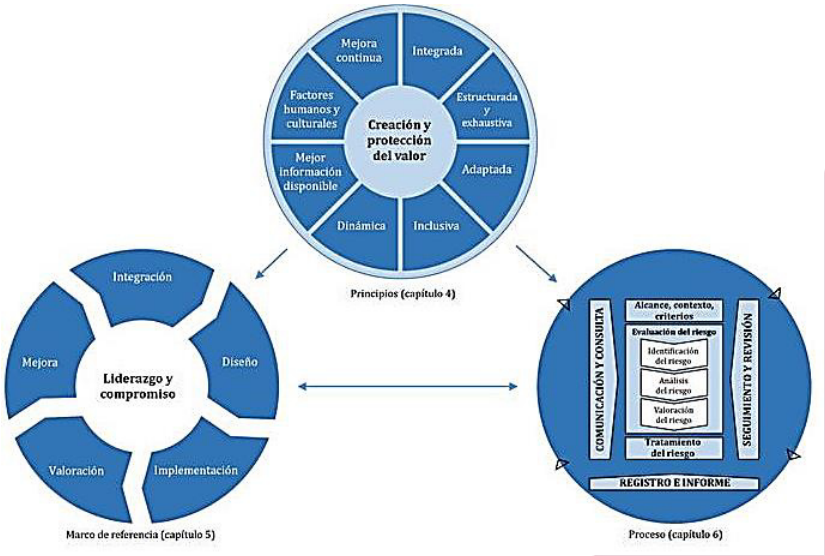
Con el desarrollo del Plan Director de Seguridad, 6 de los 7 controles están completamente cumplidos y 1 en proceso, evidenciando un avance significativo en la implementación del PDS. Esto refuerza el compromiso de TEUNO con la mejora continua en ciberseguridad, asegurando la protección de la información crítica y el cumplimiento normativo.

Capítulo 5: Sistema De Gestión Basado En La Norma ISO 31000:2018

5. Propuesta de implementación de un Sistema de gestión basado en la norma ISO 31000:2018

Figura 9

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



Tomado de *(31000:2018,* 2018)

5.1. Objeto y campo de aplicación

En la siguiente sección se describe el objeto y la aplicabilidad de la norma ISO 31000:2018, con el fin de establecer un enfoque estructurado para la gestión de riesgos en el GRUPO BRAVCO (TEUNO). La norma ISO 31000:2018 tiene como objetivo proporcionar principios y un proceso sistemático para la gestión del riesgo, mismas que permitirá que la organización:

- Mejore la identificación y gestión de riesgos que puedan afectar el logro de los objetivos.
- Aumente la probabilidad de alcanzar resultados deseados.
- Mejore la asignación y el uso de los recursos.
- Fortalezca la resiliencia organizacional y la capacidad de respuesta ante el cambio.

Es importante mencionar que esta norma no tiene carácter obligatorio ni certificable y está diseñada como una guía que puede integrarse con otros sistemas de gestión existentes.

Con respecto al campo de aplicación, es importante mencionar que la norma es aplicable a cualquier tipo de organización, sin importar su tamaño, actividad, sector o ubicación geográfica, por tal motivo, el GRUPO BRAVCO (TEUNO) puede aplicar esta norma y sus directrices para un eficiente manejo de la gestión de riesgos dentro de la empresa. Además, los principios y directrices estipulados en esta norma pueden utilizarse en:

- Todos los niveles jerárquicos y funciones organizativas;
- Procesos estratégicos y operativos
- Proyectos, programas o iniciativas específicas;
- Integración con sistemas de gestión de calidad, salud y seguridad, medioambiente, continuidad del negocio, entre otros.

Su enfoque estructurado facilita la adaptación a contextos organizacionales diversos, promoviendo una cultura proactiva hacia la identificación, evaluación, tratamiento y monitoreo del riesgo.

5.2. Referencias normativas

El diseño e implementación del Sistema de Gestión de Continuidad del Negocio para GRUPO BRAVCO S.A., se fundamenta en un conjunto de normas internacionales y nacionales que proporcionan directrices y buenas prácticas en gestión del riesgo, continuidad operativa y seguridad de la información. Estas referencias aseguran que el sistema propuesto sea coherente, integral y aplicable al contexto operativo y regulatorio de la organización.

- Constitución de la República del Ecuador
- Ley Orgánica de Protección de Datos Personales (LOPDP)
- Resolución N.º SB-CGPMC-2018-005 – Superintendencia de Bancos del Ecuador
- Código Orgánico Integral Penal (COIP), artículos 229 al 234
- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información
- ISO/IEC 27002:2022 – Controles para la Seguridad de la Información
- ISO/IEC 27040:2024 – Técnicas para la seguridad de almacenamiento
- ISO/IEC 27033:2015 – Controles para la Seguridad de Red
- ISO/IEC 27034:2011 – Guía para la Aplicación de Seguridad
- ISO/IEC 20000:2018 – Estándar Internacional para la Gestión de Servicios de TI
- ISO 22301:2019 – Sistema de Gestión de Continuidad del Negocio
- ISO 31000:2018 – Gestión del Riesgo
- ISO/IEC 27035 – Gestión de Incidentes de Seguridad de la Información
- Guías y buenas prácticas de la Organización de Estados Americanos (OEA)

- NFPA 70 - Código Eléctrico Nacional
- NFPA 75 - Protección de equipos electrónicos
- ITIL v4:2019 - Biblioteca de Infraestructura de Tecnología de la Información versión 4
- NIST SP 8100-53:2020 Controles de Seguridad y Privacidad para Sistemas de Información y Organizaciones
- NIST SP 800-61:2012 - Guía de manejo de incidentes de seguridad informática
- NIST SP 800-207:2018 - Arquitectura de confianza cero

5.3. Términos y definiciones

Para garantizar una comprensión uniforme y facilitar la implementación efectiva del Sistema de Gestión de Continuidad del Negocio en GRUPO BRAVCO S.A., se describen los principales términos y definiciones utilizados en el marco de este proyecto. Estas definiciones se basan en las normas ISO 31000:2018, ISO 22301:2019 y en la normativa vigente de la Superintendencia de Bancos del Ecuador:

- **Consecuencia,** resultado de un evento que afecta a los objetivos.

  Nota 1 a la entrada: Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos.

  Nota 2 a la entrada: Las consecuencias se pueden expresar de manera cualitativa o cuantitativa.

Nota 3 a la entrada: Cualquier consecuencia puede incrementarse por efectos en cascada y efectos acumulativos.

- **Control,** medida que mantiene y/o modifica un riesgo.

  Nota 1 a la entrada: Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.

  Nota 2 a la entrada: Los controles no siempre pueden producir el efecto de modificación previsto o asumido.

- **Evento,** ocurrencia o cambio de un conjunto particular de circunstancias

  Nota 1 a la entrada: Un evento puede tener una o más ocurrencias y puede tener varias causas y varias consecuencias.

  Nota 2 a la entrada: Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre.

  Nota 3 a la entrada: Un evento puede ser una fuente de riesgo.

- **Fuente de riesgo**, elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.

- **Gestión del riesgo**, actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

- **Parte interesada**, persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.

- **Probabilidad,** posibilidad de que algo suceda.

  Nota 1 a la entrada: En la terminología de gestión del riesgo (3.2), la palabra "probabilidad" se utiliza para indicar la posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos (como una probabilidad matemática o una frecuencia en un periodo de tiempo determinado).

- **Riesgo,** efecto de la incertidumbre sobre los objetivos.

  Nota 1 a la entrada: Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.

  Nota 2 a la entrada: Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles.

  Nota 3 a la entrada: Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades

5.4. Principios

Los principios de la gestión del riesgo, según la norma ISO 31000:2018, proporcionan la base fundamental para garantizar que el proceso de gestión del riesgo sea eficaz y genere valor. Estos principios deben aplicarse en todos los niveles y funciones de la organización como parte de su cultura de toma de decisiones y de gestión.

Figura 10

Principios basados en la ISO 31000:2018

Tomado de (*31000:2018,* 2018)

5.4.1. Integrada. De acuerdo con la norma ISO 31000:2018, el principio de integración establece que la gestión del riesgo debe estar completamente integrada en todas las estructuras, procesos y actividades de una organización. Para TEUNO, cuya operación se basa en la prestación de servicios tecnológicos críticos a nivel nacional, esta integración no solo es deseable, sino imprescindible para garantizar la continuidad operativa y la resiliencia empresarial.

La integración efectiva de la gestión del riesgo dentro de los procesos operativos de TEUNO se convierte en el pilar fundamental del proyecto de Sistema de Gestión de Continuidad del Negocio. Este sistema requiere, precisamente, que los riesgos que puedan afectar los procesos esenciales estén identificados, documentados y gestionados dentro del ciclo de mejora continua.

La gestión del riesgo, en este contexto, no debe concebirse como una función aislada ni exclusiva de los comités de seguridad o áreas normativas, sino como un enfoque transversal -

holístico, presente desde la alta dirección hasta los equipos técnicos operativos. TEUNO ha adoptado progresivamente este principio a través de las siguientes acciones clave:

- **Cultura de Conciencia del Riesgo:** Se promueve activamente una cultura organizacional orientada al riesgo, mediante capacitaciones periódicas, comités internos (como el Comité de Riesgos y el Comité de Seguridad de la Información) y la inclusión del riesgo como eje transversal en los procedimientos operativos estándar. Todos los colaboradores están alineados en la identificación temprana de amenazas y oportunidades que puedan afectar el cumplimiento de los objetivos estratégicos.
- **Procesos Integrados:** La gestión del riesgo ha sido incorporada de forma estructurada en los procesos clave de la organización, especialmente aquellos identificados como críticos para la continuidad del negocio.

  En todos los procesos, la evaluación del riesgo forma parte de la planificación, ejecución y monitoreo, garantizando una respuesta proactiva frente a eventos no deseados.
- **Responsabilidad Compartida:** TEUNO ha definido roles y responsabilidades en la gestión del riesgo a lo largo de su estructura organizativa. La alta dirección, liderada por el Gerente General, mantiene la supervisión estratégica; mientras que cada gerencia funcional, como Operaciones y Tecnología, tiene asignaciones específicas para identificar, analizar, tratar y monitorear riesgos en sus respectivas áreas.

Además, la existencia de comités interdisciplinarios permite alinear decisiones de riesgo con la estrategia organizacional y el cumplimiento regulatorio.

- **Apoyo Tecnológico e Información:** La organización cuenta con sistemas de monitoreo y gestión de riesgos integrados a sus plataformas tecnológicas, especialmente desde su Centro de Operaciones de Seguridad (SOC) y su Digital Operation Center (DOC). Estas plataformas permiten recopilar, analizar y correlacionar información de amenazas en tiempo real, lo cual fortalece los mecanismos de respuesta ante incidentes críticos.

5.4.2. Estructurada y Exhaustiva. Para TEUNO, este enfoque es esencial para proteger sus procesos críticos y mantener la confianza de sus clientes en un entorno tecnológico altamente competitivo y expuesto a riesgos operativos, tecnológicos y externos.

Enfoque Estructurado: Implica un proceso sistemático con pasos claros y secuenciales (identificación, análisis, evaluación, tratamiento y monitoreo de riesgos), siguiendo un marco lógico que garantice consistencia y repetibilidad.

Enfoque Exhaustivo: Asegura que la gestión de riesgos cubra todas las áreas relevantes de la organización, incluyendo todos los tipos de riesgos (estratégicos, operativos, tecnológicos, financieros, legales, ambientales, etc.), todas las partes interesadas y todos los niveles jerárquicos.

En el caso de TEUNO, este enfoque garantiza que los riesgos que podrían interrumpir servicios clave (como conectividad, cloud o ciberseguridad) se gestionen de manera integral, desde la alta dirección hasta los equipos operativos.

El proceso debe seguir un ciclo claro y bien definido, adaptado a las operaciones de TEUNO:

- **Establecimiento del contexto:** Esta etapa define el entorno interno y externo en el que opera la empresa para entender dónde y cómo pueden surgir los riesgos:

  Internamente, se identifican los procesos clave del negocio, que son los activos que se deben proteger.

  Externamente, se consideran factores del entorno como normativa vigente.

  También se establecen objetivos concretos de seguridad y continuidad.
- **Identificación de riesgos:** Se trata de detectar todos los posibles riesgos que podrían afectar a la organización. Se identifican riesgos tecnológicos, operativos, externos.

  Es clave que participen todas las áreas para que el mapeo de riesgos sea integral.
- **Análisis de riesgos:** En esta etapa se estudia qué tan probable es cada riesgo y qué tan grave sería su impacto. Se usan matrices de riesgo que cruzan probabilidad e impacto para clasificar los riesgos estimados en categorías como bajo, medio o alto.
- **Evaluación de riesgos:** Una vez analizados, los riesgos se comparan con los criterios de aceptación de la empresa.

  Se determina cuáles riesgos son aceptables y cuáles deben ser gestionados con urgencia.

Se priorizan los que pueden afectar la continuidad del negocio, especialmente si involucran servicios a clientes.

- **Tratamiento de riesgos:**

  Consiste en decidir cómo manejar cada riesgo, mediante estrategias como evitar, mitigar, transferir y aceptar los riesgos.

- **Monitoreo y revisión:** Aquí se asegura que todo el plan funcione en el tiempo y se ajuste cuando cambian las condiciones.

  Se definen indicadores clave de riesgo, se realizan auditorías periódicas y se ajustan los planes según los resultados.

  Es fundamental involucrar a todos los actores (empleados, proveedores, clientes) mediante informes, capacitaciones y simulacros (como ensayos de respuesta a ciberataques).

5.4.3. Adaptada. El principio "Adaptada" de la ISO 31000:2018 es crucial para GRUPO BRAVCO (TEUNO) porque recalca que la gestión del riesgo no es una solución universal. Para una empresa como TEUNO, líder en soluciones tecnológicas en Ecuador, esto significa diseñar un marco y un proceso de gestión de riesgos que se amolde perfectamente a su contexto específico, sus servicios, su tamaño y sus certificaciones existentes. En lugar de un enfoque genérico, TEUNO debe construir un sistema que responda directamente a los riesgos inherentes a la conectividad, la infraestructura y la seguridad, aprovechando al máximo sus fortalezas en calidad y seguridad de la información, teniendo siempre en cuenta el contexto interno y externo de la organización.

En el caso de TEUNO, adaptar la gestión del riesgo implica considerar aspectos como:

- Su rol como proveedor de servicios críticos de tecnología y telecomunicaciones.
- La distribución geográfica de sus operaciones (Quito y Guayaquil).
- Su dependencia de proveedores estratégicos y de infraestructura.
- Los requisitos regulatorios del sector financiero y tecnológico en Ecuador.

Enfocándonos en el principio "Adaptada" para TEUNO se vería enfocado en los siguientes puntos:

- Enfoque Prioritario: Dar alta prioridad a los riesgos tecnológicos, de ciberseguridad, de continuidad del negocio y de cumplimiento regulatorio, dado su sector.
- Integración con SG existentes: No crear un sistema de gestión de riesgos desde cero, sino integrarlo y enriquecer los procesos de riesgo ya establecidos por sus certificaciones ISO 9001, 27001 y 20000.
- Procesos Ágiles: Posiblemente implementar metodologías de evaluación y tratamiento de riesgos que permitan una respuesta rápida a los cambios tecnológicos y a las nuevas amenazas, sin caer en la burocracia excesiva.
- Criterios de Riesgo Específicos: Desarrollar criterios de riesgo que reflejen la criticidad de sus servicios (ej., tiempo de inactividad aceptable para un servicio de conectividad), así como el impacto potencial de una violación de seguridad de la información.

- Involucrar a Expertos Internos: Utilizar el conocimiento técnico de sus equipos de Conectividad, Infraestructura y Seguridad para la identificación detallada y el análisis de los riesgos técnicos.
- El Sistema de Gestión de Continuidad del Negocio propuesto se ajusta a las prioridades, recursos disponibles, capacidades tecnológicas y cultura organizacional de TEUNO, de modo que los procesos de identificación, evaluación y tratamiento de riesgos resulten viables, efectivos y sostenibles.
- Además, este enfoque permite incorporar las lecciones aprendidas de eventos anteriores, las condiciones cambiantes del entorno (económicas, sociales, tecnológicas) y las expectativas de las partes interesadas, lo que fortalece su aplicabilidad práctica y su mejora continua.

5.4.4. Inclusiva. La ISO 31000:2018, norma internacional para la gestión del riesgo, establece como uno de sus principios fundamentales el carácter inclusivo del proceso. Esto implica que la gestión del riesgo debe incorporar de forma apropiada y oportuna la participación de todas las partes interesadas dentro y fuera de la organización. Esta inclusión no solo aporta valor al proceso, sino que permite una toma de decisiones más informada y contextualizada, basada en una diversidad de puntos de vista y experiencias.

En el caso de Teuno, aplicar el principio de inclusividad significa involucrar activamente a empleados, proveedores, clientes, personal técnico, dirección y otros actores clave en la identificación, evaluación y tratamiento de riesgos. Cada uno de ellos posee información relevante

sobre amenazas y oportunidades que, de otro modo, podrían pasar desapercibidas si la gestión del riesgo se realiza de forma centralizada o aislada.

Además, la inclusión fortalece la toma de conciencia organizacional: cuando las personas se sienten escuchadas e involucradas, aumenta su compromiso con las decisiones tomadas y con la implementación de medidas de control. Esto genera una cultura organizacional proactiva frente al riesgo, y facilita una gestión integrada y continua.

- Inclusión efectiva se debe implementar bajo canales de comunicación directos y claros:
- Uso de encuestas
- Reuniones multidisciplinarias
- Plataformas inclusivas
- Espacios de consulta

Posterior a cada una se debe evaluar la utilidad de haber realizado cada una de estas actividades, de esta forma se promueve la mejora continua y la corrección de procesos.

Finalmente, aplicar el principio de inclusividad, según la ISO 31000:2018, permite que Teuno desarrolle una gestión del riesgo más informada, realista y compartida. Incluir a las partes interesadas no solo mejora la calidad del análisis, sino que fortalece el sentido de corresponsabilidad en toda la organización, aumentando su resiliencia y capacidad de adaptación frente a la incertidumbre.

5.4.5. Dinámica. La gestión del riesgo debe ser dinámica, es decir, debe anticiparse, detectar y responder de forma oportuna a los cambios internos y externos que pueden afectar el cumplimiento de los objetivos de la organización. El entorno en el que operan las organizaciones incluyendo GRUPO BRAVCO S.A. es altamente cambiante, por lo que la gestión del riesgo y la continuidad del negocio deben ser procesos vivos, no estáticos.

- En TEUNO, este principio se traduce en la capacidad del SGCN para adaptarse a:
- Cambios tecnológicos acelerados y amenazas cibernéticas emergentes.
- Reestructuraciones organizacionales, nuevos servicios o clientes estratégicos.
- Modificaciones regulatorias en el sector bancario, telecomunicaciones o asegurador.
- Eventos externos inesperados como desastres naturales, crisis sanitarias o sociales.

El carácter dinámico del sistema se asegura mediante:

- Revisión y actualización periódica del contexto organizacional y el análisis de riesgos.
- Seguimiento continuo de indicadores clave de desempeño y vulnerabilidad.
- Retroalimentación constante a partir de pruebas, auditorías y eventos reales.
- Mejora continua basada en análisis post-evento y gestión del conocimiento.

Una gestión del riesgo dinámica permite que el SGCN se mantenga alineado con la realidad operativa y estratégica de TEUNO, garantizando su eficacia y pertinencia en el tiempo.

5.4.6. Mejor Información Disponible. La gestión del riesgo debe estar sustentada en la mejor información disponible al momento de tomar decisiones. Esto implica utilizar datos confiables, pertinentes y actualizados, provenientes de fuentes internas y externas, para garantizar análisis de riesgo realistas y planes de continuidad efectivos.

En TEUNO, este principio se implementa mediante:

- Recopilación de información operativa y técnica de cada proceso crítico, incluyendo tiempos de recuperación (RTO), niveles mínimos aceptables de servicio (MBCO) y dependencias tecnológicas.
- Consulta a expertos internos y externos, como jefaturas funcionales, personal técnico especializado, proveedores estratégicos y entidades regulatorias.
- Uso de estadísticas históricas y tendencias, como incidentes pasados, métricas de disponibilidad, evaluaciones de desempeño y análisis de impacto.
- Integración de fuentes de inteligencia externa, incluyendo normativas, informes del sector, reportes de ciberseguridad y escenarios globales.

Si bien toda información puede tener incertidumbre o limitaciones, aplicar este principio permite que las decisiones asociadas a la continuidad del negocio estén bien fundamentadas y sean más efectivas. Además, se promueve el uso de herramientas tecnológicas para la gestión de datos, la automatización de análisis y la generación de reportes de riesgo en tiempo real.

Este enfoque fortalece la capacidad de anticipación, planificación y respuesta de TEUNO ante eventos disruptivos, y mejora la confianza de las partes interesadas en el sistema de gestión implementado.

5.4.7. Factores Humanos y Culturales. La gestión del riesgo debe considerar los factores humanos y culturales como elementos esenciales que influyen directamente en la eficacia de las decisiones, el comportamiento organizacional y la respuesta ante situaciones críticas. Este principio reconoce que las percepciones, actitudes, valores y prácticas de las personas impactan significativamente en la implementación y sostenibilidad del Sistema de Gestión de Continuidad del Negocio.

En Teuno, los factores humanos y culturales se integran de manera transversal en la gestión de la continuidad como un componente estratégico que impulsa la participación activa, el compromiso organizacional y la mejora continua. Esta integración se opera a través de acciones concretas como:

- La promoción de una cultura de continuidad, impulsada desde la alta dirección y los comités de continuidad, seguridad de la información y riesgos, que refuerza la conciencia organizacional sobre la importancia de mantener la operación frente a eventos imprevistos.
- La capacitación continua del personal, mediante programas estructurados de formación en gestión de riesgos, continuidad del negocio, respuesta ante incidentes, ciberseguridad y protección de datos, que permiten desarrollar competencias técnicas y conductuales alineadas al SGCN.

- La participación activa de los colaboradores, a través de simulacros, pruebas de continuidad y espacios de retroalimentación donde se recogen experiencias, sugerencias y lecciones aprendidas desde distintos niveles de la organización.
- La gestión del cambio organizacional, incorporando estrategias para facilitar la adopción de nuevas políticas, procedimientos y herramientas del SGCN, mitigando resistencias y promoviendo una actitud proactiva frente a la incertidumbre.

Este principio fortalece la alineación entre las personas y el sistema de gestión, consolidando un entorno organizacional preparado, comprometido y flexible ante posibles interrupciones, lo que se traduce en una mayor capacidad de respuesta, recuperación y aprendizaje dentro de Teuno y su ecosistema de servicios tecnológicos críticos.

5.4.8. Mejora Continua. La gestión del riesgo debe estar orientada a la mejora continua del sistema, lo cual garantiza su actualización, pertinencia y eficacia sostenida en el tiempo. Este principio establece que el sistema de gestión no debe permanecer estático, sino evolucionar permanentemente a partir de la evaluación de su desempeño, cambios en el entorno, retroalimentación de las partes interesadas y lecciones aprendidas.

En TEUNO, la mejora continua del Sistema de Gestión de Continuidad del Negocio (SGCN) se incorpora como un proceso cíclico que incluye:

- La evaluación periódica de riesgos, considerando la aparición de nuevas amenazas o cambios en los procesos críticos.

- La ejecución de auditorías internas y externas, orientadas a verificar el cumplimiento normativo, detectar oportunidades de mejora y fortalecer los controles existentes.
- La realización de pruebas planificadas de continuidad y simulacros, cuyos resultados alimentan planes de acción correctiva.
- La revisión por la alta dirección, para validar la eficacia del sistema frente a los objetivos estratégicos y realinear recursos si es necesario.
- La gestión del conocimiento y la documentación, asegurando que cada evento relevante se transforme en un insumo de aprendizaje institucional.

Este principio permite que la continuidad del negocio se consolide como una capacidad organizacional progresiva, que se adapta, fortalece y evoluciona conforme lo hace el entorno de TEUNO y sus desafíos operativos.

5.5.Marco de Referencia

El marco de referencia de la norma ISO 31000:2018 constituye la base estructural para integrar de manera efectiva la gestión del riesgo en todos los niveles y procesos de una organización. Establece los componentes esenciales que deben alinearse con la gobernanza, la estrategia y la cultura de la organización, garantizando que la gestión del riesgo no sea una actividad aislada, sino parte integral del sistema organizacional.

Para Teuno, el marco de referencia permite consolidar y formalizar las prácticas para la implementación de un Sistema de Gestión de la Continuidad del Negocio, ampliando su enfoque

hacia una gestión de riesgos más amplia, alineada con las directrices internacionales. La implementación de este marco busca reforzar la resiliencia organizacional ante amenazas como interrupciones tecnológicas, ciberataques o desastres naturales, mediante un enfoque iterativo y adaptativo que articula liderazgo, diseño, recursos, comunicación y mejora continua.

La integración de este marco asegura que la gestión del riesgo se encuentre conectada con los objetivos estratégicos de TEUNO, promueva la toma de decisiones informadas y facilite la mejora continua del desempeño organizacional, fortaleciendo así su capacidad para crear y proteger valor en un entorno dinámico y exigente.

5.5.1. Generalidades. El propósito del marco de referencia en la norma ISO 31000:2018 es asegurar que la gestión del riesgo sea sistemática, estructurada e integrada en el sistema de gestión de continuidad del negocio, como parte inherente de su gobernanza y toma de decisiones. Este enfoque busca garantizar que la gestión del riesgo contribuya a alcanzar los objetivos estratégicos, operacionales y de continuidad del negocio.

Figura 11

Gobernanza y Objetivos estratégicos

Tomado de (*31000:2018,* 2018)

5.5.2. Liderazgo y Compromiso. La implementación efectiva de un sistema de gestión del riesgo, conforme a la norma ISO 31000:2018, requiere el liderazgo activo y el compromiso visible de la alta dirección. Este compromiso no solo implica la asignación de recursos, sino también la integración del pensamiento basado en riesgos en todos los niveles de toma de decisiones y operación de la organización.

Teuno reconoce que el liderazgo y compromiso son pilares visibles dentro del desarrollo de su Sistema de Gestión de Continuidad del Negocio, la alta dirección ha asumido un rol protagónico mediante su compromiso y apoyo organizacional.

A continuación, se detalla la propuesta de acciones y compromisos que la Alta Dirección debe asumir para implementar la gestión de riesgos según ISO 31000:

Figura 12

Propuesta de acciones y compromisos

Tomado de (*31000:2018,* 2018)

1. Establecer y comunicar una política de gestión del riesgo

- Reflejar el compromiso institucional con la gestión proactiva de los riesgos.
- Integrar esta política con la visión estratégica del SGCN.
- Alinearla con la cultura organizacional de resiliencia y mejora continua.

2. Alinear la gestión del riesgo con los objetivos estratégicos

- Asegurar que el riesgo se gestione como parte integral de la planificación del negocio.
- Definir el apetito y tolerancia al riesgo en función de los niveles aceptables de interrupción.

3. Asignar funciones, responsabilidades y autoridades claras

- Nombrar responsables de riesgos a nivel estratégico, táctico y operativo.
- Integrar los roles de continuidad (SGCN) con los de gestión de riesgo empresarial.
- Promover la rendición de cuentas en todos los niveles.

4. Proveer los recursos necesarios

- Asegurar el financiamiento de actividades relacionadas con la identificación, análisis, tratamiento, monitoreo y comunicación del riesgo.
- Garantizar la disponibilidad de herramientas, tecnología, personal capacitado y tiempo para operar el sistema.

5. Integrar la gestión del riesgo en la toma de decisiones

- Incluir el análisis de riesgo como insumo en la aprobación de nuevos servicios, adquisiciones tecnológicas, contratos de outsourcing, cambios operativos o transformaciones digitales.

6. Fomentar la cultura del riesgo en toda la organización

- Promover programas de concientización, formación y liderazgo basado en el ejemplo.
- Reconocer el aprendizaje de incidentes como parte del desarrollo organizacional.

7. Supervisar y mejorar el marco de gestión del riesgo

- Establecer indicadores clave para evaluar la eficacia del sistema.
- Asegurar la revisión periódica del marco de riesgos, considerando lecciones aprendidas, resultados de pruebas del SGCN, y cambios en el contexto interno y externo.

Reforzar la conexión entre los planes de continuidad, los escenarios de crisis y los riesgos identificados.

5.5.3. Integración. La integración de la gestión del riesgo en todos los niveles y procesos de la organización es uno de los elementos clave para lograr un sistema eficaz, coherente y sostenible. Según la ISO 31000:2018, la gestión del riesgo no debe ser una función separada, sino una parte esencial de la estructura, operaciones y cultura de la organización.

En el contexto de Teuno, esto significa incorporar la gestión del riesgo en todas las etapas de sus procesos estratégicos, tácticos y operativos. Desde la formulación de nuevos servicios tecnológicos, hasta la ejecución de proyectos, atención a clientes estratégicos, sistemas de gestión y decisiones sobre infraestructura crítica, el riesgo debe ser considerado de forma sistemática y transversal.

Tabla 34

Acciones claves para facilitar la integración

Nº	Acción	Descripción
1	**Asegurar presencia en todos los niveles**	Incluir la gestión del riesgo desde la alta dirección hasta el nivel operativo, como parte de la planificación, ejecución y monitoreo de cada área.

Nº	Acción	Descripción
2	**Capacitación continua**	Formar al personal en riesgos tecnológicos, operacionales, regulatorios, reputacionales y de continuidad. Sensibilizar sobre cómo sus actividades impactan el riesgo institucional.
3	**Uso de herramientas y formatos comunes**	Aplicar plantillas de evaluación de riesgos en proyectos, cambios tecnológicos, contratación de proveedores y decisiones clave, estandarizando el enfoque organizacional.
4	**Inclusión en sistemas de gestión existentes**	Integrar la gestión del riesgo con los marcos ISO 22301 (continuidad), ISO 27001 (seguridad de la información) e ISO 20000 (gestión de servicios), ya operativos en TEUNO.
5	**Planificación estratégica**	Incorporar el análisis de riesgos en la formulación de objetivos corporativos, inversión en seguridad y expansión de servicios como VDI, CyberGuard y DOC.
6	**Gestión de proyectos y operaciones**	Requerir que cada proyecto (infraestructura, cloud, ciberseguridad) identifique, analice y trate los riesgos desde su inicio, como parte de su ciclo de vida.
7	**Procesos de soporte y continuidad del negocio**	Enlazar el análisis de riesgos con el ciclo PHVA del SGCN, fortaleciendo los escenarios de continuidad, recuperación (BCP/DRP) y evaluaciones del impacto al negocio (BIA).

5.5.4. Diseño. El diseño del marco de gestión del riesgo es una etapa crítica dentro del proceso de implementación, ya que define la estructura que permitirá a la organización integrar el riesgo en todos sus procesos. En este punto, se establecen los fundamentos que garantizarán la alineación entre el sistema de gestión del riesgo y el propósito, la cultura, los recursos y las necesidades estratégicas de la organización.

Este diseño debe responder a su contexto operativo como proveedor de soluciones tecnológicas críticas, donde la gestión del riesgo no puede limitarse a un enfoque reactivo, sino que debe estructurarse como un sistema preventivo, proactivo y adaptable. Esto incluye entender claramente el entorno interno y externo, definir responsabilidades, establecer mecanismos de

consulta y comunicación, asignar recursos, y construir una arquitectura que soporte la resiliencia de los procesos.

Un marco de diseño sólido asegurará que la gestión del riesgo no sea una función aislada, sino un eje transversal y dinámico que oriente la toma de decisiones en todos los niveles de la organización.

5.5.4.1. Comprensión de la organización y su contexto. Diseñar un sistema efectivo de gestión del riesgo requiere comprender a fondo el entorno interno y externo en el que opera la organización. Esta comprensión permite identificar factores clave que pueden influir positiva o negativamente en la capacidad de Teuno para alcanzar sus objetivos y asegurar la continuidad de sus operaciones críticas.

Contexto Interno

Teuno ha identificado como principales fortalezas su capacidad tecnológica, la experiencia en soluciones de conectividad, infraestructura y ciberseguridad, así como su posicionamiento como proveedor estratégico del sector financiero. También se reconocen debilidades como la necesidad de mejorar metodologías ágiles y la comunicación interna.

En cuanto a su estructura, se cuenta con un marco de gobierno alineado a normas internacionales, una política activa de gestión de continuidad, y procesos formalizados a través del ciclo PHVA (Planificar, Hacer, Verificar, Actuar).

Contexto Externo

Desde el análisis, se destacan los siguientes factores:

- **Político/Regulatorio:** TEUNO opera en un entorno regulado, con supervisión por parte de entidades como la Superintendencia de Bancos, ARCOTEL y el SRI. Existen desafíos normativos como altos aranceles e incentivos fiscales limitados.
- **Económico:** La planificación presupuestaria se ve afectada por la incertidumbre macroeconómica y crisis sanitarias, que impactan los niveles de inversión.
- **Social/Tecnológico:** La empresa ha sido un actor clave en la digitalización del país, mediante alianzas con marcas internacionales como Cisco, D-Link y Symantec. Esto le permite ofrecer soluciones innovadoras y mantener alta disponibilidad.
- **Ambiental:** Se promueve la sostenibilidad y el uso eficiente de los recursos, cumpliendo prácticas ambientales responsables.
- **Legal:** Se mantiene cumplimiento de la normativa de protección de datos, telecomunicaciones y seguridad de la información.

Figura 13

Análisis FODA - Teuno

Tomado de (*TEUNO*, 2024)

Fortalezas (Factores internos positivos)

1. Alta capacidad técnica y experiencia especializada: TEUNO cuenta con un equipo humano calificado en áreas clave como infraestructura TI, conectividad, cloud y ciberseguridad. Ofrece servicios gestionados de alto valor como TEUNO VDI, CyberGuard, SOC 24/7, entre otros.

2. Alianzas con fabricantes de renombre: Socios estratégicos como Cisco, Microsoft, Symantec y Palo Alto refuerzan su oferta tecnológica y le permiten mantener estándares internacionales.

3. Cobertura nacional y operaciones centralizadas: Posee sedes en Quito y Guayaquil, lo que le da presencia directa en zonas estratégicas para el sector corporativo.

4. Certificaciones y cumplimiento normativo: TEUNO alinea sus operaciones a marcos como ISO 9001, ISO 27001 e ISO 20000, lo que genera confianza ante clientes altamente regulados.

5. Modelo de gestión basado en PHVA: La implementación del ciclo Planificar-Hacer-Verificar-Actuar permite mantener mejora continua, monitoreo y adaptabilidad.

Oportunidades (Factores externos positivos)

1. Creciente demanda de continuidad operativa: Las organizaciones, especialmente financieras, exigen soluciones de alta disponibilidad, redundancia y recuperación rápida ante incidentes.

2. Digitalización acelerada en sectores público y privado: La transformación digital masiva genera oportunidades en servicios como escritorios virtuales, centros de datos, backups y seguridad gestionada.

3. Obligaciones normativas en seguridad de la información: Leyes de protección de datos y regulaciones de supervisión bancaria obligan a las empresas a buscar servicios especializados como los que ofrece TEUNO.

4. Tendencia hacia externalización de TI: Empresas están optando por delegar su infraestructura tecnológica a terceros expertos, lo cual beneficia la estrategia de servicios gestionados de TEUNO.

Debilidades (Factores internos negativos)

1. Limitaciones en metodologías ágiles de operación: Algunos procesos internos no están totalmente automatizados o requieren mayor velocidad de reacción ante cambios tecnológicos.

2. Comunicación interna por fortalecer: Existe necesidad de mejorar la coordinación entre equipos, especialmente en contextos híbridos o distribuidos.

3. Dependencia de proveedores críticos: Algunos servicios dependen fuertemente de enlaces, plataformas o licencias provistas por terceros. Esto puede afectar la continuidad en caso de fallos externos.

4. Madurez intermedia en cultura de riesgos: Aunque existen mecanismos de continuidad, la integración plena de la gestión del riesgo como sistema transversal aún está en etapa de maduración.

Amenazas (Factores externos negativos)

1. Altos aranceles e impuestos a tecnología importada: Esto afecta la competitividad y los márgenes de algunos servicios en comparación con proveedores informales o sin regulación.

2. Cambios normativos y exigencias regulatorias continuas: Normas como las de la Superintendencia de Bancos, ARCOTEL o SRI pueden cambiar rápidamente, exigiendo constante adaptación.

3. Competencia agresiva: Enfrenta competencia de empresas globales, startups locales o integradores que compiten por precio más que por valor agregado.

4. Incremento de amenazas cibernéticas: Los ataques de ransomware, phishing y denegación de servicio exigen una respuesta constante, robusta y en tiempo real.

Propósito y alineación estratégica

El propósito de TEUNO es ser el proveedor referente de soluciones tecnológicas corporativas en Ecuador, brindando servicios resilientes, seguros y disponibles. Esta misión está alineada al diseño del Sistema de Gestión de Continuidad del Negocio y a la gestión del riesgo, los cuales permiten sostener la operación ante eventos disruptivos, proteger la infraestructura crítica y cumplir con las expectativas de clientes, entes reguladores y la sociedad.

Partes Interesadas

Comprender el contexto de la organización también implica identificar y analizar a las partes interesadas: grupos o entidades que pueden afectar o verse afectadas por las decisiones, operaciones o interrupciones de la organización.

Teuno ha identificado a las siguientes partes interesadas clave, junto con sus principales necesidades y expectativas:

Tabla 35

Partes interesadas y requerimientos

Parte interesada	Requerimientos (necesidades y expectativas)
Clientes	Servicios seguros, innovadores y disponibles. Precios competitivos, confidencialidad, integridad de información, valor agregado y atención oportuna.
Proveedores	Estabilidad financiera de TEUNO, relaciones comerciales a largo plazo, cumplimiento de pagos, confidencialidad y disponibilidad de información.

Parte interesada	Requerimientos (necesidades y expectativas)
Funcionarios	Estabilidad laboral, desarrollo profesional, buen ambiente, confidencialidad, seguridad en la información, condiciones de trabajo justas y libres de contaminación.
Directorio	Rentabilidad, crecimiento sostenido, gestión eficiente y cumplimiento de metas estratégicas.
Sociedad	Responsabilidad social, protección del medio ambiente, y operaciones sin impacto negativo en la comunidad.
Entes reguladores	Cumplimiento legal, pago de impuestos, cumplimiento ambiental, ciberseguridad y protección de datos.
Alta Dirección	Gestión eficaz de los sistemas implementados, información segura, decisiones basadas en datos, personal capacitado y alineado a objetivos de sostenibilidad y mejora continua.
Competencia	Imagen de marca, cumplimiento normativo, innovación y diferenciación.
Medio ambiente	Prevención de contaminación, no generación de residuos peligrosos, compromiso ambiental.
Alianzas estratégicas	Lealtad, colaboración y entrega de servicios de alta calidad al cliente final.

Compromiso de Teuno con las partes interesadas

Teuno ha formalizado su enfoque hacia las partes interesadas bajo tres principios fundamentales:

- **Comunicación transparente:**

  Informar de manera oportuna sobre cambios significativos que pueda afectar a la organización y su normal operación.

- **Cumplimiento de expectativas:**

  Asegurar la satisfacción de las necesidades identificadas, mediante la aplicación de planes preventivos, acciones correctivas y mejora continua.

- **Colaboración activa:**

Promover el trabajo conjunto con clientes, proveedores, autoridades y empleados para fortalecer la resiliencia organizacional y la sostenibilidad de la organización.

5.5.4.2.Articulación del compromiso con la gestión del riesgo. El compromiso institucional con la gestión del riesgo debe estar claramente definido, documentado y comunicado. Este compromiso actúa como guía para orientar el comportamiento organizacional, establecer prioridades, y garantizar la coherencia entre las decisiones operativas y los objetivos estratégicos.

La articulación del compromiso con la gestión del riesgo se concreta mediante el diseño, aprobación y difusión de una Política de Gestión de Riesgos que refleje la intención formal de la organización de adoptar un enfoque estructurado, proactivo y transversal en el tratamiento del riesgo. Esta política se convierte en el pilar normativo del marco de gestión definido por la norma ISO 31000:2018, y garantiza su alineación con los objetivos estratégicos y de continuidad de Teuno.

Política de Riesgos

1. Objetivo

Establecer un marco técnico para dirigir y coordinar las actividades relacionadas con la gestión del riesgo en Teuno. Esta política busca asegurar que todos los riesgos estratégicos, operativos, tecnológicos, normativos, de continuidad y de seguridad sean:

- Identificados y analizados con criterios objetivos,
- Evaluados según el apetito de riesgo definido,
- Tratados de manera adecuada con base en controles eficaces,

- Monitoreados y revisados continuamente,
- Comunicados de forma clara a todas las partes relevantes.

De esta manera, se busca proteger y crear valor, garantizar el cumplimiento normativo y fortalecer la toma de decisiones bajo un enfoque de riesgo informado.

2. Alcance

Esta política aplica a todos los procesos, servicios, activos críticos, niveles organizativos, proyectos, sistemas de gestión y partes interesadas internas y externas relacionadas con TEUNO. Abarca el tratamiento de riesgos inherentes, residuales y las oportunidades identificadas como parte de los análisis de riesgos.

3. Principios rectores

La gestión del riesgo en TEUNO se fundamenta en los siguientes principios:

- Creación y protección de valor organizacional.
- Integración en todos los niveles y procesos de gestión.
- Participación activa de todos los colaboradores.
- Uso de información clara, estructurada y trazable.
- Adaptación al contexto cambiante.
- Enlace con los sistemas de gestión existentes.
- Enfoque proactivo y de mejora continua.

4. Políticas Específicas:

Cultura y Gestión de Riesgos: Alineadas a la norma ISO 31000:2018

1. Integración de la gestión del riesgo en la cultura organizacional: TEUNO promueve la adopción transversal de la gestión del riesgo como parte integral de su cultura corporativa, garantizando la participación activa de todas las áreas mediante procesos de concientización, formación y mejora continua, conforme al principio de integración definido por ISO 31000.

2. Análisis y documentación de riesgos relacionados a servicios críticos: Los riesgos y controles de seguridad asociados a los servicios críticos (conectividad, infraestructura, cloud y ciberseguridad) deben ser analizados y registrados conforme a la metodología de riesgos, como parte de la operación de sus sistemas de gestión.

3. Identificación de oportunidades derivadas del análisis de riesgo: Toda identificación de riesgos debe considerar si se trata de una oportunidad potencial. Estas serán tratadas bajo el marco del proceso de mejora continua, registradas y monitoreadas como parte del valor agregado del sistema de gestión.

4. Gestión de controles con enfoque basado en evidencia y efectividad: Los controles implementados deben ser continuamente evaluados en cuanto a su eficacia. Ante fallos o desviaciones, se deberán aplicar medidas correctivas y, en caso de violaciones a la política, se activarán los mecanismos disciplinarios conforme al reglamento interno y código de ética de TEUNO.

5. Registro de nuevos riesgos o modificación de riesgos existentes: Los líderes de proceso deberán generar solicitudes de cambio mediante la herramienta institucional de gestión

(Planner o Jira), detallando el tipo de riesgo, justificación y propuesta de control, con respaldo al analista de procesos.

6. Evaluación periódica de la efectividad de los puntos de control: Durante la revisión anual de los riesgos (inherentes y residuales), los responsables deben validar si los controles siguen siendo efectivos. De no ser así, deberán ajustarse conforme a lo establecido en el procedimiento de gestión de riesgos.

7. Gestión documental de evidencias de control: Las evidencias de ejecución de los controles serán almacenadas en el path definido por el área de procesos, y su registro será responsabilidad de los líderes de procesos y servicios.

8. Verificación y seguimiento de evidencias: El Gestor de Riesgos deberá verificar trimestralmente la existencia y validez de las evidencias registradas.

9. Responsabilidades clave de los responsables de riesgos: Cada líder de proceso o servicio tiene la obligación de:

- Identificar los riesgos de su área.
- Evaluarlos según los criterios de probabilidad e impacto.
- Ejecutar controles o planes de acción definidos.
- Comunicar a su equipo los riesgos vigentes y la forma de tratarlos.

10. Revisión anual coordinada del mapa de riesgos institucional: La revisión de riesgos debe realizarse una vez al año por cada responsable de área junto con el responsable de riesgos, actualizando las matrices estratégicas, operativas y de servicios.

Apetito de Riesgo

11. El perfil de riesgo institucional de TEUNO se define como “moderado” como nivel máximo de exposición aceptable, en coherencia con el apetito definido en la política general.

12. Se deberán implementar medidas preventivas que aseguren que los riesgos se mantengan dentro de los niveles tolerables.

13. Todo tratamiento de riesgo deberá ejecutarse conforme a la metodología oficial de administración de riesgos.

Comunicación del compromiso

Para asegurar su efectividad, esta política debe ser:

- Aprobada formalmente por parte del comité de riesgos de Teuno.
- Comunicada a todos los niveles de la organización mediante canales formales (reuniones de dirección, inducciones, boletines, capacitaciones, correo electrónico masivo).
- Integrada en los sistemas existentes (ISO 9001, ISO 27001, ISO 20001 planificación estratégica, proyectos, etc.).
- Visible y accesible a todos los colaboradores, con lenguaje claro y adaptado a sus responsabilidades, debe estar en el repositorio DOCs.
- Seguimiento y evaluación periódica de su efectividad, incluyendo revisión en auditorías internas y comités directivos de riesgos.

5.5.4.3.Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización. La implementación eficaz de la gestión del riesgo requiere una asignación clara de roles, responsabilidades y autoridad, así como el establecimiento de mecanismos de rendición de cuentas. Esta claridad organizacional asegura que todas las funciones involucradas en la identificación, evaluación, tratamiento y monitoreo del riesgo actúen de forma coordinada y conforme a lo establecido por la metodología interna y la norma ISO 31000:2018.

En TEUNO, el modelo de gobierno del riesgo se sustenta en una estructura organizativa definida, comités especializados y procesos formales para asegurar que cada actor conozca su rol y actúe con responsabilidad y trazabilidad.

Tabla 36

Roles y responsabilidades

Rol / Unidad	Responsabilidades clave en la gestión de riesgos
Gerencia General	- Aprobar políticas y metodologías de gestión de riesgos. - Promover la cultura organizacional de riesgos. - Rendir cuentas al Directorio.
Subgerencia de Riesgos	- Dirigir la implementación del sistema de gestión de riesgos. - Consolidar reportes institucionales. - Asegurar alineación con normas internacionales y regulaciones vigentes.
Comité de Riesgos	- Evaluar escenarios críticos y tendencias emergentes. - Aprobar planes de tratamiento. - Supervisar el apetito y perfil de riesgo institucional.
Gestor de Riesgos	- Coordinar la identificación, análisis, evaluación y seguimiento de los riesgos estratégicos, operativos y de servicios. - Validar controles y evidencias. - Actualizar las matrices y generar reportes.

Responsables de Área / Dueños de Proceso	- Identificar, evaluar y tratar los riesgos asociados a su proceso o área. - Registrar y mantener actualizadas las evidencias de los puntos de control. - Comunicar los riesgos vigentes a su personal.
Colaboradores	- Cumplir con las actividades y controles establecidos. - Reportar riesgos, incidentes u observaciones relevantes. - Participar activamente en la cultura de gestión de riesgos.

Buenas prácticas para asegurar claridad y responsabilidad:

- Publicar y actualizar el organigrama de roles en gestión de riesgos.
- Incluir funciones de riesgo en los perfiles de cargo.
- Aplicar la matriz RACI en proyectos estratégicos y procesos críticos.
- Reforzar la concientización sobre la responsabilidad individual en talleres y sesiones informativas.

5.5.4.4.Asignación de recursos. La sostenibilidad y efectividad del sistema de gestión de riesgos depende de la disponibilidad de recursos adecuados y suficientes, tanto humanos como financieros, tecnológicos y de conocimiento. Este subpunto de la norma ISO 31000:2018 establece que una organización debe asegurar los medios necesarios para diseñar, implementar, operar y mejorar continuamente su marco de gestión de riesgos.

En Teuno, la gestión del riesgo forma parte integral de la organización, por lo tanto, su fortalecimiento requiere inversiones planificadas y estructuradas que garanticen su funcionamiento en condiciones normales y de contingencia.

Tabla 37

Asignación de recursos

Tipo de recurso	Aplicación específica	Valor estimado anual (USD)
Recursos Humanos	- Gestor de riesgos, - Formación del personal en ISO 31000.	$ 15,000.00
Recursos Financieros	- Presupuesto para auditorías, consultorías, capacitaciones, etc.	$ 2,000.00
Recursos Tecnológicos	- Herramientas como Microsoft Planner, módulos de gestión documental,	$ 200.00
Recursos Documentales	- Actualización de políticas, procedimientos, metodologías, matrices de riesgo, manuales de riesgos.	$ -
	TOTAL	$ 17,200.00

Acciones de mejora

- Presupuestar anualmente los recursos del sistema de gestión de riesgos, diferenciando inversiones en tecnología, consultoría, formación y herramientas.
- Fortalecer las capacidades técnicas internas a través de formación continua en gestión de riesgos, continuidad del negocio, seguridad de la información y gestión por procesos.

- Dotar a cada área crítica de recursos mínimos funcionales (tiempo, talento, herramientas) para mantener sus matrices actualizadas y los controles en ejecución.
- Mantener activos los sistemas de seguimiento y evidencias, garantizando disponibilidad y trazabilidad para auditorías internas y externas.

5.5.4.5.Establecimiento de la comunicación y la consulta. La gestión del riesgo debe ser un proceso participativo, y para lograrlo es indispensable asegurar una comunicación efectiva y continua, así como la realización de consultas sistemáticas a todas las partes interesadas, tanto internas como externas. Según la norma ISO 31000, una buena gestión del riesgo requiere diálogo, comprensión compartida, retroalimentación oportuna y transparencia.

En Teuno, la comunicación y la consulta son componentes esenciales para garantizar que el Sistema de Gestión de Riesgos respondan a las necesidades de la organización, reflejen las expectativas de las partes interesadas y se fortalezcan con información precisa y oportuna.

Tabla 38

Plan de comunicación para la gestión del riesgo

Componente	Descripción
Objetivo	Informar, sensibilizar y alinear a todos los actores sobre los riesgos, controles, procedimientos y decisiones.
Audiencia	Colaboradores, líderes de procesos, comités, proveedores críticos, clientes estratégicos y entes reguladores.
Canales de comunicación	Reuniones internas, intranet, correo institucional, plataformas como Planner y Jira, boletines, capacitaciones y dashboards.

Frecuencia	Trimestral para internos, anual para partes externas clave. Actualizaciones inmediatas ante incidentes o cambios normativos.
Responsables	Gestor de Riesgos, Subgerente de Riesgos y responsables de área.
Contenido mínimo	Actualización de matrices, resultados de evaluaciones, cambios normativos, incidentes significativos y acciones correctivas.

Consultas internas y externas

Las consultas deben realizarse periódicamente para comprender:

- Las percepciones de riesgo de empleados y jefes de área.
- Las expectativas de clientes estratégicos respecto a la gestión de riesgos.
- Las exigencias regulatorias de entes como la Superintendencia de Bancos o ARCOTEL.
- Las recomendaciones de auditoría externa e interna. Lecciones aprendidas
- La opinión de proveedores críticos sobre su rol en la cadena de continuidad.

Es importante la retroalimentación del sistema de gestión de riesgos por lo que se plantea algunas acciones para dar seguimiento y establecer planes de mejora.

- Incorporar espacios de retroalimentación sobre riesgos en los comités internos (Riesgos, Continuidad, Seguridad, etc.).
- Establecer una encuesta semestral de percepción de riesgo dirigida a empleados.
- Ejecutar reuniones de revisión de riesgos con dueños de los procesos, personal clave de la organización, alta gerencia (mínimo anual).

- Publicar un informe de gestión de riesgos institucional al cierre de cada año fiscal.
- Crear un buzón digital (correo electrónico o aplicativo) de comunicación de incidentes o riesgos percibidos por los colaboradores.

5.5.5. Implementación. La implementación del marco de gestión de riesgos representa la fase operativa donde los principios, políticas, procesos y estructuras previamente definidos se llevan a la práctica. Este paso es esencial para asegurar que la gestión del riesgo no sea solo un enfoque teórico, sino un componente funcional y transversal de la operación de Teuno.

Esta fase tiene como objetivo asegurar que los riesgos que afectan la continuidad del negocio sean tratados de manera sistemática y eficaz.

Para Teuno, esta implementación tiene el siguiente alcance:

- Aplicación directa sobre los procesos críticos identificados en el BIA.

Este enfoque asegura que los riesgos que afectan la disponibilidad, integridad y resiliencia operativa de la organización sean gestionados de manera estructurada, conforme a los lineamientos de la norma ISO 31000:2018.

Alcance

La gestión del riesgo se aplicará únicamente a los procesos críticos definidos en el Análisis de Impacto BIA, es decir, aquellos cuya interrupción:

- Tiene impacto directo en los clientes y en la operación del negocio.

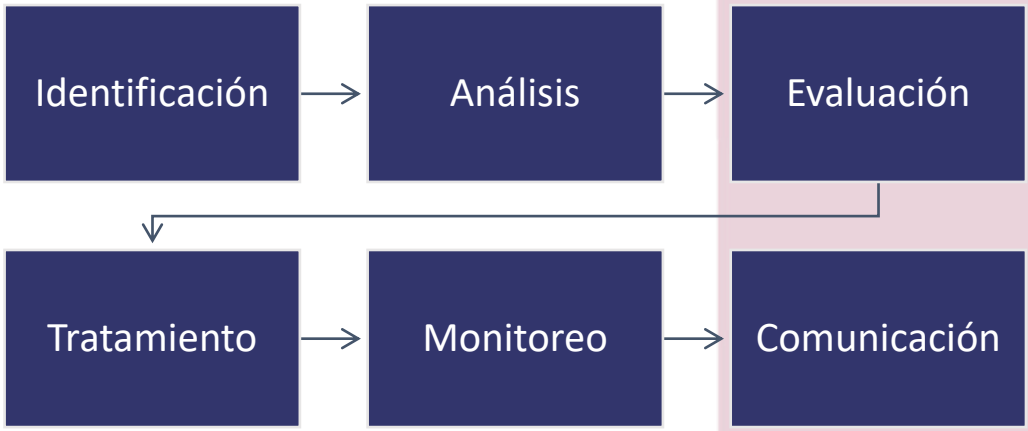
- Afecta el cumplimiento de requisitos regulatorios.
- Compromete la infraestructura, los servicios gestionados o la información sensible.
- El personal clave para la organización no está disponible.

Proceso de gestión de riesgos aplicado a procesos críticos

A continuación, se detalla el ciclo de gestión de riesgos que debe implementarse en cada proceso crítico del BIA:

Figura 14

Ciclo de gestión de riesgos



1. Identificación del riesgo

- Analizar los escenarios de interrupción que pueden afectar cada proceso crítico.
- Documentar los eventos de riesgo asociados: fallas tecnológicas, ciberataques, indisponibilidad de proveedores, errores humanos, entre otros.
- Fuente: flujos de procesos, incidentes históricos, auditorías, conocimiento experto.

Entrada: Procesos Críticos de Teuno

2. Análisis del riesgo

- Determinar la probabilidad de ocurrencia (alta, media, baja) y el impacto potencial (económico, reputacional, legal, estratégico y clientes).
- Clasificar el nivel de riesgo inherente sin considerar controles actuales.

Herramienta: Mapa de calor con resultados de probabilidad x impacto.

3. Evaluación del riesgo

- Comparar el riesgo inherente con el apetito y tolerancia de riesgo de Teuno.
- Identificar los controles existentes y valorar su eficacia (aceptable, necesita mejoras, débil).
- Calcular el riesgo residual considerando los controles aplicados.

Producto: Matriz de riesgos actualizada con clasificación residual.

4. Tratamiento del riesgo

- Para cada riesgo que supere el apetito definido:
- Determinar una estrategia de tratamiento:

- Evitar (cambiar el proceso)
- Reducir (mejorar controles)
- Transferir (seguros, contratos)
- Aceptar (si está dentro del nivel tolerable)
- Asignar responsables y plazos para ejecutar acciones correctivas.

  Producto: Plan de tratamiento de riesgos documentado.

5. Monitoreo y revisión

- Verificar la aplicación de controles y planes mediante indicadores, evidencia documentada y revisiones programadas.
- Integrar hallazgos de pruebas del SGCN, auditorías y simulacros.

  Frecuencia: Trimestral para procesos críticos o tras cualquier evento disruptivo.

6. Comunicación y consulta

- Informar los resultados del análisis de riesgos a los líderes de proceso, subgerencia de riesgos, comité de continuidad y demás partes interesadas.
- Recoger retroalimentación de los equipos operativos y ajustar controles si es necesario.

  Medios: reuniones, dashboards, matrices compartidas, canal interno

5.5.6. Valoración. La valoración del marco de gestión del riesgo tiene como finalidad verificar si las acciones implementadas están produciendo los resultados esperados, y si el sistema sigue siendo adecuado y eficaz frente a los objetivos organizacionales, las amenazas emergentes y las necesidades de las partes interesadas.

En Teuno, la valoración se enfocará tanto en los procesos críticos evaluados en el BIA como en el funcionamiento global del Sistema de Gestión de Riesgos aplicado al SGCN, bajo una estructura de mejora continua y alineación estratégica.

Objetivo de la valoración

Evaluar si:

- El sistema de gestión de riesgos está aportando valor.
- Los riesgos han sido correctamente tratados y reducidos a niveles aceptables.
- Los objetivos estratégicos de continuidad se están cumpliendo.
- Los controles definidos están funcionando como se espera.
- El sistema es capaz de adaptarse a cambios en el entorno operativo o regulatorio.

Tabla 39

Indicadores claves de desempeño KPIs

Indicador	Descripción	Frecuencia
% de procesos críticos con riesgos evaluados	Mide el avance de aplicación del proceso de riesgos en procesos definidos en el BIA.	Anual
% de riesgos con tratamiento implementado	Mide la eficacia en ejecución de planes correctivos y controles.	Trimestral
% de riesgos fuera del apetito	Mide el nivel de exposición residual por encima del umbral definido.	Trimestral
% de controles con evidencia validada	Verifica cumplimiento del registro de controles en el sistema documental.	Trimestral
N° de incidentes de continuidad registrados	Permite relacionar incidentes reales con la gestión de riesgos y planes de continuidad.	Mensual

Indicador	Descripción	Frecuencia
% de concientización nuevos colaboradores	Comunicación o concientización a los colaboradores que ingresan a la compañía sobre el SGCN y la gestión de riesgos	Mensual

Acciones de valoración complementarias

- Revisiones del sistema en comités de Riesgo y Continuidad.
- Auditorías internas y externas para verificar conformidad normativa y operativa.
- Encuestas de percepción del riesgo dirigidas a responsables de procesos y personal clave.
- Análisis de causas raíz ante eventos no previstos o incidentes no mitigados.

Herramientas de soporte

- Dashboard de riesgos, conectados a las matrices de la organización.
- Informes ejecutivos consolidados para alta dirección y comités de riesgos y continuidad.
- Planner / Jira para trazabilidad de planes de acción, tickets de apertura de incidentes.
- Revisión anual del marco como parte del ciclo PHVA del SGCN.

5.5.5. Mejora.

5.5.5.1.Adaptación. La gestión del riesgo no es estática. Requiere actualización constante para responder a los cambios en el contexto estratégico, tecnológico, regulatorio o de procesos. ISO 31000 establece que el sistema debe adaptarse proactivamente para seguir siendo eficaz y relevante.

Este principio para Teuno es fundamental, se materializa como parte de su compromiso con la mejora continua del SGCN y la resiliencia organizacional. La adaptación del marco de gestión del riesgo es esencial para mantener su alineación con los procesos críticos, las expectativas de las partes interesadas y el entorno cambiante del sector tecnológico y financiero.

Tabla 40

Situaciones que requieren adaptación

Situación de cambio	Acción de adaptación recomendada	Ejemplo en TEUNO
Cambios en el entorno normativo o regulatorio	- Revisar y actualizar políticas y procedimientos. - Comunicar los cambios a responsables y comités.	Nueva obligación de cumplimiento de la LOPDP para servicios cloud gestionados.
Actualización del portafolio de servicios o procesos críticos	- Revisar el BIA. - Evaluar nuevos riesgos. - Ajustar planes de continuidad.	Incorporación de servicios como CyberGuard SOC o Escritorios Virtuales VDI.
Eventos disruptivos o incidentes significativos	- Realizar análisis post-incidente. - Reevaluar controles y ajustar riesgos residuales.	Fallo del enlace principal de comunicaciones durante horario operativo.
Resultados de auditorías o simulacros con hallazgos	- Ejecutar planes de mejora. - Reforzar controles. - Registrar acciones correctivas.	Observación de auditoría por falta de evidencias en los puntos de control del BIA.
Rotación de personal clave o cambios estructurales	- Redefinir responsables. - Capacitar nuevos cargos. - Validar continuidad operativa.	Salida del jefe de Infraestructura sin actualización de responsables en la matriz.
Cambios en los objetivos estratégicos o apetito de riesgo	- Replantear metodologías y clasificación de riesgos según los nuevos objetivos.	Teuno define un mayor nivel de digitalización y ajusta su apetito de riesgo operativo.

Situación de cambio	Acción de adaptación recomendada	Ejemplo en TEUNO
Amenazas emergentes (ciberseguridad, proveedores, etc.)	- Actualizar catálogo de amenazas. - Evaluar controles nuevos. - Ajustar matrices.	Aumento de ataques de ransomware hacia clientes financieros gestionados por Teuno.

5.5.5.2.Mejora continua. La mejora continua es uno de los pilares fundamentales de la gestión de riesgos según ISO 31000. Este subpunto busca garantizar que el sistema no se limite a mantener el statu quo, sino que evolucione de forma permanente para responder con mayor eficacia a los cambios internos, externos y a las lecciones aprendidas.

En Teuno, la mejora continua se integra como parte del ciclo PHVA (Planificar-Hacer-Verificar-Actuar), tanto en el Sistema de Gestión de Continuidad del Negocio (SGCN) como en el proceso formal de gestión de riesgos.

Tabla 41

Acciones de mejora continua

Acción	Aplicación específica en TEUNO
Auditorías internas y externas	- Revisar cumplimiento de controles. - Evaluar coherencia entre riesgos, apetito y tratamiento.
Revisión periódica de indicadores y resultados	- Monitorear KPIs definidos en el marco de valoración (ver punto 5.5.6).
Análisis de hallazgos y brechas	- Comparar resultados esperados vs. reales. - Identificar desviaciones en controles, incidentes no gestionados.

Evaluación de lecciones aprendidas post-incidente	- Realizar análisis causa-raíz. - Ajustar matrices y tratamiento según eventos ocurridos.
Retroalimentación de partes interesadas	- Considerar opiniones de clientes estratégicos, colaboradores, entes reguladores, y auditores externos.
Aplicación de acciones correctivas o preventivas	- Documentar e implementar medidas que refuercen el sistema y prevengan la recurrencia de fallas.
Actualización de políticas, procedimientos y matrices	- Revisar y adaptar documentos normativos y metodológicos con base en los resultados anteriores.

Herramientas y mecanismos de apoyo

- Informes de cierre de auditoría y planes de mejora.
- Actas de revisión del Comité de Riesgos y Continuidad.
- Matriz de seguimiento de acciones correctivas/preventivas (AC/PA).
- Revisión anual de la política de riesgos.
- Dashboards de visualización de progreso.

Resultado esperado

- La implementación del enfoque de mejora continua permite a Teuno:
- Fortalecer la madurez del sistema de gestión de riesgos.
- Reducir la exposición a eventos no deseados por control débil o desactualizado.
- Aumentar la confianza de clientes y entes reguladores.

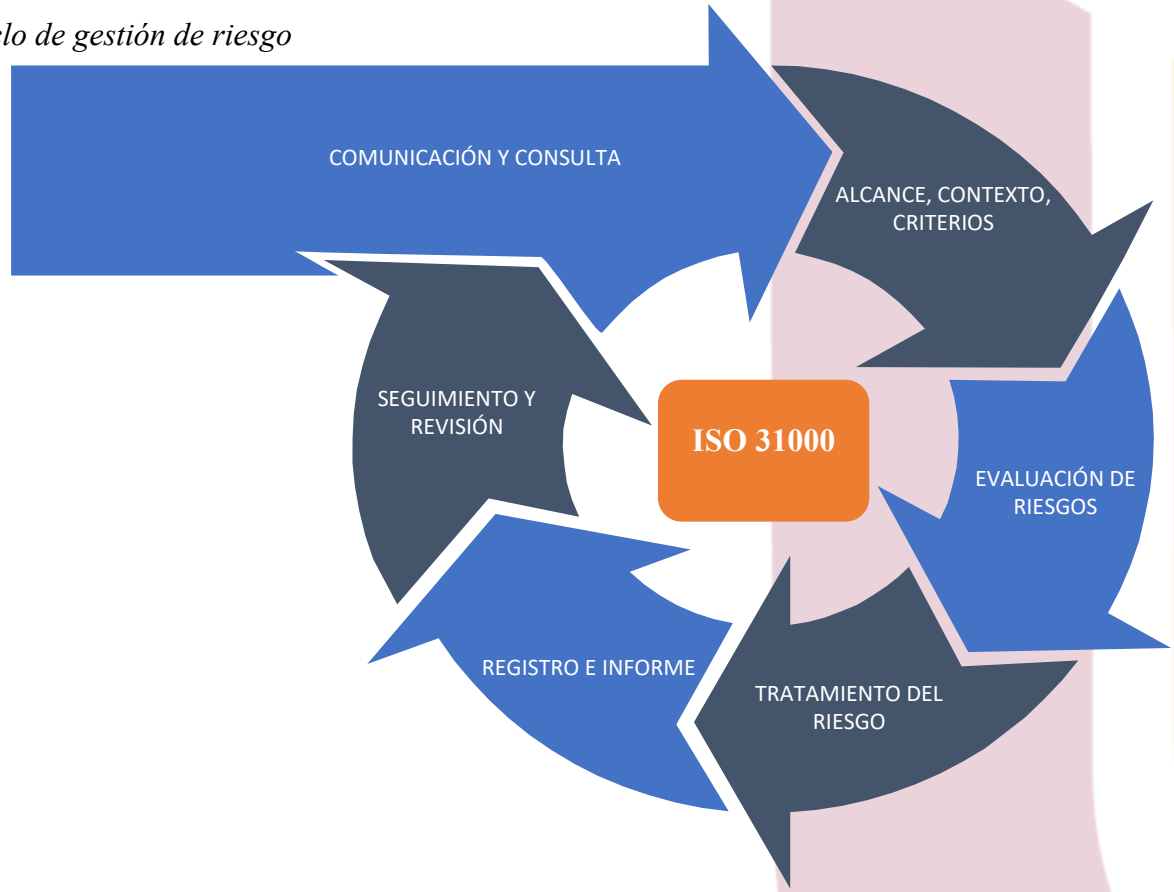
- Generar un aprendizaje organizacional sistemático, que retroalimente el SGCN y contribuya a la resiliencia empresarial.

5.6.Proceso

El proceso de gestión del riesgo constituye la columna vertebral de la norma ISO 31000:2018, y está diseñado para aplicarse de forma cíclica y sistemática. Su propósito es permitir a las organizaciones tomar decisiones informadas, anticiparse a escenarios de incertidumbre y proteger sus activos clave, especialmente en contextos críticos como la continuidad del negocio.

Figura 15

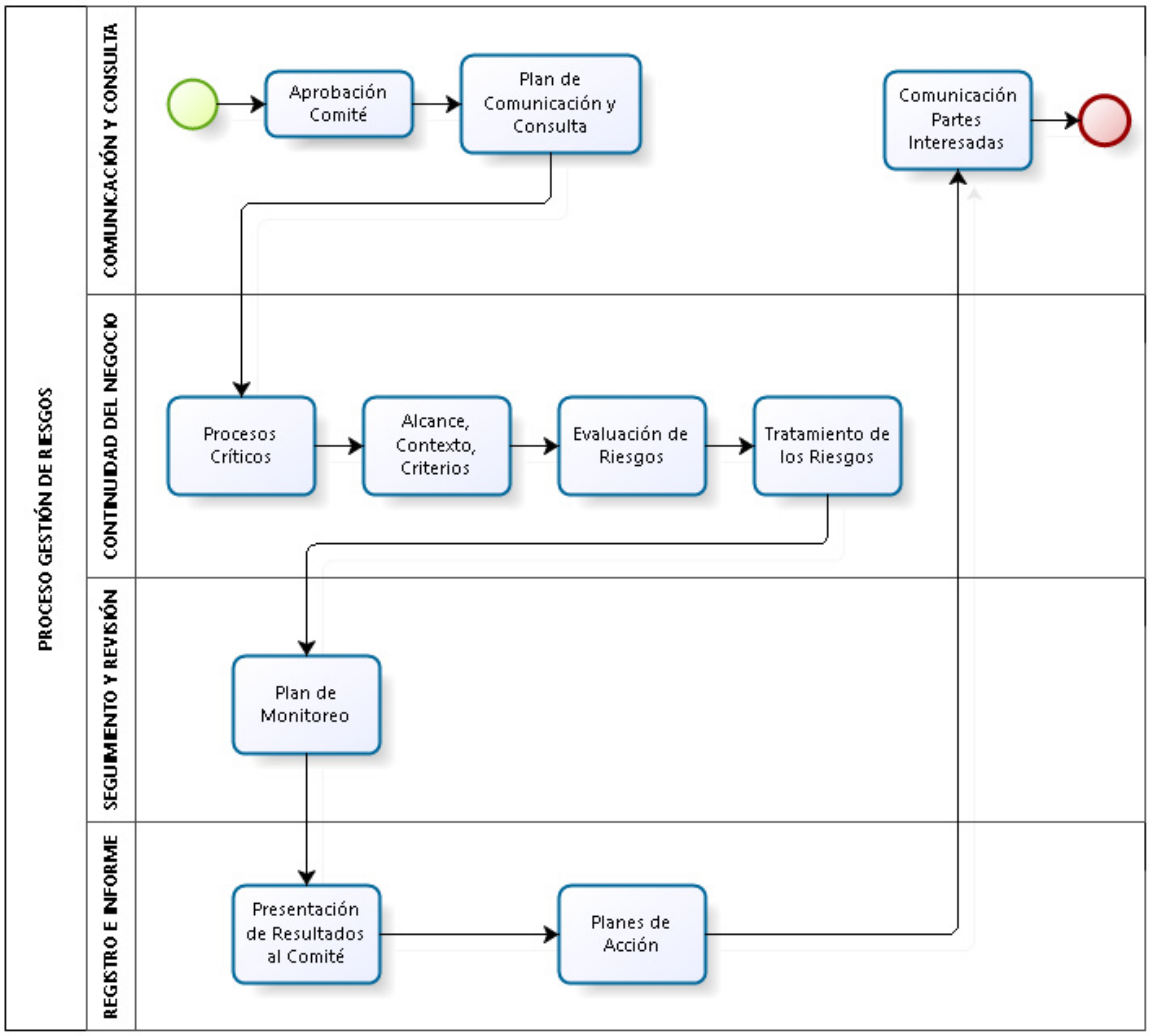
Ciclo de gestión de riesgo



En TEUNO, el funcionamiento de este sistema se ejecuta de la siguiente manera:

Figura 16

Flujograma de la gestión de riesgos de acuerdo al SGCN de TEUNO



5.6.1. Generalidades. En el marco del Sistema de Gestión de Continuidad del Negocio, Teuno Adopta este proceso como mecanismo operativo para asegurar que las amenazas que puedan interrumpir los procesos críticos sean gestionadas con eficacia.

Asimismo, la gestión de riesgos en el contexto de la continuidad del negocio tiene como finalidad proteger los procesos críticos identificados en el análisis BIA, garantizando que Teuno esté preparado para responder, adaptarse y recuperarse de cualquier evento adverso.

Este proceso apoya la toma de decisiones en momentos críticos (ej. activación de planes BCP o DRP) y está alineado con los objetivos organizacionales, especialmente con los compromisos de calidad, seguridad, disponibilidad y cumplimiento regulatorio. De la misma manera, es dinámica, iterativa y adaptable, permitiendo ajustar los planes de continuidad ante cambios internos o del entorno, como nuevos riesgos tecnológicos, incidentes ocurridos o lecciones aprendidas.

La gestión del riesgo en TEUNO se rige por los principios fundamentales definidos por la norma ISO 31000, que permiten asegurar un enfoque eficaz y coherente:

Tabla 42

Principios de la Norma ISO 31000 en TEUNO

Principio	Aplicación en el SGCN de TEUNO
Creación y protección de valor	Asegurar la operatividad de servicios como Data Center, Ciberseguridad y conectividad.
Integrada	La gestión de riesgos está incorporada en todos los procesos de continuidad, desde la alta dirección.

Principio	Aplicación en el SGCN de TEUNO
Estructurada y exhaustiva	Se emplean metodologías, matrices, criterios y herramientas formalizadas.
Adaptada	Aplicada específicamente a procesos críticos y escenarios definidos en el BIA.
Inclusiva	Participación activa del Comité de Continuidad, líderes de procesos y partes interesadas.
Dinámica	Se ajusta ante cambios regulatorios, tecnológicos y operativos.
Basada en la mejor información	Evaluaciones documentadas, simulacros, incidentes, auditorías internas y externas.
Considera factores humanos	Capacitación, roles asignados y cultura organizacional de resiliencia.
Mejora continua	Plan de mantenimiento, indicadores de seguimiento, auditorías y revisión anual.

Esta sección establece el marco conceptual que permite integrar de manera estructurada la gestión del riesgo dentro de todas las actividades del Sistema de Gestión de Continuidad del Negocio de Teuno, proporcionando los fundamentos para garantizar que la gestión del riesgo sea una práctica transversal y parte esencial del sistema de continuidad. Este enfoque integral permite proteger los objetivos estratégicos y operativos de la organización frente a eventos disruptivos, apoyando no solo la prevención y respuesta ante crisis, sino también fortaleciendo la resiliencia organizacional, el cumplimiento normativo y la confianza de las partes interesadas, en lugar de considerar la gestión del riesgo como una función aislada.

5.6.2. Comunicación Y Consulta. La comunicación y consulta son componentes transversales y permanentes en todo el proceso de gestión de riesgos, cuya finalidad es garantizar que todas las partes interesadas comprendan los riesgos, participen en su tratamiento y contribuyan activamente a la toma de decisiones informadas.

En el marco del Sistema de Gestión de Continuidad del Negocio de Teuno, la comunicación debe ser bidireccional, transparente, oportuna y adaptada al público objetivo, permitiendo tanto informar como recibir retroalimentación desde todos los niveles de la organización. A continuación se detallan los canales de comunicación y los roles y responsabilidades de los actores en TEUNO.

Tabla 43

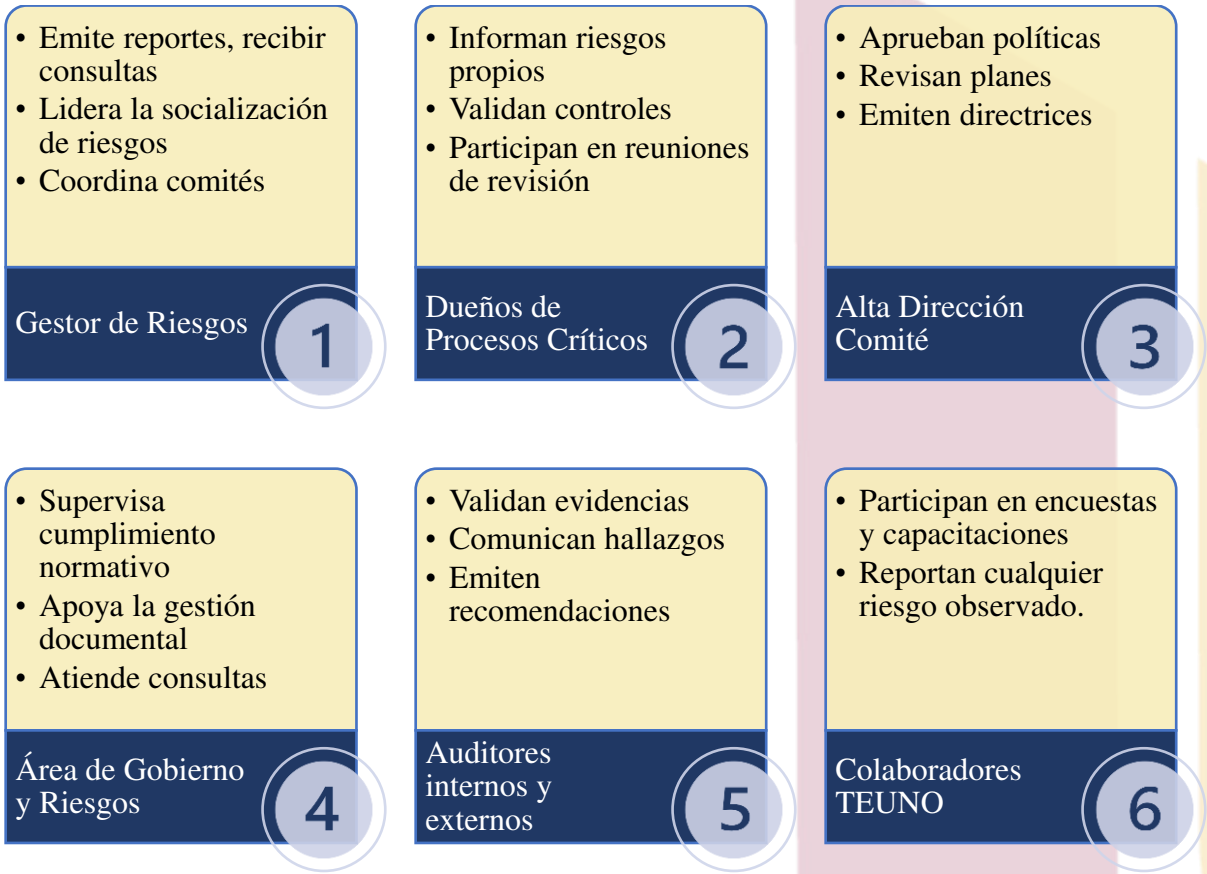
Métodos de comunicación y consulta en TEUNO

Medio / Canal	Finalidad / Aplicación
Comité de Riesgos y Comité de Continuidad	Presentación de resultados, aprobación de políticas, revisión de matrices y validación de acciones.
Boletines por correo electrónico	Socialización de políticas, cambios normativos, actualizaciones de planes y alertas.
Videos corporativos	Capacitación visual sobre continuidad, seguridad, amenazas emergentes y simulacros.
Encuestas institucionales	Medir la percepción de riesgos, efectividad de controles y nivel de conocimiento.
Reuniones con dueños de procesos	Validación de riesgos identificados, establecimiento de controles y revisión de impactos.
Auditorías internas y externas	Canales formales para consulta, evidencia y mejora del sistema.

Certificaciones ISO	Mecanismos de consulta y verificación técnica por entes de certificación externos.
Correo institucional del Gestor de Riesgos	Canal oficial para consultas, sugerencias o reportes de riesgos por parte de cualquier colaborador.
Área de Gobierno Corporativo	Apoyo normativo y estratégico, responsable de canalizar inquietudes con enfoque legal y normativo.

Figura 17

Roles y responsabilidades



La estrategia de comunicación y consulta del SGCN de Teuno está diseñada para involucrar activamente a todos los actores clave en la identificación, tratamiento y seguimiento de

riesgos. Esta práctica asegura una cultura de transparencia, colaboración y mejora continua, pilares esenciales de una gestión eficaz de la continuidad del negocio. Así, se establecen los siguientes ejemplos por etapa del proceso:

Tabla 44

Comunicación en cada etapa del proceso de gestión de riesgos

Etapa del Proceso	Ejemplo de Comunicación Interna	Ejemplo de Comunicación Externa
Establecimiento del contexto	Reunión entre gestores de riesgo y líderes de procesos para definir el alcance y criterios.	Consulta con entes reguladores para validar obligaciones normativas.
Identificación del riesgo	Taller con jefaturas para levantar escenarios de riesgo por área.	Revisión de incidentes con proveedores críticos.
Análisis del riesgo	Comité técnico de riesgos analiza matrices de impacto y probabilidad.	Benchmarking con socios estratégicos del sector tecnológico.
Evaluación del riesgo	Sesión con la dirección para validar apetito de riesgo institucional.	Reporte ejecutivo a entes de certificación (ISO).
Tratamiento del riesgo	Presentación de acciones en comité de continuidad.	Informe de acciones correctivas ante auditorías externas.
Seguimiento y revisión	Indicadores mensuales presentados por el Gestor de Riesgos.	Entrega de resultados de simulacros a entes regulatorios.
Registro e informe	Almacenamiento en repositorio institucional, envío por correo.	Registro formal en informes de cumplimiento y auditoría.

5.6.3. Establecimiento del Alcance, Contexto y Criterios

5.6.3.1. Generalidades. Esta etapa representa el pilar fundamental sobre el cual se construye todo el proceso de gestión del riesgo. Establecer claramente estos elementos es crucial para asegurar que la evaluación y tratamiento de los riesgos se realicen de manera alineada a la realidad

organizacional, los objetivos estratégicos y los procesos críticos definidos en el análisis BIA del SGCN. A TEUNO le permitirá definir con claridad los límites y objetivos del análisis de riesgos aplicables al SGCN. Así, se dispondría del marco necesario para comprender el contexto organizacional, considerando factores internos (estructura, procesos, recursos) y externos (entorno regulatorio, amenazas tecnológicas, proveedores). De esta manera, se refleja la urgencia de definir criterios objetivos, como escalas de impacto, niveles de probabilidad y umbrales de tolerancia, necesarios para gestionar los riesgos de manera sistemática.

Consecuentemente, TEUNO requiere formalizar y aprobar una metodología de evaluación de riesgos alineada con la ISO 31000, que permita aplicar el análisis de riesgos de forma coherente sobre los procesos críticos definidos en el BIA. Esta metodología debe integrar criterios de valoración (impacto, probabilidad), mapas de riesgo, definición de niveles de exposición aceptables (apetito/tolerancia al riesgo), y procedimientos de tratamiento y monitoreo de riesgos.

Esto permitirá cerrar la brecha actual en la implementación del sistema y avanzar hacia una futura certificación del SGCN, con una base sólida de análisis de riesgos que garantice la protección y continuidad de los procesos clave.

5.6.3.2.Definición Del Alcance. Permite establecer con claridad cuáles serán los procesos, actividades, recursos y decisiones que serán objeto de evaluación y control. En el caso de TEUNO, este alcance debe enfocarse directamente en los 14 procesos críticos identificados en el análisis BIA abarcando desde la continuidad operativa hasta la necesidad de gestionar los riesgos que los afectan. Sobre ellos, se aplicará progresivamente la metodología de gestión de riesgos, que

incluirá la identificación de amenazas, evaluación de impactos, riesgo inherente, riesgo residual, definición de controles, monitoreo y acciones correctivas:

1) Procedimiento Contable
2) Procedimiento de Facturación y Cobranzas
3) Gestión de Seguridad de la Información (Gestión de Incidentes de Ciberseguridad)
4) Administración del Data Center
5) Ciberseguridad
6) Tecnología
7) Gestión de Cambios y Entregas
8) Gestión de Eventos (DOC)
9) Gestión de Incidentes
10) Gestión de Peticiones
11) Servicio ADC (Application Data Control)
12) Servicio SOC
13) Servicio de Transmisión de Datos e Internet
14) Procedimiento de Pago de Nómina

Como se observa en la siguiente figura, si bien TEUNO dispone de un SGCN documentado, con componentes clave, aún no se ha definido formalmente una metodología

específica de evaluación de riesgos ni para el sistema ni para los procesos críticos. Esto limita la capacidad de priorización, asignación de recursos y mejora continua del SGCN, al no contar con una base cuantitativa o cualitativa para la toma de decisiones basada en riesgo.

Es necesario avanzar en el diseño e implementación de una metodología formal para valorar los riesgos asociados a estos procesos críticos, lo que fortalecerá el SGCN y preparará a la organización para enfrentar futuros desafíos y procesos de certificación.

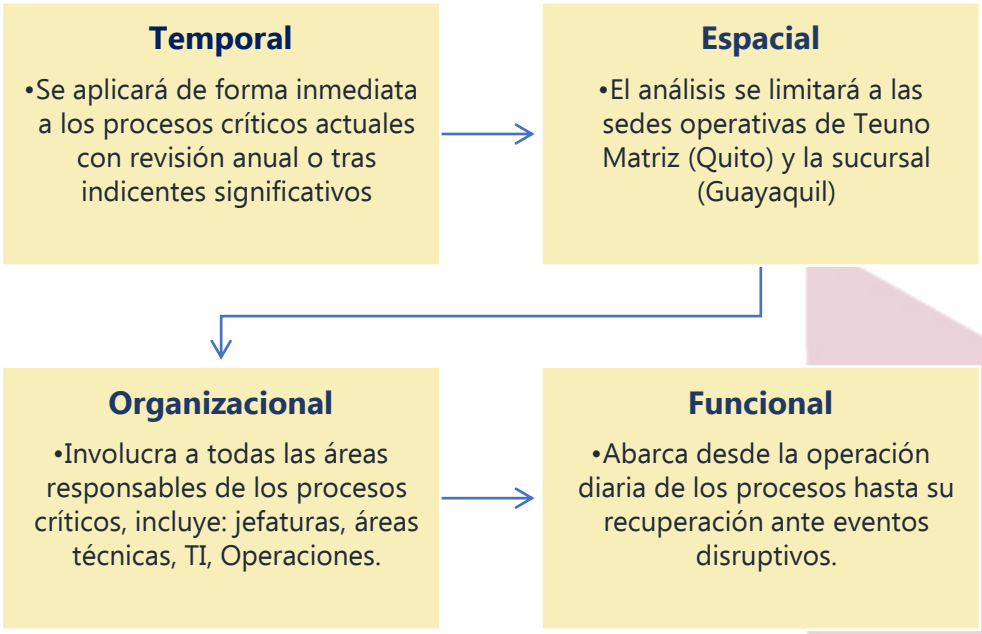
Figura 18

Recursos disponibles vs. Recursos por implementar

A la par, se definen los límites del alcance para contar con expectativas claras, una planificación realista y que los productos que se generen sean específicos.

Figura 19

Límites del alcance



5.6.3.3.Contexto Externo E Interno. Comprender los contextos externo e interno es clave para establecer un análisis de riesgos que refleje fielmente el entorno en el que opera Teuno. Esta etapa permite identificar factores que pueden generar o agravar los riesgos que afectan la continuidad de los procesos críticos.

Contexto Externo. Corresponde al entorno macro que influye en la operación y exposición al riesgo de Teuno. Este contexto se puede evaluar bajo el modelo PESTEL, considerando los siguientes factores:

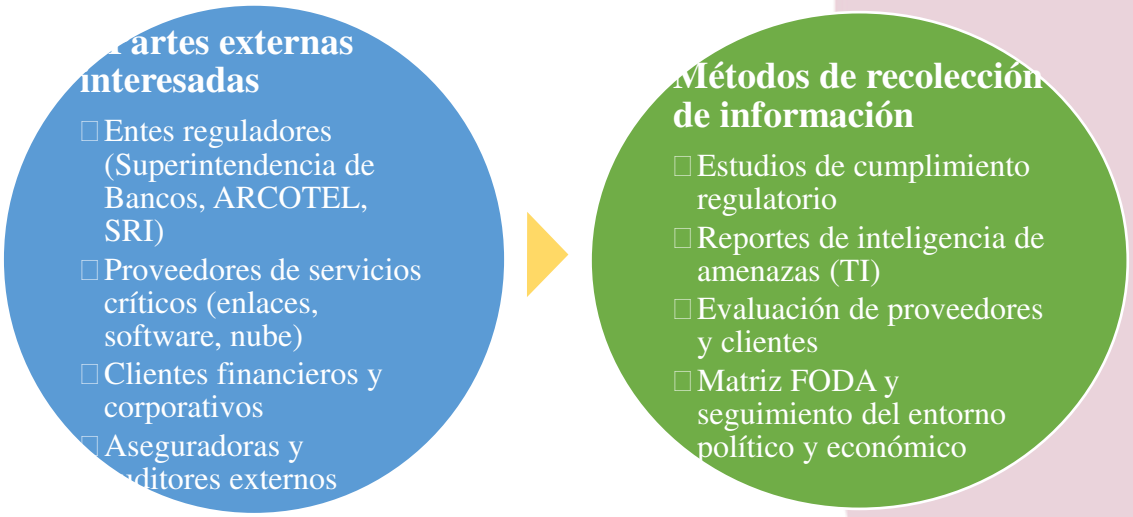
Tabla 45

Contexto externo de TEUNO de acuerdo al modelo PESTEL

Factor	***Descripción aplicada a TEUNO***
Político	Cambios regulatorios en telecomunicaciones y protección de datos. Prioridad del Estado hacia entidades públicas.
Económico	Volatilidad en presupuestos de inversión tecnológica, dependencia de licencias importadas.
Social	Exigencias de disponibilidad de servicios tecnológicos por parte de clientes corporativos.
Tecnológico	Alta velocidad de cambio en plataformas cloud, ciberseguridad y conectividad.
Ambiental	Riesgos físicos (inundaciones, incendios) que pueden afectar data centers o servicios remotos.
Legal	Cumplimiento de normativas de la Superintendencia de Bancos, ARCOTEL, LOPDP, entre otros.

Figura 20

Partes externas interesadas y los métodos para recolección de información



Contexto Interno. Hace referencia a los factores internos que pueden generar vulnerabilidades u oportunidades dentro del sistema organizativo.

Tabla 46

Factores internos potencialmente vulnerables

Factor Interno	Situación en TEUNO
Cultura organizacional	Fuerte orientación a la mejora continua y la innovación, pero con necesidad de madurar la cultura de riesgo transversal.
Estructura organizacional	Compuesta por áreas técnicas, operativas y estratégicas, con roles definidos, pero en proceso de fortalecer la integración de riesgos.
Recursos	Se cuenta con documentación del SGCN, comités activos y personal técnico capacitado, pero falta formalizar metodologías de análisis de riesgos.
Estrategias y objetivos	La empresa busca posicionarse como referente tecnológico, lo que exige alta disponibilidad, seguridad y cumplimiento.

Es importante considerar que la gestión de riesgos de continuidad exige coordinación entre los Sistemas de Gestión Teuno (ISO 27001, ISO 9001, ISO 20001), Tecnología (infraestructura, SOC, DOC), Operaciones (gestión de incidentes, cambios y peticiones), Finanzas (procesos contables y nómina) y Alta Dirección y comité de continuidad. Esto, reduce la exposición a riesgos no detectados o mal gestionados, ya que cada uno aportará información crítica sobre procesos, amenazas, vulnerabilidades y prioridades de recuperación.

5.6.3.4.Análisis FODA aplicado al SGCN de TEUNO. Significa otra manera de evaluar el contexto interno y externo de la empresa, definiendo Fortalezas, Oportunidades, Debilidades y Amenazas para visualizar de forma estratégica los elementos que influyen sobre los riesgos que podrían afectar la continuidad del negocio.

Tabla 47

Fortalezas (Factores internos positivos)

Fortaleza	Descripción
Documentación del SGCN	Se cuenta con planes, metodologías e instructivos operativos (BIA, BCP, DRP, plan de emergencias).
Comités organizados	Existen el Comité de Continuidad y el Comité de Riesgos, lo que facilita la coordinación.
Alta capacidad técnica	TEUNO dispone de personal con experiencia en áreas críticas como ciberseguridad, infraestructura y redes.
Orientación a la mejora continua	La organización aplica el enfoque PHVA en sus procesos clave.
Plataformas tecnológicas robustas	Operación en centros de datos con respaldo y servicios redundantes.

Tabla 48

Debilidades (Factores internos negativos)

Debilidad	Descripción
Ausencia de metodología de evaluación de riesgos	Aunque existen los procesos críticos identificados, aún no se ha formalizado la evaluación de riesgos sobre ellos.
Cultura de riesgos en maduración	El enfoque de riesgos aún no está plenamente interiorizado en todas las áreas.
Dependencia de proveedores críticos	Algunos servicios esenciales dependen de enlaces o software externo, lo que podría generar puntos únicos de falla.
Falta de integración tecnológica de la gestión de riesgos	Aún no se cuenta con herramientas automatizadas para registrar, monitorear y dar seguimiento a riesgos.

Tabla 49

Oportunidades (Factores externos positivos)

Oportunidad	Descripción
Aumento de exigencias normativas	Las normativas de entes como la Superintendencia de Bancos y ARCOTEL impulsan la formalización del SGCN.
Demanda del mercado por alta disponibilidad	Clientes corporativos buscan servicios resilientes, lo que alinea con los objetivos del SGCN.
Tendencia a certificaciones ISO	El interés por obtener certificaciones como ISO 22301 abre oportunidades para estructurar el sistema.
Madurez en digitalización del país	Las alianzas con fabricantes y partners tecnológicos fortalecen el ecosistema operativo de TEUNO.

Tabla 50

Amenazas (Factores externos negativos)

Amenaza	Descripción
Incremento de ciberataques	La exposición constante a amenazas como ransomware o denegación de servicio impacta directamente los procesos críticos.
Inestabilidad económica y altos costos de tecnología	Dificulta la inversión en soluciones resilientes y planes de contingencia.
Cambios normativos acelerados	Exigen adaptación rápida y aumentan el riesgo de incumplimiento.
Competencia desleal en el sector	Empresas no reguladas pueden ofrecer servicios con menor estructura, presionando los precios del mercado.

El análisis FODA evidencia que Teuno cuenta con una base sólida para implementar una gestión de riesgos efectiva en su SGCN. No obstante, enfrenta una brecha técnica clave: la falta de una metodología formal de evaluación de riesgos sobre procesos críticos, lo cual debe ser abordado como una prioridad estratégica. A su vez, las amenazas externas exigen consolidar las fortalezas institucionales para preservar la disponibilidad, seguridad y resiliencia de los servicios.

Figura 21

Cruce del Análisis FODA – Estrategias para el SGCN de TEUNO

Las estrategias clave se pueden resumir de la siguiente manera:

1) **Formalizar la metodología de evaluación de riesgos:** Desarrollar un enfoque institucional basado en ISO 31000 para analizar riesgos en los 14 procesos críticos. Validar el producto con los comités existentes y documentarlo como procedimiento oficial.

2) **Impulsar la certificación del SGCN:** Aprovechar la documentación ya existente (BIA, BCP, DRP) como base y utilizar la exigencia regulatoria como catalizador interno para justificar recursos.
3) **Reducir vulnerabilidades estructurales:** Establecer redundancia tecnológica para minimizar la dependencia de proveedores únicos e incluir cláusulas de continuidad en contratos estratégicos (SLA, DRP del proveedor).
4) **Reforzar la cultura y práctica del riesgo:** Capacitar a dueños de procesos y responsables de áreas en análisis de riesgos. Realizar simulacros alineados al BIA para evaluar reacciones y medidas reales ante amenazas emergentes.
5) **Implementar una herramienta tecnológica de seguimiento:** Evaluar plataformas como Planner, Jira u otras con flujos para evaluación, seguimiento y cierre de riesgos y controles.

5.6.3.5. Definición De Los Criterios De Riesgo. Proporcionan una base objetiva y estandarizada para valorar, clasificar y priorizar los riesgos que pueden afectar la continuidad de los procesos críticos identificados en el análisis BIA.

Los criterios de riesgo permiten establecer umbrales claros sobre qué riesgos son aceptables para la organización, cuáles deben ser tratados, y cuáles requieren una intervención inmediata. Además, aseguran la coherencia entre las distintas unidades de la empresa al momento de tomar decisiones sobre aceptación, mitigación, monitoreo o transferencia de riesgos.

Esta etapa se encuentra alineada con lo establecido en la norma ISO 31000:2018 y con el marco metodológico interno de Teuno, considerando tanto el contexto externo como interno, los

valores institucionales, los requisitos legales y regulatorios, así como el apetito y la tolerancia al riesgo definidos.

Es menester tomar en cuenta las siguientes consideraciones adicionales:

- El riesgo se calcula como:

  Riesgo = Probabilidad x Impacto

- El apetito de riesgo de Teuno está definido como nivel máximo aceptable: “Bajo” (según política vigente).
- Se utilizará un mapa de calor para visualizar los niveles de riesgo inherente y residual.
- En casos donde existan controles efectivos, la probabilidad podrá disminuir en 1 grado. El impacto solo disminuirá si se puede mitigar económicamente o por respaldo (p.ej. póliza de seguros).

5.6.3.6. Descripción de la Probabilidad. La probabilidad se cuantifica utilizando una escala de cinco niveles, que permite clasificar los riesgos de forma coherente y medible. Cada nivel define un rango de ocurrencias esperadas por año, facilitando la priorización de los riesgos y la toma de decisiones sobre su tratamiento.

La probabilidad se evalúa con base en históricos, experiencia organizacional o registros de incidentes. Cuando no exista dato numérico exacto, se recomienda aplicar juicio experto, priorizando el contexto del proceso y la naturaleza del riesgo. Puede utilizarse esta escala tanto para riesgos inherentes como residuales, siempre que se documente la base del criterio.

Figura 22

Caracterización de los niveles de probabilidad

Valor	Nivel de Probabilidad	Descripción	Frecuencia Estimada (No. veces/año)
5	Muy Alta	Ocurre en múltiples procesos al menos semanalmente. Parte del entorno actual.	Más de 48 veces al año (1 o más veces por semana)
4	Alta	Evento ocurre mensualmente o más, en procesos clave o críticos.	Entre 24 y 48 veces al año
3	Moderada	Ocurre de forma periódica, cada uno a dos meses.	Entre 6 y 24 veces al año
2	Baja	Evento poco frecuente. Hay antecedentes, pero no es común.	Entre 2 y 5 veces al año
1	Muy Baja	Evento raro o nunca ocurrido. Solo bajo circunstancias extraordinarias.	1 vez al año o menos

5.6.3.7. Descripción del Impacto. El impacto representa la magnitud de las consecuencias negativas que un evento de riesgo puede causar sobre los procesos críticos, los activos, la reputación y el cumplimiento normativo de Teuno. Este se valora en función de cinco dimensiones clave: financiera, cliente, legal/normativa, estratégica y reputacional.

Los niveles de impacto permiten establecer el grado de severidad de un evento no deseado, y son fundamentales para determinar las prioridades de acción y asignación de recursos para el tratamiento del riesgo.

Figura 23

Caracterización de los niveles de impacto

Valor	Nivel del Impacto	Financiero	Cliente	Legal, Normativo y Contractual	Estratégico	Reputacional
5	Crítico	Pérdidas mayores a $500.000	Interrupción grave, pérdida de clientes clave.	Riesgo de pérdida de licencias o contratos clave.	Impacto mayor: más del 60% de los objetivos comprometidos.	Daño reputacional grave e irreparable.
4	Alto	Pérdidas entre $10.001 a $500.000	Afectación generalizada, requiere esfuerzo de recuperación.	Multas o sanciones entre $10.000 y $500.000.	Cumplimiento estratégico afectado hasta 40%.	Daño reputacional moderado que requiere gestión activa.
3	Medio	Pérdidas menores a $10.000	Quejas leves y fáciles de gestionar.	Multas o sanciones menores a $10.000	Retraso leve en objetivos (hasta 20%).	Afectación leve, limitada a pocos actores
2	Bajo	No tiene impacto	Sin afectación perceptible al cliente.	Sin implicaciones legales ni contractuales.	Sin impacto en la estrategia.	Sin afectación a la reputación.
1	Muy Bajo	Sin consecuencia económica	Totalmente transparente para el cliente.	Irrelevante jurídicamente	Sin relación con objetivos estratégicos	Imperceptible, sin repercusión pública.

5.6.3.8. Niveles De Riesgo.

Tabla 51

Niveles de Riesgo – Teuno

Valor	Nivel de Riesgo	Rango numérico	Descripción	Acción Requerida
5	Muy Alto	21-25	Riesgo inaceptable que excede completamente el apetito institucional, con potencial de paralizar procesos críticos o comprometer gravemente la continuidad del negocio.	**NO ACEPTABLE** Requiere intervención inmediata, activación de contingencias y ejecución de planes de acción correctiva de forma prioritaria
4	Alto	15-20	Riesgo con impacto severo y alta probabilidad, que puede interrumpir objetivos estratégicos clave y comprometer la operación de manera significativa.	**NO ACEPTABLE** Requiere un plan de mitigación urgente, revisión del proceso afectado y posible rediseño de controles
3	Moderado	9-14	Riesgo con consecuencias relevantes pero dentro de márgenes tolerables. Puede afectar temporalmente objetivos operacionales o de servicio.	**ACEPTABLE** Se debe aplicar controles adicionales, reforzar la supervisión y establecer monitoreo frecuente
2	Bajo	5-8	Riesgo manejable dentro del apetito definido por la organización. Su impacto es limitado y las condiciones actuales	**RIESGO ACEPTABLE** Puede mantenerse con los controles existentes, pero debe incluirse en el monitoreo periódico

Valor	Nivel de Riesgo	Rango numérico	Descripción	Acción Requerida
			permiten controlarlo adecuadamente.	
1	Muy bajo	1-4	Riesgo menor con impacto residual prácticamente insignificante sobre la operación, sin amenaza directa a la continuidad.	**RIESGO ACEPTABLE**. No requiere acciones inmediatas. Debe registrarse y revisarse al menos una vez al año

Mapa de Calor: Es una herramienta visual utilizada por Teuno para representar la severidad de los riesgos, combinando dos dimensiones fundamentales: probabilidad e impacto. Esta matriz facilita la clasificación de los riesgos en niveles cuantificables, permitiendo priorizar su tratamiento de acuerdo con el apetito y tolerancia al riesgo definidos por la organización.

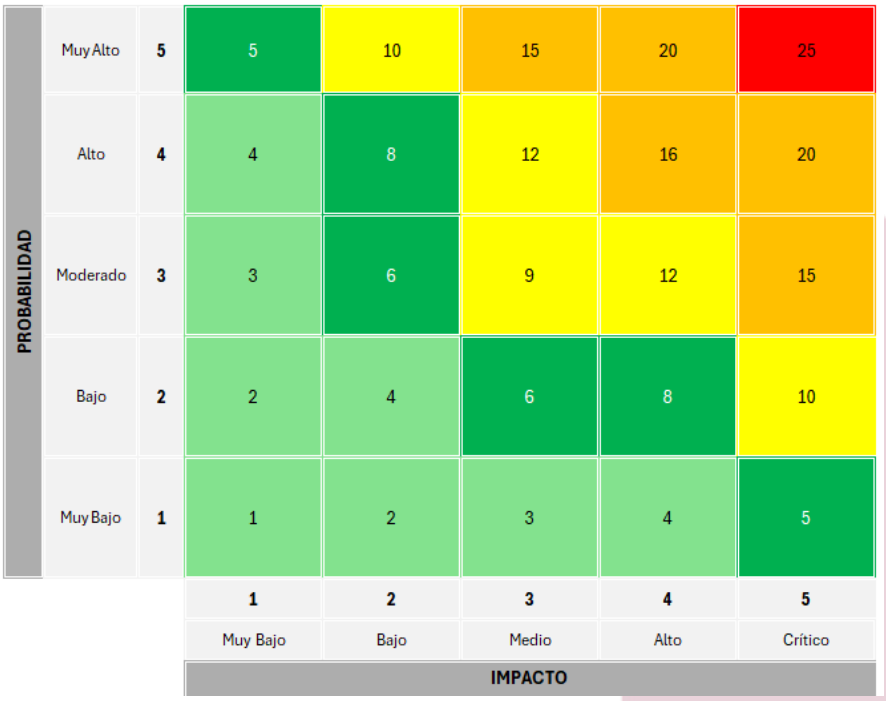
El enfoque adoptado permite identificar con claridad qué riesgos son aceptables, cuáles requieren monitoreo o mitigación, y cuáles deben ser tratados de forma inmediata, garantizando así la continuidad de los procesos críticos.

La matriz a continuación se compone de cinco niveles de probabilidad (en filas) y cinco niveles de impacto (en columnas). El producto de ambas variables genera un total de 25 combinaciones posibles y cada una de ellas, representa un valor numérico de riesgo que guía su clasificación. Cada nivel de riesgo se basará en el rango numérico de la Tabla 51 y así, permitirá establecer prioridades de respuesta ante los eventos adversos que puedan afectar la continuidad de los procesos críticos.

Es importante considerar que los criterios de riesgo para la evaluación y clasificación deben encontrarse en el marco de tres aspectos importantes:

Figura 24

Matriz para la estimación del nivel de riesgo



1) **Requisitos legales:** Los riesgos deben evaluarse considerando la legislación nacional vigente y cualquier normativa aplicable al sector en que opera TEUNO. Esto incluye:

- Requisitos de la Superintendencia de Compañías, Bancos u otros entes reguladores.
- Exigencias contractuales que impliquen obligaciones frente a clientes o proveedores.

El incumplimiento legal puede generar sanciones económicas, pérdida de licencias, afectación reputacional e incluso responsabilidades penales, por lo que su impacto debe ser priorizado.

2) **Expectativas de las partes interesadas:** La percepción, necesidades y preocupaciones de las partes interesadas (clientes, socios, proveedores, entes reguladores y personal interno) deben formar parte de los criterios de evaluación. Se debe considerar:

- Nivel de tolerancia al riesgo que tienen los clientes respecto a interrupciones o fallos.
- Requisitos contractuales sobre continuidad del servicio.
- Expectativas de transparencia, confianza y reacción ante incidentes.

El desalineamiento entre las expectativas externas e internas puede traducirse en pérdida de competitividad o ruptura de relaciones comerciales.

3) **Valores organizacionales:** Los criterios también deben reflejar los principios y compromisos estratégicos definidos por la Alta Dirección de TEUNO. Esto garantiza coherencia en la toma de decisiones, reforzando:

- El compromiso con la continuidad operativa.
- La priorización de procesos que sostienen la misión institucional.
- La cultura organizacional orientada a la mejora continua y la resiliencia.

En este sentido, si un riesgo compromete valores fundamentales como la integridad, transparencia o servicio al cliente, puede ser catalogado como inaceptable incluso si su impacto es moderado.

5.6.4. Evaluación del riesgo

5.6.4.1. Generalidades. La evaluación del riesgo constituye el eje central del proceso de gestión de riesgos conforme a la norma ISO 31000:2018. Su objetivo es entregar información estructurada que permita a TEUNO tomar decisiones informadas respecto a los eventos que podrían afectar la continuidad de sus procesos críticos. Esta evaluación incluye tres componentes clave: identificación, análisis y valoración del riesgo.

En el contexto del Sistema de Gestión de Continuidad del Negocio (SGCN) de TEUNO, la evaluación del riesgo busca identificar aquellos eventos que puedan impactar la disponibilidad, integridad y continuidad de los 14 procesos críticos definidos en el análisis BIA. Se consideran tanto amenazas internas como externas, así como las vulnerabilidades estructurales, operativas o tecnológicas que podrían facilitar dichos eventos.

5.6.4.2. Identificación del Riesgo. La identificación del riesgo constituye el primer paso del proceso de evaluación de riesgos según la norma ISO 31000, ya que permite construir una base estructurada para los análisis posteriores. Teuno utilizó una matriz diseñada específicamente para asociar cada riesgo con un proceso crítico previamente definido en el Análisis de Impacto al Negocio (BIA).

Tabla 52

Estructura de la matriz de Identificación del Riesgo aplicada

Campo	Descripción
ID-Riesgo	Código único que permite rastrear y clasificar cada riesgo de forma sistemática (ej. R-001 a R-170).
ID-Proceso Crítico	Código que identifica al proceso dentro del catálogo del SGCN (ej. PRC-01 a PRC-14).
Área	Unidad organizativa responsable del proceso. Permite trazar la responsabilidad funcional y operativa del riesgo.
Proceso Crítico	Nombre del proceso evaluado según lo definido en el BIA. Está alineado con el mapa de procesos de la organización.
Responsable del Proceso	Cargo o rol que tiene la custodia funcional y técnica del proceso, clave para las acciones de mitigación.
Descripción del Proceso	Explica brevemente el propósito y alcance del proceso, lo que ayuda a contextualizar su criticidad.
Escenario de Indisponibilidad	Se describe la condición que afecta la operación (Sin Personal Crítico, Sin Instalaciones, Sin Sistemas Críticos, Sin Proveedores Críticos).
Amenaza	Evento o condición externa o interna que podría activar un riesgo. Se clasifica conforme al catálogo institucional (ej. malware, corte eléctrico, manipulación, etc.).
Descripción de la Amenaza	Detalle narrativo del evento de amenaza que contribuye a la situación de riesgo.
Vulnerabilidad	Condición interna que aumenta la probabilidad de que la amenaza tenga consecuencias negativas (ej. ausencia de respaldo, sin monitoreo, falta de personal de reemplazo, etc.).
Descripción de la Vulnerabilidad	Explicación concreta de cómo la debilidad interna habilita el riesgo.
Tipo de Riesgo	Categorización superior para facilitar la gestión estratégica del riesgo. Se utilizan cinco tipos: Personas, Tecnología, Procesos, Eventos Externos, Terceros.

Campo	Descripción
Riesgo	Nombre resumido del riesgo, formulado como causa-consecuencia, útil para registrar, comunicar y priorizar.
Riesgos Relacionados	Riesgo Relacionado, según clasificación operativa del impacto. Este campo puede usarse para vincular riesgos secundarios.
Descripción del Riesgo	Redacción completa que integra la amenaza, vulnerabilidad y riesgo en forma de narrativa estructurada, como secuencia de eventos desde una causa hasta una consecuencia no deseada.

En el contexto del SGCN de Teuno, se identificaron 170 riesgos inherentes distribuidos entre los 14 procesos críticos. Se consideró un enfoque sistemático utilizando como base los escenarios de indisponibilidad previamente definidos por la organización, que representan las situaciones de disrupción más relevantes para la continuidad operativa.

Figura 25

Escenarios de riesgo

A partir de estos escenarios, se construyó un catálogo de amenazas y vulnerabilidades específicas y asociadas directamente a cada situación de indisponibilidad. Estas amenazas y vulnerabilidades fueron tomadas del inventario de Teuno y se complementaron con la experiencia del equipo de gestión de riesgos, gestión de incidentes, informes de auditorías, etc., incluyendo insumos del comité de continuidad del negocio.

Como parte del proceso de identificación, los riesgos se agruparon por su naturaleza en cinco categorías principales, lo cual facilitó su análisis, comparación, evaluación y futura gestión. Esta clasificación fue determinada de acuerdo con el impacto en la continuidad operativa y las características de la amenaza y vulnerabilidad involucradas.

Tabla 53

Caracterización de los riesgos por naturaleza

Tipo naturaleza	Descripción	Ejemplos de Riesgos Identificados en TEUNO
Personas	Riesgos derivados de la ausencia, sobrecarga, error o manipulación humana que comprometan la operación de procesos críticos.	- Ausencia de personal clave (R-01) - Rotación sin transferencia de conocimiento (R-02) - Fatiga operativa por alta carga de trabajo (R-03) - Manipulación intencionada o negligente de información (R-122, R-148)

Tipo naturaleza	Descripción	Ejemplos de Riesgos Identificados en TEUNO
		- Falta de relevos en turnos críticos (R-95, R-159)
Tecnología	Riesgos asociados a la indisponibilidad, fallos o vulnerabilidades en plataformas tecnológicas, equipos, redes o sistemas críticos.	- Caída del SIEM o ITSM (R-07, R-89, R-101) - Saturación de sistemas por ataques o eventos masivos (R-09, R-103, R-152) - Malware, ransomware o intrusión no controlada (R-91, R-104, R-116, R-154) - Error en automatización o fallas lógicas (R-115, R-90) - Configuraciones erróneas o firmware obsoleto (R-102, R-153)

Procesos	**Riesgos derivados de fallas en los procedimientos, errores humanos, falta de controles, políticas o revisión adecuada en la ejecución operativa.**	**- Error de clasificación o cierre indebido de solicitudes (R-86)** **- Evaluación técnica errónea en decisiones estratégicas (R-132)** **- Fallos de control en versiones documentales o registros (R-139)** **- Procesos detenidos por falta de documentación (R-131)** **- Falsificación de datos o indicadores internos (R-134, R-161)**
Eventos Externos	Riesgos derivados de situaciones ambientales, desastres naturales o condiciones fuera del control directo de la organización.	- Incendios, cortes eléctricos o desastres naturales (R-04, R-05, R-100, R-149) - Inundaciones o afectación física del entorno SOC o DC (R-113, R-164) - Daños físicos accidentales en instalaciones clave (R-137, R-150)
Terceros	Riesgos originados por la dependencia de proveedores externos para servicios críticos,	- Caída de proveedor de internet, DNS o ITSM (R-10, R-92, R-128, R-155) - Soporte deficiente que extiende fallas (R-93, R-130, R-169)

	telecomunicaciones, infraestructura o soporte.	- Fallo del proveedor de energía o climatización (R-117, R-118) - Fallos de ruteo BGP o backbone del proveedor (R-158) - Vulnerabilidad en herramientas del proveedor (R-170)

Esta organización por tipo de riesgo permitió priorizar la gestión de riesgos con mayor claridad, identificando cuáles áreas (capital humano, infraestructura, plataformas, procesos o servicios contratados) requerían mayor nivel de atención y resiliencia dentro del sistema de gestión de continuidad del negocio (SGCN).

5.6.4.3.Análisis del Riesgo. El objetivo del análisis del riesgo es comprender la naturaleza de los riesgos identificados, estimar su nivel mediante la evaluación de la probabilidad y el impacto, y establecer una base técnica para su priorización y tratamiento. Este análisis permite determinar cómo las amenazas, vulnerabilidades y escenarios de indisponibilidad podrían afectar los procesos críticos del Sistema de Gestión de Continuidad del Negocio de Teuno.

Tabla 54

Estructuración de la matriz de análisis de riesgos

Campo	Descripción
Probabilidad	Categoría cualitativa asignada a la posibilidad de ocurrencia del evento. Ej.: Muy Alta, Alta, Moderada, Baja, Muy Baja. Es asignada mediante sesiones de análisis con los dueños de procesos críticos y expertos en continuidad, en base a la experiencia previa, ocurrencia histórica y vulnerabilidad actual
Valor Probabilidad	Valor numérico correspondiente a la categoría de probabilidad (1 a 5).
Impacto	Categoría cualitativa del efecto del riesgo en los procesos críticos. En este caso, se definió siempre como **Crítico**, por ser procesos de alta prioridad.
Valor Impacto	Valor numérico correspondiente al impacto alto por decisión institucional.
Nota del Riesgo Inherente	Resultado de multiplicar la probabilidad por el impacto. Fórmula: Probabilidad × Impacto.

Campo	Descripción
Nivel del Riesgo Inherente	Clasificación cualitativa del nivel del riesgo, según la matriz de riesgo de Teuno: **Muy Alto** (21–25) **Alto** (15-20) **Moderado** (9-14) **Bajo** (5-8) **Muy Bajo** (1-4)
Valor del Riesgo Inherente	Representa la cuantificación total del riesgo antes de aplicar controles, también denominado **riesgo sin tratar**. Es el riesgo natural de los procesos críticos.

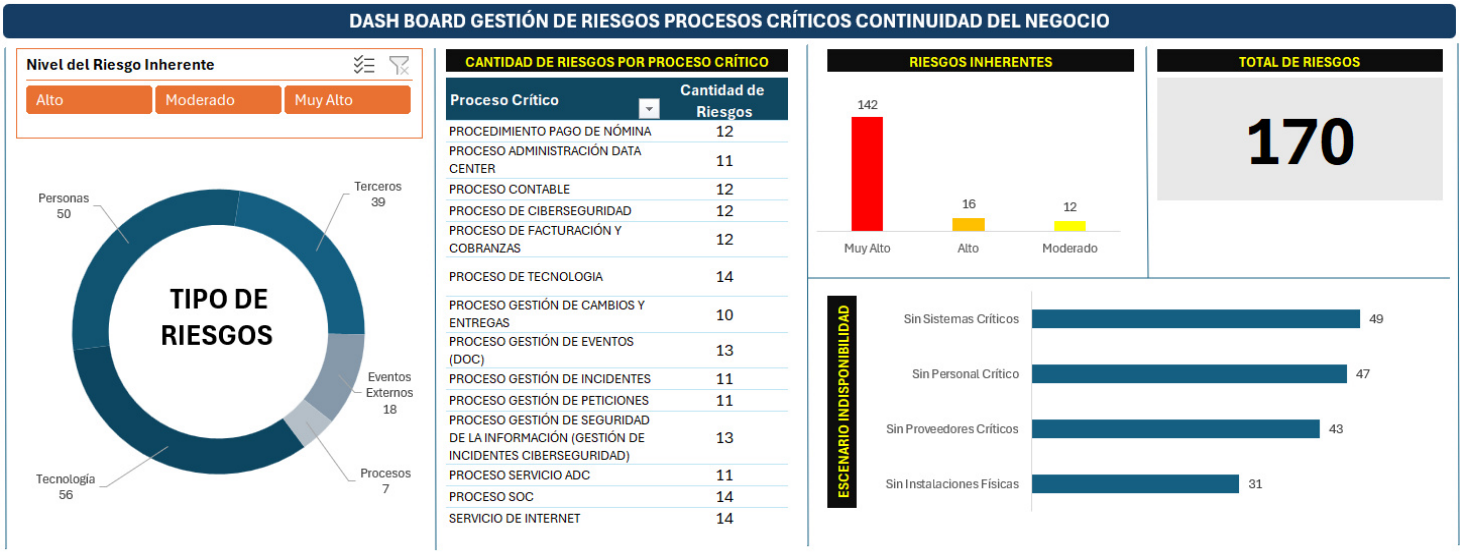
Bajo la estructura indicada, se realizó la evaluación integral de 170 riesgos inherentes que afectan a los 14 procesos críticos definidos por el Sistema de Gestión de Continuidad del Negocio de Teuno. La evaluación consideró los 4 escenarios de indisponibilidad institucionales: Sin Personal Crítico, Sin Instalaciones Físicas, Sin Sistemas Críticos y Sin Proveedores Críticos, y se estructuró por tipo de riesgo para facilitar el análisis. Los riesgos se clasifican en 5 categorías; Personas, Tecnología, Procesos, Eventos Externos y Terceros.

Cada riesgo fue identificado, analizado y valorado conforme a criterios de probabilidad e impacto preestablecidos por la organización, combinando la información levantada en el BIA (Business Impact Analysis) con juicio experto y sesiones con responsables de proceso. Los

resultados se integraron en una matriz que permite establecer el nivel de riesgo inherente, su criticidad y las acciones necesarias para su tratamiento.

Figura 26

DashBoard de la gestión de riesgos de los procesos críticos de Teuno



- **Análisis por Nivel de Riesgo Inherente**

Más del 80% de los riesgos presentan un nivel muy alto, lo que exige respuesta inmediata institucional y priorización estratégica

Figura 27

Análisis por nivel de riesgo

Nivel del Riesgo	Cantidad	Porcentaje	Acción requerida según matriz
Muy Alto	142	84%	Intervención inmediata y planes de contingencia.
Alto	16	9%	Plan de mitigación urgente.
Moderado	12	7%	Controles adicionales y monitoreo frecuente.
Total	**170**	**100%**	—

Figura 28

Análisis por tipo de riesgo

Tipo de Riesgo	Total de Riesgos	Porcentaje (%)
Tecnología	56	32,9%
Personas	50	29,4%
Terceros	39	22,9%
Eventos Externos	18	10,6%
Procesos	7	4,1%
Total	**170**	**100%**

- **Análisis por tipo de riesgo**

El análisis de los 170 riesgos identificados en el marco de la evaluación permitió agrupar y clasificar los escenarios de riesgo según su naturaleza, lo cual facilita la priorización de acciones de tratamiento y fortalece la orientación estratégica.

- **Análisis Cualitativo**

Tecnología (56 riesgos - 32,9%): Es la categoría con mayor concentración de riesgos. Esto se debe a la alta dependencia de sistemas críticos como SIEM, plataformas de monitoreo, servidores, redes, firewalls, etc. Las principales amenazas incluyen: caídas de sistemas, malware, fallas de configuración, automatización incorrecta y saturación por ataques. Esta categoría representa un foco crítico de atención para asegurar la continuidad de negocio.

Personas (50 riesgos - 29,4%): El segundo tipo más frecuente. Refleja una importante vulnerabilidad operativa por la dependencia de personal clave, fatiga laboral, errores humanos y falta de suplentes. Estos riesgos impactan directamente la gestión diaria de incidentes, peticiones, monitoreo y gobierno TI, lo cual exige fortalecer medidas de capacitación, turnos, backup de funciones y bienestar organizacional.

Terceros (39 riesgos - 22,9%): Esta categoría evidencia una fuerte dependencia de proveedores externos, principalmente en conectividad, sistemas SaaS (SIEM, Microsoft), energía, climatización y soporte técnico. Los escenarios más críticos se relacionan con fallas sin plan de contingencia, mal soporte, ausencia de SLA o eventos de ruteo externo. Se destaca la necesidad de reforzar los contratos, acuerdos de continuidad y planes de sustitución.

Eventos Externos (18 riesgos - 10,6%): Aunque no son tan frecuentes, su potencial impacto es significativo. Incendios, cortes eléctricos, desastres naturales o afectaciones estructurales podrían paralizar completamente los servicios críticos. Requieren estrategias de contingencia física, redundancia de sitio, y resiliencia ambiental.

Procesos (7 riesgos - 4,1%): Si bien es la categoría con menor número, representa debilidades en la gestión documental, control de versiones, errores metodológicos y decisiones incorrectas por falta de revisión técnica. Estas fallas pueden socavar la eficacia del gobierno TI y la trazabilidad de decisiones clave.

El análisis evidencia que los mayores vectores de riesgo en Teuno están relacionados con Tecnología y Personas, acumulando juntos más del 60% del total. Esta concentración demanda medidas robustas de gestión técnica y operativa, acompañadas de una política clara de gestión del conocimiento, capacitación y monitoreo continuo.

Asimismo, la dependencia de terceros (casi un cuarto del total) es un aspecto estratégico que requiere atención en la formalización de relaciones, mejora de SLAs y evaluación continua de proveedores críticos.

- **Análisis de riesgos por escenario de indisponibilidad**

Para reforzar el análisis de tipos de riesgos también hemos analizado los riesgos por escenario de indisponibilidad de los 170 riesgos inherentes, se organizaron los escenarios según las 4 grandes categorías de indisponibilidad definidas. Esta clasificación permite abordar las principales fuentes de interrupción que afectan la continuidad operativa.

Figura 29

Análisis por escenario

Escenario de Indisponibilidad	Total de Riesgos	Porcentaje (%)
Sin Sistemas Críticos	49	28,8%
Sin Personal Crítico	47	27,6%
Sin Proveedores Críticos	43	25,3%
Sin Instalaciones Físicas	31	18,2%
Total	170	1

Del análisis conjunto se concluye que los riesgos de continuidad identificados en los procesos críticos de Teuno están principalmente relacionados con fallas tecnológicas (56 riesgos) y con la no disponibilidad del personal crítico (50 riesgos). Esta tendencia se alinea directamente con los escenarios de "Sin Sistemas Críticos" (49 riesgos) y "Sin Personal Crítico" (47 riesgos), lo que demuestra una fuerte correlación entre la tipología del riesgo y la fuente de interrupción operativa.

Adicionalmente, el alto número de riesgos clasificados bajo la categoría de “Terceros” (39 riesgos) guarda estrecha relación con el escenario de "Sin Proveedores Críticos" (43 riesgos), evidenciando una vulnerabilidad significativa frente a la dependencia de servicios externos como conectividad, soporte cloud, plataformas SaaS y energía.

Por su parte, los riesgos de tipo "Eventos Externos" y "Procesos", aunque en menor proporción, reflejan incidentes de alto impacto como incendios, cortes eléctricos, errores metodológicos o fallos estratégicos, muchos de los cuales se agrupan en el escenario de "Sin Instalaciones Físicas" (31 riesgos).

En conjunto, esta relación cruzada confirma que la resiliencia del SGCN de Teuno depende en gran medida de la robustez tecnológica, la disponibilidad del personal clave y la gestión eficaz de proveedores críticos, por lo que estos factores deben ser priorizados en los planes de tratamiento y continuidad del negocio.

Figura 30

Procesos críticos con mayor número de riesgos

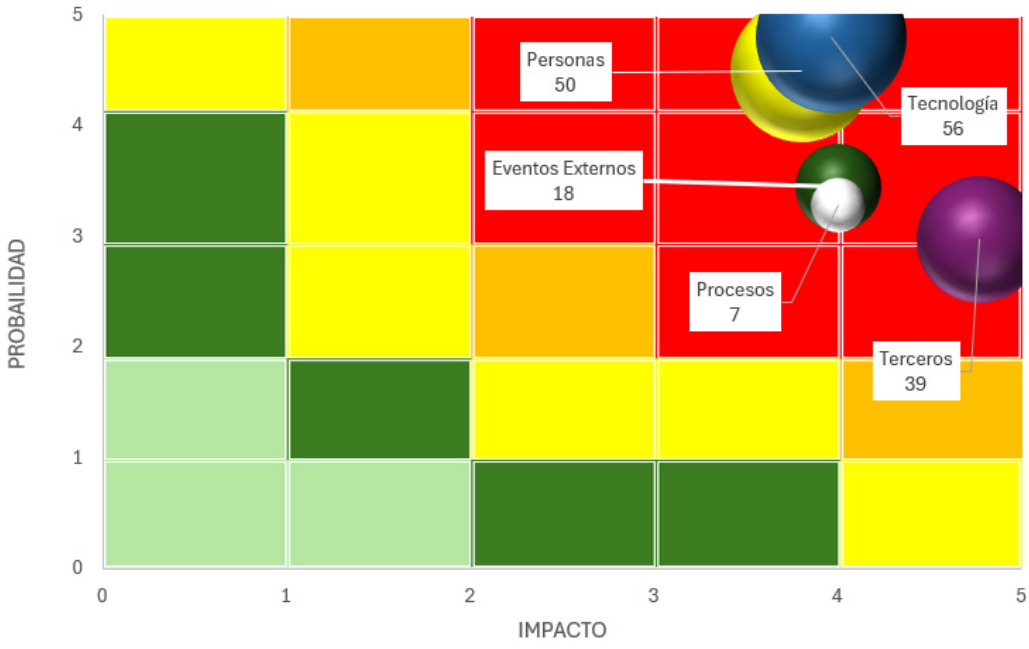
Proceso Crítico	Nº Riesgos
Proceso de Tecnología	14
Servicio de Internet	14
Servicio ADC	14
Proceso de Ciberseguridad	13
Gestión de Seguridad de la Información (SOC)	13
Pago de Nómina / Administración Data Center	12

Los procesos tecnológicos y de soporte transversal concentran los mayores riesgos por su papel estructural en la operación.

Por otro lado, el mapa de calor confirma que el contexto operativo de TEUNO presenta un perfil de riesgo alto en continuidad del negocio. Esto valida la necesidad de contar con un SGCN robusto, monitoreado y con planes de acción claros frente a escenarios de interrupción. La herramienta visual facilita la priorización de esfuerzos y permite al comité de riesgos enfocar sus recursos en las amenazas más críticas.

Figura 31

Mapa de calor TEUNO



El diagnóstico general de los 170 riesgos evaluados permite evidenciar:

- Una alta criticidad operativa y estratégica en los procesos clave.
- La necesidad de fortalecer controles tecnológicos, capacitación del personal y contratos con terceros.

- La urgencia de implementar acciones correctivas, especialmente sobre los 142 riesgos catalogados como “Muy Alto".

5.6.4.4.Valoración del Riesgo. La valoración del riesgo constituye la última fase del proceso de evaluación. Esta etapa tiene como objetivo determinar el riesgo residual, una vez aplicados los controles, planes de continuidad, y mecanismos de mitigación existentes en la organización. La valoración permite decidir si el riesgo debe ser tratado, aceptado, monitoreado o transferido, con base en el apetito de riesgo institucional.

Para Teuno, se utilizó una matriz estructurada de valoración que considera múltiples variables clave para cuantificar la efectividad de los controles de continuidad y determinar el nivel residual de riesgo por proceso crítico. Esta valoración incluye tanto controles operativos como contingencias documentadas (planes de continuidad, planes de recuperación, estrategias de alta disponibilidad, etc.).

Tabla 55

Estructuración de la matriz de valoración

Campo	Descripción
¿Existe control o contingencia en Teuno?	Determina si hay medidas implementadas que reduzcan el riesgo.
Control o Contingencia	Nombre del plan, sistema o estrategia de mitigación.

Campo	Descripción
Descripción del Control o Contingencia	Detalle operativo del mecanismo aplicado.
Responsable de ejecutar el control	Rol encargado de la implementación del control.
Documentación	Se verifica si el control está documentado, actualizado y referenciado.
Periodicidad de las pruebas	Indica si el control es permanente, periódico, ocasional o a demanda.
Tipo de control	Se clasifica como preventivo, detectivo o correctivo.
Automatización	Grado de automatización (manual, semiautomático, automático).
Porcentaje total (efectividad)	Se calcula con base en un modelo ponderado previamente definido.
Valor del Control	Valor numérico del control (1–4), asociado al nivel de eficiencia.
Valor de Probabilidad e Impacto con Control	Nuevos valores ajustados del riesgo con control aplicado.
Nota del Riesgo Residual	Resultado final tras aplicar el control.

La valoración del riesgo es el paso que permite comparar el riesgo inherente previamente analizado con la eficacia de los controles y contingencias existentes, con el fin de estimar el riesgo residual, esta etapa fue esencial para determinar cuáles riesgos requieren tratamiento inmediato, cuáles deben ser monitoreados y cuáles se consideran aceptables dentro del apetito institucional.

Determinación del riesgo residual: Para cada riesgo identificado se comparó el nivel de riesgo inherente (antes de aplicar controles) con el nivel de riesgo residual posterior a la valoración de los controles. Se aplicó la siguiente lógica de transformación:

Controles o contingencias existentes en TEUNO: Se incluyeron controles operativos, procedimientos de continuidad, contingencias tecnológicas, respaldos documentales y acuerdos con proveedores críticos. Además, se verificó si los controles estaban documentados, actualizados y en qué grado eran automatizados.

Criterios de evaluación de controles: Periodicidad (periódico, permanente, ocasional, a demanda), Tipo de control (preventivo, detectivo, correctivo), Automatización (automático, semiautomático, manual), Documentación y actualización del control.

Cálculo de eficiencia del control: Se asignó un porcentaje de eficiencia con base en los factores anteriores, determinando su categoría como:

- Fuerte (81%–100%)
- Satisfactorio (71%–80%)
- Regular (61%–70%)

- Deficiente (1%–60%)
- Inexistente (0%)

Reducción de impacto esperada

Figura 32

Ajuste del impacto residual de acuerdo a la eficiencia del control

Eficiencia del control	Valor	Reducción del Impacto
Fuerte (81–100%)	5	-4
Satisfactorio (71–80%)	4	-3
Regular (61–70%)	3	-2
Deficiente (1–60%)	2	-1
Inexistente (0%)	1	-1

Valoración residual final: Se aplicó nuevamente la matriz de riesgo (Probabilidad × Impacto) usando los valores ajustados de impacto post-control, obteniendo así el nivel de riesgo residual: Muy Alto, Alto, Moderado, Bajo o Muy Bajo.

Se recopilaron evidencias para cada riesgo identificado a lo largo de los 14 procesos críticos del SGCN. Los controles fueron evaluados conforme a:

Documentación formal existente.

- Grado de actualización de los planes de continuidad.
- Frecuencia de pruebas de contingencia.

- Presencia de automatización y responsabilidad definida.
- A través de este proceso, se logró:
- Estimar de forma objetiva la capacidad de mitigación real de los controles existentes.
- Reclasificar riesgos según su exposición residual.
- Identificar aquellos escenarios donde el riesgo residual aún se mantenía en niveles Muy Altos o Altos, pese a la existencia de controles, lo cual exigirá un tratamiento formal posterior.

Análisis del Riesgo Residual: A continuación, se presenta el análisis integral de los resultados obtenidos de la valoración de riesgos de continuidad del negocio en Teuno, enfocado en el apetito de riesgo, riesgo residual, tipo de riesgo y escenarios de indisponibilidad.

Figura 33

Análisis del Apetito de Riesgo

Clasificación	Cantidad de Riesgos	Observación
Riesgos aceptados	106	Son los riesgos que están por debajo del apetito de riesgos y que son aceptados por la organización
Riesgos no aceptados	**64**	**Son los riesgos que no pudieron ser mitigados con los controles y que se debe realizar un tratamiento de riesgo**

El 62% de los riesgos han sido aceptados por la organización tras aplicar medidas de tratamiento, controles y/o mitigación. Sin embargo, 64 riesgos (38%) no cumplen con el nivel de apetito definido y requieren acciones inmediatas de tratamiento adicional o rediseño de controles.

Figura 34

Análisis del Riesgo Residual (Riesgos no aceptados)

Nivel de Riesgo Residual	Cantidad de Riesgos
Muy Alto	4
Alto	10
Moderado	50

Aunque la mayoría de los riesgos residuales se redujeron a un nivel moderado, aún 14 riesgos (4 muy altos + 10 altos) superan el umbral aceptado. Estos deben ser priorizados en la fase de rediseño de controles o modificación de su tratamiento actual.

Figura 35

Análisis por Tipo de Riesgo (Riesgos no aceptados)

Tipo de Riesgo	Riesgos No Aceptados
Personas	26
Tecnología	17
Terceros	12
Eventos Externos	5
Procesos	4

El mayor volumen de riesgos no aceptados está relacionado con factores humanos (Personas) y fallas tecnológicas, lo cual sugiere:

- Necesidad de fortalecer la resiliencia operativa del personal clave.
- Evaluar y modernizar sistemas críticos y controles tecnológicos.

Figura 36

Análisis por Escenario de Indisponibilidad (solo riesgos no aceptados)

Escenario de Indisponibilidad	Riesgos No Aceptados
Sin Personal Crítico	26
Sin Sistemas Críticos	19
Sin Proveedores Críticos	14
Sin Instalaciones Físicas	5

El escenario “Sin Personal Crítico” representa el mayor volumen de riesgos no aceptados, lo cual evidencia la alta dependencia operativa en roles clave. Esto hace crítica la implementación de:

- Planes de respaldo de personal.
- Capacitación cruzada y transferencia de conocimiento.
- Automatización de tareas repetitivas donde sea posible.

Figura 37

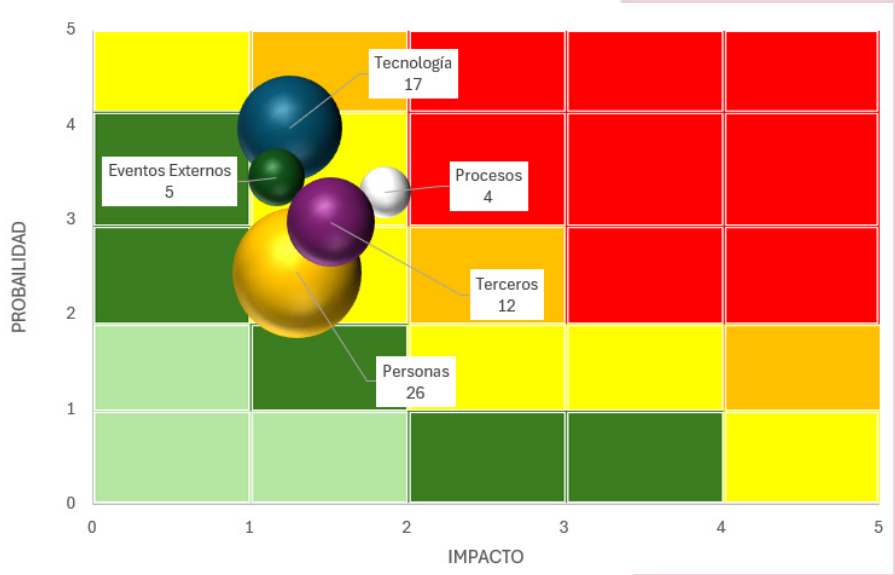
Comparación Riesgo Inherente vs Residual (Solo riesgos no aceptados)

Riesgo	Inherente	Residual	Observación
Total Muy Alto (antes)	142	4	Reducción significativa, pero aún persisten riesgos muy críticos.
Total Alto (antes)	16	10	Riesgos parcialmente mitigados, algunos permanecen en zona no aceptable.
Total Moderado (antes)	12	50	La mayoría de los riesgos se redujeron a **nivel moderado**, lo que indica eficiencia en el tratamiento, aunque no todos son aceptables.

La estrategia de tratamiento redujo efectivamente los niveles de riesgo inherente, sin embargo, persisten brechas de control que exigen atención prioritaria, especialmente en riesgos con tratamiento ineficaz (residual alto o muy alto).

Figura 38

Mapa de calor residual



Conclusión del Análisis Residual

- El total de riesgos residuales fuera del apetito (Muy Alto) valor 4, lo que representa una gestión bastante efectiva del riesgo.
- El mapa residual muestra un desplazamiento general hacia zonas amarillas y verdes del mapa de calor, lo cual indica una reducción satisfactoria del nivel de riesgo.
- Personas es el único tipo de riesgo que aumentó proporcionalmente su representación en el residual, lo que sugiere que los controles actuales no están siendo suficientemente eficaces o no son sostenibles en el tiempo.

Recomendaciones Finales

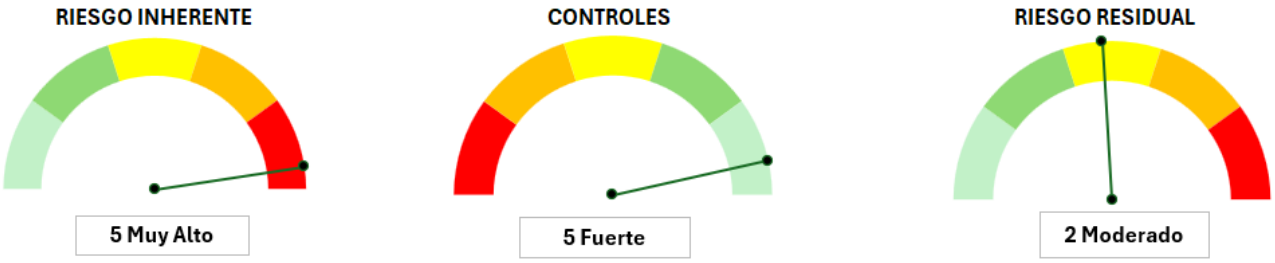
- Rediseñar controles para los 14 riesgos con nivel residual alto o muy alto.
- Reevaluar el tratamiento actual aplicado a los 64 riesgos no aceptados.
- Reforzar controles sobre personas y tecnología, dado que son los mayores generadores de riesgo no tolerado.
- Implementar estrategias de resiliencia operativa en los escenarios más vulnerables: sin personal crítico y sin sistemas críticos.
- Incorporar un programa continuo de revisión del apetito de riesgo, considerando cambios en el entorno tecnológico y de negocio.

Resumen General del Análisis de Riesgos

La siguiente gráfica permiten visualizar de manera clara y comparativa la evolución del riesgo desde su estado inicial (inherente) hasta su situación posterior al tratamiento (residual), considerando además la eficacia de los controles implementados.

Figura 39

Evolución del riesgo después de la aplicación de controles



Existe una reducción significativa del riesgo, gracias a la implementación de controles fuertes y adecuados.

Esta evolución demuestra que el modelo de gestión de riesgos está funcionando correctamente.

El paso de un riesgo “Muy Alto” a "Moderado" valida que las acciones de tratamiento son eficaces y que pueden sostenerse en el tiempo si se mantienen las condiciones de control.

5.6.5. Tratamiento del Riesgo.

5.6.5.1. Generalidades. El tratamiento del riesgo constituye la etapa final del proceso de evaluación, cuyo propósito es reducir el nivel del riesgo residual a un valor aceptable dentro del apetito de riesgo definido por la organización. En Teuno, este tratamiento se aplicó una vez evaluados los 170 riesgos inherentes identificados en los 14 procesos críticos del SGCN, permitiendo determinar si los riesgos requieren acciones correctivas, controles adicionales o estrategias de mitigación específicas.

Los tratamientos se establecieron considerando:

- El apetito de riesgo institucional (nivel aceptable definido por la Alta Dirección).
- La eficiencia de los controles actuales (documentación, actualización, tipo, automatización, periodicidad).
- La criticidad del proceso afectado.
- El tipo de escenario de indisponibilidad.
- Las acciones de continuidad o contingencia disponibles.

5.6.5.2. Selección de las opciones para el tratamiento del riesgo. Una vez determinada la valoración del riesgo residual y contrastado con el apetito de riesgo definido por la organización, se procedió a seleccionar las opciones más apropiadas para su tratamiento, de acuerdo con las directrices de la norma ISO 31000:2018 y los criterios definidos por Teuno.

Figura 40

Resumen cuantitativo de tipos de tratamiento seleccionados

Tipo de Tratamiento	Nº de riesgos tratados
Modificar la probabilidad	41
Compartir	9
Modificar el impacto	7
Eliminar la fuente	4
Retener	3
Aceptar o aumentar	0
Evitar	0

Estos resultados reflejan que la organización ha priorizado medidas proactivas orientadas a reducir la probabilidad de ocurrencia de los eventos de riesgo (64% de los casos tratados), lo cual es coherente con una estrategia de mitigación anticipada para garantizar la continuidad del negocio.

Descripción de las opciones aplicadas

1. Modificar la probabilidad: Consiste en implementar acciones que reduzcan la posibilidad de que ocurra el evento de riesgo. En Teuno, este tratamiento incluyó actividades como:

- Autenticación multifactor (MFA)
- Fortalecimiento de endpoints
- Revisión técnica periódica y validaciones cruzadas
- Automatización de procesos críticos

- Optimización de cargas laborales
- Planes de reemplazo documentado

2. Modificar el impacto: Este tratamiento se enfocó en reducir las consecuencias si el riesgo se materializa. Las acciones implementadas incluyeron:

- Procedimientos contables de contingencia
- Acceso remoto a sistemas críticos
- Continuidad operativa en facturación y pagos
- Simulacros y procedimientos de respuesta

3. Compartir: Transferencia del riesgo a un tercero a través de contratos, seguros u otros mecanismos. En este caso, se aplicaron soluciones como:

- Contratos de respaldo activo/pasivo con proveedores
- Activación de servicios SaaS redundantes
- Establecimiento de SLAs con penalizaciones

4. Eliminar la fuente: En algunos casos críticos, Teuno opta por erradicar completamente la causa del riesgo, implementando:

- Rediseño de procesos
- Migración tecnológica
- Automatización completa de funciones sensibles

5. Retener: Se aplicó cuando el riesgo fue evaluado como aceptable o cuando el tratamiento resultaba más costoso que el propio impacto del riesgo. Las medidas adoptadas fueron:

- Documentación explícita de aceptación del riesgo
- Seguimiento continuo del SLA
- Inclusión en planes futuros de contingencia

Criterios utilizados para la selección

La elección del tipo de tratamiento para cada riesgo se basó en los siguientes factores:

- Nivel del riesgo residual vs apetito de riesgo
- Capacidad organizacional para implementar el tratamiento
- Relación costo-beneficio del tratamiento
- Disponibilidad de recursos y tiempos de implementación
- Impacto potencial sobre los objetivos del negocio

La estrategia de tratamiento de riesgos adoptada por TEUNO refleja una orientación preventiva, alineada con los objetivos del SGCN. La amplia aplicación de medidas para modificar la probabilidad demuestra un enfoque proactivo, complementado con alternativas como compartir y eliminar la fuente en escenarios más complejos. Esto ha permitido reducir de forma significativa el nivel de riesgo residual, como evidencia el análisis comparativo entre el riesgo inherente y residual previamente presentado.

5.6.5.3.Preparación e implantación de los planes de tratamiento del riesgo

La preparación e implantación de los planes de tratamiento de riesgo responde al paso final del proceso de tratamiento. En esta etapa se consolidan todas las acciones propuestas y se organizan en

iniciativas que permiten su ejecución efectiva, bajo seguimiento formal y en coherencia con el apetito de riesgo de la organización.

Las iniciativas se agrupan por tipo de tratamiento, asignando un identificador, un título descriptivo, una descripción clara de su propósito, responsable designado, tipo de acción, coste estimado, prioridad y los escenarios de indisponibilidad a los que contribuyen.

Tabla 56

Iniciativas por tipo de tratamiento

Tipo de tratamiento: Modificar la probabilidad							
Identificador	**Título**	**Descripción**	**Responsable**	**Tipo**	**Coste estimado**	**Prioridad**	**Escenarios de Indisponibilidad**
IN_PRCPROB_001	Fortalecimiento de configuración y segmentación de red	Revisar, documentar y aplicar configuraciones de red segura para servicios de facturación, pagos, segmentando	Coordinación de Infraestructura	Tecnológica	0	ALTA	Sin Sistemas Críticos, Sin Proveedores Críticos

		críticamente servicios internos.					
IN_PRCPROB_002	Reasignación de turnos con automatización de derivaciones	Ajustar turnos críticos con sobrecarga de personal e incluir automatización para derivación de incidentes a canales alternativos cuando no haya disponibilidad	Gestor SOC	Organizativa	0	ALTA	Sin Personal Crítico
IN_PRCPROB_003	Automatización y respaldo en sistemas de monitoreo	Implementar SIEM espejo y monitoreo alternativo con failover automático en caso de caída del principal	Jefe de Ciberseguridad	Tecnológica	0	ALTA	Sin Sistemas Críticos

IN_PRCPROB_004	Plan de reemplazo documentado	Definir manuales de reemplazo para roles clave en facturación, contabilidad y gestión de eventos, con revisión anual obligatoria	Dirección de Áreas Funcionales	Organizativa	0	MEDIA	Sin Personal Crítico
IN_PRCPROB_005	Fortalecimiento del endpoint contable y de facturación	Instalar antivirus con control de funciones y activar monitoreo de endpoints por riesgo de malware en estaciones críticas	Departamento de Seguridad TI	Tecnológica	0	ALTA	Sin Sistemas Críticos

Tipo de tratamiento: Compartir

Identificador	Título	Descripción	Responsable	Tipo	Coste estimado	Prioridad	Escenarios de

							Indisponibilidad
IN_PRCCOM_001	Contratación de proveedor alterno de SIEM	Establecer contrato con proveedor alternativo con capacidad de SIEM modo activo-pasivo	Subgerencia de Seguridad	Contractual	0	ALTA	Sin Sistemas Críticos, Sin Proveedores Críticos
IN_PRCCOM_002	Redundancia geográfica de ITSM	Contratar proveedor SaaS ITSM geolocalizado y configurar failover multi-región	Jefatura de Servicios TI	Contractual	0	MEDIA	Sin Proveedores Críticos

Tipo de tratamiento: Eliminar la fuente							
Identificador	**Título**	**Descripción**	**Responsable**	**Tipo**	**Coste estimado**	**Prioridad**	**Escenarios de Indisponibilidad**

IN_PRCELIM_001	Eliminación de dependencia del proveedor SIEM	Migrar a infraestructura local con alta disponibilidad y personal propio entrenado	Dirección de Tecnología	Infraestructura	0	MEDIA	Sin Proveedores Críticos

Tipo de tratamiento: Modificar el impacto							
Identificador	**Título**	**Descripción**	**Responsable**	**Tipo**	**Coste estimado**	**Prioridad**	**Escenarios de Indisponibilidad**
IN_PRCIMP_001	Matriz de reemplazos contables y tributarios	Definir matriz de reemplazos con roles clave en la emisión contable y fiscal, con simulacros de ejecución de continuidad trimestral	Gerencia Financiera	Organizativa	0	ALTA	Sin Personal Crítico

IN_PRCIMP_002	Plataforma redundante para pagos críticos	Activar ambiente espejo para pagos con transferencias bancarias y monitoreo remoto	Departamento de Finanzas	Tecnológica	0	ALTA	Sin Sistemas Críticos

Tipo de tratamiento: Retener

Identificador	Título	Descripción	Responsable	Tipo	Coste estimado	Prioridad	Escenarios de Indisponibilidad
IN_PRCRET_001	Formalización de aceptación de riesgo	Documento firmado por la gerencia en el que se acepta el riesgo residual y se monitorea mediante SLA y mecanismos correctivos	Gerencia General	Documental	0	BAJA	Varios según riesgo aceptado

Roadmap de Ejecución – Planes de Tratamiento del Riesgo (2026)

Como parte del compromiso estratégico de Teuno con la resiliencia operativa y la mejora continua, se ha definido la ejecución durante el año 2026 de un conjunto de iniciativas clasificadas como planes de tratamiento del riesgo. Estas acciones forman parte del proyecto integral de fortalecimiento del Sistema de Gestión de Continuidad del Negocio alineado al estándar de la norma ISO 31000:2018.

El objetivo es fortalecer las capacidades de prevención, respuesta y recuperación ante escenarios de interrupción en Teuno, mediante la ejecución planificada de medidas de tratamiento del riesgo que aseguren la continuidad de procesos y servicios críticos.

Enero 2026

- **IN_PRC_001** – Fortalecimiento de configuración y segmentación de red
  (Tecnológica – ALTA – Sin Sistemas Críticos, Sin Proveedores Críticos)
- **IN_PRC_006** – Contratación de proveedor alterno de SIEM
  (Contractual – ALTA – Sin Sistemas Críticos, Sin Proveedores Críticos)

Febrero 2026

- **IN_PRC_002** – Reasignación de turnos con automatización
  (Organizativa – ALTA – Sin Personal Crítico)
- **IN_PRC_005** – Fortalecimiento del endpoint contable y de facturación
  (Tecnológica – ALTA – Sin Sistemas Críticos)

- **IN_PRC_010** – Plataforma redundante para pagos críticos

  (Tecnológica – ALTA – Sin Sistemas Críticos)

Marzo 2026

- **IN_PRC_003** – Automatización y respaldo en monitoreo

  (Tecnológica – ALTA – Sin Sistemas Críticos)

- **IN_PRC_009** – Matriz de reemplazos contables y tributarios

  (Organizativa – ALTA – Sin Personal Crítico)

Abril 2026

- **IN_PRC_004** – Plan de reemplazo documentado

  (Organizativa – MEDIA – Sin Personal Crítico)

- **IN_PRC_011** – Formalización de aceptación de riesgo

  (Documental – BAJA – Varios según riesgo aceptado)

Mayo 2026

- **IN_PRC_007** – Redundancia geográfica de ITSM

  (Contractual – MEDIA – Sin Proveedores Críticos)

Junio 2026

- **IN_PRC_008** – Eliminación de dependencia del proveedor SIEM

  (Infraestructura – MEDIA – Sin Proveedores Críticos)

Figura 41

Plan de tratamiento de riesgos y plazos de ejecución

Identificador	Tipo de Tratamiento	Título	Descripción	Responsable	Tipo	Coste estimado	Prioridad	Escenarios de Indisponibilidad	Plazo de ejecución
IN_PRC_001	Modificar la probabilidad	Fortalecimiento de configuración y segmentación de red	Configuración de red segura para servicios críticos	Coordinación de Infraestructura	Tecnológica	0	ALTA	Sin Sistemas Críticos, Sin Proveedores Críticos	2026-01-01
IN_PRC_002	Modificar la probabilidad	Reasignación de turnos con automatización de	Automatizar derivación de incidentes ante ausencia de personal	Gestor SOC	Organizativa	0	ALTA	Sin Personal Crítico	2026-02-01
IN_PRC_003	Modificar la probabilidad	Automatización y respaldo en sistemas de monitoreo	Implementar SIEM espejo y failover automático	Jefe de Ciberseguridad	Tecnológica	0	ALTA	Sin Sistemas Críticos	2026-03-01
IN_PRC_004	Modificar la probabilidad	Plan de reemplazo documentado	Manuales de reemplazo con revisión anual	Dirección de Áreas Funcionales	Organizativa	0	MEDIA	Sin Personal Crítico	2026-04-01
IN_PRC_005	Modificar la probabilidad	Fortalecimiento del endpoint contable y de facturación	Antivirus y monitoreo en endpoints críticos	Departamento de Seguridad TI	Tecnológica	0	ALTA	Sin Sistemas Críticos	2026-02-01
IN_PRC_006	Compartir	Contratación de proveedor alterno de SIEM	Contrato con proveedor en modo activo-pasivo	Subgerencia de Seguridad	Contractual	0	ALTA	Sin Sistemas Críticos, Sin Proveedores Críticos	2026-01-01
IN_PRC_007	Compartir	Redundancia geográfica de ITSM	SaaS ITSM con failover multirregión	Jefatura de Servicios TI	Contractual	0	MEDIA	Sin Proveedores Críticos	2026-05-01
IN_PRC_008	Eliminar la fuente	Eliminación de dependencia del proveedor SIEM	Migración a infraestructura local con personal entrenado	Dirección de Tecnología	Infraestructura	0	MEDIA	Sin Proveedores Críticos	2026-06-01
IN_PRC_009	Modificar el impacto	Matriz de reemplazos contables y tributarios	Roles clave definidos y simulacros trimestrales	Gerencia Financiera	Organizativa	0	ALTA	Sin Personal Crítico	2026-03-01
IN_PRC_010	Modificar el impacto	Plataforma redundante para pagos críticos	Ambiente espejo para transferencias bancarias	Departamento de Finanzas	Tecnológica	0	ALTA	Sin Sistemas Críticos	2026-02-01
IN_PRC_011	Retener	Formalización de aceptación de riesgo	Documento de aceptación firmado por la gerencia	Gerencia General	Documental	0	BAJA	Varios según riesgo aceptado	2026-04-01

5.6.6. Seguimiento y revisión. El seguimiento y revisión del riesgo constituye una etapa fundamental para garantizar que el proceso de gestión de riesgos permanezca efectivo, actualizado y alineado con los objetivos estratégicos de la organización, esta actividad es continua y debe estar formalmente integrada dentro de la gobernanza del sistema.

Propósito del seguimiento:

- Verificar que los riesgos identificados siguen siendo relevantes bajo nuevas condiciones.

- Confirmar que los tratamientos implementados están funcionando como se esperaba.
- Detectar señales de alerta temprana de nuevos riesgos o fallos de los controles establecidos.
- Evaluar el cumplimiento de los planes de tratamiento y sus cronogramas.

Figura 42

Métodos de revisión establecidos

Método de Seguimiento	Descripción	Periodicidad	Responsable
Revisión de matriz de riesgos	Verificación de los niveles de riesgo residual y análisis de su evolución.	Trimestral	Gestor de Riesgos
Auditorías internas del SGCN	Evaluación sistemática de controles y cumplimiento de planes de tratamiento.	Semestral	Auditor de Continuidad
Evaluaciones post-evento	Revisión de la respuesta ante incidentes reales o simulados.	A demanda	Comité de Continuidad
Actualización de controles	Validación de la vigencia, documentación y efectividad de controles implementados.	Trimestral	Responsable de los Procesos Teuno
Revisión de apetito de riesgo	Comparación del riesgo residual frente al apetito institucional.	Anual	Área de Riesgos

Indicadores de desempeño (KRI/KPI)

Para asegurar trazabilidad y eficacia en la gestión, se utilizan los siguientes indicadores:

- % de riesgos con tratamiento en ejecución o cerrado.
- % de iniciativas priorizadas con seguimiento actualizado.

- Tiempo promedio de revisión de riesgos críticos.
- Porcentaje de desviación entre riesgo residual estimado y real.

Criterios de actualización

Un riesgo o tratamiento será revisado o actualizado en caso de:

- Cambios en el contexto externo (regulatorio, tecnológico, económico).
- Cambios internos relevantes (procesos, infraestructura, personal).
- Resultados de auditorías o evaluaciones externas.
- Incidentes, fallos de control, desviaciones en impacto o probabilidad.

Herramientas de apoyo

- Registro centralizado en hoja de control de riesgos.
- Dashboard de monitoreo en sistema de continuidad.
- Matriz de trazabilidad de planes de tratamiento y responsables.
- Registro de eventos críticos y lecciones aprendidas.

Dentro del proceso de gestión de riesgos de continuidad del negocio implementado en Teuno, el seguimiento y revisión se encuentran formalmente integrados dentro de la Matriz de Evaluación de Riesgos, la cual no solo recoge las acciones planificadas, sino también la trazabilidad de su implementación y eficacia.

Figura 43

Campos clave para el control de los tratamientos

Columna en la Matriz	Propósito
Fecha de inicio	Registrar el momento en que se comienza la ejecución del tratamiento.
Fecha de seguimiento	Permite evidenciar la frecuencia con la que se evalúa el avance y efectividad del tratamiento.
Cumple / No Cumple	Indica si el tratamiento ha sido ejecutado en tiempo, forma y con los resultados esperados.
Observación del evaluador	Campo destinado a incluir hallazgos, desviaciones, lecciones aprendidas o recomendaciones tras el seguimiento.

Esta estructura garantiza un ciclo de vida completo del tratamiento del riesgo, conforme a los principios de la norma ISO 31000 y específicamente a lo exigido en el punto 5.6.6. Seguimiento y revisión, permitiendo que el sistema de gestión de continuidad del negocio permanezca dinámico, controlado y alineado con el apetito de riesgo institucional.

5.6.7. Registro e informe. El registro y la generación de informes permiten validar las decisiones adoptadas, evidenciar el cumplimiento del marco de referencia y facilitar la mejora continua.

- **Registro estructurado de riesgos:** Todos los riesgos identificados, analizados y evaluados son almacenados en una base de datos maestra, bajo codificación única (ej. R-01 a R-170), junto con la evidencia documental correspondiente.

- **Trazabilidad del tratamiento:** Se documentan los tratamientos seleccionados, responsables, fechas, costos, controles asociados y nivel residual, permitiendo una revisión completa de la evolución del riesgo.
- **Informes periódicos de gestión de riesgos:** Emitidos por el Gestor de Riesgos al Comité de Continuidad y la Alta Dirección.

5.6.7.1.Medios de comunicación. La comunicación eficaz es un componente esencial de la Gestión de Riesgos. Garantiza que la información crítica llegue a las personas adecuadas para tomar decisiones informadas y oportunas.

Figura 44

Mecanismos de comunicación utilizados en Teuno

Medio de Comunicación	Audiencia	Frecuencia	Contenido
Informes ejecutivos de riesgos	Alta Dirección	Trimestral	Riesgos prioritarios, evolución de riesgo residual, brechas de tratamiento
Dashboard en Power BI	Gestores y responsables de proceso	Permanente	Riesgos por proceso, tratamiento, cumplimiento y apetito
Reuniones de comité de continuidad	Comité de Continuidad del Negocio	Mensual	Seguimiento de riesgos críticos, nuevos riesgos y avance de controles
Correo electrónico con alertas	Equipos de operación y TI	A demanda	Riesgos emergentes, cambios en el perfil de riesgo o eventos activados
Reportes de auditoría	Auditoría interna y externa	Anual	Conformidad de la gestión de riesgos con la norma ISO 22301 e ISO 31000

5.6.7.2. Cronograma de actividades para la implementación de procesos. Se establece un cronograma estratégico que articula las acciones necesarias para la implantación total del modelo de gestión de riesgos en los procesos críticos del SGCN.

Figura 45

Fases del cronograma de acuerdo a las responsabilidades asignadas

Cada fase considera actividades específicas asociadas a los tipos de tratamiento de riesgo (modificar, compartir, eliminar, etc.) y a los escenarios de indisponibilidad relevantes (sin personal, sin sistemas, etc.), priorizando aquellos riesgos fuera del apetito definido.

Figura 46

Detalle de las actividades por fase

Fase	Actividades	Responsable	Plazo estimado
1. Sensibilización	Capacitación en ISO 31000 e ISO 22301	Talento Humano y Seguridad	1 semana
2. Formalización	Aprobación de matriz de riesgos y apetito	Dirección General	2 semanas
3. Implementación	Ejecución de controles y planes de tratamiento	Dueños de proceso	4 semanas
4. Seguimiento	Revisión de cumplimiento y resultados	Gestor de Riesgos	Mensual
5. Mejora Continua	Ajustes de controles, revisión residual	Comité de Continuidad	Trimestral

5.6.8. Auditoría Interna. La auditoría interna es un componente esencial dentro del Sistema de Gestión de Continuidad del Negocio (SGCN) de TEUNO, pues permite verificar de manera sistemática y objetiva la efectividad y conformidad de los controles, planes y procedimientos implementados para el tratamiento de riesgos. Además, garantiza que las opciones seleccionadas para mitigar los riesgos identificados sean prácticas, efectivas y alineadas con el apetito de riesgo institucional.

5.6.8.1. Objetivos. El principal objetivo de la auditoría interna es asegurar que las opciones y planes implementados para el tratamiento de riesgos sean eficaces y aplicables en el contexto operativo de TEUNO. Esto implica evaluar si los controles y acciones correctivas están funcionando según lo previsto, detectar posibles desviaciones o deficiencias, y verificar que los riesgos residuales se mantengan dentro del nivel aceptable definido. De esta manera, la auditoría contribuye a mantener la integridad, robustez y mejora continua del SGCN.

5.6.8.2. Procesos de la Auditoría Interna. La auditoría interna se desarrolla en cuatro fases principales, que estructuran el ciclo completo de revisión y seguimiento:

- **Planificación:** En esta etapa se determina el alcance específico de la auditoría, los criterios contra los cuales se evaluará el sistema (normativas internas, ISO 31000:2018, planes de continuidad, etc.) y se establece un cronograma detallado que asegura la cobertura

oportuna y eficiente de los procesos críticos. La planificación también define los recursos humanos y técnicos involucrados.

- **Ejecución:** Comprende la revisión exhaustiva de documentos, registros y evidencias del SGCN, así como entrevistas con responsables y personal clave. Se realizan evaluaciones en terreno para constatar la correcta aplicación de los controles, planes de contingencia y mecanismos de mitigación, asegurando que estos se ejecuten conforme a lo documentado.
- **Informe:** Los hallazgos recopilados durante la auditoría se documentan de manera clara y estructurada. Se registran observaciones, fortalezas, debilidades y especialmente las no conformidades encontradas. Este informe es un insumo fundamental para la toma de decisiones en la gestión del riesgo y para la mejora continua del sistema.
- **Seguimiento:** Posterior a la auditoría, se realiza una verificación rigurosa para asegurar que las acciones correctivas derivadas de las no conformidades hayan sido implementadas efectivamente. Esta etapa es clave para cerrar el ciclo de auditoría y mantener el sistema alineado con los objetivos de continuidad.

5.6.8.3.No conformidades y acciones correctivas. Cuando durante la auditoría se detecta una no conformidad, se inicia un proceso sistemático para corregirla y evitar su repetición, compuesto por los siguientes pasos:

1. **Identificación de la causa raíz:** Se realiza un análisis profundo para determinar el origen real de la no conformidad, más allá de sus síntomas inmediatos. Esta etapa es fundamental para asegurar que las acciones posteriores sean efectivas y no meramente paliativas.
2. **Implementación de acciones correctivas:** Se diseñan y aplican medidas específicas que eliminan la causa raíz, garantizando que la no conformidad no vuelva a ocurrir. Estas acciones pueden incluir revisiones de procedimientos, capacitación adicional, ajustes en controles tecnológicos o cambios en contratos con terceros.
3. **Verificación de la eficacia:** Finalmente, se evalúa si las acciones correctivas implementadas han logrado solucionar la no conformidad y prevenir su recurrencia. Este seguimiento puede implicar auditorías de seguimiento, revisiones periódicas o monitoreo continuo, asegurando la mejora sostenida del SGCN.

La auditoría interna en TEUNO, desarrollada bajo estos lineamientos, constituye una herramienta fundamental para mantener la capacidad de respuesta ante riesgos, garantizar la resiliencia operativa y fortalecer la cultura de mejora continua alineada con la norma ISO 31000:2018 y las mejores prácticas internacionales en gestión de continuidad del negocio.

CAPITULO 6

6. CONCLUSIONES Y APLICACIONES

6.1. Conclusiones generales

El estudio permite diseñar una propuesta técnica de elaboración de un Sistema de Gestión de Continuidad del Negocio (SGCN) para GRUPO BRAVCO S.A., basado en la norma ISO 31000:2018. Se aborda de forma estructurada la necesidad de fortalecer la capacidad organizacional ante eventos disruptivos, formulando una herramienta que articula principios de gestión del riesgo con criterios de continuidad operativa. La propuesta ofrece un marco de referencia útil y adaptable al contexto institucional, alineado a estándares internacionales, que permite a la empresa contar con una guía clara para el diseño futuro de su sistema de continuidad.

La elaboración de esta propuesta permite identificar la importancia de institucionalizar una cultura de continuidad dentro de GRUPO BRAVCO S.A., orientada a la anticipación, gestión y tratamiento de riesgos con enfoque estratégico. El modelo planteado no solo facilita una respuesta estructurada ante escenarios de crisis, sino que también se proyecta como una herramienta para fortalecer la toma de decisiones a nivel directivo, optimizar procesos y garantizar la sostenibilidad operativa en entornos dinámicos. Su carácter adaptable permite que la empresa continúe evolucionando hacia una gestión resiliente y proactiva, alineada con los desafíos actuales y futuros del sector tecnológico.

6.2. Conclusiones específicas

A continuación, se presentan las conclusiones específicas derivadas del desarrollo del proyecto, las cuales abordan el cumplimiento de los objetivos planteados, así como el aporte de la propuesta en distintos niveles: empresarial, académico y personal.

6.2.1. Análisis del cumplimiento de los objetivos de la investigación.

Mediante el presente documento se presenta una guía estructurada mediante la cual se identifican riesgos y amenazas inherentes al giro de negocio. De igual forma se caracterizan los procesos críticos de GRUPO BRAVCO S.A., a través del análisis de Impacto al Negocio (BIA) siendo un total de 14 procesos producto de amenazas internas y externas. Esta identificación permite sentar las bases para una gestión efectiva de la continuidad del negocio.

La evaluación de los riesgos vinculados a los procesos críticos se realiza aplicando metodologías cualitativas y cuantitativas basadas en la norma ISO 31000:2018, incluyendo el análisis de impacto, probabilidad y eficacia de controles. Los resultados permiten establecer niveles de riesgo inherente y residual, así como visualizar escenarios con mayor afectación, lo cual genera iniciativas de mejora.

Las estrategias de gestión de riesgos formuladas en este proyecto están orientadas a la continuidad operativa de TEUNO, articulando medidas concretas para las fases de prevención, mitigación, respuesta y recuperación.

Se establece un sistema documentado y estructurado de gestión del riesgo que permite a TEUNO adoptar un enfoque sistemático para asegurar la continuidad de sus procesos críticos. Las iniciativas propuestas se integran de manera estratégica para reducir la probabilidad de interrupciones, mitigar impactos, responder de forma efectiva y recuperar operaciones con agilidad.

Se cumplen los objetivos y con ello se garantiza un documento que brinda información organizada desde la información general y relevante, así como el análisis, evaluación y tratamiento del riesgo enfocado en la Gestión de Continuidad del Negocio.

6.2.2. Contribución a la gestión empresarial.

La implementación del manual de continuidad del negocio permite a GRUPO BRAVCO S.A. contar con un plan estructurado y adaptado a sus procesos más críticos, como la distribución y comercialización de productos en centros logísticos. Este manual no solo establece procedimientos claros para actuar frente a interrupciones, sino que también mejora la capacidad de respuesta ante eventos como fallas operativas, desastres naturales o ciberataques. Para la empresa, esto significa reducir el tiempo de inactividad, proteger su reputación ante los clientes y cumplir con exigencias regulatorias del sector logístico y comercial. Además, al tener roles, responsabilidades y protocolos definidos, se facilita la toma de decisiones oportuna y se fortalecen los procesos de evaluación y mejora continua dentro de su gestión estratégica.

6.2.3. Contribución a nivel académico.

Desde el punto de vista académico, la realización del proyecto representa una experiencia formativa significativa para el grupo de trabajo. Se aplican conocimientos adquiridos durante la

carrera en un contexto real, integrando teoría y práctica en áreas como la gestión de riesgos, normativas internacionales, continuidad del negocio. A lo largo del desarrollo del manual, se fortalecieron habilidades como la investigación aplicada, el trabajo colaborativo, el análisis crítico y la resolución de problemas.

6.2.4. Contribución a nivel personal

El desarrollo del proyecto exige un alto nivel de compromiso individual y colectivo. Aplicamos los conocimientos adquiridos a lo largo de la maestría dentro de un plazo establecido, lo que pone a prueba nuestra capacidad de organización, análisis y toma de decisiones. Esta experiencia fortalece nuestras competencias cognitivas, consolida el trabajo en equipo y contribuye a nuestro crecimiento profesional. Además, reafirma nuestro compromiso con el servicio a la sociedad, guiado por principios éticos en el ejercicio responsable de la gestión de riesgos.

6.3.*Limitaciones a la Investigación*

Durante el desarrollo del proyecto, nos enfrentamos a diversas limitaciones que influyen en el alcance del trabajo. Una de las principales es el acceso restringido a cierta información interna de la empresa, debido a políticas de confidencialidad. Esto condiciona el nivel de detalle en el análisis de algunos procesos críticos. Asimismo, el tiempo disponible para la ejecución del proyecto fue limitado, lo que condiciona la profundidad del levantamiento de información y la aplicación real del Sistema de Gestión de Continuidad. Pese a estas limitaciones, se logró cumplir con los objetivos establecidos, adaptando la metodología y ajustando el enfoque del trabajo a las condiciones reales del entorno.

BIBLIOGRAFÍA

Constitución de la República del Ecuador. (2008). *Registro Oficial Suplemento 449 de 20 de octubre de 2008*.

Instituto Nacional de Ciberseguridad (INCIBE). *INCIBE*. https://www.incibe.es/

International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements*.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*.

International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls*.

International Organization for Standardization. (2018). *ISO 31000:2018 Risk management – Guidelines*.

Ley Orgánica de Protección de Datos Personales. (2021). *Registro Oficial Suplemento 459 de 26 de mayo de 2021*.

Ley Orgánica de la Seguridad de la Información Pública (LOSEP). (2004). *Registro Oficial Suplemento 337 de 31 de marzo de 2004*.

Teuno. *Tecnología para un nuevo orden*. https://www.teuno.com/

ANEXOS

ANEXO: 1 PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO

Tabla de Contenido

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Cargo: Analista de Procesos	**Cargo:** Subgerente de Gobierno	**Cargo:** Gerente General

1. Objetivo

Establecer las directrices para la elaboración, documentación, implementación y control de los procedimientos de TEUNO, garantizando la estandarización y alineación con el sistema de gestión organizacional y normativas aplicables.

2. Alcance

Inicia con la solicitud de elaboración o actualización de un procedimiento por parte de un área responsable y finaliza con la publicación, difusión y control de cambios del documento en el gestor documental institucional.

Responsabilidad de Aplicación:

Este procedimiento debe ser aplicado por los dueños de procesos, jefes de área y gerencias de Teuno, quienes son responsables de documentar, mantener actualizados y validar los procedimientos correspondientes a sus funciones.

3. Definiciones

Procedimiento: Documento que describe el conjunto ordenado de actividades necesarias para ejecutar un proceso específico, incluyendo sus responsables, entradas, salidas y puntos de control.

Proceso: Conjunto de actividades mutuamente relacionadas que transforman elementos de entrada en resultados, contribuyendo al cumplimiento de los objetivos institucionales.

Procedimiento de Procedimientos: Documento institucional que establece los lineamientos generales para la elaboración, control y mejora continua de los procedimientos de Teuno.

Jefe de Área: Responsable de validar, revisar y promover el uso de los procedimientos dentro de su unidad, coordinando con el dueño del proceso y asegurando su aplicación efectiva.

Dueño del Proceso: Persona responsable de liderar la elaboración, revisión y mejora del procedimiento, así como de asegurar que las actividades estén alineadas con los objetivos de la organización.

Diagrama de flujo: Representación gráfica del procedimiento, que muestra la secuencia de actividades, decisiones y responsables mediante símbolos estandarizados.

Control de Cambios: Registro documentado de las modificaciones realizadas a un procedimiento a lo largo de su ciclo de vida, indicando fecha, versión, responsable y descripción del cambio.

Gestor Documental (DOCS): Plataforma oficial de Teuno para el almacenamiento, control de versiones y publicación de procedimientos institucionales.

4. Políticas Específicas

1. Todos los procedimientos deben ser elaborados y documentados utilizando el formato institucional. Este formato incluye: portada con logo y metadatos (versión, código, página), tabla de contenido, estructura estandarizada de secciones (objetivo, alcance, definiciones, etc.), control de cambios y firmas de aprobación.

2. La revisión y actualización de los procedimientos debe realizarse al menos una vez al año, o de forma inmediata cuando se produzcan cambios significativos en procesos, estructuras organizativas, normativa aplicable o plataformas tecnológicas asociadas.

3. Cada procedimiento debe ser elaborado por el dueño del proceso y revisado y autorizado por su jefatura directa antes de ser registrado formalmente en el gestor documental institucional (DOCS).

4. Es responsabilidad del dueño del proceso cargar el procedimiento actualizado en la plataforma DOCS, asegurando que se incluya toda la información requerida y esté debidamente firmado. En caso de no contar con acceso al sistema, deberá solicitar permisos al Área de Procesos mediante correo.

5. Ningún procedimiento podrá ser oficial si no ha pasado por la revisión formal, ha sido firmado manual o electrónicamente, registrado en el repositorio DOCs y socializado a toda la compañía.

6. Las versiones anteriores de los procedimientos deben mantenerse archivadas digitalmente por parte del dueño del proceso, al menos por un período de dos años, para fines de trazabilidad o auditoría.

7. El control de cambios debe completarse con el número de RFC (Requerimiento de Cambio) correspondiente, incluyendo una descripción clara del ajuste realizado, su fecha, y la nueva versión asignada.

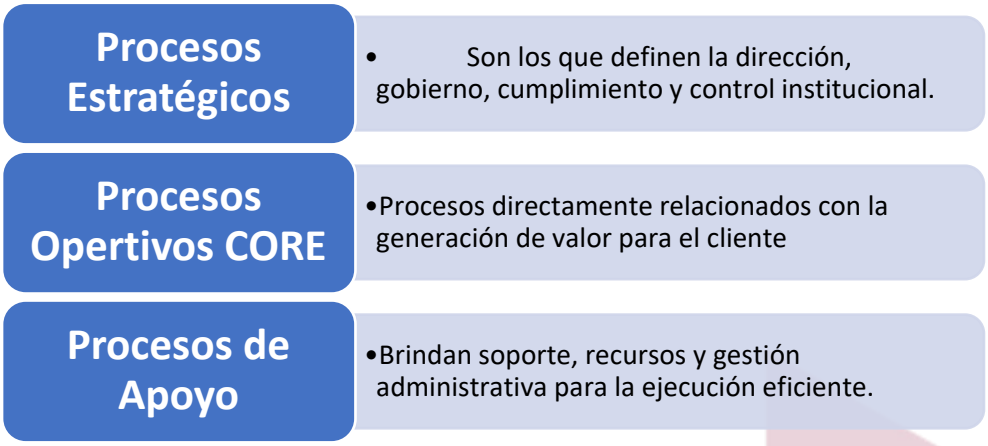
8. Toda persona involucrada en la ejecución del procedimiento debe ser debidamente notificada por el responsable del proceso, y de ser necesario, debe recibir inducción sobre el nuevo contenido aprobado.

9. Los diagramas de flujo deben elaborarse en Bizagi y reflejar fielmente el paso a paso descrito en la sección “Descripción de Actividades”, incluyendo decisiones, responsables y registros asociados.

5. Descripción

En Teuno, los procedimientos deben estar organizados y clasificados en función del tipo de proceso al que pertenecen, conforme al Mapa de Procesos institucional (MP-PRO-01). Esto permite estandarizar, codificar y ubicar de forma ágil cada procedimiento en el sistema de gestión documental.

Tipos de procesos según el Mapa de Procesos:



Codificación de Procedimientos

Cada procedimiento debe tener una codificación estructurada como sigue:

PR-XXX-YY

PR: Indica que se trata de un procedimiento.

XXX: Siglas del proceso o área funcional.

YY: Número secuencial según orden de registro.

Ejemplos de codificación:

Proceso	*Tipo*	*Código ejemplo*	*Descripción*
Contabilidad	Apoyo	PR-CBL-10	Revisión de descuentos e ingresos a organismos externos.
Facturación y Cobranzas	Operativo Core	PR-FYC-03	Procedimiento de facturación electrónica.

Proceso	*Tipo*	*Código ejemplo*	*Descripción*
Gobierno de Seguridad	Estratégico	PR-GSI-01	Evaluación y tratamiento de riesgos de seguridad de la info.
Gestión de Proveedores	Apoyo	PR-PRO-02	Alta, evaluación y seguimiento de proveedores.
Comercial	Operativo Core	PR-COM-05	Gestión de propuestas comerciales.

Estructura del Procedimiento

Todos los procedimientos institucionales de TEUNO deben elaborarse utilizando el formato estándar, el cual garantiza uniformidad, trazabilidad y cumplimiento documental. La estructura es de carácter obligatorio y debe mantenerse en el orden y contenido establecido.

Sección	*Contenido que debe incluir*
Portada institucional	Logotipo de Teuno, nombre del procedimiento, fecha de aprobación, versión, código y paginación.
Tabla de contenido	Índice automático con las secciones del procedimiento y su ubicación por página.
1. Objetivo	Verbo en infinitivo que describa el propósito general del procedimiento.
2. Alcance	Indicación clara del inicio y fin del procedimiento, incluyendo la responsabilidad de aplicación.
3. Definiciones	Términos técnicos o internos necesarios para comprender el procedimiento.
4. Políticas específicas	Reglas obligatorias que deben cumplirse, redactadas con verbo “debe”.

Sección	*Contenido que debe incluir*
5. Descripción	Explicación del procedimiento según su tipo, clasificación y codificación.
6. Responsabilidad y Autoridad	Detalle de cada cargo involucrado y sus funciones dentro del proceso.
7. Diagrama de flujo	Representación gráfica en Bizagi con cargos a la izquierda y flujo de actividades horizontal.
8. Descripción de actividades	Tabla paso a paso que detalla las actividades, responsables y registros/documentos asociados.
9. Puntos de control	Verificaciones clave del procedimiento, con responsable, frecuencia y evidencia requerida.
10. Referencia a otros documentos	Normas ISO y documentos internos del sistema de gestión relacionados con el procedimiento.
11. Anexos	Formularios, formatos o documentos de apoyo utilizados en la ejecución del procedimiento.
12. Control de Cambios	Tabla de versión, fecha y descripción del cambio. Incluir firmas con nombre y cargo.

Redacción de los procedimientos

Para asegurar que los procedimientos institucionales de Teuno sean comprendidos y aplicables por todo el personal, su redacción debe cumplir con las siguientes pautas:

Los procedimientos se redactarán de forma clara, precisa y concisa, evitando tecnicismos innecesarios, y deben ser comprensibles para el personal operativo, técnico y administrativo.

Se debe evitar cualquier ambigüedad o elemento que dé lugar a diferentes interpretaciones del contenido.

Cuando alguno de los apartados establecidos en el formato no aplique a un proceso específico, se deberá indicar explícitamente como “No procede” o “No aplica”.

Todos los procedimientos son de lectura obligatoria para el personal involucrado en su ejecución y deben estar disponibles en todo momento en el sistema documental DOCS, garantizando acceso oportuno.

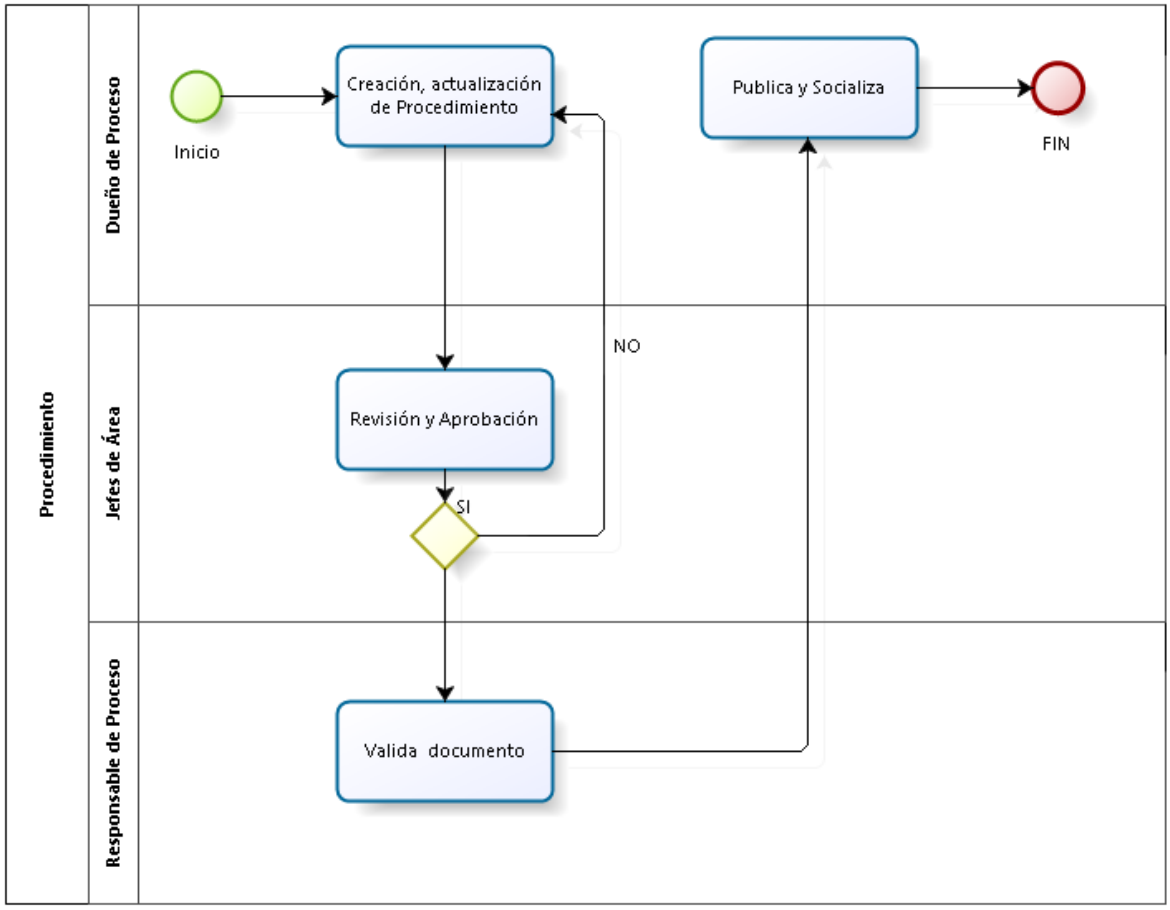
6. Responsabilidad y Autoridad

A continuación, se detallan los cargos involucrados en el proceso de elaboración, revisión, aprobación, publicación y mantenimiento de los procedimientos institucionales, así como sus funciones específicas:

Cargo	Responsabilidad / Autoridad
Dueño del Proceso	Lidera la elaboración y actualización del procedimiento correspondiente a su proceso. Asegura que el contenido refleje fielmente las actividades operativas y normativas.
Jefe de Área	Revisa y valida técnicamente el procedimiento elaborado por el dueño del proceso. Asegurar su alineación con los objetivos del área y las políticas institucionales.
Gerente del Área	Autorizar formalmente el procedimiento y remitirlo para su publicación en DOCS. Aprueba la vigencia y asume responsabilidad sobre su implementación.
Área de Procesos	Brindar lineamientos metodológicos, formatos oficiales, y control sobre la codificación. Gestiona el acceso a la plataforma DOCS y vela por la estandarización documental.
Área de Gobierno y Riesgos	Validar los procedimientos que aborden temas relacionados con seguridad de la información, continuidad del negocio, gestión de riesgos o cumplimiento regulatorio.
Usuarios involucrados	Conocer, aplicar y dar retroalimentación sobre el procedimiento. Su participación puede ser requerida en revisiones o ajustes. 8 de 11

7. Diagrama de Flujo

El diagrama de flujo es un componente obligatorio de todos los procedimientos de Teuno. Su objetivo es representar visualmente la secuencia lógica de actividades del procedimiento, mostrando la relación entre las tareas, decisiones y responsables.



8. Descripción de Actividades

Esta sección detalla paso a paso las actividades involucradas en el proceso de creación, revisión, aprobación y publicación de procedimientos en Teuno. Cada actividad está alineada al diagrama de flujo y contempla al responsable, así como los registros o documentos que deben generarse como evidencia del cumplimiento.

N°	DESCRIPCIÓN DE LAS ACTIVIDADES	RESPONSABLE	DOCUMENTOS Y REGISTROS
1	Identificar la necesidad de creación o actualización de un procedimiento.	Dueño del Proceso	Solicitud por correo / Acta / Requerimiento
2	Elaborar el procedimiento siguiendo el formato FO-PRO-06 y la estructura institucional.	Dueño del Proceso	Borrador del procedimiento
3	Revisar técnica y formalmente el procedimiento.	Jefe de Área	Procedimiento en revisión
4	¿Cumple con los requisitos establecidos? Si no, devolver al dueño del proceso con observaciones para ajustes.	Jefe de Área	Registro de observaciones
5	Validar el documento final que será registrado en DOCS.	Área de Procesos / Responsable del Proceso	Procedimiento validado
6	Publicar el procedimiento en la plataforma DOCS y comunicar a los involucrados.	Dueño del Proceso / Área de Procesos	Procedimiento publicado / Evidencia de difusión
7	Concluir el proceso asegurando que el documento esté disponible	Dueño del Proceso	Historial de versiones en DOCS

	en el repositorio institucional.		

9. Puntos de Control

Los siguientes puntos de control aseguran la calidad, trazabilidad y cumplimiento del procedimiento de elaboración y actualización documental en TEUNO. Cada punto incluye su responsable y frecuencia de verificación.

N°	Punto de Control	Responsable	Frecuencia
1	Verificar que todos los procedimientos estén redactados en el formato	Área de Procesos	En cada revisión
2	Validar que el control de cambios esté completo y firmado electrónicamente	Dueño del Proceso	Con cada actualización
3	Confirmar que el documento esté cargado en la plataforma DOCS y con permisos de visualización vigentes	Dueño del Proceso / Área de Procesos	Al momento de publicación
4	Verificar que el procedimiento cuente con aprobación de jefatura y gerencia registrada	Área de Procesos / Jefe de Área	En la publicación inicial
5	Revisar el cumplimiento de la actualización anual del procedimiento	Dueño del Proceso / Área de Procesos	Anualmente

10. Referencia a otros documentos

Este procedimiento se fundamenta en normas y documentos que definen los principios, lineamientos y requisitos para la gestión y control documental en Teuno. A continuación, se listan los documentos y normas de referencia:

Norma ISO 9001:2015 – Sistemas de gestión de la calidad: establece los requisitos para la estandarización, control y mejora continua de los procesos documentados.

Norma ISO 27001:2022 – Gestión de la seguridad de la información: aplicable a procedimientos vinculados a protección de activos y control de documentación.

Mapa de Procesos TEUNO (MP-PRO-01) – Clasificación de procesos estratégicos, operativos y de apoyo.

11. Anexos

N/A

12. Control de Cambios

VERSION	FECHA (dd/mm/aa)	CAMBIOS
00	**(dd/mm/aa)**	RFC XXX-XXXXX Versión Inicial

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Cargo: Analista de Procesos	**Cargo:** Subgerente de Gobierno	**Cargo:** Gerente General

ANEXO 2: AUDITORÍA INTERNA

1. Propósito

Establecer los lineamientos para planificar, ejecutar y documentar auditorías internas al Sistema de Gestión Integrado (SGI) de TEUNO, verificando el cumplimiento de los requisitos normativos, los principios de la Norma ISO 31000:2018 y promoviendo la mejora continua.

Este procedimiento se basa en los principios fundamentales de la gestión de riesgos: integración en los procesos organizacionales, toma de decisiones basada en evidencias, y mejora continua.

2. Alcance

Aplica a todas las áreas que intervienen en la gestión de riesgos dentro del SGI de TEUNO. El procedimiento cubre desde la planificación de la auditoría hasta el cierre documentado de las no conformidades en la plataforma **Docs TEUNO**.

3. Responsabilidades

Auditor Líder Interno:

Coordina la auditoría.

Dirige las reuniones de apertura y cierre.

Elabora y aprueba el informe final.

Auditor Interno:

Ejecuta la auditoría conforme al plan.

Recopila evidencias.

Redacta informes de hallazgos.

Dueños de Proceso / Jefaturas:

Proveen evidencias requeridas.

Lideran la formulación e implementación de planes de acción.

Gestionan el cierre de las no conformidades.

Responsable del Sistema de Gestión:

Supervisa el proceso de auditoría.

Realiza seguimiento a las acciones correctivas.

Valida los cierres de no conformidades en **Docs TEUNO**.

Gerente General:

Aprueba el informe final de auditoría.

Participa en la reunión de cierre.

4. Definiciones

Auditoría Interna: Proceso independiente y documentado para evaluar la conformidad del SGI con los requisitos establecidos, incluyendo los principios de la gestión de riesgos según ISO 31000:2018.

No Conformidad: Incumplimiento de un requisito del sistema de gestión o de la normativa aplicable.

Acción Correctiva: Medida tomada para eliminar la causa de una no conformidad detectada y prevenir su recurrencia.

5. Procedimiento

5.1. Planificación de la Auditoría

Preparación Inicial:

Realizar un estudio preliminar para comprender:

La estructura de procesos de TEUNO.

Objetivos organizacionales.

Marco legal y regulatorio aplicable.

Cultura organizacional y documentos internos relevantes.

Definir Alcance y Objetivos:

Determinar procesos y áreas clave a auditar.

Establecer objetivos alineados con la gestión de riesgos.

Elaborar el Plan de Auditoría:

Incluir:

Objetivos y criterios.

Procesos y áreas a auditar.

Cronograma de auditoría.

Equipo auditor.

Aspectos críticos según análisis de riesgos.

Estructura del informe.

Reglas de confidencialidad.

Designar al Equipo Auditor:

Asegurar independencia, imparcialidad y competencia en gestión de riesgos.

Validar el plan con el Auditor Líder y aprobarlo con la Dirección.

5.2. Ejecución de la Auditoría

Actividad	Descripción
Reunión de Apertura	El Auditor Líder presenta el equipo, confirma alcance y metodología, asigna roles y establece normas de seguridad y confidencialidad.
Recolección de Evidencias	Revisión de documentos, entrevistas al personal, observación de actividades en campo.
Verificación de Conformidad	Evaluar si los procesos cumplen con los procedimientos, si las actividades se realizan conforme a lo documentado, y si el personal conoce sus funciones en la gestión de riesgos.
Informe Preliminar	Se realiza reunión con responsables de áreas para comunicar hallazgos preliminares, resolver dudas y registrar conclusiones.

5.3. Informe de Auditoría

Elaboración del Informe Final:

Contenido:

Datos generales de la auditoría.

Alcance, objetivos y criterios.

Resultados y hallazgos.

No conformidades detectadas.

Recomendaciones y oportunidades de mejora.

Declaración de confidencialidad.

Aprobación y Distribución:

El informe es aprobado por el Auditor Líder y remitido a:

Responsable del SGI.

Gerencia General.

Jefaturas de áreas auditadas.

5.4. Seguimiento

Gestión de No Conformidades y Acciones Correctivas:

Registrar formalmente la no conformidad.

Realizar análisis de causa raíz.

Elaborar plan de acción con responsables y plazos.

Ejecutar acciones correctivas.

Registrar y verificar el cierre en **Docs TEUNO**.

Validación y Cierre:

Verificación de eficacia de las acciones por parte del Responsable del SGI.

Cierre documentado de no conformidades.

Aprobación final por parte del Gerente General si corresponde.

6. Registros

Plan de Auditoría Interna

Lista de Verificación basada en ISO 31000:2018

Informes de Hallazgos

Informe Final de Auditoría

Registro de Acciones Correctivas

Evidencias de cierre en **Docs TEUNO**

Formatos de apertura y cierre de auditoría

7. Referencias

- **ISO 31000:2018** – Directrices para la Gestión de Riesgos
- Política de Gestión de Riesgos de TEUNO
- Manual y Procedimientos del SGI de TEUNO
- Requisitos legales y normativos aplicables

ANEXO 3: INFORME DE NO CONFORMIDAD

- Empresa: [TEUNO]
- Centro: [Plataforma Digital / Sitio Web Institucional]
- Tipo de Auditoría: [Auditoría Interna SGI – Cumplimiento Normativo (Protección de Datos Personales]. Número: [**V-04-2025**]
- Auditor/Responsable: [**NOMBRE_APELLIDOS_AUDITOR**]
- Fecha: [18 de junio de 2025]
- Referencia No Conformidad nº: [**NC-DP-001-2025**]

PROCESO/S	**[DESCRIPCION]** **Gestión de la Protección de Datos Personales y Cumplimiento Normativo Digital**
CRITERIOS DE REFERENCIA:	**[NORMATIVA]** o Ley Orgánica de Protección de Datos Personales (LOPDP). o Reglamento General de Protección de Datos (RGPD) – Aplicación supletoria. o Guía sobre uso de cookies y consentimiento informado (Agencia de Protección de Datos del Ecuador y EDPB). **[DESCRIPCION]** o Evaluación técnica (abril 2025) sobre formularios de contacto, inscripción y postulaciones en línea. o Procedimiento interno de recolección de datos personales – versión 2.3 (15/03/2025).

	"Todo tratamiento de datos personales debe sustentarse en una base legal válida, incluyendo la obtención de consentimiento libre, específico, informado e inequívoco por parte del titular". "En los formularios digitales debe garantizarse que las finalidades estén diferenciadas, no premarcadas, y que se brinde una política de privacidad clara y accesible".

DESCRIPCIÓN DE LA NO CONFORMIDAD:	Durante la revisión de los formularios digitales habilitados en: o Portal Web Principal de TEUNO o Plataforma de Gestión de Talento Externo "Genoma Work" Se evidenció lo siguiente: o Las casillas de consentimiento estaban premarcadas por defecto, lo cual invalida el consentimiento según LOPDP y RGPD. o No se distingue de manera separada el consentimiento para diferentes finalidades (procesos de selección vs. envío de comunicaciones). o No se proporciona una opción sencilla de revocación del consentimiento. o En Genoma Work no se informa el responsable del tratamiento ni el tiempo de conservación de los datos, afectando el principio de transparencia. Dado que los formularios recogen datos personales identificativos y sensibles, **se levanta una No Conformidad Interna para que se inicie el análisis de causa y un plan.**

CAUSA IDENTIFICADA:	Durante el rediseño del portal institucional (enero de 2025) y la integración con la plataforma Genoma Work, no se consideró la revisión jurídica por parte del Comité de Protección de Datos. Además, por priorizar la rapidez de publicación y la experiencia de usuario, se reutilizaron formularios antiguos, sin adaptar la estructura del consentimiento a los cambios normativos incorporados en la LOPDP desde el segundo semestre de 2024.

PROPUESTA DE ACCIÓN CORRECTIVA Y/O PREVENTIVA: SI	**[DESCRIPCION]** Se propone la actualización inmediata de los formularios digitales, asegurando: ○ Eliminación de casillas premarcadas. ○ Inclusión de consentimiento granular y diferenciación de finalidades. ○ Inclusión de información sobre el responsable del tratamiento, duración del almacenamiento y canal de revocación. Además, se establecerá un protocolo de revisión legal obligatoria para todos los formularios que recolecten datos personales.
	FICHA DE ACCIONES CORRECTIVAS: ○ ACCIÓN: Rediseño legal de los formularios web según LOPDP y validación jurídica. ○ RESPONSABLE: Comité de Protección de Datos / Dirección de Tecnología y Legal. ○ NOMBRE Y FIRMA DEL RESPONSABLE: [**NOMBRE_APELLIDOS_CARGO**] ○ PROPUESTA REALIZADA POR: [**NOMBRE_APELLIDOS_CARGO**]

Fecha prevista de inicio: 01/07/2025	**Fecha prevista de finalización: 15/08/2025**

[FIRMA] **Firma del Auditado:**	**[FIRMA]** **Firma del Auditor:**

FICHA DE VERIFICACIÓN

RESPONSABLE DE LA VERIFICACIÓN: [NOMBRE_APELLIDOS_CARGO]	**FECHA PREVISTA DE VERIFICACIÓN: 30/08/2025**
MÉTODO DE VERIFICACIÓN:	**DESCRIPCIÓN** Evidencias constatadas: ○ En fecha 10/08/2025 se publicó la nueva versión de los formularios con consentimiento explícito y casillas no premarcadas. ○ El nuevo aviso de privacidad incluye responsable, plazos de conservación y base legal. ○ Se habilitó un canal de revocación vía correo electrónico y sección de derechos ARCO. ○ El Comité de Protección de Datos validó el diseño el 08/08/2025. ○ Se actualizó la política institucional en el portal y se notificó al personal.

[FIRMA] **Firma del responsable de verificación**	**FECHA CIERRE DE LA VERIFICACIÓN:** **31/08/2025**
[FIRMA] **Firma del auditor jefe de auditoría interna**	

OBSERVACIÓN:	La no conformidad ha sido cerrada satisfactoriamente. Se recomienda actualizar el procedimiento interno de desarrollo de formularios para incluir la validación jurídica como paso obligatorio y garantizar sostenibilidad del cumplimiento legal en futuras modificaciones digitales.