Maestría en

Gestión de Riesgos

Trabajo de investigación previo a la obtención del título de

Magíster en Magíster en Gestión de Riesgos

AUTORES:
JUAN DANIEL RUALES NOVILLO
TANIA VIVIANA SALAZAR PERALTA
GALO ALEXANDER RUBIO ZAPATA
VERONICA TALIA ROMERO GUARQUILA
GEIMY SILVANA GAVILANEZ PASTO
HERNÁN ROBERTO MUÑOZ RODRÍGUEZ

TUTORES:
David G. Benavides Gutiérrez
Paloma Manzano Martínez
Enrique Molina Suárez

"CREACIÓN DE UN MANUAL DE GESTIÓN DE RIESGOS BASADOS EN LA NORMA ISO 31000-2018 PARA INSTITUCIONES EDUCATIVAS EN LA CORPORACIÓN DE SEGURIDAD GER"

Quito, (junio 2025)

Certificación de autoría

Nosotros, Juan Daniel Ruales Novillo, Tania Viviana Salazar Peralta**,** Galo Alexander Rubio Zapata, Geimy Silvana Gavilanez Pasto, Veronica Talia Romero Guarquila, Hernán Roberto Muñoz Rodríguez. 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:
JUAN DANIEL RUALES NOVILLO
Validar únicamente con FirmaEC

Juan Daniel Ruales Novillo

Firmado electrónicamente por:
TANIA VIVIANA SALAZAR PERALTA
Validar únicamente con FirmaEC

Tania Viviana Salazar Peralta

Firmado electrónicamente por:
GALO ALEXANDER RUBIO ZAPATA
Validar únicamente con FirmaEC

Galo Alexander Rubio Zapata

Firmado electrónicamente por:
GEIMY SILVANA GAVILANEZ PASTO
Validar únicamente con FirmaEC

Geimy Silvana Gavilanez Pasto

Firmado electrónicamente por:
HERNAN ROBERTO MUÑOZ RODRIGUEZ
Validar únicamente con FirmaEC

Hernán Roberto Muñoz Rodríguez

Firmado electrónicamente por:
VERONICA TALIA ROMERO GUARQUILA
Validar únicamente con FirmaEC

Verónica Talía Romero Guarquila

Autorización de Derechos de Propiedad Intelectual

Nosotros, Juan Daniel Ruales Novillo, Tania Viviana Salazar Peralta, Galo Alexander Rubio Zapata,Geimy Silvana Gavilanez Pasto, Hernán Roberto Muñoz Rodríguez, Verónica Talia Romero Guarquila, en calidad de autores del trabajo de investigación titulado ***"CREACIÓN DEL MANUAL DE GESTIÓN RIESGOS BASADOS EN LA NORMA ISO 31000-2018 PARA LAS INSTITUCIONES EDUCATIVAS DE LA CORPORACIÓN DE SEGURIDAD GER"***, 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,08 de abril.

Firmado electrónicamente por:
JUAN DANIEL RUALES NOVILLO
Validar únicamente con FirmaEC

Juan Daniel Ruales Novillo

Firmado electrónicamente por:
TANIA VIVIANA SALAZAR PERALTA
Validar únicamente con FirmaEC

Tania Viviana Salazar Peralta

Firmado electrónicamente por:
GALO ALEXANDER RUBIO ZAPATA
Validar únicamente con FirmaEC

Galo Alexander Rubio Zapata

Firmado electrónicamente por:
GEIMY SILVANA GAVILANEZ PASTO
Validar únicamente con FirmaEC

Geimy Silvana Gavilanez Pasto

Firmado electrónicamente por:
HERNAN ROBERTO MUÑOZ RODRIGUEZ
Validar únicamente con FirmaEC

Hernán Roberto Muñoz Rodríguez

Firmado electrónicamente por:
VERONICA TALIA ROMERO GUARQUILA
Validar únicamente con FirmaEC

Verónica Talía Romero Guarquila

Aprobación de dirección y coordinación del programa

Nosotros, **Paloma Manzano Martínez y David G. Benavides Gutiérrez,** declaramos que los graduandos: Juan Daniel Ruales Novillo, Tania Viviana Salazar Peralta, Alexander Rubio Zapata, Geimy Silvana Gavilanez Pasto, Hernán Roberto Muñoz Rodríguez, Verónica Talia Romero Guarquila, 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 10:36:15 +02'00'

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

PALOMA MANZANO MARTINEZ	DAVID GENARO BENAVIDES GUTIERREZ
Director/a de la	Coordinador/a de la
Maestría en Maestría en Gestión de Riesgos	Maestría en Gestión de Riesgos

DEDICATORIA

Este trabajo va dedicado a Dios, Creador, porque sin Él nada sería posible, por guiarme en cada paso, ser mi refugio en los momentos difíciles y llenar mi vida de propósito y fe. A mis padres, quienes me han forjado, y con su ejemplo me han enseñado a ser fuerte, y a no rendirme a pesar de los obstáculos. A mi esposo, mi compañero de vida, por ser mi soporte, y estar junto a mí en los días buenos y en los no tan buenos, y compartir conmigo este camino con amor, paciencia y fe. Y a mis hijas, mi mayor tesoro, la razón de ser. el motor que me impulsa a seguir adelante, mi alegría diaria y mi mayor inspiración. Todo lo que soy y lo que logro es también por ustedes y para ustedes.

Verónica Talía Romero.

Mi dedicatoria va extendida con todo mi corazón a Dios a mis padres que en el transcurso de mi vida me supieron inculcar valores y confiaron en mi persona y en mis deseos de superación siempre han sido mi sostén para cada uno de mis logros.
A mi amado esposo y padre de mis hijos su amor y motivación han sido la base de nuestro hogar, este logro es un tributo a la colaboración y apoyo incondicional que me ha brindado a lo largo de este viaje académico.
A mis preciosos hijos Camila y Sebastián: que son el regalo que la vida me dio, son mi motor mi fuerza y mi inspiración, esta meta la he logrado pensando en ustedes.
Gracias por llenar mi vida de amor y dulzura.
Con amor y admiración

Geimy Gavilanez.

Dedico a quienes son nuestros pilares únicos en mi vida.
A Dios, Al Gran Espíritu Santo, Jesús, Señor de la Justicia, a la Virgen Dolorosa, Inmaculada Concepción, María Auxiliadora, Padre Pío de Pietrelcina, Santo Hermano Miguel y San Don Bosco, mi dedicatoria porque desde que llegué y en todo el transcurso de la maestría me encomendé siempre ya que Ellos me dieron esta habilidad de comprender cada materia y por la oportunidad que recibí de estudiar en la Universidad y ante cualquier adversidad seguir adelante con su único apoyo.
A mis padres, hermana, novia, con su amor, comprensión, apoyo, y su motivación fue lo más importante para que pudiera ser mejor y con más ánimos terminar cada palabra, cada pensamiento hacerlo realidad con mi conocimiento, sin su recomendación no hubiese podido resolver cada adversidad.

Hernán Roberto Muñoz Rodríguez.

El presente proyecto de tesis va dedicado a DIOS creador de todo el universo que ha permitido que este hasta esta etapa final de mi maestría, también quiero agradecer a mi esposo mi compañero de vida el que me ha impulsado día a día a superarme y a seguir creciendo como profesional, gracias por motivarme aun cuando ya no he querido continuar, tu amor, apoyo y paciencia ha sido clave en este proceso gracias por creer en mí y tengo la convicción que juntos somos un gran equipo y podemos superar toda adversidad.
A mis hijos Juanse, Elías y Abby que son mi motor para seguir adelante y luchar por un mejor futuro, los amo con todo mi corazón sin su apoyo no sería esto posible.
A mis padres les dedico cada logro profesional porque me han inculcado que no existen límites ni barreras para seguir creciendo cuando te lo propones con esfuerzo y dedicación, especialmente a mi Padre Mario Salazar mi ángel que siempre me impulsó en mi carrera profesional siempre estuviste y seguirás conmigo hasta la eternidad.

Tania Viviana Salazar Peralta.

Dedico este proyecto de tesis a Dios que nos da las oportunidades de servir a través de nuestro esfuerzo y conocimiento, a mi esposa Viviana compañera de vida, que ha sido mi apoyo incondicional y me ha impulsado a ser mejor cada día, no tengo duda que juntos somos un gran equipo, a mis hijos Juan Sebastián, Elías Daniel y Abigail, que con su amor y ternura motivaron cada jornada aunque que en muchas ocasionas tuvieron que prescindir de nuestro tiempo, a mis padres y hermanos que en todo momento creyeron en mí, a mi suegra por sus palabras de aliento y a mis compañeros de maestría que trabajaron con mucha dedicación para que todo esto sea posible. Finalmente quiero agradecer a nuestros maestros y tutores por darnos abiertamente los recursos para poder aprender y poner en práctica lo aprendido.
“Mejorar la vida del prójimo no es una posibilidad sino una oportunidad de crecer en sociedad”

Juan Daniel Ruales Novillo.

Para mi amada abuelita Julia, cuya presencia, aunque ya no física, sigue iluminando cada paso de mi camino. Su amor incondicional y su sabiduría son el legado más preciado que llevo en el corazón. Esta obra es un humilde tributo a la huella imborrable que dejó en mi vida.

Galo Alexander Rubio Zapata.

AGRADECIMIENTO

Queremos agradecer de manera especial a la Universidad ECOTEC por su colaboración al facilitarnos la información necesaria para el desarrollo de este trabajo.

la Universidad Internacional del Ecuador (UIDE), institución donde realizamos nuestra formación de maestría, por brindarnos las herramientas académicas y el acompañamiento que hicieron posible este logro.

A docentes, compañeros y a todas las personas e instituciones que, de una u otra forma, nos apoyaron a lo largo de este camino, les extendemos nuestro sincero agradecimiento.

RESUMEN

La presente investigación abordó la creación de un Manual de Gestión de Riesgos basado en la norma ISO 31000:2018 para la Universidad Tecnológica ECOTEC, este proyecto buscó fortalecer los procedimientos existentes relacionados con la gestión de riesgos, especialmente aquellos enfocados en la protección de datos personales y la seguridad informática. A través de un análisis detallado de los sistemas actuales y la identificación de los riesgos más relevantes, se propusieron medidas correctivas y preventivas que permitió a la institución mejorar la gestión de su infraestructura tecnológica, garantizar la seguridad de la información y cumplir con las normativas vigentes, como la Ley Orgánica de Protección de Datos Personales (LOPDP). La implementación de este manual tuvo como objetivo no solo la mejora de la eficiencia interna, sino también la creación de una cultura organizacional que valore la seguridad de los datos y proteja la integridad de la comunidad universitaria. Además, se evaluaron los aspectos relacionados con la certificación de seguridad, propuso el alineamiento con estándares internacionales como ISO 27001. Esta investigación contribuyó significativamente al desarrollo institucional de ECOTEC y ofreció un modelo que puede ser replicado en otras instituciones educativas del país, promoviendo la seguridad y la protección de los datos en entornos académicos.

Palabras Clave: gestión de riesgos, ISO 31000, protección de datos personales, seguridad informática, manual de gestión.

ABSTRACT

This research focuses on the creation of a Risk Management Manual based on the ISO 31000:2018 standard for the Universidad Tecnológica ECOTEC. This project aims to strengthen existing procedures related to risk management, particularly those focused on personal data protection and cybersecurity. Through a detailed analysis of current systems and the identification of the most relevant risks, corrective and preventive measures were proposed to improve the institution's management of its technological infrastructure, ensure the security of information, and comply with current regulations such as the Organic Law on the Protection of Personal Data (LOPDP). The implementation of this manual aims not only to improve internal efficiency but also to create an organizational culture that values data security and protects the integrity of the university community. Additionally, aspects related to security certification were evaluated, proposing alignment with international standards such as ISO 27001. This research significantly contributes to the institutional development of ECOTEC and provides a model that can be replicated in other educational institutions in the country, promoting data security and protection in academic environments.

Keywords: risk management, ISO 31000, personal data protection, cybersecurity, management manual.

Tabla de Contenidos

Índice de Tablas

Índice de Ilustraciones

Capítulo 1

Introducción

Este trabajo se centra en la gestión de riesgos informáticos y la protección de datos personales en la Universidad Tecnológica ECOTEC, ya que es un tema en creciente importancia especialmente en el área digital. A medida que la tecnología se expande en el ámbito académico, la protección de la información y la gestión efectiva de los riesgos asociados se han convertido en aspectos fundamentales para el buen funcionamiento de las organizaciones educativas.

Se analizará cómo ECOTEC gestiona la seguridad de la información y los riesgos informáticos, identificando áreas de mejora y proponiendo acciones concretas para fortalecer sus procesos. La investigación se enmarca en el contexto de la norma ISO 31000:2018, la cual proporciona directrices internacionales para una gestión eficaz de riesgos.

La relevancia de este trabajo radica en la necesidad urgente de garantizar la seguridad de los datos sensibles de estudiantes, docentes y personal administrativo. En un entorno digital, la protección de esta información es crucial para mantener la confianza de la comunidad universitaria y asegurar la continuidad operativa de la institución.

Este proyecto tiene como objetivo no solo diagnosticar los riesgos actuales en ECOTEC, sino también proponer un plan de acción para mejorar la gestión de la seguridad informática y la protección de los datos personales, alineado con las mejores prácticas internacionales. A lo largo de la investigación, se presentarán los riesgos identificados, las estrategias adoptadas por la institución y una serie de recomendaciones para una gestión de riesgos más segura y eficiente.

1. Planteamiento del Problema e Importancia del Estudio

1.1. Definición del Proyecto

El presente proyecto consiste en la creación de un Manual de Gestión de Riesgos para una parte las instituciones educativas de la Corporación de Seguridad GER, (Universidad ECOTEC)

La propuesta contempla tanto la mejora de los procedimientos ya implementados y que actualmente se encuentran funcionando, como la incorporación de nuevas estrategias, protocolos y herramientas que resultan indispensables para lograr una gestión de riesgos efectiva, conforme a los estándares internacionales establecidos en la ISO 31000:2018.

Este proyecto tiene como base los principios de la ISO 31000:2018, que establece un marco general para gestionar cualquier tipo de riesgo, y adaptarlo a la realidad particular de la institución tanto en el contexto educativo y a los servicios que presta, que incluirá normativas nacionales vigentes en materia de seguridad, protección de datos personales, gestión de emergencias y regulación educativa, garantizando así su aplicabilidad legal y técnica, y representa un aporte significativo ya que se podrá ampliar su visión integral de seguridad.

1.2. Naturaleza o Tipo de Proyecto

El proyecto se clasifica como un proyecto de diseño, ya que la Universidad ECOTEC no cuenta con manual de gestión de riesgos estructurado.

Sin embargo, esta institución cuenta con procedimientos para preveer riesgos que no están normados, por lo tanto, es necesario desarrollar un manual aplicando la norma ISO 31000:2018., que integre estos procesos institucionales, enfocado en optimizar y elaborar

nuevos procesos, desarrollando su efectividad y cumplimiento con los estándares internacionales.

1.3. Objetivos

1.3.1. Objetivo General

Desarrollar un Manual de Gestión de Riesgos basado en la norma ISO 31000:2018 para la Universidad ECOTEC, que permita fortalecer sus procesos internos de gestión de riesgos, alineándolos con las mejores prácticas internacionales, y garantizando una mayor protección de la infraestructura tecnológica, los datos sensibles y la seguridad de la comunidad educativa.

1.3.2. Objetivos Específicos

Analizar los riesgos actuales que enfrenta la Institución en sus diferentes actividades tanto académicas como administrativas, identificando las áreas que necesitan fortalecerse para cumplir con los estándares de la norma ISO 31000: 2018.

Integrar prácticas que faciliten la aplicación del manual dentro de los procesos existentes en ECOTEC, asegurando su efectividad en la protección de datos y la infraestructura tecnológica.

Establecer un sistema de monitoreo y mejora continua para evaluar la eficacia del manual de gestión de riesgos, garantizando su actualización y alineación con las normativas vigentes, además de promover la capacitación y sensibilización del personal en ciberseguridad.

1.4. Justificación e Importancia del Trabajo de Investigación.

El diseño del manual de gestión de riesgos basado en la norma ISO 31000:2018, es muy importante para la Universidad ECOTEC, para fortalecer la gestión de riesgos institucional. Tomando en cuenta que en el contexto académico es cada vez más digitalizado, y la importancia de la protección de la información y los sistemas tecnológicos para garantizar la continuidad operativa de la universidad. En este contexto las instituciones educativas enfrentan vulnerabilidades crecientes relacionadas con ciberataques, fallos tecnológicos y errores humanos que pueden poner en riesgo tanto la seguridad de los datos como la operación institucional (Castañeda, 2020), es por esto que lo planteado por la ISO 31000:2018, la gestión de riesgos debe ser un proceso sistemático y continuo que permita identificar, evaluar, tratar, monitorear y comunicar los riesgos de manera efectiva.

La importancia de contar con un manual estructurado y alineado a esta normativa es reconocida internacionalmente, ya que este marco establece una metodología sólida para abordar los riesgos de manera proactiva, minimizando sus impactos negativos sobre las organizaciones, así lo destaca los estudios desarrollados por el ISO Survey y diversas consultoras como PwC y Deloitte, evidencian que las organizaciones que implementan sistemas de gestión de riesgos estructurados aumentan hasta en un 30 % su capacidad de resiliencia operativa, minimizan incidentes severos en más del 40 % y mejoran la confianza institucional y reputacional de cara a sus stakeholders. Por lo tanto mediante una conclusión operativa es efectiva en trabajar para acercarse hasta un 50% a nivel de una institución, sin embargo, no dejar de lado que la aplicación ha permitido obtener oportunidades por medio de los diferentes riesgos, Aguas de Calpe lograron obtuvieron la certificación en la cual su

propia institución en base a su calidad y seguridad dio un gran paso en fortalecer sus procesos para que la credibilidad de la imagen y los riesgos por los cuales atravesaron se esclarecieran al obtener una mayor confianza por parte del consumidor, que es, muy importante en la garantía exacta de una empresa, no lo mejoraron los riesgos encontrados sino que permitió visionar los siguientes riesgos legislativos, financieros y estratégicos, además de que su rentabilidad creció, la evaluación del riesgo formo la capacidad de ser mas estrictos con cada trabajador y con cada servidor, es una referencia en la cual da un giro total de obtener la ISO 31000:2018. Es una referencia muy importante, el mercado es muy extenso, diversos servicios, diversos productos, no obstante, no lo consiguen fácilmente, el identificar, acetar los riesgos y dar la atenciones lo que ha permitido que el valor incremente en relación a la competencia estándar.

Aplicar esta norma en el contexto educativo permite reducir vulnerabilidades en su infraestructura digital, proteger la información de estudiantes y docentes, y alinearse a los requerimientos legales y normativos vigentes, como la Ley Orgánica de Protección de Datos Personales (LOPDP).

Este proyecto no solo responde a una necesidad institucional inmediata, sino que además posesiona a la universidad como una institución moderna, responsable y comprometida con la excelencia organizacional.

Capítulo 2

La Organización

2. Perfil de la Organización.

La Universidad Tecnológica ECOTEC es una institución de educación superior privada, con sede principal en la ciudad de Guayaquil, Ecuador. Fundada en 2007, ECOTEC ha experimentado un crecimiento sostenido, consolidándose como una universidad de referencia en el ámbito nacional e internacional, comprometida con la formación de profesionales humanistas e innovadores, con responsabilidad social, empresarial y ambiental. Su misión es formar profesionales a través de la docencia y la investigación de calidad, para contribuir al desarrollo del país.

2.1. Nombre, Actividades, Mercados Servidos Y Principales Cifras

2.1.1. Nombre de la Empresa

La empresa elegida a desarrollar el trabajo es Universidad Tecnológica ECOTEC

2.1.2. Misión, Visión, Valores.

Misión

La Universidad Tecnológica ECOTEC tiene como misión formar profesionales humanistas e innovadores, con responsabilidad social, empresarial y ambiental, mediante procesos de docencia e investigación de calidad, orientados al desarrollo sostenible del país. Este propósito guía la acción institucional hacia la formación integral de sus estudiantes, promo0076iendo el pensamiento crítico, el emprendimiento, el liderazgo y el compromiso ético con la sociedad.

Visión

ECOTEC se proyecta a futuro con la visión de consolidarse a nivel nacional e internacional como una institución de docencia e investigación, reconocida como referente científico, tecnológico y ambiental, gracias a la calidad de sus procesos sustantivos y su contribución al desarrollo del conocimiento.

Valores

La Universidad ECOTEC promueve una cultura organizacional basada en los siguientes valores fundamentales:

- Ética: Actuar con integridad, transparencia y justicia en todos los niveles de la vida institucional.
- Ecología: Promover la sostenibilidad y el respeto por el entorno natural.
- Respeto: Fomentar relaciones interpersonales basadas en la aceptación y la consideración mutua.
- Responsabilidad: Cumplir con los compromisos académicos, sociales y profesionales.
- Servicio: Contribuir activamente al bienestar de la comunidad universitaria y la sociedad.
- Honestidad: Mantener una conducta coherente, honesta y auténtica en todos los actos.
- Igualdad: Garantizar un trato justo e inclusivo para todos los miembros de la comunidad.
- Solidaridad: Apoyar al prójimo y actuar con empatía ante las necesidades de los demás.

- Liderazgo: Impulsar iniciativas que generen impacto positivo y transformación social.
- Lealtad: Compromiso con la institución, sus principios y objetivos.

2.1.3. Actividades, Marcas, Productos y Servicios.

Actividades

La Universidad ECOTEC desarrolla actividades académicas de pregrado y posgrado, investigación científica, vinculación con la sociedad, programas de educación continua y formación en idiomas. Además, promueve actividades culturales, deportivas y de bienestar estudiantil.

Marcas

Figura 1.

Logotipo universidad

Nota. Ilustración tomada de la universidad ECOTEC, logotipo institucional 2025.

La institución opera bajo la marca registrada Universidad ECOTEC, reconocida a nivel nacional por su enfoque innovador y por ofrecer una formación académica de calidad. Esta marca refleja los valores de compromiso, excelencia y responsabilidad social.

Productos

Los productos principales de ECOTEC son los programas académicos en diversas áreas del conocimiento, tales como administración, derecho, ingeniería, salud, educación y comunicación. Además, ofrece programas de formación continua, cursos de actualización profesional y programas de idiomas.

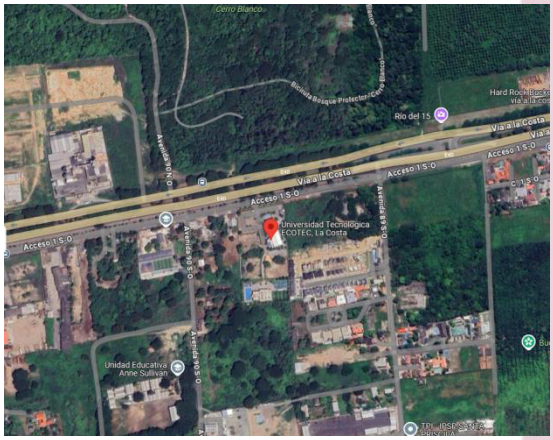
Servicios

Entre sus servicios, ECOTEC brinda asesoría académica, servicios de bienestar estudiantil, orientación profesional, acceso a bibliotecas físicas y virtuales, plataformas digitales de aprendizaje, movilidad académica, prácticas preprofesionales, y servicios de investigación y extensión universitaria.

2.1.4. Ubicación de la Empresa

Figura 2.

Ubicación de la empresa Ecotec



Nota. Ilustración generada por https://www.google.com/maps, muestra la ubicación de la empresa Ecotec.

La sede principal de la Universidad Tecnológica ECOTEC se encuentra en el kilómetro 16.5 de la Vía a la Costa, en la ciudad de Guayaquil, Ecuador. Este campus, conocido como "La Costa", fue inaugurado en 2019 y cuenta con una extensión de aproximadamente 19,417 m².

El campus La Costa está diseñado para ofrecer un ambiente académico moderno y sostenible, rodeado de áreas verdes que promueven la conexión con la naturaleza. Entre sus instalaciones destacan aulas equipadas con tecnología de punta, auditorio, salas de estudio, áreas deportivas y espacios destinados al bienestar estudiantil. Este entorno propicia una experiencia universitaria enriquecedora, combinando la excelencia académica con el desarrollo personal y profesional de los estudiantes.

2.1.5. Ubicación de las Operaciones

La Universidad Tecnológica ECOTEC desarrolla sus actividades académicas y administrativas principalmente en su campus Vía a la Costa Km 16.5, en la ciudad de Guayaquil. Además, cuenta con otras sedes lo que permite ampliar su cobertura geográfica dentro del país y facilitar el acceso a sus servicios educativos. Las ubicaciones no solo fortalecen su presencia institucional, sino que también consolidan su compromiso con la formación académica en diferentes zonas del Ecuador.

2.1.6. Propiedad y Forma Jurídica.

ECOTEC es una universidad de carácter privado, debidamente registrada y reconocida por el Consejo de Educación Superior (CES) y acreditada por el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES). Su forma jurídica es la de

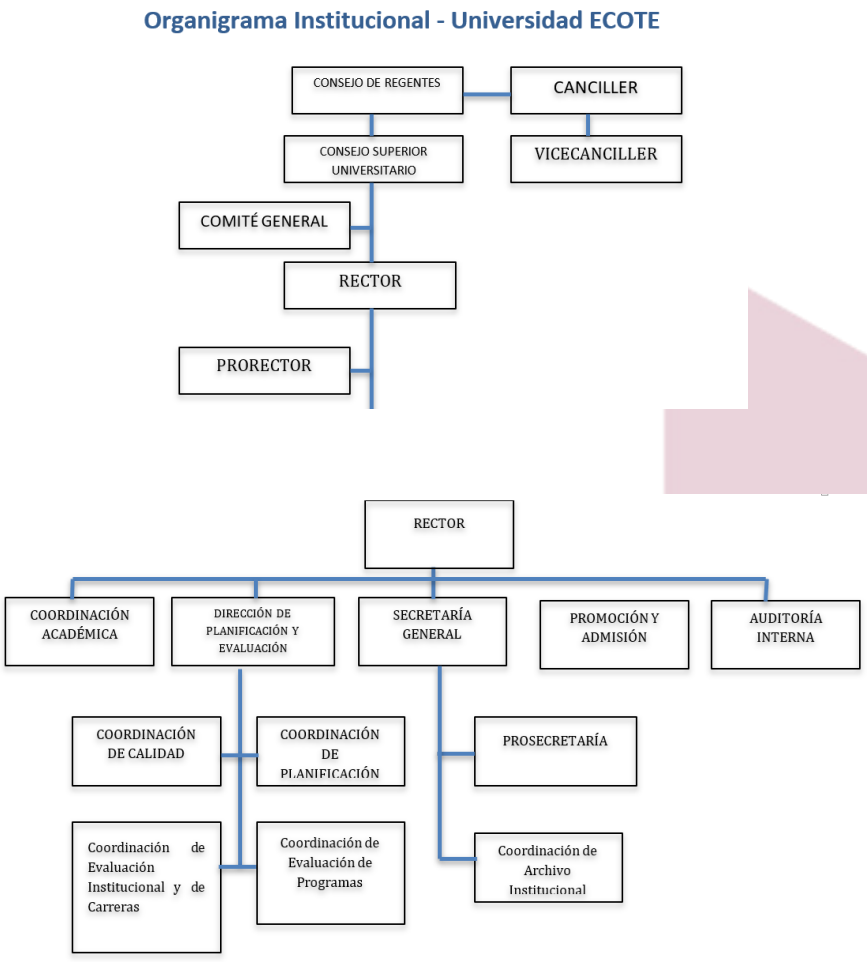
persona jurídica de derecho privado sin fines de lucro, lo que implica que sus recursos y excedentes se reinvierten en actividades académicas, infraestructura, investigación y desarrollo institucional, en lugar de ser distribuidos entre socios o accionistas. Esta estructura le permite enfocar sus esfuerzos en el fortalecimiento de la calidad educativa y la innovación.

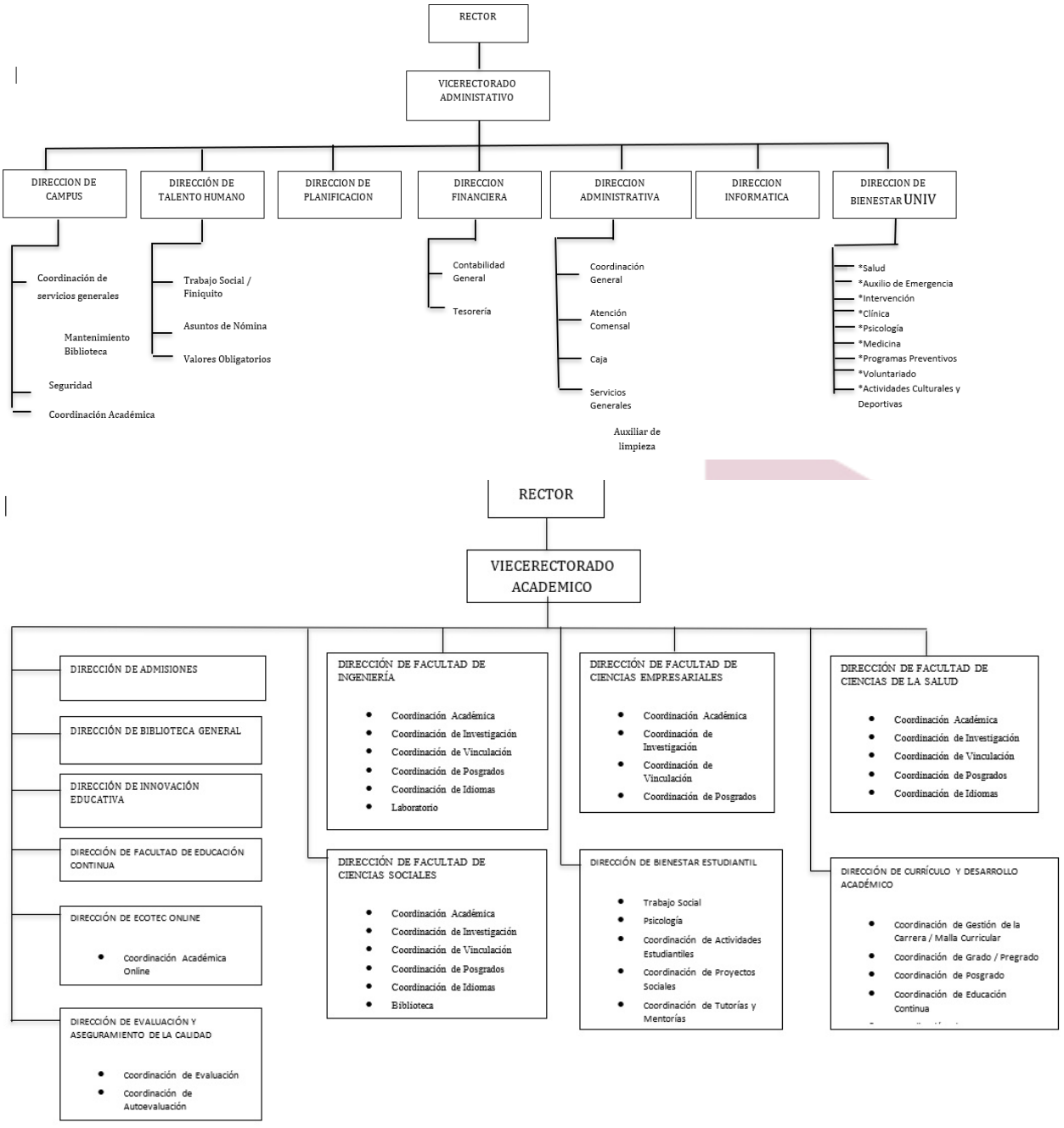
2.1.7. Mercados Servidos o Ubicación de sus Actividades de Negocio

La universidad presta sus servicios educativos principalmente en el ámbito nacional, atendiendo a estudiantes de diferentes provincias del Ecuador. No obstante, gracias a su enfoque internacional, también ha establecido convenios con instituciones en países como Estados Unidos, España, Chile y Canadá, ampliando así su proyección y participación en mercados educativos del exterior. ECOTEC ofrece carreras de grado, maestrías y programas de educación continua en modalidades presencial, híbrida y online, lo que le permite llegar a una población estudiantil diversa.

2.1.8. Tamaño De La Organización

Figura 3.
Organigrama funcional de ECOTEC





Nota. La ilustración muestra en cuatro partes el organigrama funcional de la universidad Ecotec, obtenido de la Planificación Operativa Anual PEI 2021-2026 Ec.

El campus ubicado en la Vía a la Costa Km 16.5, cuenta con una superficie de 19.058,41 m 2. Este espacio está diseñado para albergar aulas modernas, laboratorios, zonas verdes, áreas deportivas y de esparcimiento, así como espacios administrativos. La infraestructura responde a un modelo sostenible y funcional, acorde con las necesidades de una comunidad académica en constante crecimiento.

2.1.9. Información Sobre Empleados y Otros Trabajadores.

La institución cuenta con un equipo humano diverso y multidisciplinario en distintos niveles y departamentos.

El personal se agrupa en las siguientes categorías:

Directivos: Incluye autoridades como el secretario general, el Director de Admisiones, la Directora Administrativa y el Director Financiero, quienes lideran las áreas estratégicas y toman decisiones de alto nivel.

Personal docente: Profesores de distintas áreas académicas, como economía, marketing, comunicación, ingeniería, derecho, salud, entre otras, encargados de la formación de los estudiantes.

Investigadores: Profesores y personal especializado dedicados a la investigación en distintos campos del conocimiento, que impulsan proyectos científicos y académicos.

Personal administrativo: Encargado de la gestión administrativa, financiera, académica y de recursos humanos de la universidad.

Personal de apoyo: Personal que brinda soporte en áreas como biblioteca, tecnología de la información, mantenimiento, limpieza y otros servicios esenciales para el funcionamiento diario.

En términos generales (estos son ejemplos aproximados que puedes ajustar con cifras reales):

Número de empleados por tipo de contrato:

Fijos: 75% del personal total.

Eventuales o por contrato temporal: 25%.

Distribución por género:

Mujeres: 55% (ocupando principalmente cargos administrativos, docentes y de apoyo).

Hombres: 45% (mayoritariamente en cargos directivos, mantenimiento y tecnología).

Distribución por nivel jerárquico:

Directivos de alto nivel: 5% del personal.

Mandos medios (coordinadores, jefaturas): 15%.

Operativo-administrativo y docentes: 80%.

Distribución por edad (estimada):

Menores de 30 años: 20%.

Entre 30 y 50 años: 50%.

Mayores de 50 años: 30%.

Actualmente, ECOTEC cuenta con aproximadamente 350 personas trabajando en todos los niveles, incluyendo personal fijo y eventual. La diversidad de perfiles y funciones

permite a la universidad cumplir de manera eficiente con sus objetivos académicos, administrativos y de vinculación con la sociedad.

2.1.10. Procesos Claves Relacionados con el Objetivo Propuesto

Los procesos clave de ECOTEC se articulan en torno a la docencia de calidad, la investigación aplicada y la vinculación con la sociedad. A esto se suman procesos estratégicos como la gestión tecnológica, el aseguramiento de la calidad académica, la protección de datos personales, y la sostenibilidad institucional. Todos estos elementos están alineados con los objetivos de formar profesionales competentes e innovadores, y garantizar un entorno digital seguro para los miembros de la comunidad universitaria.

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

A continuación, se presenta un resumen con los indicadores clave que definen a la Universidad Tecnológica ECOTEC, destacando aspectos relevantes que permiten comprender su impacto, infraestructura, oferta académica y compromiso con la sostenibilidad. Estos datos proporcionan un panorama claro del contexto institucional y del esfuerzo de la universidad por mantenerse a la vanguardia en educación superior:

Tabla 1.

Datos principales de la universidad Ecotec

Datos institucionales básicos	
Indicador	**Valor**
Año de fundación	2006 (como instituto), 2007 (como universidad)
Número de sedes	3 (Samborondón, Guayaquil, Vía a la Costa)
Estudiantes activos	~15,000
Graduados	Más de 8,000
Oferta académica	

Indicador	Valor
Facultades	6
Carreras de pregrado	28
Programas de posgrado	14 maestrías
Infraestructura y recursos	
Indicador	**Valor**
Libros físicos	6,398
Libros digitales	44,339
Paneles solares (campus total)	>2,500 (u 1,889 según fuente 2021)
Reducción CO_2 por año	539 toneladas
Aporte energético al país	5,000 kW/día
Posicionamiento y rankings	
Indicador	**Valor**
Posición en GreenMetric	Top 3 en Ecuador, #426 mundial (2021)
ODS 13 en THE Impact Rankings	1ª universidad privada en Ecuador
ODS 16 en THE Impact Rankings	3ª universidad en Ecuador
Vinculación y sostenibilidad	
Indicador	**Valor**
Carbono-neutral certificada	Primera universidad en Ecuador en 2020
Proyecto emblemático	Biorremediación del estero Salado

Nota. Elaboración propia en base a datos de la Universidad ECOTEC (2021-2022).

2.1.12. Modelo de negocio.

El modelo de negocio de ECOTEC se basa en una estructura de autogestión financiera, bajo la figura de universidad particular sin fines de lucro. Su financiamiento proviene de matrículas, colegiaturas, programas de formación continua, consultorías, y alianzas estratégicas con instituciones públicas y privadas. A esto se suma la reinversión de sus excedentes en infraestructura, calidad educativa y tecnología, alineado con su misión institucional

2.1.13. Grupos de interés internos y externos.

Los grupos de interés internos incluyen a los estudiantes, docentes, personal administrativo, investigadores y directivos. Externamente, ECOTEC mantiene relaciones con entidades gubernamentales, empresas privadas, instituciones educativas nacionales e internacionales, comunidades locales, organizaciones sin fines de lucro, proveedores tecnológicos y entes de acreditación. La interacción con estos grupos es fundamental para fortalecer la pertinencia académica, la vinculación social y el desarrollo de proyectos conjuntos

2.1.14. Otros datos de interés.

Entre otros aspectos destacables, ECOTEC ha fortalecido su compromiso con la sostenibilidad, la ética institucional y la innovación digital. Cuenta con políticas claras de protección de datos, accesibilidad, equidad de género y prevención de riesgos laborales. También impulsa la mejora continua mediante certificaciones de calidad, sistemas de evaluación docente, y programas de formación permanente para su personal.

Capítulo 3

3. Manual Documento de Seguridad

3.1. Análisis de Riesgos

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

La Universidad ECOTEC, con su campus principal ubicado en la Vía a la Costa km 13.5, en la ciudad de Guayaquil, es una institución de educación superior que imparte carreras de pregrado y programas de posgrado.

3.1.2. Representante Legal y Responsable de Seguridad

El representante legal de la institución es el Dr. Joaquín Hernández Alvarado, Rector de la Universidad ECOTEC, el director ejecutivo es el Dr. Vicente Taiano. El responsable de seguridad para los fines del presente documento es el Sr. Edwin Galindo, Jefe de Seguridad, quien lidera el equipo encargado de la implementación de políticas, procedimientos y sistemas de gestión de riesgos, conforme a los lineamientos institucionales y normativas nacionales.

3.1.3. Actividades de la Organización

La Universidad ECOTEC desarrolla actividades académicas, administrativas, investigativas, de extensión y de vinculación con la comunidad. Estas actividades implican el uso intensivo de información personal, infraestructura tecnológica y espacios físicos que pueden estar expuestos a riesgos naturales, tecnológicos y antrópicos, los cuales deben ser identificados, evaluados y controlados.

3.1.4. Tratamiento de la Organización y sus Riesgos

La Universidad Tecnológica ECOTEC, en su calidad de responsable del tratamiento de datos personales, ejecuta diversas actividades académicas, administrativas, investigativas, de vinculación con la sociedad y de gestión operativa, que conlleva el manejo intensivo de información personal, financiera, laboral y sensible de múltiples actores: estudiantes, aspirantes, docentes, personal administrativo, proveedores, contratistas y visitantes. Estas actividades se desarrollan tanto en entornos físicos como digitales, mediante el uso de plataformas institucionales, software de gestión, correo institucional, registros físicos y sistemas de videovigilancia.

Tipos de tratamientos realizados

Los tratamientos de datos se ejecutan a través de medios automatizados (software, correo interno, plataformas digitales) y no automatizados (bitácoras físicas, kardex impresos), incluyendo procesos como recolección, almacenamiento, consulta, modificación, transferencia, eliminación y análisis. Entre los principales tratamientos destacan:

- Estudiantes y aspirantes: gestión de admisiones, matrícula, becas, seguimiento académico y bienestar estudiantil. Se manejan datos identificativos, académicos, financieros, de salud (en casos específicos) y sensibles como discapacidad.
- Docentes y personal administrativo: se gestiona información contractual, académica, financiera y biométrica (huella digital para control de acceso), además de datos de desempeño y evaluaciones.

- Trabajadores operativos (limpieza, seguridad, mantenimiento): administración de horarios, funciones, seguridad y control de asistencia, con registros físicos, fotográficos y de videovigilancia.
- Proveedores y contratistas: tratamiento de información identificativa, legal y financiera para procesos de contratación y cumplimiento de obligaciones contractuales.
- Visitantes: registros en bitácoras vehiculares y peatonales de acceso al campus.
- Videovigilancia: captura de imágenes y audio en tiempo real en accesos, aulas, espacios comunes y zonas estratégicas, para fines de monitoreo y seguridad institucional.
- Hojas de vida y procesos de selección: recopilación de datos laborales, formativos y referencias de aspirantes en procesos de talento humano.

Riesgos derivados del tratamiento de la información

A partir de las actividades antes descritas, la universidad se expone a diversos riesgos institucionales, especialmente vinculados a la protección de datos personales y a la seguridad de la información. Estos riesgos afectan la confidencialidad, integridad, disponibilidad y legalidad del tratamiento, y podrían repercutir en la reputación institucional y la confianza de sus usuarios. Los principales riesgos identificados son:

Tabla 2.

Riesgos derivados del tratamiento de la información

Grupo de datos tratados	Riesgos identificados	Impacto	Probabilidad	Tratamiento propuesto
Estudiantes y aspirantes	Pérdida o alteración de datos académicos, fuga de información personal, suplantación de identidad.	Alto	Media	Doble autenticación, políticas de acceso, encriptación, capacitación al personal.
Docentes y administrativos	Fugas de datos laborales, acceso no autorizado, alteración de evaluaciones o historial contractual.	Alto	Media	Segmentación de acceso, acuerdos de confidencialidad, control de permisos.
Videovigilancia	Acceso indebido a imágenes, uso no autorizado, almacenamiento sin protección adecuada.	Medio	Alta	Consentimiento informado, control de accesos, cifrado de archivos, monitoreo continuo.
Proveedores y contratistas	Exposición de información contractual, uso fuera del alcance permitido, tratamiento no regulado.	Medio	Baja	Inclusión de cláusulas contractuales, revisión periódica, plataformas seguras.
Personal operativo y visitantes	Exposición injustificada de datos, uso indebido de registros físicos o grabaciones, pérdida de bitácoras.	Medio	Media	Protocolos de tratamiento físico, almacenamiento seguro, digitalización y custodia.

Candidatos en procesos de selección	Uso sin consentimiento de hojas de vida, conservación indebida de información.	Medio	Media	Políticas de retención de datos, eliminación segura, gestión documentaria controlada.

Nota. Los datos presentados en esta tabla corresponden a los riesgos asociados al tratamiento de información en distintas áreas de la Universidad ECOTEC. Las propuestas de tratamiento incluidas están alineadas con las mejores prácticas de seguridad de la información, con el objetivo de mitigar los impactos negativos de los riesgos identificados y garantizar la protección de los datos personales y académicos, conforme a las normativas nacionales e internacionales sobre protección de datos y privacidad.

3.1.5. Consentimientos y Notas Informativas

CONSENTIMIENTO INFORMADO ESTUDIANTES
CONSENTIMIENTO INFORMADO PARA EL TRATAMIENTO DE DATOS PERSONALES Y USO DE IMAGEN
UNIVERSIDAD TECNOLÓGICA ECOTEC

Yo, ……, con cédula de ciudadanía N.º…… , estudiante de la Universidad Tecnológica ECOTEC, declaro haber sido informado/a sobre el tratamiento de mis datos personales, conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP), y en relación con los siguientes aspectos:

1. Tratamiento obligatorio de datos personales

Autorizo el tratamiento de mis datos personales (identificativos, académicos, de contacto, financieros y de salud si aplica) por parte de la Universidad, para las siguientes finalidades:

Proceso de admisión, matrícula, gestión académica, administrativa y financiera.

Gestión de plataformas educativas y correo institucional.

Evaluaciones, tutorías, seguimiento académico y actividades complementarias.

Cumplimiento de obligaciones legales y reglamentarias.

Este tratamiento es obligatorio para mantener mi vínculo académico con la institución.

2. Tratamiento opcional – uso de imagen y voz

Conforme a la normativa vigente, el uso de mi imagen, voz o grabaciones para fines institucionales y de difusión requiere mi consentimiento expreso y específico.

Marque si autoriza el siguiente tratamiento opcional:

☐ Autorizo a la Universidad ECOTEC a usar mi imagen y/o voz en redes sociales institucionales (Facebook, Instagram, YouTube, etc.)

☐ Autorizo el uso de mi imagen y/o voz en la página web oficial de la Universidad

☐ Autorizo el uso de mi imagen en materiales internos (boletines, eventos, murales digitales)

Este consentimiento es voluntario. No afecta mi condición de estudiante.

3. Videovigilancia

Fui informado/a que las instalaciones de la Universidad cuentan con sistemas de videovigilancia con fines de seguridad institucional. Estos sistemas operan bajo lo establecido en la LOPDP. La existencia de cámaras está debidamente señalizada mediante cartelería visible en los accesos al campus.

4. Información adicional sobre protección de datos

Responsable del tratamiento: Universidad Tecnológica ECOTEC

Finalidad del tratamiento: Académica, administrativa, institucional y de difusión (cuando aplique)

Plazo de conservación: Durante la vigencia de la relación académica y los plazos legales aplicables

Ejercicio de derechos: Acceso, rectificación, oposición, supresión y portabilidad.

Contacto del delegado de Protección de Datos: [correo electrónico institucional]

Fecha: dd/mm/aa

Firma del estudiante: CI

3.2. Registro de Actividades de Tratamiento

En esta Universidad aún no se ha implementado el RAT, ya que el tratamiento de la información se la realiza únicamente a nivel interno, sin embargo, han mostrado su interés en generar un documento donde se especifique el tratamiento de los datos, los usuarios y la finalidad de su uso.

3.2.1. Grupos de Información.

En la Universidad Tecnológica ECOTEC se identifican los siguientes grupos de información, atendiendo a la naturaleza del vínculo con la institución y al tipo de datos personales tratados:

- **Estudiantes y Aspirantes**

Datos tratados: Identificación (nombres, cédula/pasaporte), edad, contacto, historial académico, situación socioeconómica, datos de financiamiento, imagen, voz, firma, documentos escaneados.

Finalidad: Admisión, matrícula, seguimiento académico, comunicación institucional, acceso a plataformas virtuales, gestión de becas y análisis institucional.

Riesgos: Acceso no autorizado, suplantación de identidad, alteración de registros académicos, uso indebido de imagen.

- **Docentes y personal administrativo**

Datos tratados: Identificación, historial laboral y académico, contratos, evaluaciones, datos bancarios, imagen y voz.

Finalidad: Gestión de talento humano, nómina, desempeño, asignaciones académicas, gestión documental.

Riesgos: Fugas de información sensible, manipulación de datos, acceso no autorizado a cuentas institucionales.

- **Personal operativo y logístico (limpieza, seguridad, mantenimiento, mensajería)**

Datos tratados: Identificación, contacto, datos laborales, registros de asistencia, control de ingreso, registros de videovigilancia, uniforme, zonas de acceso.

Finalidad: Administración del personal, control de funciones, seguridad institucional.

Riesgos: Uso indebido de imágenes, exposición injustificada, pérdida de documentos físicos.

- **Departamento contable y financiero**

Datos tratados: Información financiera, datos de proveedores, contratos, facturación, transferencias bancarias, comprobantes de pago, RUC, contacto.

Finalidad: Gestión contable, cumplimiento tributario, pagos y contratos.

Riesgos: Filtración de datos bancarios, mal uso de información tributaria.

- **Proveedores y contratistas**

Datos tratados: Identificación legal, datos de contacto, datos bancarios, RUC, contratos, credenciales de acceso, cumplimiento de servicios.

Finalidad: Contratación, cumplimiento de servicios, pagos, control de ingreso a instalaciones.

Riesgos: Exposición indebida, acceso sin autorización, uso no previsto de sus datos.

- **Candidatos (hojas de vida)**

Datos tratados: Datos personales, formación académica, experiencia laboral, referencias, documentos adjuntos (cédula, certificados, etc.).

Finalidad: Procesos de selección de personal, evaluación de perfiles.

Riesgos: Conservación indebida, uso sin consentimiento, acceso no autorizado.

- **Videovigilancia**

Datos tratados: Imágenes y video en tiempo real de estudiantes, docentes, visitantes, trabajadores y proveedores.

Finalidad: Seguridad institucional, control de accesos, prevención de incidentes.

Riesgos: Uso indebido de imágenes, falta de control en el almacenamiento, reproducción no autorizada.

3.2.2. Sistemas de Tratamientos y Niveles de Seguridad.

Los sistemas de tratamiento que maneja la universidad se dividen en:

- Bitácoras escritas
- Kardex impresos
- Correo interno
- Software de gestión de información de la universidad.

Tabla 3.

Sistemas de tratamientos y niveles de seguridad

Sistema	Función	Datos principales tratados	Responsable	Nivel de seguridad	Medidas de tratamiento
Bitácoras escritas	Documentación de procesos, auditorías y mejoras continuas	Actividades de profesores, alumnos y administrativos	Área administrativa	Media	Registro legible con hojas numeradas y escritura clara.
Kárdex impresos	Control de costos, facturación e inventario	Datos de profesores, alumnos, clientes y proveedores	Dirección de contabilidad	Alta	Descripción detallada, almacenamiento restringido y acceso protegido.
Correo interno	Comunicación institucional entre áreas, tanto interna como externa	Datos personales verificados	Área de gestión documental	Alta	Antivirus, seguimiento de actividad, notificación de cambios.
Software de gestión de información	Gestión técnica de accesos y respaldo de información legal	Respaldos, documentos oficiales con validez institucional	Departamento de Sistemas	Alta	Monitoreo de accesos, contraseñas seguras, copias de respaldo con posibilidad de recuperación.

Nota. La tabla muestra los sistemas de tratamiento utilizados en la Universidad Tecnológica ECOTEC, describiendo su función, los datos principales tratados, el responsable de cada sistema, el nivel de seguridad asociado y las medidas de tratamiento implementadas para garantizar la protección de los datos y la eficiencia operativa.

Los niveles de seguridad de cada sistema de tratamiento de información son diferentes. Mediante una clasificación de cada uno de los niveles de riesgo ordenados de bajo, medio y alto.

Datos Sensibles: Alto - Información contable oficial de cada estudiante y condiciones de salud del personal y alumnos internos.

Datos identificativos: Medio - dirección vial online, datos personales y profesionales.

Datos de contacto: Bajo - Registro telefónico, correos electrónicos que son visualizados externamente.

Bitácoras y los kardex se designa un custodio de seguridad que en este caso es el encargado de registrar la información y proteger los datos, estos datos son almacenados en archivadores que reposan en la garita de acceso y cuyas llaves únicamente se relevan entre los custodios de turno.

Para el correo interno y el software de gestión de información de la Universidad en cambio se almacena en un servidor con sus respectivos respaldos y cuyo acceso es registrado automáticamente cada vez que acceden al sistema con su usuario y contraseña.

Cabe indicar que los responsables del tratamiento de datos, quienes tienen acceso a categorías de datos específicas deben mantener la reserva y el cuidado de los datos y son los únicos responsables de que estos no sean vulnerados y usados para fines distintos para los que fueron recolectados. Por ejemplo, de existir un delito dentro de la Universidad se debe otorgar el consentimiento el Señor Rector a través de la Jefe Administrativa, o por disposición de autoridad competente, siendo los únicos responsables del manejo de las

imágenes y de la información recopilada y siendo los mismos de eliminar la información en base a la normativa de protección de datos personales, la cual para su destrucción debe ser autorizada en base un proceso certificado el cual pueda dar una credibilidad que la información eliminada no tendrá ninguna recuperación absoluta, registrando la fecha, hora y el responsable del área técnica de haber dado de baja su información de la red.

3.2.3. Finalidades, categorías de datos, de interesados y de destinatarios.

Finalidades del tratamiento

Los datos personales son gestionados en la Universidad ECOTEC para las siguientes finalidades específicas:

- ✓ Gestión académica y administrativa del estudiante.
- ✓ Prestación del servicio educativo.
- ✓ Facturación, pagos, trámites contables y cumplimiento legal.
- ✓ Gestión del talento humano.
- ✓ Seguridad institucional (acceso, vigilancia, control).
- ✓ Publicidad institucional (imagen y voz con consentimiento).
- ✓ Evaluación de candidatos en procesos de selección.
- ✓ Comunicación institucional y marketing (previo consentimiento).

Categorías de datos tratados

- ✓ Datos identificativos (nombre, cédula, contacto, firma).
- ✓ Datos académicos (historial, calificaciones, matrícula).
- ✓ Datos financieros (métodos de pago, cuentas bancarias, RUC).

- ✓ Datos biométricos (imagen, voz, videovigilancia).
- ✓ Datos laborales (contratos, roles de pago, experiencia).
- ✓ Datos sensibles (discapacidad, salud –si aplica–).

Categoría de interesados

- ✓ El propio titular de los datos (estudiantes, docentes, proveedores, trabajadores).
- ✓ Representantes legales (en caso de menores o tutores)
- ✓ Postulantes (proporcionan sus datos en procesos de selección).

Categoría de destinatarios de datos

- ✓ Administraciones públicas (Ministerio de Educación, SENESCYT, SRI).
- ✓ Entidades financieras (para procesos de pago)
- ✓ Aseguradoras (en caso de cobertura institucional)
- ✓ Empresas de seguridad y videovigilancia contratadas
- ✓ Proveedores tecnológicos (mantenimiento de software o plataformas).
- ✓ Plataformas de marketing y redes sociales (previo consentimiento del titular).

3.2.4. Encargados de Tratamientos

La Universidad Tecnológica ECOTEC puede designar tanto a personal interno como a proveedores externos como encargados del tratamiento de datos personales, exclusivamente para el cumplimiento de los fines legítimos establecidos en sus procesos académicos, administrativos, contables, legales y de seguridad.

Cada uno de los encargados, sean personas naturales o jurídica, deberá cumplir con lo dispuesto en la Ley Orgánica de Protección de Datos Personales (LOPDP), y está obligado a suscribir acuerdos de confidencialidad y cláusulas específicas de protección de datos, garantizando así un tratamiento seguro, lícito y proporcional.

A continuación, se detalla el listado actualizado de los encargados del tratamiento y la materia del servicio prestado:

Tabla 4.

Encargados de tratamiento

ENCARGADO	TIPO	MATERIA DE SERVICIO	TRATAMIENTO DE DATOS ASOCIADO
Corporación de Seguridad GER	Externo	Monitoreo y control de accesos	Captura y gestión de imágenes, registro biométrico
Empresa proveedora de software institucional	Externo	Plataforma académica, correo, gestión educativa	Registro, procesamiento y acceso a datos académicos y personales
Asesoría contable externa	Externo	Contabilidad y tributación	Manejo de nómina, contratos de proveedores, pagos, SRI
Proveedor de hosting y servicios en la nube	Externo	Almacenamiento y respaldo digital	Datos académicos, administrativos y financieros almacenados en la nube
Proveedor de servicios de RRHH	Externo	Reclutamiento y selección	Tratamiento de hojas de vida, historial laboral y profesional
Proveedor de mantenimiento técnico	Externo	Mantenimiento de equipos y red	Acceso ocasional a equipos con datos internos (bajo supervisión)

Nota. La tabla describe los encargados del tratamiento de datos personales en la Universidad Tecnológica ECOTEC, tanto internos como externos, detallando las materias del servicio prestado y el tratamiento de datos asociado a cada uno. Estos encargados cumplen con la Ley Orgánica de Protección de Datos Personales (LOPDP) y están sujetos a acuerdos de confidencialidad para garantizar la protección y el tratamiento adecuado de la información personal.

3.3. Registro de Dispositivos (Dispositivos Digitales)

Como parte del cumplimiento de los principios de seguridad, responsabilidad proactiva y minimización de riesgos, 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.

Tipos de dispositivos digitales registrados:

- ✓ Computadores de escritorio (sobremesa): utilizados principalmente por personal administrativo y departamentos académicos para la gestión documental, correos institucionales, bases de datos y plataformas de matrícula.

- ✓ Computadoras portátiles (laptops): asignadas a personal docente, directivos y administrativos para trabajo remoto o trabajo móvil institucional.
- ✓ Tablets y dispositivos móviles institucionales: empleados en actividades de control, inspección, vinculación comunitaria y ciertos servicios académicos.
- ✓ Dispositivos móviles personales: pueden ser utilizados por el personal bajo políticas de uso autorizado, con conexión controlada a redes internas (BYOD - Bring Your Own Device).
- ✓ Servidores físicos y virtuales: que alojan sistemas institucionales, bases de datos académicas y administrativas, plataformas LMS y backups.
- ✓ Cámaras de videovigilancia: instaladas estratégicamente en campus, aulas, accesos y zonas comunes, gestionadas a través de software centralizado de monitoreo.
- ✓ Software y plataformas en la nube: herramientas como correo institucional, sistemas académicos, almacenamiento en la nube, sistemas de gestión documental, videoconferencias y evaluación en línea.

Gestión del registro y monitoreo:

Cada dispositivo cuenta con un registro único por modelo, código y número de serie, desde el momento de su activación. Este registro permite un rastreo continuo y confiable del uso, supervisado exclusivamente por personal autorizado de la institución.

En caso de reasignación de dispositivos a nuevos usuarios, se realiza una actualización de credenciales, así como el correspondiente cambio en la base de datos interna del sistema de gestión de activos tecnológicos.

Para dispositivos como cámaras de seguridad, el software institucional permite su bloqueo, activación o desactivación remota desde el servidor central. En el caso de dispositivos móviles (como celulares o tablets), estos pueden ser administrados de forma remota desde otras terminales, permitiendo la desactivación o localización en caso de pérdida o uso indebido.

La institución no permite configuraciones externas ni accesos no autorizados, asegurando que el uso de cada dispositivo sea consentido y registrado por la Universidad, bajo protocolos internos de control y trazabilidad.

3.4. Registro de Sistemas de Información

La Universidad ECOTEC, en su rol de responsable del tratamiento de datos personales, emplea diferentes sistemas de información tanto físicos como electrónicos para asegurar la gestión eficiente y segura de los datos de su comunidad universitaria. Estos sistemas permiten realizar tratamientos de datos conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP) y están asociados a diferentes niveles de seguridad dependiendo de la sensibilidad de los datos tratados.

A continuación, se describen los principales sistemas de información empleados en la institución:

Tabla 5.

Sistemas de Información en Ecotec

Sistema	Función	Datos principales tratados	Responsable	Nivel de seguridad	Medidas de tratamiento
Sistema de gestión académica (SGA)	Matriculación, gestión de calificaciones y registros estudiantiles	Datos personales, académicos, financieros y sensibles (ej. discapacidad)	Departamento Académico	Alta	Políticas de acceso, autenticación, encriptación y respaldo diario.
Plataforma virtual (Moodle/LMS)	Gestión del aprendizaje, tareas, evaluaciones y comunicación docente-estudiante	Datos académicos, participaciones, archivos entregados	Coordinación Académica	Media	Acceso restringido con usuario/clave, monitoreo básico.
Sistema de videovigilancia (VMS)	Seguridad y monitoreo de instalaciones	Imágenes, video, audio y reconocimiento facial	Departamento de Seguridad Institucional	Muy alta	Encriptación, geocercas, tokens, control de accesos.
CRM de admisiones	Seguimiento de aspirantes y procesos de inscripción	Datos personales, académicos previos, financieros y de contacto	Departamento de Admisiones	Media	Sistema cerrado con acceso segmentado.
Sistema de proveedores y contratistas	Registro y control de servicios externos y cumplimiento contractual	Datos financieros, legales, de contacto e identificativos	Dirección Administrativa / Jurídica	Alta	Cláusulas de confidencialidad, acceso seguro, monitoreo de cumplimiento.

Sistema de selección y currículums	Gestión de procesos de selección de personal	Hojas de vida, historial académico, referencias personales, resultados de pruebas	Dirección de Talento Humano	Media	Protección física y digital, eliminación segura de documentación no vigente.

Nota. La tabla describe los sistemas de información utilizados en la Universidad Tecnológica ECOTEC para el tratamiento de datos personales en conformidad con la Ley Orgánica de Protección de Datos Personales (LOPDP). Cada sistema se clasifica según el nivel de seguridad requerido, las medidas de tratamiento implementadas y los datos principales tratados, garantizando la protección adecuada de la información de la comunidad universitaria.

Utilizan el sistema SAUE para el control y seguimiento académico de los estudiantes, adicional utiliza sistemas operativos de Windows Server y Office actualizados, para gestionar sus sistemas informáticos, incluyendo el portal web, el sistema financiero, sistema de admisiones, sistemas de cobros y pagos y de registros de carreras. Mensualmente actualizan los parches de seguridad.

La política de gestión de actualizaciones va acorde a las disposiciones que emite el Director de sistemas y lo hace sin un cronograma establecido, es decir a veces lo hace mensualmente otras veces trimestralmente, dependiendo las necesidades.

3.5. Registro Personal

3.5.1. Con Acceso a Datos

El personal responsable del tratamiento de datos que tiene acceso a datos es el siguiente:

En la Universidad ECOTEC existe personal que tiene acceso a los datos personales y sensibles según sus funciones. El acceso está vinculado directamente a sus responsabilidades y al área en la que desempeñan sus labores:

Tabla 6.

Personal con acceso a datos

Área / Departamento	Puesto de trabajo	Tipo de datos a los que accede	Cantidad de personas con acceso
Departamento de Sistemas	Administrador de sistemas	Credenciales de usuarios, logs de actividad, respaldos, bases de datos.	3
Dirección de Talento Humano	Analista de personal	Datos personales, contractuales, académicos y médicos del personal.	2
Dirección Académica	Coordinador académico	Datos académicos de docentes y estudiantes.	3
Secretaría General	Secretaria académica	Historial académico, datos de matrícula, certificados.	2
Dirección Administrativa	Responsable de proveedores	Datos financieros, legales y de contacto de contratistas y proveedores.	1
Gestión Documental	Encargado de archivo físico/digital	Currículos, documentos de identidad, contratos, hojas de vida.	1

Departamento de Seguridad	Jefe de seguridad	Videovigilancia, bitácoras, imágenes y registros de accesos	1
Departamento Financiero	Contador general / analista contable	Datos bancarios, nóminas, facturación de estudiantes y proveedores	2
Coordinación de Admisiones	Técnico de admisiones	Datos personales y académicos de aspirantes	2

Nota. La tabla presenta el personal de la Universidad Tecnológica ECOTEC con acceso a datos personales y sensibles, detallando los puestos de trabajo, los tipos de datos a los que tienen acceso y la cantidad de personas con acceso a cada tipo de información. Estos datos están organizados según las funciones y responsabilidades de cada área, garantizando que el acceso sea adecuado y conforme a las normativas de protección de datos vigentes.

Tabla 7.

Nómina de empleados con acceso a datos

DEPARTAMENTO	NOMBRE Y APELLIDO DEL RESPONSABLE	NUMERO DE EMPLEADOS
ADMISIONES	Eileen Anchundia	Srta. Victoria Lindao
FINANCIERO	Srta. Jhazming Medina	Sr. Jonathan Hurtado
SISTEMAS	Tlgo. José Gómez	Sr. Gabriel Miranda
SEGURIDAD	Sr Edwin Galindo y Luis Mera	
RECURSOS HUMANOS	Abg. Patricia Bodero	Lcda.Katty Feijó
BAR	Sr Nayev Tannouri	Sr. Carlos Castillo
GYM	Lcdo. Maven Barrios	Sr. José Pizco
ASEO	Sr. Robert Gonzáles	Sr. Sergio Ortega

BODEGA	Sr Robert Gonzáles	Sr. Jesús Obando
ARCHIVO	Srta. Emily Graziani	00
DIRECCIÓN ACADÉMICA	Srta. Daniela Ayala	00
DIRECCIÓN EJECUTIVA	Sr. Julio Álvarez	Srta. Nicole Megía
RECTORADO	Dr. Vicente Taiano	Ingreso. Katherine Badillo
JURÍDICO	Abg. Daniela Ayala	Srta. Erika Echeverria
RECEPCIÓN	Srta. Eileen Anchundia	Srta. Victoria Lindao

Nota. La tabla muestra la nómina de empleados con acceso a datos personales y sensibles en diversas áreas de la Universidad Tecnológica ECOTEC, detallando los nombres de los responsables y la cantidad de empleados por departamento. Esta información es clave para garantizar que el acceso a los datos esté debidamente autorizado y controlado conforme a las normativas de protección de datos personales y la ley vigente.

3.5.2. Sin Acceso a Datos.

El personal que no accede a datos personales o sensibles dentro de la Universidad ECOTEC, ya que estos cargos están relacionados con funciones operativas, logísticas o de soporte, por lo cual no requieren tratamiento de información sensible.

Tabla 8.

Personal sin acceso a datos

Área / Departamento	Puesto de trabajo	Acceso a datos personales/sensibles	Justificación	Cantidad de personas

Seguridad	Guardia / Apertura de plumas	No	Control de acceso físico sin manipulación de información.	4
Limpieza	Auxiliar de limpieza	No	Actividades de aseo sin contacto con bases de datos.	6
Alimentación	Personal de bar y cocina	No	Preparación y atención alimentaria sin tratamiento de datos.	3
Deportes / Bienestar	Instructor deportivo / gimnasio	No	Actividades físicas sin uso de información personal.	2
Áreas verdes	Jardinero	No	Labores de jardinería sin intervención en procesos digitales.	2
Mensajería	Mensajero motorizado	No	Entrega de documentos sin acceso a contenido.	1
Mantenimiento	Técnico de mantenimiento	No	Reparaciones técnicas sin contacto con sistemas informáticos.	3
Logística	Personal de carga y descarga	No	Actividades físicas sin manipulación de datos.	2

Nota. La tabla muestra el personal que no tiene acceso a datos personales o sensibles dentro de la Universidad Tecnológica ECOTEC, detallando los departamentos, los puestos de trabajo, y la justificación de su exclusión en el tratamiento de datos. Estos empleados realizan tareas específicas que no requieren el manejo de información confidencial, lo que asegura el cumplimiento de las políticas de protección de datos de la institución.

3.5.3. Accesos Físicos

La gestión de accesos físicos en la universidad es un tema clave para garantizar la seguridad y el funcionamiento adecuado de las instalaciones.

Accesos con Llaves

Las llaves deben estar bajo control y distribución estricta para evitar pérdidas o accesos no autorizados. Las personas que generalmente tienen llaves de los departamentos o áreas son:

Tabla 9.

Personal con llaves de las instalaciones

ÁREA O DEPARTAMENTO	NOMBRE Y APELLIDO DEL ENCARGADO
EDIFICIO PRINCIPAL	Sr. Robert Gonzáles
PUERTAS DE ACCESO AL COMPLEJO UNIVERSITARIO	Sr. José Pizco
PUERTAS DEL PARQUEADERO	Agentes de seguridad VIGSEPE-GER
COMPLEJO DEPORTIVO	Sr. José Pizco
AULAS	Sr Sergio Ortega
CUARTO DE MONITOREO	No existe
BODEGA	Sr. Jesús Obando

Nota. La tabla detalla el personal encargado de las llaves de diferentes áreas en las instalaciones de la Universidad Tecnológica ECOTEC, resaltando la importancia de mantener un control estricto sobre el acceso a cada área. El manejo adecuado de las llaves contribuye a la seguridad institucional, garantizando que los accesos a las zonas sensibles estén restringidos y bajo supervisión.

3.6. Registro de Prestadores de Servicios

3.6.1. Con Acceso a Datos Catalogados

Tabla 10.

Con acceso a datos catalogados

ÁREA	PUESTO O CARGO	NOMBRE	CONDICIÓN	ACCESO A LA INFORMACIÓN
SISTEMAS	TÉCNICO DE SOPORTE EXTERNO		Encargado de Tratamiento	SÍ (Sistemas y bases de datos)
PLATAFORMA VIRTUAL	SOPORTE MOODLE	Ing. Pablo Zambrano	Encargado de Tratamiento	SÍ (Datos académicos)
TALENTO HUMANO (OUTSOURCING)	PROVEEDOR DE NÓMINA		Encargado de Tratamiento	SÍ (Datos laborales y financieros)
JURÍDICA / ADMINISTRACIÓN	ASESOR LEGAL EXTERNO	Ab. Mariana Cedeño	Encargado de Tratamiento	SÍ (Datos contractuales)
CONSULTORÍA EXTERNA	AUDITOR / ASESOR EN PROTECCIÓN DE DATOS		Encargado de Tratamiento	SÍ (Datos sensibles en auditorías)

Nota. La tabla presenta al personal con acceso a datos catalogados en la Universidad Tecnológica ECOTEC, detallando su puesto, la condición de encargado del tratamiento y los tipos de información a los que tienen acceso. Es fundamental que este personal siga los lineamientos establecidos por la Ley Orgánica de Protección de Datos Personales (LOPDP) y las políticas internas de seguridad de la institución, garantizando el manejo adecuado de los datos sensibles y personales en cumplimiento con las normativas vigentes.

3.6.2. Sin Acceso a Datos Catalogados.

Tabla 11.

Sin acceso a datos catalogados

ÁREA	PUESTO O CARGO	ACCESO A LA INFORMACIÓN
SEGURIDAD	APERTURA DE PLUMAS	NO
CONSERJE	APERTURA DE PUERTAS	NO
AUXILIAR DE LIMPIEZA	ASEO	NO
BAR	COCINERO	NO
GYM	VARIOS SERVICIOS	NO
ÁREAS VERDES	JARDINERO	NO
ADMINISTRATIVA	MENSAJERO MOTORIZADO	NO

Nota. La tabla muestra el personal que no tiene acceso a datos catalogados en la Universidad Tecnológica ECOTEC. Estas personas desempeñan funciones operativas, como seguridad, limpieza, cocina y mantenimiento, y no están involucradas en el tratamiento de información sensible o personal. Es esencial que este personal también siga las políticas de seguridad institucional para garantizar que no haya acceso no autorizado a los datos.

3.7. Sistemas de Captación de Imágenes y Audio

La Universidad Tecnológica ECOTEC cuenta con un sistema de videovigilancia (CCTV) estructurado mediante cámaras tipo bullet, domo y PTZ. Este sistema está diseñado para cumplir funciones de seguridad, control de accesos y protección de la integridad física de la comunidad universitaria.

El sistema permite la captación de imágenes y audio mediante cámaras equipadas con micrófono y altavoz, cuyas funcionalidades están limitadas exclusivamente a situaciones de control y vigilancia activa, la grabación de sonido no se realiza de forma generalizada ni continua, y su activación está justificada únicamente para:

- Proporcionar alertas auditivas en tiempo real ante comportamientos de riesgo detectados por el sistema analítico.
- Comunicarse con personas en zonas restringidas como parte de las funciones de control de ingreso o atención en emergencias.
- Responder a eventos en tiempo real, como intrusiones detectadas, disuasión mediante voz o activación remota de seguridad.

Todos los archivos generados (imágenes, video y, en los casos justificados, audio) son almacenados en servidores protegidos, bajo mecanismos de cifrado y autenticación mediante tokens de seguridad con accesos limitados únicamente al personal autorizado.

El sistema incorpora tecnología de reconocimiento facial, cuyo uso está limitado al control de ingreso a zonas específicas del campus (como laboratorios, áreas administrativas o

centros de datos) y a la identificación de personas no autorizadas en el campus, garantizando que dicho tratamiento se ajusta a los principios de licitud, proporcionalidad y minimización.

3.7.1. Número de Cámaras

En la Universidad existen 86 cámaras distribuidas en diferentes áreas y departamentos:

Para entender mejor cómo se distribuyen las cámaras, a continuación, se desglosa el total por tipo de cámara en cada área:

- 7 cámaras para los accesos
- 79 cámaras para áreas administrativas, complejo deportivo, áreas comunes y parqueaderos.

Tabla 12.

Número de cámaras por áreas, Ecotec

ÁREA/DEPARTAMENTO	N° CAMARAS BULLET	N° CAMARAS DOMO	N° CAMARAS PTZ
COMPLEJO DEPORTIVO	16 HIKVISION		
GYM		08 DOMO	
TORNIQUETE GYM		02 DOMO	
PARQUEADERO			01 PTZ
BAR		01 DOMO	
EXTERIORES DEL PARQUEADERO	10 ANÁLOGAS		
PARQUEADERO 1			01 PTZ
GARITA PRINCIPAL		03 DOMO	

AMBIENTE PARÍS	02 ANÁLOGAS	
INGRESO DEP. MÉDICO	01 ANÁLOGA	
PASILLO AULAS PLANTA BAJA	05 ANÁLOGAS	
LABORATORIO FORENSE	01 ANÁLOGA	
AULAS 102, 108,202,205,206	05 ANÁLOGAS	
LABORATORIO 1	01 ANÁLOGA	
SALA DE ESTRADO	01 ANÁLOGA	
ZONA DE JUEGOS (PLAY)	01 ANÁLOGA	
AULA COSTA	01 ANÁLOGA	
SIMULACIÓN VIRTUAL	01 ANÁLOGA	
SALA DE JUEGOS	01 ANÁLOGA	
RECEPCIÓN	03 ANÁLOGAS	
PASILLO AULAS PLANTA ALTA		04 DOMO
INGRESO AL COMEDOR	01 ANÁLOGA	

Nota. La tabla muestra la distribución del sistema de videovigilancia en la Universidad Tecnológica ECOTEC, que consta de 86 cámaras en total, distribuidas entre cámaras bullet, domo y PTZ, según el área correspondiente. Las cámaras se encuentran ubicadas en áreas clave como el complejo deportivo, parqueaderos, pasillos de aulas, y otros espacios críticos de la universidad, con el fin de garantizar la seguridad tanto de los estudiantes como del personal administrativo. Las cámaras de tipo PTZ (Pan-Tilt-Zoom) y domo permiten un mayor control y cobertura en áreas específicas, mientras que las cámaras analógicas, que predominan en algunas zonas, brindan vigilancia continua.

3.7.2. Zonas de Influencias.

Las cámaras están ubicadas estratégicamente en accesos principales, pasillos, parqueaderos, aulas, laboratorios, auditorios, cafeterías, áreas verdes y zonas deportivas. Esto permite un monitoreo integral del entorno universitario, garantizando protección y seguimiento ante cualquier eventualidad, estas cámaras también cuentan con un sistema infrarrojo que permite el monitoreo nocturno, generando geocercas con detección de movimiento y mapas de calor para la detección de personas que accedan por sitios no autorizados.

3.7.3. Sistema de Tratamiento y Almacenamiento

La Universidad Tecnológica ECOTEC implementa un sistema mixto para el tratamiento de datos personales, utilizando tanto archivos electrónicos como físicos. Estos datos son gestionados por las unidades correspondientes de acuerdo con protocolos internos rigurosos que aseguran su seguridad, integridad y confidencialidad, cumpliendo con las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP) y su reglamento. Estos protocolos están alineados con las mejores prácticas internacionales en cuanto a la protección de datos personales, asegurando que los datos se manejen de manera responsable y conforme a la normativa vigente.

En cuanto al plazo de conservación, la universidad sigue una política oficial que establece que los datos personales serán conservados solo por el tiempo necesario para cumplir con los fines para los cuales fueron recolectados. Esta política se basa en el principio de minimización de datos, lo que implica que no se almacenarán datos por períodos más largos de lo estrictamente necesario. Una vez cumplidas las finalidades para las que se

recolectaron los datos, y en ausencia de una obligación legal de conservación, los datos serán eliminados, anonimizados o bloqueados conforme a los procedimientos internos establecidos por la universidad.

Es importante destacar que, para los datos utilizados con fines comerciales, estos solo serán conservados mientras el titular no revoque su consentimiento. Esta medida garantiza que los derechos de los titulares sean respetados y que su consentimiento sea gestionado de manera adecuada, conforme a las disposiciones legales sobre protección de datos personales.

En el caso de las imágenes obtenidas a través del sistema de videovigilancia, estas son almacenadas por un período aproximado de 20 días. Sin embargo, si existen circunstancias que justifiquen una retención más prolongada, como un proceso investigativo o judicial, las imágenes podrán ser conservadas por un período mayor. Esta práctica está en línea con las recomendaciones sobre la seguridad y el tratamiento de datos sensibles, tal como se establece en la normativa correspondiente.

3.7.4. Usuarios Autorizados

Tabla 13.

Usuarios Autorizados

Puesto	Nombre	Nivel de acceso
Jefe de Seguridad	Sr. Edwin Galindo	Operativo y Videovigilancia
Jefe Administrativa	Ing. Pamela Portilla	Administrativo y Base de Datos
Gerente de Seguridad	Crnl. Rodrigo Braganza	Operativo, Administrativo y Base de Datos
Monitoristas	Personal Corporación GER	Operativo

Nota: La tabla detalla los usuarios autorizados para acceder a los sistemas de la Universidad ECOTEC, de acuerdo con sus roles y niveles de acceso específicos.

3.8. Dispositivos. Medidas de seguridad

3.8.1. Análisis de las Medidas de Seguridad de los Dispositivos

a) Dispositivos utilizados.

En la Universidad ECOTEC se utilizan ordenadores de escritorio, laptops, celulares institucionales, tablet, dispositivos GPS (en vehículos y para control de seguridad), así como cámaras conectadas a servidores. Todos estos dispositivos están asignados a áreas específicas y se utilizan para actividades administrativas, académicas, operativas y de seguridad.

b) Ordenadores con acceso a información.

Los ordenadores están asignados según el puesto de trabajo. Por ejemplo, el personal de Talento Humano accede a datos laborales y personales de los empleados; los administrativos del área académica acceden a registros de estudiantes; y el área contable a

información financiera. Cada ordenador está configurado con accesos diferenciados según el tipo de datos que deben gestionarse.

c) Inserción de dispositivos externos.

En la mayoría de los ordenadores institucionales no está permitido insertar dispositivos externos como memorias USB. Solo se autoriza en casos justificados, con aprobación del Departamento de Sistemas, ya que su riesgo es elevado de que sea ingresado virus la cual infecte en cadena el servidor y cada uno de los equipos, dañando y sobrepasando presupuesto de mantenimiento para una recuperación total de la información que puede y será extraída de manera maliciosa.

Si es necesario entregar una memoria USB se la hace a través de actas de entrega-recepción y con acuerdos de responsabilidad.

d) Contraseñas y control de acceso.

Todos los ordenadores cuentan con acceso mediante usuario y contraseña individual. Algunas estaciones de trabajo acceden a servidores, pero ninguna contraseña está memorizada automáticamente. En todos los casos, para ingresar a sistemas o aplicaciones, es necesario digitar las credenciales cada vez. Sin embargo, aún no existe una política obligatoria de rotación de contraseñas, estas deben cumplir con una complejidad de seguridad, es decir, no ser predecibles en base a la información personal la cual puedan recalcar en sus contraseñas.

e) Copias de seguridad.

Las copias de seguridad de la información se realizan de forma diaria en los servidores locales y una vez por semana en un servidor externo dedicado a respaldos. El

Departamento de Sistemas verifica su ejecución y guarda los registros de los respaldos realizados.

f) Licencias y permisos de software.

Todos los equipos de la Universidad Tecnológica ECOTEC utilizan software con licencias institucionales vigentes, incluyendo sistemas operativos, herramientas ofimáticas, aplicaciones académicas y de gestión. Estas licencias son gestionadas de forma centralizada por el Departamento de Sistemas, el cual realiza controles periódicos para garantizar la legalidad, actualización y cumplimiento de las condiciones de uso del software instalado.

Asimismo, todos los dispositivos cuentan con antivirus corporativos debidamente licenciados, que son renovados y monitoreados de forma regular. Estos programas de seguridad están configurados para realizar análisis automáticos, actualizaciones diarias de definiciones de virus y protección en tiempo real contra amenazas. Su correcta gestión forma parte de las medidas preventivas establecidas en las políticas institucionales de seguridad de la información.

g) Actualizaciones del sistema.

Las actualizaciones se realizan automáticamente para el sistema operativo y los antivirus. Estas actualizaciones son configuradas por el área técnica, y se revisan con frecuencia para asegurar su correcta aplicación.

h) Almacenamiento de información.

La información institucional no se almacena en los ordenadores personales, sino en servidores internos y en la nube institucional, a través del sistema de Drive corporativo

vinculado a Outlook 365. Esta medida permite asegurar que los datos no se pierdan en caso de daño o pérdida del dispositivo.

i) Encargado del tratamiento.

Sí existe un encargado del tratamiento de la información: el Departamento de Sistemas. Esta unidad controla el acceso a la información, realiza monitoreo de dispositivos, gestiona permisos, y garantiza el cumplimiento de las políticas internas de seguridad en un plazo determinado aplicable a su normativa.

3.8.2. Propuesta de Mejora de las Medidas de Seguridad

a) Política de rotación de contraseñas

Se debe implementar una política formal que obligue a los usuarios a cambiar sus contraseñas cada 90 días. Esto disminuirá el riesgo de accesos indebidos por uso prolongado de credenciales antiguas.

b) Autenticación en dos pasos (2FA).

Se recomienda habilitar un sistema de doble autenticación para acceder a sistemas críticos como el servidor de datos, el sistema académico y el sistema de nómina, con el fin de aumentar la seguridad.

c) Gestión de dispositivos móviles (MDM.

Se debe incorporar una solución tecnológica que permita controlar celulares y tablets institucionales, activar funciones como geolocalización, bloqueo remoto y borrado en caso de pérdida o robo.

d) Control del uso de dispositivos externos

Es necesario fortalecer las políticas de uso de USB y otros dispositivos externos. Se debe establecer un sistema de registro, control y autorización de uso temporal, gestionado por el área de sistemas.

e) Registro de accesos por dispositivo y usuario

Se debería implementar una base de datos interna que registre quién accede a qué equipo y cuándo, lo cual facilitará auditorías y aumentará la trazabilidad de incidentes.

f) Formalización de traslados de dispositivos

Los traslados temporales o definitivos de equipos deben ser autorizados por escrito y registrados en la recepción institucional. Esto debe incluir el motivo del traslado, destino, responsable y fecha de devolución.

Para traslados de dispositivos, el encargado de llevar el dispositivo debe elaborar un mail con el respectivo pedido dirigido administración con copia al jefe de seguridad, en el cual indica a donde va ser llevado el dispositivo, que actividad va realizar y quien autorizó el traslado del dispositivo, eso debe ser registrado en recepción y cuando regrese de igual forma debe ser registrado en recepción y mediante correo electrónico debe comunicar que ya está en la universidad nuevamente el dispositivo.

g) Detección de accesos inusuales.

Se sugiere la implementación de un sistema de detección de intrusiones o accesos inusuales (IDS/IPS) que alerte al personal técnico sobre posibles vulneraciones o actividades sospechosas.

3.9. Puestos de Trabajo

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

Las áreas de trabajo están divididas en 3 actividades principales:

- ✓ Actividades administrativas
- ✓ Actividades educativas
- ✓ Actividades operativas

Independientemente de la actividad que realicen, todas las áreas están capacitadas para manejar eventos adversos como incendios, terremotos y dar primeros auxilios básicos, sin embargo, cada actividad también debe poseer consideraciones específicas de seguridad especialmente con los datos que gestionan con sus respectivas medidas.

Área Administrativa. - Esta área maneja la mayor cantidad de datos de la universidad, por ende, las medidas de seguridad de este puesto de trabajo están enfocada principalmente a la protección de estos datos, para esto implementan las siguientes medidas:

- Uso exclusivo de dispositivos dotados por la institución.
- Los dispositivos están conectados a la red protegida de cada área.
- Está prohibido el uso de redes públicas o conectar a redes propias los dispositivos de la institución.
- Está prohibido abrir redes sociales en los dispositivos de la universidad.
- Los usuarios y claves se cambian periódicamente.
- Las computadoras se apagan después de cada jornada.

- Las impresoras están asignadas a cada departamento y la persona que imprime retira cada impresión.
- Las computadoras tienen protector de pantalla que se activa después de un minuto de no usarse.
- Está prohibido compartir usuarios y contraseñas.
- los trabajadores del área administrativa firman acuerdos de confidencialidad.

Estudiantes y docentes. - Los estudiantes y maestros que realizan actividades académicas toman las siguientes medidas de seguridad:

- Utilizan solamente el correo institucional para las comunicaciones con la universidad
- Poseen usuario y contraseña para los softwares académicos y plataformas
- Su ingreso al campus y aulas se lo realiza por un torniquete que se apertura a través de un sistema de reconocimiento facial.
- No se conectan a redes públicas ni a otras redes de otras áreas o que sean poco confiables para evitar e**l man in the middle.**
- Para los docentes es importante mantener en secreto las credenciales de acceso a la plataforma académica en especial para la opción de asignar calificaciones. Para cambiar una calificación se debe notificar al coordinador académico y queda registrado el motivo en la plataforma.

Área Operativa. - Aquí se encuentran incluido el personal de aseo, guardias de seguridad, custodio de llaves, monitoristas y supervisores de seguridad. Manejan información sensible y su acceso en muchas ocasiones es poco limitado es por eso que aplican las siguientes medidas de seguridad:

- Se registran en bitácoras físicas y digitales.
- Se establecen horarios, turnos y perímetros de seguridad por donde deben o están autorizados a circular.
- Firman acuerdos de confidencialidad
- Están prohibidos ingresar con dispositivos móviles, tarjetas de memoria, pen drive o cámaras a las áreas administrativas.
- Son monitoreados constantemente a través de las cámaras de seguridad.
- Su acceso es a través de las puertas designadas para el servicio con reconocimiento facial.
- En el caso del personal de seguridad y vigilancia privada están obligados a realizar pruebas de confianza de forma periódica.

3.9.2. Acuerdo de Confidencialidad Para Trabajadores

ACUERDO DE CONFIDENCIALIDAD Y TRATAMIENTO DE DATOS PERSONALES PARA TRABAJADORES

Entre la Universidad Tecnológica ECOTEC y el/la trabajador/a
En la ciudad de Guayaquil, a ___ de _____ de 2025, comparecen por una parte la Universidad Tecnológica ECOTEC, representada por el Dr. Joaquín Hernández Alvarado, en su calidad de Rector, a quien en adelante se denominará "LA INSTITUCIÓN"; y por otra parte el/la señor/a con cédula de ciudadanía N° , en calidad de trabajador/a, a quien en adelante se denominará "EL/LA FIRMANTE"; quienes libre y voluntariamente acuerdan lo siguiente:

PRIMERA: Objeto del Acuerdo

Este acuerdo tiene por objeto establecer los términos y condiciones bajo los cuales EL/LA **FIRMANTE** se compromete a respetar la confidencialidad, integridad, disponibilidad y

legalidad del tratamiento de datos personales y otra información sensible o reservada a la que tenga acceso en virtud de su relación laboral con LA INSTITUCIÓN.

SEGUNDA: Finalidad y uso de los datos del firmante

LA INSTITUCIÓN informa a EL/LA FIRMANTE que recopilará y tratará sus datos personales con la finalidad de gestionar la relación laboral, procesos administrativos, control de acceso, cumplimiento de obligaciones legales, seguridad institucional y comunicación interna. Los datos serán tratados de forma confidencial.

TERCERA: Datos a los que accede

Datos personales y académicos de estudiantes.

Datos laborales y personales de docentes y personal administrativo.

Información contable, financiera y contractual.

Registros audiovisuales provenientes de sistemas de videovigilancia.

CUARTA: Obligación de Confidencialidad

No divulgar, copiar, modificar ni utilizar para fines personales o externos la información a la que tenga acceso.

Mantener la confidencialidad incluso una vez finalizada su relación con LA INSTITUCIÓN**.**

Cumplir con la LOPDP y las políticas institucionales**.**

QUINTA: Medidas de Seguridad

Usar contraseñas seguras.

No almacenar información en dispositivos no autorizados.

Respetar protocolos de uso de plataformas digitales y servidores.

SEXTA: Conservación de datos personales del firmante

Los datos serán conservados durante la vigencia del contrato laboral y hasta cinco (5) años posteriores a su finalización.

SÉPTIMA: Ejercicio de derechos del firmante

EL/LA FIRMANTE podrá ejercer sus derechos ante el Delegado de Protección de Datos (DPD), por correo: [correo institucional], o en la Dirección Jurídica de LA INSTITUCIÓN.

OCTAVA: Vigencia del acuerdo

Este acuerdo estará vigente durante la relación laboral y por cinco (5) años posteriores a su finalización.

Dr. Joaquín Hernández Alvarado

Rector – Universidad Tecnológica ECOTEC

Nombre del/la Firmante:

Firma CI

3.10. Encargado del Tratamiento

La Universidad ECOTEC, como responsable del tratamiento de datos personales, mantiene convenios con proveedores externos que, en el marco de sus servicios, acceden y gestionan datos por cuenta de la institución. Estos encargados del tratamiento actúan bajo instrucciones precisas de ECOTEC, y están obligados a cumplir con medidas técnicas y contractuales que garantizan la seguridad, confidencialidad y legalidad en el uso de los datos. Esta delegación forma parte de una estrategia institucional orientada a optimizar procesos y asegurar el cumplimiento de la normativa vigente en materia de protección de datos.

3.10.1. Contrato de Tratamiento de Datos Personales

El Contrato de Tratamiento de Datos Personales es un acuerdo formal entre el responsable del tratamiento de los datos y el encargado del tratamiento, con el fin de establecer las condiciones bajo las cuales se gestionarán y protegerán los datos personales, de acuerdo con las disposiciones de la Ley Orgánica de Protección de Datos Personales (LOPDP) y los principios de seguridad y confidencialidad estipulados en dicha normativa.

En este caso, la Universidad Tecnológica ECOTEC actúa como responsable del tratamiento de los datos personales de su comunidad educativa y externa, mientras que la empresa IMGroup S.A. se encarga del tratamiento de los datos específicamente para el servicio de gestión de nómina y administración de personal.

CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS PERSONALES

Entre:

RESPONSABLE DEL TRATAMIENTO:
Nombre: Universidad ECOTEC
RUC: 1791339207001
Dirección: Km. 13.5 Vía a la Costa, Guayaquil, Ecuador
Representante Legal: Dra. María Fernanda Vargas – Rectora
Correo electrónico: rectorado@ecotec.edu.ec
Teléfono: (04) 3700 100

ENCARGADO DEL TRATAMIENTO:
Nombre: IMGroup S.A.
RUC: 0998765432001
Dirección: Av. Francisco de Orellana, Centro Empresarial Colón, Guayaquil
Representante Legal: Ing. Juan Carlos Zambrano
Correo electrónico: jczambrano@imgroup.ec
Teléfono: (04) 2200 500

IDENTIFICACIÓN DEL ENCARGADO DE LOS DATOS DENTRO DE LA EMPRESA:
Nombre: Lcda. Gabriela Morales
Cargo: Responsable de Protección de Datos
Correo: privacidad@imgroup.ec

OBJETO DEL CONTRATO
Este contrato regula el acceso y tratamiento de los datos personales proporcionados por la Universidad ECOTEC a IMGroup para la ejecución del servicio de gestión de nómina y administración de personal**.**
Duración del contrato
Vigencia de 12 meses, renovable automáticamente si no existe notificación de terminación con al menos 30 días de anticipación.
Naturaleza del contrato

Relación de prestación de servicios en la cual IMGroup actúa como encargado del tratamiento de datos personales exclusivamente para el cumplimiento del servicio pactad**o.**

Finalidad del tratamiento

El encargado utilizará los datos personales para procesar la nómina, elaborar contratos laborales, afiliar al personal al IESS y elaborar reportes para el Ministerio de Trabajo.

Tipo de datos personales tratados

Datos identificativos (nombres, cédula, correo), laborales (cargo, fecha de ingreso), económicos (sueldo, cuenta bancaria), y sensibles (afiliación al IESS, licencias médicas).

Obligaciones del responsable de tratamiento: ECOTEC, como responsable del tratamiento, debe garantizar que los encargados cuenten con las condiciones técnicas, jurídicas y organizativas necesarias para cumplir con la normativa vigente. También debe supervisar, auditar y asegurar el cumplimiento continuo del tratamiento por parte de estos terceros.

Subcontratación: Se establece que el encargado no podrá subcontratar el tratamiento de datos sin previa autorización expresa, escrita y específica por parte de ECOTEC. En caso de aprobarse, el subencargado deberá cumplir con las mismas obligaciones contractuales.

Transferencia internacional de datos: En los casos en que el tratamiento implique la transferencia internacional de datos (por ejemplo, uso de servicios en la nube), se exige que el país receptor cuente con un nivel adecuado de protección reconocido por la autoridad competente o que se suscriban cláusulas contractuales tipo que aseguren dicha protección.

Ejercicio de derechos: Los contratos establecen que los encargados deben asistir a ECOTEC en la gestión de solicitudes de derechos de los titulares (acceso, rectificación, eliminación, oposición, entre otros), sin que puedan responder directamente al titular salvo autorización expresa.

Comunicación de brechas de seguridad: Se obliga al encargado a notificar a ECOTEC de forma inmediata, y no más allá de 72 horas, cualquier incidente o brecha de seguridad que afecte datos personales. Asimismo, debe colaborar en la mitigación del riesgo y en la documentación del evento conforme a lo establecido en el plan de respuesta institucional.

Tratar los datos conforme a las instrucciones del responsable.
No usarlos para fines propios ni comunicarlos sin autorización.
Implementar medidas de seguridad adecuadas.
Garantizar confidencialidad del personal que accede a los datos.
Suprimir los datos al finalizar el contrato.
Colaborar en el ejercicio de derechos de los titulares.

Firmas

En constancia de conformidad, las partes firman el presente contrato en dos ejemplares de igual tenor, en la ciudad de Guayaquil, a los ___ días del mes de _____ de 2025.

Por la Universidad ECOTEC

Firma: _____
Nombre: Dra. María Fernanda Vargas
Cargo: Rectora C.I.: 0900000000

Por IMGroup S.A.
Firma: _____
Nombre: Ing. Juan Carlos Zambrano
Cargo: Gerente General
C.I.: 0911111111

3.11. Análisis WEB

3.11.1. Análisis, Configuración y Política de Cookies

El sitio web institucional de la Universidad Tecnológica ECOTEC (https://www.ecotec.edu.ec) cuenta con medidas de seguridad esenciales para la protección de los datos personales de sus usuarios. Según lo evidenciado en las imágenes proporcionadas:

- Utiliza el protocolo HTTPS, lo cual garantiza una conexión segura mediante cifrado de extremo a extremo.
- Posee un certificado digital válido, emitido por una autoridad reconocida, tal como se muestra en la sección de seguridad del navegador.
- El navegador confirma que la conexión es segura y que el certificado es válido, lo cual permite establecer confianza sobre la autenticidad del sitio.
- Respecto a las cookies, se verificó que el sitio utiliza 31 cookies activas, las cuales pueden almacenar información de navegación, preferencias de usuario y datos de interacción. Esta recopilación exige que la universidad cumpla con principios fundamentales como:
- Consentimiento informado: el usuario puede aceptar o rechazar las cookies no esenciales

desde un banner inicial.

- Configuración: el navegador permite gestionar los permisos relacionados con ubicación, cámara, micrófono, JavaScript, imágenes, ventanas emergentes, entre otros. Este control refuerza la protección del usuario al permitirle decidir sobre el uso de sus datos.

El Manual Interno de Protección de Datos Personales de ECOTEC, disponible en su sitio institucional, confirma el compromiso de la universidad con la transparencia y la protección de los datos personales, incluyendo lo relacionado con la navegación y el uso de cookies. Se detalla que el sistema de navegación puede captar dirección IP, dominio y datos técnicos del equipo, usados exclusivamente con fines estadísticos y para garantizar la funcionalidad del sitio.

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

El sitio web de la Universidad Tecnológica ECOTEC ofrece diversos formularios electrónicos, entre ellos el de postulación a programas de posgrado, contacto general y otros relacionados con procesos académicos y administrativos. Desde la perspectiva de la protección de datos personales, estos formularios deben cumplir varios criterios legales y técnicos fundamentales.

Análisis del formulario

En la imagen del formulario de postulación se recogen datos como:

- Nombres y apellidos
- Correo electrónico
- Cédula de identidad

- Teléfono celular
- Ciudad de residencia
- Maestría de interés

Este conjunto de información incluye datos identificativos y datos de contacto, por lo que su recolección está sujeta al principio de minimización, es decir, se han solicitado únicamente los datos estrictamente necesarios para cumplir con la finalidad informada.

Consentimiento y transparencia

El formulario incluye una casilla de verificación ("check box") obligatoria, en la que se menciona "Acepto Términos y Condiciones", lo cual implica consentimiento. En el formulario analizado, se observa que al hacer clic en "Enviar" también se autoriza el envío de información de posgrados por diferentes medios, lo que sugiere una confusión entre consentimiento para tratamiento y consentimiento para marketing, lo cual no cumple con el principio de consentimiento informado y separado.

3.11.3. Avisos Legales

En el sitio web de la Universidad Tecnológica ECOTEC se puede visualizar un banner de cookies que incluye un acceso directo a la Política de Privacidad. Sin embargo, no se encuentra publicado de forma visible un Aviso Legal completo ni una Política de Cookies detallada accesible desde el menú o pie de página.

Actualmente, la única referencia visible a textos legales es la mención a la política de privacidad dentro del banner de configuración de cookies, sin contar con enlaces independientes y claramente identificables al resto de los avisos obligatorios.

3.12. Medidas de Seguridad

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

El sitio web institucional de ECOTEC está configurado para funcionar correctamente en navegadores actualizados y compatibles con HTTPS, como Google Chrome, Mozilla Firefox, Edge y Safari. Se verifica que el portal esté protegido mediante certificados TLS/SSL válidos, lo cual garantiza el cifrado de la información entre el navegador del usuario y el servidor web.

En cuanto a la configuración de seguridad y privacidad, el navegador permite controlar:

- El acceso a cookies y almacenamiento local.
- La ejecución de JavaScript.
- Permisos sobre cámara, micrófono y ubicación.
- La detección de sitios maliciosos o no seguros.

Estas configuraciones, combinadas con el cifrado HTTPS y el certificado válido, permiten establecer un entorno de navegación seguro para los usuarios del portal de ECOTEC, disminuyendo riesgos como suplantación de identidad (phishing), robo de credenciales o exposición de información sensible.

3.12.2. Hosting y Servidores

La página web de ECOTEC está alojada en una plataforma virtual de servicios en la nube, lo cual responde tanto a criterios de eficiencia operativa como a disponibilidad

presupuestaria. La nube permite escalar recursos según demanda y reduce los costos de infraestructura física local.

Este entorno virtual cuenta con características que favorecen la disponibilidad continua del sitio, la seguridad en el acceso remoto, y la implementación de soluciones de respaldo, monitoreo y recuperación ante fallos. Aunque no se detalla públicamente el proveedor exacto, es evidente que ECOTEC utiliza servicios cloud bajo modelo SaaS para diversas plataformas (como el sistema académico Banner).

3.12.2.1. Medidas de Seguridad

Los servidores donde se aloja la información aplican medidas de seguridad sólidas, incluyendo:

- ✓ Implementación de firewalls (contrafuegos) que controlan el tráfico de red y bloquean accesos no autorizados.
- ✓ Verificación de certificados digitales válidos (TLS/SSL), garantizando la autenticidad del sitio.
- ✓ Sistemas de respaldo automático y almacenamiento redundante para prevenir pérdida de datos.
- ✓ Monitoreo de actividad y registro de accesos, lo que facilita auditorías e identificación de incidentes.

Estas medidas permiten mitigar riesgos asociados a la pérdida, alteración o divulgación no autorizada de datos personales y académicos.

3.12.2.2. Prestadores de Servicios

Entre los proveedores tecnológicos que brindan soporte a ECOTEC se identifican:

- ✓ **Ellucian**, con su sistema académico Banner (modelo SaaS).

- ✓ **Microsoft Corporation**, proveedor de Microsoft 365, utilizado como plataforma de correo, almacenamiento y productividad.
- ✓ **Corporación GER**, encargada de los sistemas de videovigilancia y control de accesos físicos y digitales.

Estos prestadores cuentan con contratos específicos que regulan el tratamiento de datos personales, incluyendo cláusulas sobre confidencialidad, medidas de seguridad, notificación de brechas y cumplimiento normativo. Además, se asegura que todos los proveedores cumplan con estándares internacionales como ISO/IEC 27001, especialmente en lo relativo al alojamiento y gestión segura de la información.

3.12.3. Gestores de Correo Electrónico

La universidad utiliza un servicio de correo institucional corporativo, integrado en la suite de Microsoft 365, lo cual indica que es un servicio de pago, con soporte y garantías de seguridad avanzadas.

3.12.3.1. Medidas de Seguridad.

El correo electrónico institucional está protegido mediante:

- ✓ Autenticación multifactor (MFA) para el acceso.
- ✓ Cifrado de mensajes en tránsito y almacenamiento mediante protocolos TLS.
- ✓ Filtros antispam y antiphishing para prevenir ataques o correos maliciosos.
- ✓ Políticas de contraseñas seguras y rotación periódica.
- ✓ Activación de alertas ante accesos no autorizados.
- ✓ Capacidad de rastreo y registro de actividad de usuarios.

- ✓ Reglas automatizadas para bloquear remitentes falsos y prevenir campañas de suplantación de identidad.

3.12.3.2. Prestadores de Servicios.

El prestador del servicio es Microsoft Corporation, a través de su plataforma Microsoft 365, lo cual garantiza:

- ✓ Almacenamiento en la nube seguro bajo jurisdicción con protección de datos adecuada.
- ✓ Cumplimiento con certificaciones de seguridad como ISO 27001, SOC 2 y GDPR.
- ✓ Soporte técnico ante incidentes, trazabilidad completa de la actividad del correo, y herramientas de administración centralizada por parte del Departamento de Sistemas.

Capítulo 4

4. Plan Director de Seguridad

Descripción del Plan Director de Seguridad y sus beneficios

El Plan Director de Seguridad (PDS) es una herramienta estratégica que permite a las organizaciones definir, estructurar y gestionar de manera integral las políticas, acciones y controles en materia de seguridad de la información y protección de datos personales. En el caso de las instituciones educativas vinculadas a la Corporación de Seguridad GER, la implementación de un PDS es fundamental para mitigar riesgos tecnológicos, cumplir con la normativa vigente (como la LOPDP en Ecuador) y garantizar la continuidad operativa en entornos digitales.

4.1. Check List PDS

El Check List del Plan Director de Seguridad (PDS) aplicado a la Universidad Tecnológica ECOTEC permitió verificar el cumplimiento de los principales elementos estructurales requeridos para la implementación de un sistema integral de protección de datos y seguridad de la información. Entre los puntos evaluados están: análisis de la situación actual, alineación estratégica, definición y priorización de proyectos, ejecución de medidas, aprobación institucional y futuras certificaciones en normas internacionales como ISO 27001.

El diagnóstico mostró que ECOTEC ha desarrollado acciones importantes en cuanto a protección de infraestructura tecnológica, control de accesos, videovigilancia, respaldo de información y acuerdos de confidencialidad, aunque aún tiene pendiente formalizar la aprobación institucional del PDS y establecer procesos de certificación.

Tabla 14.

Check list PDS

Nivel	Alcance	Control	Marcado
A	PRO	Analizar la situación actual de la empresa: Se identificaron activos, riesgos, amenazas, medidas y sistemas existentes.	☑
A	PRO	Alinear el PDS con la estrategia de la empresa: El PDS se articula con los objetivos institucionales de seguridad, protección de datos y continuidad educativa digital.	☑
A	PRO	Definir los proyectos a ejecutar: Se han definido proyectos como mejora de infraestructura TI, capacitación continua y fortalecimiento de medidas de protección de datos.	☑
A	PRO	Clasificar y priorizar los proyectos: Se utilizó una matriz de riesgos para priorizar intervenciones tecnológicas y legales.	☑
B	PRO	Aprobar el PDS: Se encuentra en proceso de validación por el comité institucional de seguridad de la información.	☐
A	PRO	La implementación de controles como acuerdos de confidencialidad, controles de acceso y mecanismos de respaldo ha sido planificada y se encuentra en etapa de preparación para su ejecución formal, pendiente de aprobación institucional. Sin embargo, algunas acciones iniciales ya han sido adoptadas de manera preliminar en departamentos clave, en espera de su consolidación en registros y documentación oficial.	☐

A	PRO	Certificación en seguridad: Se encuentra como objetivo estratégico a mediano plazo alineado a estándares como ISO 27001 y cumplimiento LOPDP.	☐

Nota. La información contenida en esta tabla ha sido extraída del análisis del Plan Director de Seguridad (PDS) aplicado a la Universidad Tecnológica ECOTEC, en el cual se identificaron acciones importantes en cuanto a la protección de infraestructura tecnológica, control de accesos, videovigilancia y respaldo de información. Sin embargo, se encontró que aún está pendiente la formalización de la aprobación institucional del PDS y la implementación de procesos de certificación conforme a normativas internacionales, como ISO 27001

.

4.1.1. Análisis de la Situación Actual de la Empresa

La Universidad Tecnológica ECOTEC, como institución educativa de carácter tecnológico, presenta una infraestructura sólida en cuanto al uso de tecnologías de la información, plataformas en la nube, sistemas académicos (Moodle), videovigilancia con analítica facial, servidores físicos y virtuales, y soluciones integradas para gestión administrativa y financiera.

A través del inventario de activos y las matrices de riesgo desarrolladas, se identificaron amenazas potenciales como: acceso no autorizado, errores humanos, pérdida de datos, denegación de servicio y corte de energía. Si bien existen medidas de mitigación como contraseñas, antivirus, respaldo, capacitación, cifrado y segmentación de red, aún es necesario robustecer la gobernanza institucional en torno a la seguridad de la información, consolidando políticas escritas, auditorías y cultura de protección de datos.

4.1.2. Plan Estratégico en Materia Tecnológica

El plan estratégico en materia tecnológica para ECOTEC propone fortalecer la seguridad institucional desde los siguientes frentes:

- ✓ **Infraestructura:** actualización continua de hardware, virtualización de servidores, sistemas redundantes y fuentes de alimentación ininterrumpida.

  Software: implementación de políticas de actualización, antivirus corporativo, sistemas ERP y control de accesos a través de plataformas con autenticación multifactor.
- ✓ **Nube y virtualización:** consolidación del uso de almacenamiento en la nube y backup externo cifrado, evitando dependencia exclusiva de recursos locales.
- ✓ **Capacitación y cultura institucional:** campañas de sensibilización, formación al personal en buenas prácticas de ciberseguridad y protocolos ante incidentes.
- ✓ **Cumplimiento normativo:** alineación continua con la Ley Orgánica de Protección de Datos Personales (LOPDP), preparación para certificaciones ISO y auditorías internas.

Este plan estratégico busca garantizar la continuidad operativa, la protección de los datos personales y el cumplimiento normativo, elevando los estándares de confianza digital en el ámbito académico-administrativo de la universidad.

4.2. Verificador de Controles

La verificación de controles en la Universidad Tecnológica ECOTEC se llevó a cabo mediante una revisión detallada de los elementos que garantizan la seguridad de los sistemas y datos

personales en uso. Este proceso se basó en el análisis de cumplimiento frente a estándares normativos (LOPDP) y buenas prácticas de ciberseguridad.

Tabla 15.

Verificadores de controles de seguridad

VERIFICACIÓN DE CONTROLES DE SEGURIDAD				
Identificador	**Aspecto a evaluar**	**Respuesta**	**Responsable**	**Fecha**
ID_0001	¿La organización ha definido un documento con la política de seguridad de la información?	Sí, ECOTEC cuenta con un documento formal del PDS aprobado por la Dirección Jurídica.	Jefe de Seguridad	20/5/2025
ID_0002	¿La política de seguridad de la información se revisa periódicamente?	Sí. La política de protección de datos está aprobada y comunicada al personal.	Jefe de Seguridad	20/5/2025
ID_0003	¿Se han definido las responsabilidades en materia de seguridad de la información?	Sí. Las funciones están asignadas dentro del reglamento interno y el manual de funciones.	Jefe de Seguridad	20/5/2025
ID_0004	¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?	Sí. Existe un Comité de Seguridad de la Información con representación académica y técnica.	Jefe de Seguridad	20/5/2025
ID_0005	¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la organización? (Confidencialidad, propiedad intelectual, etc.).	Sí. Se aplican controles como contraseñas personales, acceso por roles y videovigilancia.	Área Jurídica	20/5/2025
ID_0006	¿Se dispone de un inventario de activos?	Sí. Los acuerdos son firmados por docentes, administrativos y proveedores.	Área Administrativa	20/5/2025
ID_0007	¿Se ha definido quien es el responsable de los activos?	Sí. El inventario es gestionado por el Departamento de Sistemas y actualizado periódicamente.	Área Administrativa	20/5/2025

ID_0008	¿Se comprueban las referencias de todos los candidatos a empleo?	Sí. Se aplica una política de BYOD con autorización previa y monitoreo de dispositivos.	Recursos Humanos	20/5/2025
ID_0009	¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?	Sí. Se hacen respaldos diarios y semanales con almacenamiento en nube institucional.	Jefe de Seguridad	20/5/2025
ID_0010	¿Los equipos TIC críticos de la organización están ubicados en salas de CPD?	Sí. Existen UPS y generador de respaldo para mantener servicios esenciales activos.	Jefe de Sistemas	20/5/2025
ID_0011	¿Se han definido y documentado los procedimientos operacionales TIC?	Sí. Se cuenta con videovigilancia en áreas estratégicas con análisis facial.	Jefe de Sistemas	20/5/2025
ID_0012	¿Las copias se seguridad se realizan regularmente de acuerdo con la política de backup establecida?	Sí. Las políticas de seguridad se revisan	Área de Sistemas	20/5/2025
ID_0013	¿Se verifica regularmente la correcta realización de las copias se seguridad?	Sí. Se notifican los riesgos mediante charlas, circulares y boletines internos.	Área de Sistemas	20/5/2025
ID_0014	¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?.	Sí. Los usuarios reciben capacitaciones sobre protección de datos y ciberseguridad.	Área de Sistemas	20/5/2025
ID_0015	¿Se registran las actividades de los administradores y operadores de sistema?	Sí. Se usan cifrados y plataformas como Teams, Moodle con HTTPS y VPN institucional.	Área de Sistemas	20/5/2025
ID_0016	¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?.	Sí. El software se actualiza quincenalmente desde el área técnica.	Área de Sistemas	20/5/2025
ID_0017	¿Se ha definido, documentado e implantado un proceso formal para la asignación de contraseñas?	Sí. Los accesos son controlados mediante claves y perfiles por rol.	Área de Sistemas	20/5/2025
ID_0018	¿Se exige a los usuarios que sigan buenas prácticas en	Sí. Se implementa monitoreo y registro de accesos en tiempo real.	Área de Sistemas	20/5/2025

	materia de seguridad en la selección y uso de contraseñas?			
ID_0019	¿Los usuarios se aseguran de proteger los equipos desatendidos? (¿Ej. bloqueando o cerrando la sesión?	Sí. Existen políticas que regulan la transferencia de información.	Usuarios	20/5/2025
ID_0020	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?	Sí. Se firmaron cláusulas de confidencialidad y tratamiento en los contratos de servicios.	Área de Sistemas	20/5/2025
ID_0021	¿Se controla la instalación de software en sistemas en producción?	Sí. Se aplica monitoreo en redes LAN y wifi con filtros de contenido.	Área de Sistemas	20/5/2025
ID_0022	¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	Sí. Los logs se almacenan por 6 meses y se auditan cada trimestre.	Área de Sistemas	20/5/2025
ID_0023	¿Se ha definido, documentado e implantado un proceso formal para la gestión de los incidentes de seguridad?	Sí. Las copias de seguridad están protegidas mediante cifrado y autenticación.	Área de Sistemas	20/5/2025
ID_0024	¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?	Sí. Solo TI puede instalar software previa solicitud y verificación.	Dirección Administrativa	20/5/2025
ID_0025	¿Se han definido, documentado e implantado planes de continuidad de negocio?	Sí. Existen mecanismos de bloqueo de sesión tras inactividad.	Dirección Administrativa	20/5/2025
ID_0026	¿Los planes de continuidad de negocio se revisan y prueban formalmente?	Sí. El DPD está designado oficialmente y capacitado según LOPDP.	Dirección Administrativa	20/5/2025
ID_0027	¿Todos los requisitos relevantes de carácter legal se mantienen identificados?	Sí. Se mantiene una matriz de riesgos actualizada en el plan de seguridad.	Área Legal	20/5/2025
ID_0028	¿Se han implementado procedimientos para asegurar el cumplimiento de los requisitos relevantes de carácter legal?	Sí. El control de acceso físico se realiza mediante tarjetas y registro biométrico.	Área Legal	20/5/2025

ID_0029	¿Se han establecido e implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	Sí. Los dispositivos móviles institucionales están registrados y gestionados por TI.	Área Legal	20/5/2025
ID_0030	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?	Sí. Hay una política clara para uso de servicios cloud con medidas de protección activas.	Área de Sistemas	20/5/2025

Nota. La información presentada en esta tabla corresponde al proceso de verificación de controles de seguridad llevado a cabo en la Universidad Tecnológica ECOTEC, con el fin de asegurar el cumplimiento de los estándares de seguridad de la información establecidos. Los responsables de cada área verificaron los aspectos clave para garantizar la protección de datos, como la gestión de contraseñas, control de accesos, protección de sistemas críticos y medidas de respaldo, entre otros. Las respuestas obtenidas se documentaron y sirven como base para las acciones de mejora continua en la seguridad institucional.

4.3. Inventario de Activos

El inventario de activos digitales de ECOTEC es un elemento central del Plan Director de Seguridad. Este inventario identifica, clasifica y evalúa los recursos tecnológicos involucrados en el tratamiento de información institucional y datos personales.

Tabla 16.

Inventario de activos

INVENTARIO DE ACTIVOS						
Identificador	**Nombre**	**Descripción**	**Responsable**	**Tipo**	**Ubicación**	**Crítico**
ID_0001	Servidor 01 (Contabilidad)	Servidor de contabilidad.	Director Financiero.	Servidor (físico)	Sala de CPD1	Sí
ID_0002	Router Wifi (Clientes)	Router para la red Wifi de cortesía a los clientes.	Dpto. Informática.	Router (físico)	Sala de CPD1	No
ID_0003	Servidor 02 (Web)	Servidor para la página web corporativa.	Dpto. Informática.	Servidor (físico)	CPD Externo	Sí
ID_0004	Sistema de Gestión Académica (SGA)	Plataforma para la administración de matrículas, notas y horarios.	Dirección Académica	Software	Servidor central ECOTEC	Sí
ID_0005	Base de Datos de Estudiantes	Base de datos que contiene información personal y académica de los estudiantes.	Departamento de TI	Base de datos	Servidor central / nube institucional	Sí
ID_0006	Servidor de Respaldo (Backup)	Servidor destinado a almacenar las copias de seguridad de información institucional.	Área de Tecnología / Seguridad	Servidor (físico)	Sala de respaldo (CPD externo)	Sí
ID_0007	Sistema de Videovigilancia	Sistema de cámaras conectadas a red para monitoreo y control.	Departamento de Seguridad	Sistema de seguridad	Áreas comunes y administrativas	Sí
ID_0008	Página web institucional	Sitio web oficial (www.ecotec.edu.ec) que aloja información pública, formularios y acceso a sistemas.	Dirección de Comunicación	Activo digital / web	Servidor web / dominio externo	Si

Nota. El inventario de activos presentado corresponde a los recursos tecnológicos que ECOTEC utiliza para el tratamiento de información institucional y datos personales. Los

activos identificados han sido clasificados según su importancia y criticidad en relación con la seguridad de la información. Los responsables de cada área han asegurado la correcta gestión de estos activos, ubicados en distintas zonas, ya sea en servidores locales o en la nube institucional, con medidas de seguridad adaptadas a su nivel de criticidad.

4.4. Análisis de Riesgos

El análisis de riesgos constituye una herramienta clave para la toma de decisiones en el marco del Plan Director de Seguridad de la Universidad Tecnológica ECOTEC. Este proceso permite identificar vulnerabilidades y amenazas sobre los activos tecnológicos que tratan información personal y sensible, asignando un nivel de riesgo en función de la probabilidad de ocurrencia y el impacto potencial.

Para la evaluación, se empleó una matriz cualitativa de valoración, considerando:

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

A continuación, se resumen algunos de los riesgos analizados:

Tabla 17.

Análisis de riesgos para la toma de decisiones en el marco del Plan Director de Seguridad

ANÁLISIS DE RIESGOS				
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
ordenador(es)	Introducción de falsa información	Medio (2)	Alto (3)	6
ordenador(es)	Alteración de la información	Medio (2)	Alto (3)	6

ordenador(es)	Corrupción de la información	Medio (2)	Medio (2)	4
ordenador(es)	Destrucción de información	Bajo (1)	Medio (2)	2
ordenador(es)	Fallo de servicios de comunicaciones	Medio (2)	Medio (2)	4
ordenador(es)	Degradación de los soportes de almacenamiento de la información	Medio (2)	Alto (3)	6
ordenador(es)	Errores de mantenimiento / actualización de equipos (hardware)	Bajo (1)	Alto (3)	3
ordenador(es)	Caída del sistema por sobrecarga	Medio (2)	Medio (2)	4
ordenador(es)	Errores de los usuarios	Alto (3)	Alto (3)	9
ordenador(es)	Errores del administrador	Bajo (1)	Medio (2)	2
ordenador(es)	Errores de configuración	Medio (2)	Medio (2)	4
ordenador(es)	Robo	Bajo (1)	Bajo (1)	1
WIFI	Interceptación de información (escucha)	Medio (2)	Alto (3)	6
WIFI	Fallo de servicios de comunicaciones	Medio (2)	Medio (2)	4
WIFI	Errores de configuración	Medio (2)	Medio (2)	4
WIFI	Denegación de servicio	Medio (2)	Alto (3)	6
WIFI	Fallo de servicios de comunicaciones	Medio (2)	Medio (2)	4
Trabajos moviles (telefono)	Fuga de información	Alto (3)	Alto (3)	9
Trabajos moviles (telefono)	Introducción de falsa información	Medio (2)	Alto (3)	6
Trabajos moviles (telefono)	Alteración de la información	Alto (3)	Alto (3)	9

Trabajos moviles (telefono)	Corrupción de la información	Medio (2)	Medio (2)	4
Trabajos moviles (telefono)	Destrucción de información	Medio (2)	Alto (3)	6
Dispositivos de internet en dispositivos con datos	Acceso no autorizado	Medio (2)	Medio (2)	4
Dispositivos de internet en dispositivos con datos	Errores de los usuarios	Medio (2)	Medio (2)	4
Dispositivos de internet en dispositivos con datos	Robo	Alto (3)	Alto (3)	9
Dispositivos de internet en dispositivos con datos	Ingeniería social	Medio (2)	Medio (2)	4
Dispositivos de internet en dispositivos con datos	Introducción de falsa información	Alto (3)	Medio (2)	6
Dispositivos de internet en dispositivos con datos	Errores de mantenimiento / actualización de programas (software)	Alto (3)	Medio (2)	6
Dispositivos de internet en dispositivos con datos	Acceso no autorizado	Medio (2)	Medio (2)	4
Dispositivos de internet en dispositivos con datos	Denegación de servicio	Medio (2)	Alto (3)	6

Servidores externos	Corte del suministro eléctrico	Alto (3)	Alto (3)	9
Servidores externos	Fallo de servicios de comunicaciones	Alto (3)	Alto (3)	9
Servidores externos	Errores de configuración	Medio (2)	Medio (2)	4
Servidores externos	Denegación de servicio	Medio (2)	Medio (2)	4
Almacenamiento interno	Introducción de falsa información	Alto (3)	Medio (2)	6
Almacenamiento interno	Difusión de software dañino	Alto (3)	Alto (3)	9
Almacenamiento interno	Errores de configuración	Alto (3)	Medio (2)	6

Nota. La tabla muestra el análisis de riesgos realizado por la Universidad Tecnológica ECOTEC para el Plan Director de Seguridad, basado en una metodología cualitativa de valoración que incluye la probabilidad e impacto de cada riesgo. El objetivo de este análisis es priorizar los riesgos identificados en función de su probabilidad y impacto, con el fin de implementar medidas de mitigación que garanticen la protección de la infraestructura tecnológica y los datos personales de la institución.

4.5. Clasificación y Priorización

Una vez realizado el análisis de riesgos sobre los activos tecnológicos de ECOTEC, se procedió a su clasificación y priorización con base en los siguientes criterios:

- ✓ **Nivel de riesgo** (producto de la probabilidad × impacto)
- ✓ **Tipo de activo** (si trata datos personales, académicos, financieros, etc.)
- ✓ **Grado de criticidad** en los procesos institucionales (docencia, administración, comunicación, etc.)
- ✓ **Posibilidad de aplicación inmediata de medidas de mitigación**

Tabla 18.

Criterios de clasificación de riesgo

Nivel de Riesgo	Interpretación	Acción recomendada
Alto (6-9)	Riesgo inaceptable	Requiere intervención inmediata
Medio (4-5)	Riesgo moderado	Requiere medidas correctivas
Bajo (1-3)	Riesgo aceptable con control	Mantener controles actuales

Nota. La tabla presenta los criterios utilizados por la Universidad Tecnológica ECOTEC para clasificar y priorizar los riesgos identificados en función de su nivel de gravedad. Estos criterios incluyen el cálculo del nivel de riesgo (producto de la probabilidad y el impacto), el tipo de activo involucrado, el grado de criticidad en los procesos institucionales y la posibilidad de aplicar medidas de mitigación de forma inmediata. La clasificación de los riesgos permite establecer acciones prioritarias para garantizar la seguridad de los activos tecnológicos y la protección de la información en la institución.

La clasificación y priorización de los activos críticos en la Universidad Tecnológica ECOTEC es un paso fundamental dentro del proceso de gestión de riesgos. Esta clasificación tiene como objetivo identificar y priorizar los activos más importantes que podrían verse afectados por los riesgos identificados, con el fin de implementar las medidas de mitigación más adecuadas y oportunas. Al clasificar los activos según su nivel de riesgo y la prioridad de atención, ECOTEC puede asegurar que los recursos tecnológicos más sensibles, tales como

servidores, sistemas de gestión académica y plataformas de videovigilancia, sean protegidos de manera adecuada.

Tabla 19.

Clasificación y priorización de activos críticos

Activo	Riesgo Identificado	Nivel de Riesgo	Prioridad de Atención
Servidor 01 (Contabilidad)	Fuga de información	Alto (6)	Alta
Sistema de Gestión Académica (SGA)	Acceso inseguro a datos	Alto (6)	Alta
Software de respaldo	Saturación o pérdida de información	Alto (6)	Alta
Página web institucional	Acceso no autorizado / defacement	Alto (6)	Alta
Sistema de videovigilancia	Falla de configuración	Medio (4)	Media
Router WiFi (clientes)	Caída del sistema por sobrecarga	Bajo (2)	Baja
Servidor 02 (Web)	Corte del suministro eléctrico	Bajo (2)	Baja

Nota. La tabla presenta la clasificación de los activos más críticos de ECOTEC, identificando los riesgos asociados y determinando la prioridad de atención en función del nivel de riesgo. Los activos con un riesgo clasificado como "Alto" son aquellos que requieren intervención inmediata, mientras que los activos con riesgos "Medios" o "Bajos" son gestionados con medidas correctivas o controles actuales. La priorización asegura que las acciones de mitigación se enfoquen en los activos que son esenciales para el funcionamiento continuo de la institución.

Priorización de Medidas

Las acciones correctivas se priorizaron considerando los siguientes aspectos:

- ✓ **Impacto académico**: se priorizan los sistemas que contienen datos de estudiantes y docentes.
- ✓ **Impacto legal**: se priorizan activos que manejan información financiera o protegida por la LOPDP.
- ✓ **Disponibilidad**: se priorizan activos cuya falla afectaría la continuidad operativa.

Tabla 20.

Priorización de Medidas de Seguridad en los Activos de ECOTEC

	Identificador	Activo	Aplicación
Modelo A	A1	Ordenadores de escritorio institucionales	SI
	A2	Dispositivos móviles institucionales y personales autorizados (BYOD)	SI
	A3	Conexión a Internet y redes Wifi internas	SI
Modelo B	B1	Laptops para personal docente, administrativo y directivo	SI
	B2	Celulares y tablets institucionales para trabajo móvil y académico	SI
	B3	Plataformas educativas y colaborativas como Moodle y Microsoft Teams	SI
	B4	Sitio web alojado en servidor externo con medidas de seguridad avanzadas	SI
Modelo C	C1	Servidores institucionales locales y virtualizados	SI
	C2	Servicios de conexión segura con certificado SSL/TLS	SI
	C3	Plataformas académicas, financieras y administrativas en la nube	SI
	C4	Sistemas ERP y CRM institucionales	SI

	C5	Sistemas de videovigilancia con análisis facial y monitoreo en tiempo real	SI
	C6	Soluciones cloud para almacenamiento documental	SI
	C7	Plataforma e-Gobierno y SRI para trámites digitales y declaración tributaria	SI

Nota. La tabla presenta los activos clave de la Universidad Tecnológica ECOTEC, clasificados en tres modelos (A, B y C) según su nivel de criticidad y la aplicación de medidas de seguridad. Los activos fueron priorizados en función de tres factores clave: impacto académico, impacto legal y disponibilidad. Los activos clasificados como "SI" en la columna "Aplicación" son aquellos identificados como esenciales para el funcionamiento institucional, con medidas correctivas o preventivas para garantizar su seguridad y continuidad operativa.

Tabla 21.

Cruce de Activos y Amenazas en el Plan Director de Seguridad de ECOTEC

Amenaza/Activo	A1	A2	A3	B1	B2	B3	B4	C1	C2	C3	C4	C5	C6	C7
Fuego	no	no	no	no	no	no	no	no	no	no	no	no	no	no
Daños por agua	no	si	si	si	si	si	no	no	no	no	no	no	no	no
Desastres naturales	no	no	no	no	no	no	no	no	no	no	no	no	no	no
Fuga de información	si	si	si	si	si	si	si	si	si	si	si	no	si	si
Introducción de falsa información	si	si	si	si	si	si	si	si	si	si	si	no	si	si
Alteración de la información	si	si	si	si	si	si	si	si	si	si	si	no	si	si
Corrupción de la información	si	si	si	si	si	si	si	si	si	si	si	si	si	si
Destrucción de información	no	si	si	si	si	si	si	si	si	si	si	no	si	si

Interceptación de información (escucha)	no	si	si	si	si	si	si	si	si	si	si	no	si	si
Corte del suministro eléctrico	si	si	si	si	si	si	si	si	si	si	si	si	si	si
Condiciones inadecuadas de temperatura o humedad	no	no	no	no	no	no	no	no	si	si	si	si	si	si
Fallo de servicios de comunicaciones	no	si	si	si	si	si	si	si	si	si	si	no	si	si
Interrupción de otros servicios y suministros esenciales	si	si	si	si	si	si	si	si	si	si	si	no	si	si
Desastres industriales	no	si	si	si	si	si	si	si	no	si	si	si	si	si
Degradación de los soportes de almacenamiento de la información	si	si	si	si	si	si	si	si	si	si	si	si	si	si
Difusión de software dañino	si	si	si	si	si	si	si	si	si	si	si	si	si	si
Errores de mantenimiento / actualización de programas (software)	si	si	si	si	si	si	si	si	si	si	si	si	si	si
Errores de mantenimiento / actualización de equipos (hardware)	si	si	si	si	si	si	si	si	si	si	si	si	si	si
Caída del sistema por sobrecarga	si	si	si	si	si	si	si	si	si	si	si	si	si	si
Pérdida de equipos	no	no	no	no	no	no	no	si	no	si	si	si	no	si
Indisponibilidad del personal	no	no	no	no	no	no	no	no	si	si	si	si	no	no
Abuso de privilegios de acceso	si	si	si	si	si	si	si	no	si	si	si	si	si	si
Acceso no autorizado	si	si	si	si	si	si	si	si	no	si	si	si	si	si

Errores de los usuarios	si	si	si	si	si	si	si	si	si	si	si	si	si	si
Errores del administrador	si	si	si	si	si	si	si	no	no	si	si	si	si	si
Errores de configuración	si	si	si	si	si	si	si	no	si	si	si	si	si	si
Denegación de servicio	si	si	si	si	si	si	si	si	si	si	si	si	si	si
Robo	si	si	si	si	si	si	si	no	no	si	si	si	si	no
Extorsión	no	no	si	no	no	no	no	si	si	si	si	no	si	si
Ingeniería social	no	si	si	si	si	si	si	no	si	si	si	no	si	si

Nota. La tabla muestra la relación entre los activos críticos de la Universidad ECOTEC y las amenazas identificadas, con el objetivo de priorizar medidas de protección. Las casillas marcadas como "sí" indican que el activo en cuestión está expuesto a la amenaza correspondiente. La información proporciona una base para la clasificación y priorización de riesgos, permitiendo tomar decisiones informadas sobre los controles de seguridad a implementar en los diferentes activos de la universidad.

Registro, clasificación y priorización de iniciativas.

Tabla 22.

Registro, clasificación y priorización de iniciativas

REGISTRO, CLASIFICACIÓN Y PRIORIZACIÓN DE INICIATIVAS							
Identificador	**Título Amenaza**	**Descripción**	**Responsable**	**Tipo**	**Coste**	**Fecha**	**Revisión**
IN_0001	Introducción de falsa información	Verificación de autenticidad, filtros - revisión	TICS	Físico/lógico	2000	5 días	MES
IN_0001	Alteración de la información	integridad, auditoría de cambios	TICS	Físico/lógico	500	7 días	SEMANA
IN_0003	Degradación de los soportes de almacenamiento de la información	Backups, almacenamiento redundante/monitoreo	TICS	Físico/lógico	1000	7 días	SEMANA

IN_0004	Errores de los usuarios	Capacitación, interfaces amigables, validaciones	TICS	Físico/lógico	5000	9 días	MES
IN_0005	Interceptación de información (escucha)	Cifrado/VPN, monitoreo de red	DPT TI	Físico/lógico	3000	8 días	AÑO
IN_0006	Denegación de servicio	firewall, redundancia, mitigación DDoS	DPT TI	Físico/lógico	2500	10 días	SEMANA
IN_0007	Fuga de información	Política de privacidad, cifrado, control de accesos	DPT TI	Lógico	1700	2 días	SEMANA
IN_0008	Introducción de falsa información	Verificación de autenticidad, filtros - revisión	DPT TI	Lógico	300	15 días	MES
IN_0009	Alteración de la información	control de versiones, logs, roles definidos	DPT TI	Lógico	600	5 días	MES
IN_0010	Destrucción de información	Backups automáticos, políticas de seguridad, cifrado	DPT TI	Lógico	2500	8 días	SEMANA
IN_0011	Robo	Control de accesos físicos, seguros, registro	DPT TI	Lógico	1200	9 días	SEMANA
IN_0012	Introducción de falsa información	Seguridad perimetral, contraseñas fuertes, monitoreo	DPT TI/ áreas ADM	Físico/lógico	4000	9 días	SEMANA
IN_0013	Errores de mantenimiento / actualización de programas (software)	Actualización regular, validación, revisión	DPT TI	Lógico	2000	4 días	MES
IN_0014	Denegación de servicio	Sistemas tolerantes a fallos, redundancia	DPT TI	Lógico	3500	3 días	MES
IN_0015	Corte del suministro eléctrico	UPS, generador de respaldo, monitoreo	DPT TI	Lógico	400	8 días	SEMANA
IN_0016	Fallo de servicios de comunicaciones	Redundancia, mantenimiento preventivo, alertas	DPT TI/ c área funcional (según el servicio)	Lógico	1000	6 días	AÑO

IN_0017	Introducción de falsa información	Verificación de autenticidad, filtros, revisión	DPT TI/ c área funcional (según el servicio)	Lógico	550	3 días	MES
IN_0018	Difusión de software dañino	Antivirus, reglas de firewall, revisión manual	Departamento TI/ cada área funcional (según el servicio)	Lógico	330	5 días	MES
IN_0019	Errores de configuración	Monitoreo, políticas de instalación, firewall	Departamento TI/ cada área funcional (según el servicio)	Lógico	2600	8 días	SEMANA

Nota. La tabla muestra un registro detallado de las iniciativas para tratar diversas amenazas identificadas en el Plan Director de Seguridad (PDS) de la Universidad ECOTEC. Cada iniciativa se clasifica según el tipo de tratamiento (físico/lógico) y se asigna un responsable, coste y tiempo estimado para su ejecución. Este registro permite priorizar las acciones correctivas a implementar y establecer un cronograma para su seguimiento, asegurando que los riesgos sean gestionados de manera eficiente y conforme a las normativas de seguridad establecidas.

4.6. Check List

La aplicación del Check List del Plan Director de Seguridad (PDS) permitió identificar el estado inicial de los controles estratégicos de seguridad de la información y compararlos con el estado posterior a la implementación de las acciones correctivas y de mejora.

Estado Inicial (antes del proceso):

- ✓ No existía una sistematización completa del PDS.

- ✓ El análisis de situación de seguridad se realizaba de forma parcial y no estructurada.
- ✓ Los proyectos relacionados con seguridad tecnológica estaban dispersos y no priorizados.
- ✓ No existía una hoja de ruta clara para la alineación con la estrategia institucional.
- ✓ No se había formalizado el proceso de aprobación del PDS por una autoridad superior.
- ✓ La ejecución de controles de seguridad se aplicaba, pero sin documentación ni seguimiento específico.
- ✓ No existía un plan establecido para certificaciones futuras ni auditorías internas.

Resumen comparativo del estado de cumplimiento antes y después del proceso de elaboración del Plan Director de Seguridad.

Tabla 23.

Resumen comparativo del estado de cumplimiento antes y después del proceso de elaboración del Plan Director de Seguridad

Elemento del Check List	Estado Inicial (Antes del proceso)	Estado Actual (Después del proceso)
Análisis de situación de la organización	Parcial, no documentado ni actualizado	Realizado con base en inventario de activos y amenazas
Alineación con estrategia institucional	No estructurado ni formalizado	Integrado al PDS con objetivos y metas
Definición de proyectos	Dispersos, sin planificación priorizada	Proyectos priorizados con base en matriz de riesgos
Clasificación y priorización	No existía una matriz formal	Matriz de riesgos desarrollada y aplicada

Aprobación del PDS	No implementada	En proceso de validación por directivos
Ejecución del PDS	Controles aplicados sin trazabilidad	Controles documentados e implementados
Certificación en seguridad	No contemplada	Planificada como objetivo a mediano plazo

Nota. La tabla resume el estado de cumplimiento del Plan Director de Seguridad (PDS) de la Universidad ECOTEC, antes y después de su implementación. En el estado inicial, el proceso de seguridad era fragmentado y carecía de una estructura clara, sin alineación con la estrategia institucional ni un plan formal de certificaciones y auditorías. Sin embargo, con la elaboración del PDS, se logró una mejora significativa, incluyendo la sistematización de los procesos de seguridad, la alineación con los objetivos institucionales y la implementación de controles documentados, lo que permite un seguimiento más efectivo y la planificación de futuras certificaciones en seguridad.

La siguiente tabla resume el estado de cumplimiento de los controles estratégicos del Plan Director de Seguridad (PDS) antes y después del proceso de análisis e implementación de mejoras. Los controles marcados con '☑' indican que se han cumplido tras la revisión; los marcados con '☐' aún se encuentran en proceso o pendientes.

Tabla 24.

Estado de cumplimiento de los controles estratégicos del PDS

Nivel	Control Evaluado	Cumplimiento
A	Analizar la situación actual de la empresa: Se identificaron activos, riesgos, amenazas, medidas y sistemas existentes.	☑

A	Alinear el PDS con la estrategia de la empresa: El PDS se articula con los objetivos institucionales de seguridad, protección de datos y continuidad educativa digital.	☑
A	Definir los proyectos a ejecutar: Se han definido proyectos como mejora de infraestructura TI, capacitación continua y fortalecimiento de medidas de protección de datos.	☑
A	Clasificar y priorizar los proyectos: Se utilizó una matriz de riesgos para priorizar intervenciones tecnológicas y legales.	☑
B	Aprobar el PDS: Se encuentra en proceso de validación por el comité institucional de seguridad de la información.	☐
A	Ejecución del PDS: La implementación de controles como acuerdos de confidencialidad, controles de acceso y mecanismos de respaldo se encuentra en marcha y ha sido aplicada en todos los departamentos administrativos, académicos y tecnológicos de la universidad, aunque algunos registros aún se consolidan en documentación formal.	☑
A	Certificación en seguridad: Se encuentra como objetivo estratégico a mediano plazo alineado a estándares como ISO 27001 y cumplimiento LOPDP.	☐

Nota. La tabla muestra el estado de cumplimiento de los controles estratégicos del Plan Director de Seguridad (PDS) en la Universidad ECOTEC, reflejando el progreso logrado en

la implementación de medidas clave para fortalecer la seguridad institucional. Los controles marcados con '☑' indican que se han implementado con éxito, mientras que los controles con '☐' están en proceso de ejecución o aún pendientes de completarse. Esta revisión es parte del esfuerzo continuo para alinear las prácticas de seguridad con los objetivos estratégicos de la institución y los estándares internacionales en ciberseguridad.

4.7. Registro de actividades de tratamientos.

En esta Universidad aún no se ha implementado el RAT, ya que el tratamiento de la información se la realiza únicamente a nivel interno, sin embargo, han mostrado su interés en generar un documento donde se especifique el tratamiento de los datos, los usuarios y la finalidad de su uso.

Capítulo 5

Propuesta De Implementación De Un Sistema De Gestión Basado En La Norma ISO 31000:2018.

5.1. Objeto y Campo de Aplicación

La presente propuesta tiene como objetivo establecer un sistema de gestión de riesgos institucional, fundamentado en los lineamientos de la norma ISO 31000:2018, adaptado a las necesidades de la Universidad ECOTEC. Este sistema proporcionará un marco metodológico para identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en todos los niveles y funciones de la institución, con el propósito de fortalecer la toma de decisiones y fomentar una cultura de prevención sostenible.

El sistema ha sido diseñado para integrarse de manera fluida con los procesos clave de gobernanza, planificación, gestión académica, servicios administrativos y tecnológicos, asegurando así que se cumplan los objetivos estratégicos de la universidad, se mejore su desempeño institucional y se protejan sus activos tangibles e intangibles.

El campo de aplicación cubre todas las áreas funcionales y niveles jerárquicos de ECOTEC, incluidas las unidades académicas, administrativas, tecnológicas, financieras y de vinculación, adoptando un enfoque transversal que refuerza la gobernanza y genera valor dentro del contexto institucional.

Tabla 25.

Campo de Aplicación del Sistema de Gestión de Riesgos Basado en la Norma ISO 31000:2018 en la Universidad ECOTEC

Área de Aplicación	Descripción
Gestión Académica	Procesos de admisión, matrícula, calificaciones, administración de programas académicos y formación continua.
Gestión Administrativa	Actividades de gestión de personal, finanzas, compras, mantenimiento de infraestructura y servicios externos.
Seguridad de la Información	Protección de sistemas tecnológicos que procesan datos personales, académicos y administrativos, con políticas de acceso y control de datos.
Seguridad Física y Videovigilancia	Supervisión de instalaciones físicas y el uso de sistemas de videovigilancia para el control de accesos, protección de áreas clave y prevención de incidentes.
Tecnología y Sistemas	Protección de activos tecnológicos como servidores, redes de comunicación, plataformas educativas y otros sistemas informáticos críticos.
Cumplimiento Legal	Aseguramiento del cumplimiento de las leyes locales e internacionales, incluyendo la Ley Orgánica de Protección de Datos Personales (LOPDP) y estándares ISO.

Nota. Esta tabla resume el ámbito de aplicación del Sistema de Gestión de Riesgos basado en la Norma ISO 31000:2018 en la Universidad ECOTEC, considerando los principales procesos y áreas de la institución que requieren el manejo de riesgos.

5.2. Referencias Normativas

Este sistema de gestión del riesgo se fundamenta en un conjunto de normas y documentos técnicos que proporcionan las directrices esenciales para el diseño, desarrollo, implementación y mejora continua del proceso de gestión del riesgo. Estas referencias se han seleccionado por su pertinencia y compatibilidad con el enfoque propuesto.

A continuación, se presentan las normas y documentos de referencia considerados en esta propuesta:

Tabla 26.

Referencias Normativas del Sistema de Gestión de Riesgos

Norma/Documento	Descripción	Fuente/Referencia
ISO 31000:2018	*Gestión del riesgo (Directrices)*. Establece los principios, el marco de trabajo y el proceso de gestión del riesgo aplicables a cualquier organización.	International Organization for Standardization (ISO). (2018). ISO 31000:2018 Risk management – Guidelines. https://www.iso.org/standard/65694.html
ISO Guide 73:2009	*Gestión del riesgo (Vocabulario)*. Proporciona definiciones comunes y términos clave relacionados con la gestión del riesgo.	International Organization for Standardization (ISO). (2009). ISO Guide 73:2009 Risk management – Vocabulary. https://www.iso.org/standard/44651.html
ISO/IEC 31010:2019	*Gestión del riesgo (Técnicas de evaluación del riesgo)*. Describe métodos y herramientas para identificar, evaluar y tratar riesgos.	International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC). (2019). ISO/IEC 31010:2019 Risk assessment techniques. https://www.iso.org/standard/65657.html
Ley Orgánica de Educación Superior (LOES)	Marco legal nacional que regula el funcionamiento de las instituciones de educación superior en Ecuador.	Asamblea Nacional del Ecuador. (2010). Ley Orgánica de Educación Superior (LOES). https://www.asambleanacional.gob.ec
Ley Orgánica de Protección de Datos Personales (LOPDP)	Norma clave para la identificación y tratamiento de riesgos relacionados con la seguridad y confidencialidad de la información.	Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales (LOPDP). https://www.asambleanacional.gob.ec
Normas y reglamentos internos de la Universidad ECOTEC	Disposiciones académicas, administrativas, tecnológicas y de seguridad institucional.	Universidad Tecnológica ECOTEC. (2025). *Normas y reglamentos internos*. Universidad ECOTEC.
Plan Estratégico Institucional (PEI) de la Universidad ECOTEC	Documento que orienta la planificación a mediano y largo plazo de la universidad.	Universidad Tecnológica ECOTEC. (2025). *Plan Estratégico Institucional (PEI)*. Universidad ECOTEC.

Nota. Esta tabla presenta las principales normas y documentos de referencia que sustentan el diseño e implementación del sistema de gestión de riesgos basado en la norma ISO 31000:2018 para la Universidad ECOTEC.

5.3. Términos y definiciones

Para garantizar una comprensión clara, uniforme y coherente de los conceptos fundamentales utilizados en esta propuesta, se definen a continuación los términos clave empleados en el diseño e implementación del sistema de gestión de riesgos basado en la norma ISO 31000:2018. Las definiciones que se presentan a continuación han sido tomadas como referencia del ISO Guide 73:2009 y adaptadas al contexto institucional de la Universidad ECOTEC.

Tabla 27.

Términos y Definiciones del Sistema de Gestión de Riesgos

Término	Definición
Riesgo	Efecto de la incertidumbre sobre los objetivos, que puede ser positivo, negativo o ambos. El riesgo puede originarse por factores internos o externos. En el contexto universitario, un riesgo puede estar relacionado con la seguridad de la información, la calidad académica o la continuidad operativa.
Gestión del riesgo	Conjunto de actividades y procesos coordinados utilizados para dirigir y controlar una organización con respecto al riesgo. Este proceso incluye la identificación, análisis, evaluación, tratamiento, monitoreo y revisión de los riesgos, así como la comunicación y consulta con las partes interesadas.
Parte interesada	Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad. En ECOTEC, esto incluye a estudiantes, docentes, personal administrativo, autoridades, proveedores, entes reguladores, familias y la comunidad en general.
Contexto	El entorno interno y externo en el que la organización busca alcanzar sus objetivos. Esto incluye factores culturales, sociales, legales, tecnológicos, económicos y políticos, así como el entorno institucional propio de ECOTEC.

Tratamiento del riesgo	Proceso que consiste en modificar el riesgo. Esto puede implicar evitar el riesgo, asumirlo, reducir su probabilidad o consecuencias, compartirlo con otras entidades (como seguros) o aprovechar oportunidades.
Análisis del riesgo	Proceso que permite comprender la naturaleza del riesgo y determinar su nivel, evaluando su probabilidad y consecuencias.
Evaluación del riesgo	Proceso mediante el cual se comparan los resultados del análisis del riesgo con criterios preestablecidos para determinar si el riesgo es aceptable o si requiere tratamiento adicional.
Mapa de riesgos	Representación visual que agrupa e identifica los principales riesgos de una organización, clasificándolos por áreas, niveles de impacto y probabilidad de ocurrencia.
Política de gestión del riesgo	Declaración formal que expresa la intención y el compromiso de la organización con respecto a la gestión del riesgo, alineada con sus principios, valores y objetivos estratégicos.
Marco de referencia (framework)	Conjunto de componentes que proporciona las bases organizativas necesarias para diseñar, implementar, monitorear y mejorar continuamente la gestión del riesgo.

Nota. Esta tabla presenta los términos y definiciones clave empleados en el diseño e implementación del sistema de gestión de riesgos basado en la norma ISO 31000:2018 adaptados al contexto institucional de la Universidad ECOTEC.

5.4. Principios

La implementación del sistema de gestión del riesgo en la Universidad ECOTEC se rige por una serie de principios que garantizan su eficacia, sostenibilidad y alineación con los objetivos institucionales. A continuación, se detallan los ocho principios fundamentales propuestos por la norma ISO 31000:2018 y su aplicación concreta en el entorno universitario.

5.4.1 Integrada

La gestión del riesgo debe estar plenamente incorporada en todas las estructuras, operaciones y procesos institucionales. En el caso de ECOTEC, esto implica que la gestión del riesgo no se limita a una función aislada, sino que forma parte de la toma de decisiones en

todas las áreas: académica, administrativa, tecnológica, financiera y de vinculación con la comunidad. Su integración asegura coherencia con la planificación estratégica y la operatividad diaria de la universidad.

5.4.2 Estructurada y Exhaustiva

Para garantizar la efectividad del sistema, la gestión del riesgo debe desarrollarse de manera metódica, documentada y sistemática. En ECOTEC, esto se traduce en la implementación de metodologías claras para la identificación, análisis, evaluación, tratamiento y monitoreo de riesgos. La aplicación estructurada y exhaustiva evita omisiones críticas y permite una visión completa del panorama de riesgos institucionales.

5.4.3 Adaptada

Cada organización tiene características únicas, por lo que el sistema debe adecuarse a su contexto específico. ECOTEC, como institución educativa con un enfoque tecnológico, requiere un sistema que se adapte tanto a su modelo académico como a sus retos administrativos, regulatorios y tecnológicos. Esta adaptación se logra mediante el análisis constante del entorno y la revisión periódica de los procesos de riesgo.

5.4.4 Inclusiva

La gestión del riesgo debe involucrar a todas las partes interesadas pertinentes. En ECOTEC, esto significa que estudiantes, docentes, personal administrativo, directivos y otros actores relevantes participen en la identificación y tratamiento de riesgos. La inclusión promueve la apropiación del sistema por parte de toda la comunidad universitaria y fortalece su legitimidad.

5.4.5 Dinámica

Los riesgos evolucionan constantemente; por tanto, el sistema de gestión debe ser flexible y capaz de ajustarse rápidamente a los cambios. En la universidad, esto es crucial ante nuevas regulaciones educativas, crisis sanitarias, avances tecnológicos o amenazas cibernéticas. Un enfoque dinámico asegura la capacidad de respuesta institucional y fomenta la anticipación frente a escenarios emergentes.

5.4.6 Mejor información disponible

La toma de decisiones en la gestión del riesgo debe sustentarse en información pertinente, actualizada y verificable. En ECOTEC, esto implica integrar datos académicos, financieros, tecnológicos y de satisfacción de partes interesadas para fundamentar el análisis y tratamiento de riesgos. No obstante, se reconoce que toda decisión conlleva cierto grado de incertidumbre, por lo que se promueve la evaluación constante de la calidad de la información.

5.4.7 Factores humanos y culturales

El comportamiento humano, los valores organizacionales y la cultura institucional influyen directamente en la gestión del riesgo. En ECOTEC, se reconoce que la participación, el liderazgo y la actitud frente al riesgo varían según el perfil del personal y su experiencia. Por ello, se fomentará una cultura de gestión del riesgo basada en la responsabilidad, la comunicación abierta y la mejora continua.

5.4.8 Mejora continua

El sistema de gestión del riesgo debe estar en permanente evolución. ECOTEC promoverá la revisión sistemática del sistema, identificando oportunidades de mejora,

corrigiendo desviaciones y adaptándose a los cambios del entorno. Esta mejora continua es esencial para garantizar que el sistema mantenga su vigencia, eficacia y alineación con los objetivos institucionales.

5.5. Marco de referencia

La implementación eficaz de la gestión de riesgos requiere más que herramientas y metodologías técnicas; demanda la construcción de un marco de referencia sólido que establezca cómo se articulará el sistema de manera coherente con la misión, visión, estructura y procesos de la organización. Este marco debe permitir no solo implementar, sino también mantener y mejorar la gestión del riesgo de forma continua a lo largo del tiempo.

En la Universidad ECOTEC, el marco de referencia propuesto responde a las particularidades del entorno universitario y se ajusta a los principios establecidos por la norma ISO 31000:2018. Su objetivo principal es asegurar que la gestión del riesgo esté integrada en la toma de decisiones institucionales, en los procesos académicos y administrativos, y en la cultura organizacional. Para ello, se han definido pasos clave que permitirán construir una estructura de gobernanza robusta, con roles claros, procesos bien definidos y mecanismos sostenibles.

Este marco se alinea con los objetivos estratégicos de ECOTEC, los cuales incluyen:

- ✓ Garantizar la calidad de los servicios educativos ofrecidos.
- ✓ Proteger la información y los activos institucionales.
- ✓ Promover un entorno de trabajo seguro, ético y resiliente.
- ✓ Cumplir con las regulaciones vigentes y anticiparse a los cambios normativos.
- ✓ Fomentar la sostenibilidad y la innovación educativa.

Asimismo, se propone que el marco de gestión del riesgo de ECOTEC sea un sistema permanente, que se mantenga a lo largo del tiempo como parte esencial de la gobernanza institucional. Este enfoque permitirá que la universidad no solo enfrente los riesgos actuales, sino que fortalezca su capacidad de adaptación ante riesgos emergentes, tales como ciberataques, pandemias, cambios regulatorios o transformaciones tecnológicas.

5.5.1. Generalidades

El propósito del marco de referencia es garantizar que la gestión del riesgo esté sólidamente integrada en la estructura y los procesos de la Universidad ECOTEC. Esta integración no debe considerarse como un componente adicional o temporal, sino como una parte esencial de la cultura institucional, que guíe la toma de decisiones y refuerce la capacidad de anticipación ante posibles eventos adversos.

De acuerdo con la ISO 31000:2018, la gestión del riesgo debe aplicarse de manera sistemática, estructurada y oportuna en todos los niveles de la organización. Para lograrlo, es fundamental diseñar un marco adaptado al contexto universitario, con políticas claras, principios compartidos y alineado con los objetivos estratégicos y operativos de ECOTEC.

A nivel estratégico, el marco respalda la excelencia académica, la sostenibilidad institucional y la transparencia en la gestión. A nivel operativo, fortalece la seguridad digital, la protección de datos, la continuidad académica y la prevención de incidentes en procesos clave. Esto requiere el compromiso de todos los actores institucionales: desde las autoridades rectorales hasta el personal administrativo, docentes, estudiantes y proveedores.

5.5.2. Liderazgo y Compromiso

El liderazgo es uno de los pilares fundamentales en la gestión del riesgo. La alta dirección de ECOTEC debe asumir un rol visible, proactivo y constante en la promoción del sistema de gestión de riesgos, demostrando su compromiso mediante acciones concretas. Este compromiso no debe limitarse a la firma de documentos, sino que debe reflejarse en la asignación de recursos, la participación activa en los procesos clave y una comunicación clara sobre la importancia del sistema.

La dirección institucional tiene la responsabilidad de integrar la gestión del riesgo en la planificación estratégica, estableciendo objetivos claros y medibles relacionados con la prevención, mitigación y respuesta ante amenazas. Además, debe facilitar la creación de una cultura organizacional que valore la identificación temprana de riesgos y fomente el reporte oportuno de incidentes sin temor a represalias.

El compromiso también se traduce en la creación de canales de retroalimentación, la evaluación periódica de la eficacia del sistema y el liderazgo de los procesos de mejora continua. Es esencial que cada miembro del equipo directivo transmita este mensaje con coherencia a toda la comunidad universitaria, consolidando así una visión compartida orientada a la resiliencia institucional.

5.5.3. Integración

La integración de la gestión del riesgo en ECOTEC implica que este enfoque no sea una actividad aislada ni delegada exclusivamente a una unidad técnica. Por el contrario, debe

estar presente en todos los niveles jerárquicos y en todos los procesos institucionales, desde la formulación de políticas hasta las actividades cotidianas.

Este principio exige que la planificación estratégica, la gestión académica, los procesos financieros, tecnológicos y de vinculación con la comunidad incorporen evaluaciones de riesgo como una parte regular de su funcionamiento. Para ello, es fundamental que los líderes de cada unidad comprendan su rol en el sistema, asuman la responsabilidad de identificar y gestionar riesgos específicos, y promuevan la participación activa de su personal en la gestión de riesgos.

Asimismo, se implementarán programas de sensibilización y formación para capacitar a todos los colaboradores, permitiéndoles reconocer los riesgos asociados a sus actividades y participar activamente en su gestión. La integración también se reflejará en documentos institucionales (reglamentos, procedimientos, protocolos), sistemas informáticos y plataformas de monitoreo que facilitarán la articulación y evaluación continua del sistema.

5.5.4. Diseño

El diseño del marco para la gestión del riesgo es una fase crítica dentro del sistema, ya que su efectividad determinará la capacidad de la organización para identificar, analizar, evaluar y tratar los riesgos de manera efectiva. La norma ISO 31000:2018 establece que el diseño debe ser adaptable, integral y alineado con el propósito institucional, considerando el contexto específico en el que opera la organización.

En la Universidad ECOTEC, este diseño parte de una comprensión profunda de sus necesidades, entorno y objetivos. El marco se concibe como un conjunto articulado de

elementos que dan soporte al sistema de gestión de riesgos, integrando procesos, políticas, recursos, estructuras de decisión y mecanismos de evaluación y mejora.

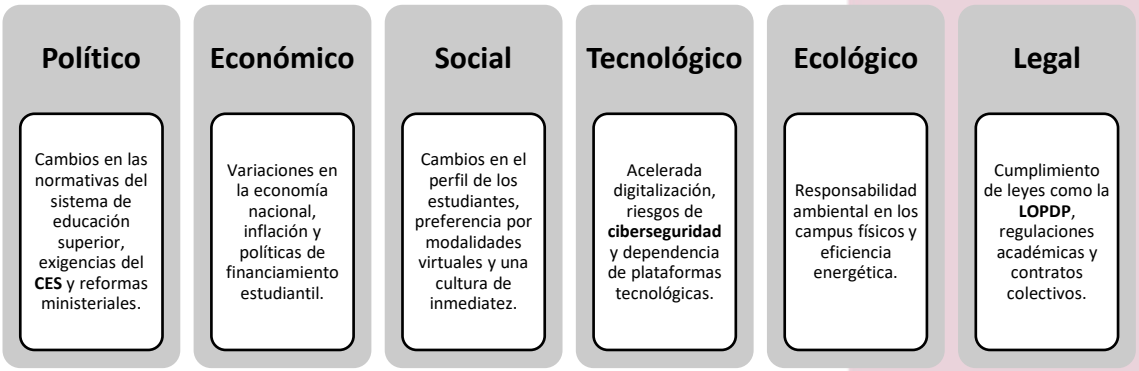
El diseño debe permitir no solo una implementación técnica, sino también una apropiación cultural del sistema. Es decir, debe facilitar que los distintos niveles de la institución se identifiquen con sus objetivos y comprendan cómo su cumplimiento fortalece la seguridad, sostenibilidad y resiliencia institucional.

5.5.4.1. Comprensión de la organización y su contexto

Comprender el entorno en el que opera ECOTEC es esencial para anticiparse a los riesgos que podrían obstaculizar el cumplimiento de sus objetivos institucionales. Esta comprensión requiere un análisis tanto interno como externo, con el fin de identificar los factores que influyen directa o indirectamente en su funcionamiento y sostenibilidad.

Figura 4.

Análisis PESTEL del Contexto Externo de la Universidad ECOTEC



Nota. Esta figura presenta un análisis PESTEL del entorno externo que influye en la gestión de riesgos de ECOTEC, considerando los factores políticos, económicos, sociales, tecnológicos, ecológicos y legales.

5.5.4.2. Articulación del compromiso con la gestión del riesgo

Para formalizar el compromiso de la Universidad ECOTEC con la gestión de riesgos, se elaborará una Política de Gestión de Riesgos institucional, suscrita por la Alta Dirección y difundida a través de todos los canales oficiales. Este documento reflejará el propósito de proteger los activos institucionales, garantizar la continuidad operativa y fomentar una cultura de gestión preventiva.

La política incluirá los siguientes elementos clave:

- ✓ El propósito: Asegurar la anticipación y respuesta ante eventos adversos.
- ✓ Los principios rectores: Proactividad, transparencia, responsabilidad compartida y mejora continua.
- ✓ El alcance: Aplicable a todos los procesos y unidades académicas y administrativas.
- ✓ La metodología adoptada: Basada en los lineamientos de la ISO 31000:2018.
- ✓ La comunicación: Dirigida tanto al personal interno como a las partes interesadas externas.

La política será publicada digitalmente y también será exhibida en espacios visibles como murales institucionales. Además, formará parte de los documentos obligatorios en inducciones al personal y capacitación.

Este compromiso también se reflejará en los recursos asignados, en la revisión periódica del sistema y en la integración de la política en reglamentos, planes de acción y criterios de evaluación institucional.

5.5.4.3. Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas

Una distribución adecuada de responsabilidades es clave para asegurar que la gestión del riesgo no dependa exclusivamente de una unidad específica, sino que involucre activamente a toda la organización.

En el caso de ECOTEC, se propone la siguiente estructura de roles y responsabilidades:

Tabla 28.

Asignación de Roles y Responsabilidades en la Gestión del Riesgo en ECOTEC

Nivel	Rol	Responsabilidades clave
Alta Dirección (Rectorado y Vicerrectorados)	Dirección estratégica del sistema	Aprobar la política, asignar recursos, liderar revisiones anuales, integrar riesgos en la planificación institucional.
Comité Institucional de Gestión de Riesgos	Coordinación central del sistema	Analizar riesgos institucionales, emitir directrices, generar reportes a la alta dirección.
Directores Académicos y Administrativos	Implementación por unidad	Adaptar políticas al contexto de su unidad, identificar y monitorear riesgos específicos, coordinar acciones correctivas.
Responsables de riesgos por área	Ejecución técnica	Mantener registros de incidentes, aplicar herramientas de evaluación, reportar indicadores.
Todo el personal	Participación activa	Reportar riesgos, cumplir protocolos, proponer mejoras, asistir a capacitaciones.

Nota. Esta tabla presenta la asignación de roles y responsabilidades clave dentro de la gestión del riesgo en ECOTEC, distribuidos en los diferentes niveles jerárquicos y áreas de la institución.

5.5.4.4. Asignación de recursos

La implementación y sostenibilidad de un sistema de gestión de riesgos en la Universidad ECOTEC exige una asignación adecuada de recursos en diversas áreas clave, garantizando que cada componente del sistema esté respaldado de manera efectiva. A continuación, se detallan los recursos necesarios para la implementación del sistema:

Tabla 29.

Asignación de Recursos para el Sistema de Gestión de Riesgos en ECOTEC

TIPO DE RECURSO	DESCRIPCIÓN
RECURSOS FINANCIEROS	Se destinará un presupuesto específico para consultorías externas, adquisición de herramientas tecnológicas, capacitaciones especializadas y campañas de sensibilización. Estos fondos formarán parte del presupuesto institucional anual, gestionado por el Rectorado y Planificación Estratégica.
RECURSOS HUMANOS	La universidad aprovechará su estructura organizativa existente, asignando responsabilidades a personal actual sin crear nuevas dependencias. Se contratarán expertos temporales cuando sea necesario. Además, se designarán enlaces de riesgos por facultad o unidad, quienes canalizarán la información y coordinarán las acciones locales.
RECURSOS TECNOLÓGICOS	Se implementarán herramientas digitales para el monitoreo de riesgos, análisis de impacto, gestión documental y comunicación interna. Se evaluarán soluciones de software compatibles con la ISO 31000, con módulos de trazabilidad, alertas y visualización gráfica de indicadores.
RECURSOS DE FORMACIÓN	La capacitación será fundamental. El personal directivo, académico y administrativo recibirá formación en gestión de riesgos, con entrenamientos continuos adaptados a los cambios institucionales y del entorno.

Nota. Esta tabla detalla los recursos necesarios para la implementación y sostenibilidad del sistema de gestión de riesgos en ECOTEC, distribuidos en las áreas clave de finanzas, recursos humanos, tecnología y formación.

1. **Recursos de formación:**

La capacitación será una piedra angular del sistema. El personal directivo, académico y administrativo será entrenado en conceptos básicos y específicos de gestión de riesgos. Estas formaciones deberán ser continuas y adaptadas a los cambios institucionales y del entorno.

Tabla 30.

Estimación de Recursos Necesarios para el Primer Año

Tipo de Recurso	Descripción	Monto Estimado (USD)	Observaciones
Consultoría externa	Asesoría técnica para diseño e implementación inicial	$1,000.00	Etapa inicial del sistema
Licencias de software	Plataforma de gestión de riesgos compatible con ISO 31000	$5,000.00	Evaluación de 2 proveedores
Capacitaciones internas	Formación y talleres para personal clave	$3,500.50	Modalidad presencial y virtual
Desarrollo de materiales comunicativos	Manuales, infografías, cartelería institucional	$7,500.00	Para socialización y consulta pública
Recursos tecnológicos (TI)	Fortalecimiento de infraestructura digital	$16,000.00	Equipos, servidores, respaldo y ciberseguridad
Contingencia operativa	Fondo rotativo para eventos inesperados	$12,000.00	Supervisado por Comité Institucional de Riesgos
Total estimado		**$45,000.00**	

Nota. Esta tabla presenta una estimación de los recursos necesarios para la implementación del sistema de gestión de riesgos en ECOTEC durante su primer año.

5.5.4.5. Establecimiento de la comunicación y la consulta

La gestión del riesgo eficaz requiere una comunicación continua, estructurada y oportuna con todas las partes interesadas, tanto internas como externas. La norma ISO 31000:2018 establece que este componente debe mantenerse activo durante todo el ciclo de gestión de riesgos, desde la identificación hasta la evaluación y tratamiento de los mismos.

En el marco de su sistema de gestión de riesgos, la Universidad ECOTEC reconoce que un flujo de información claro, bidireccional y transversal es esencial para garantizar que las decisiones se tomen sobre una base de entendimiento común, transparente y participativa. Objetivos de la comunicación y consulta:

- ✓ Asegurar que todas las partes interesadas comprendan los riesgos relevantes y su impacto.
- ✓ Recoger aportes de expertos, personal operativo, estudiantes y actores externos.
- ✓ Facilitar la toma de decisiones informadas y alineadas con la política institucional de riesgos.
- ✓ Fortalecer la cultura organizacional en torno a la gestión de riesgos.

5.5.4.5.1. Propuesta de mecanismos institucionales para comunicar y consultar:

Se propone establecer el Sistema Institucional de Información y Consulta de Riesgos (SIIC-R), una plataforma híbrida (física y digital) que centralice la comunicación y consulta de aspectos relacionados con los riesgos universitarios. Este sistema operará bajo los siguientes componentes:

Tabla 31.

Mecanismos de Comunicación y Consulta para la Gestión de Riesgos en ECOTEC

Mecanismo	Descripción	Frecuencia / Acceso
Boletines electrónicos mensuales	Informes breves sobre los riesgos identificados, las medidas tomadas y las recomendaciones preventivas.	Enviados mensualmente al correo institucional de toda la comunidad.
Panel de gestión de riesgos	Sección en el portal interno donde se publican la política, reportes, matrices y documentos relacionados.	Disponible 24/7 para personal y estudiantes a través de la intranet.
Canal de reportes y sugerencias	Formulario digital y físico para informar sobre riesgos o anomalías.	Acceso anónimo y confidencial; revisión semanal.
Jornadas participativas y foros abiertos	Encuentros presenciales y virtuales con representantes de áreas académicas y administrativas.	Trimestrales, con actas de compromisos y seguimiento.
Carteleras físicas informativas	Espacios visibles con infografías, alertas, normas y protocolos de seguridad.	Actualización mensual en facultades y zonas comunes.
Capacitaciones interactivas	Talleres y cursos sobre gestión de riesgos, con materiales accesibles y casos reales.	Plan anual aprobado por el Comité de Riesgos.

Nota. La tabla presenta los mecanismos propuestos para la comunicación y consulta en la gestión de riesgos de ECOTEC, detallando los canales, la frecuencia y el acceso a cada uno, con el fin de garantizar una comunicación fluida y eficaz entre todos los actores institucionales.

5.5.4.5.2. Responsables y evaluación del proceso:

El Comité Central de Gestión de Riesgos coordinará el SIIC-R, con apoyo del Departamento de Comunicación Institucional. Se realizará un informe semestral que analice el impacto de las acciones comunicacionales, midiendo indicadores como nivel de participación, consultas atendidas, mejoras implementadas y efectividad del canal de reportes.

Este enfoque garantiza que la comunicación no sea un acto unidireccional, sino un proceso integrador que permita mejorar la gestión de riesgos, fortalecer la gobernanza institucional y fomentar el compromiso colectivo con la seguridad y la sostenibilidad.

5.5.5. Implementación

La implementación del sistema de gestión de riesgos en la Universidad ECOTEC marca la fase de operativización del marco diseñado. Es en esta etapa donde las políticas, estrategias y recursos previamente definidos se traducen en acciones concretas y sistemáticas.

Este proceso se llevará a cabo de manera progresiva y estructurada, respetando la cultura organizacional existente y adaptándose al entorno institucional. Para garantizar su éxito, los responsables designados deben tener claras sus funciones y, sobre todo, contar con los medios adecuados para cumplir con los objetivos establecidos.

5.5.5.1. Fases de la implementación:

Tabla 32.

Fases de Implementación del Sistema de Gestión de Riesgos en ECOTEC

Fase	Descripción de la acción
1. Socialización del sistema de gestión de riesgos	- Lanzamiento oficial mediante jornadas institucionales. - Entrega de material informativo (manuales, trípticos, videos explicativos). - Publicación de la política de gestión de riesgos en medios físicos y digitales.
2. Capacitación y formación continua	- Cronograma de formación adaptado a cada nivel organizacional. - Talleres prácticos para identificar, analizar, valorar y responder a los riesgos. - Evaluación de las competencias adquiridas en los talleres y programas de formación.
3. Incorporación del riesgo en los procesos institucionales	- Integración en los planes estratégicos, operativos y de contingencia de la universidad. - Revisión de procedimientos clave para asegurar que el enfoque preventivo sea parte de los mismos.

4. Puesta en marcha de herramientas de seguimiento	- Activación del sistema de monitoreo digital de riesgos. - Establecimiento de rutinas de revisión periódica de eventos y controles para evaluar su efectividad.
5. Retroalimentación y mejora continua	- Revisión de resultados iniciales para evaluar el progreso de la implementación. - Identificación de brechas y ajustes en las acciones para mejorar el sistema de gestión de riesgos.

Nota. Esta tabla presenta las fases clave de la implementación del sistema de gestión de riesgos en ECOTEC, detallando las acciones necesarias para cada etapa del proceso.

La implementación contará con una supervisión permanente del Comité Central de Gestión de Riesgos, que garantice que cada área cumpla con lo planificado y que los recursos estén siendo utilizados de manera eficiente. La dirección universitaria debe mantener su compromiso activo durante esta etapa, promoviendo el aprendizaje organizacional y la adaptación continua.

5.5.6. Valoración

Una vez implementado el sistema de gestión de riesgos, es indispensable valorar su efectividad y eficiencia. La valoración, conforme a la norma ISO 31000:2018, tiene como propósito determinar en qué medida se están cumpliendo los objetivos propuestos, si los riesgos están siendo gestionados adecuadamente y si los controles son eficaces y pertinentes.

Este proceso de valoración debe ser sistemático, objetivo y basado en evidencia verificable.

5.5.6.1. Componentes de la valoración:

Frecuencia y responsabilidad de la valoración:

La valoración se realizará de manera semestral y anual, de acuerdo al cronograma institucional aprobado. Será responsabilidad del Comité Central de Gestión de Riesgos, en coordinación con la Dirección de Planificación y la Unidad de Control Interno.

Los resultados se presentarán en informes detallados ante la Alta Dirección, quienes deberán tomar decisiones oportunas para reforzar las fortalezas detectadas y atender las debilidades identificadas.

Esta etapa fortalece el principio de mejora continua, permitiendo una evolución progresiva del sistema, adaptado a los cambios del entorno, a los nuevos desafíos institucionales y a las lecciones aprendidas de eventos pasados.

5.5.7. Mejora

El sistema de gestión de riesgos no debe concebirse como una estructura estática, sino como un proceso dinámico que evoluciona en función de los cambios internos y del entorno. La mejora del sistema garantiza su vigencia, pertinencia y eficacia, permitiendo que la Universidad ECOTEC mantenga un alto nivel de resiliencia institucional frente a amenazas emergentes.

Este componente del marco de referencia busca establecer mecanismos formales que permitan identificar oportunidades de mejora y actuar proactivamente frente a fallas, desviaciones o condiciones cambiantes. Todo sistema que no mejora, inevitablemente pierde capacidad de respuesta ante nuevos escenarios.

5.5.7.1. Adaptación

La capacidad de adaptación es fundamental para que el sistema de gestión de riesgos conserve su funcionalidad y aporte valor a lo largo del tiempo. Esta capacidad requiere observar continuamente el contexto organizacional, revisar los factores internos y externos, y ajustar las políticas, procesos y herramientas del sistema.

En el caso de ECOTEC, la adaptación será especialmente importante ante los siguientes escenarios:

- ✓ Cambios en la normativa educativa nacional o internacional.
- ✓ Incorporación de nuevas tecnologías o modalidades académicas (por ejemplo, educación híbrida).
- ✓ Cambios en las expectativas de los estudiantes o en la composición del personal.
- ✓ Eventos inesperados como emergencias sanitarias, conflictos sociales o ciberataques.

Para facilitar la adaptación, se establecerán revisiones periódicas del marco de gestión, al menos una vez por año, o cada vez que se produzca un cambio significativo en el entorno institucional. Estas revisiones estarán a cargo del Comité Central de Gestión de Riesgos, el cual contará con insumos proporcionados por todas las unidades académicas y administrativas.

El sistema podrá incorporar nuevos indicadores, redefinir prioridades de tratamiento de riesgos, o incluso rediseñar mecanismos de control cuando estos resulten ineficaces o superados por los acontecimientos.

5.5.7.2. Mejora continua

La mejora continua es uno de los principios fundamentales de la norma ISO 31000:2018. Implica un compromiso institucional constante con la excelencia, mediante el aprendizaje organizacional, la innovación y la revisión crítica del propio desempeño.

En ECOTEC, este principio se materializará a través de las siguientes acciones:

Tabla 33.

Acciones para la Mejora Continua en ECOTEC

Acción	Descripción
Evaluación constante de resultados	Realización de auditorías internas, análisis de desempeño e informes de gestión para identificar no conformidades, brechas y oportunidades de mejora.
Lecciones aprendidas	Documentación y análisis de cada incidente, simulacro o desviación para extraer aprendizajes y evitar su repetición o permitir mejoras sustanciales.
Propuestas desde los equipos de trabajo	Fomento de una cultura de participación donde todo el personal pueda sugerir mejoras, innovaciones o alertas sobre debilidades del sistema.
Actualización del marco normativo interno	Revisión periódica de manuales, políticas, procedimientos y protocolos, incorporando ajustes y novedades derivadas del monitoreo y evaluación.
Reconocimiento del buen desempeño	Establecimiento de incentivos o certificaciones internas para unidades que destaquen por su gestión eficaz del riesgo.

Nota. Esta tabla sintetiza las acciones clave para la mejora continua del sistema de gestión de riesgos en ECOTEC, alineadas con los principios de la ISO 31000:2018.

Este enfoque garantizará que el sistema de gestión de riesgos no solo se mantenga operativo, sino que evolucione con la universidad, promoviendo una cultura institucional de responsabilidad, sostenibilidad y prevención.

5.6. Proceso

La gestión de riesgos en la Universidad Tecnológica ECOTEC se concibe como un proceso estructurado y sistemático que aplica políticas, procedimientos y prácticas enfocadas en la identificación, análisis, evaluación, tratamiento, seguimiento, comunicación y registro de los riesgos que puedan afectar el cumplimiento de sus objetivos institucionales.

Este proceso permite a la universidad anticiparse proactivamente a los eventos adversos que puedan surgir, particularmente en áreas clave como la continuidad académica virtual, la integridad de la información, la disponibilidad de las plataformas tecnológicas y la confianza de los grupos de interés.

La gestión de riesgos se lleva a cabo dentro de un ciclo continuo que incluye los siguientes componentes interdependientes:

Tabla 34.

Componentes del Proceso de Gestión de Riesgos en ECOTEC

Componente	Descripción
Comunicación y consulta	Garantizar el flujo de información claro y bidireccional entre las partes interesadas.
Establecimiento del alcance, contexto y criterios	Definir los parámetros dentro de los cuales se gestionan los riesgos.
Evaluación del riesgo	Incluye la identificación, análisis y valoración de los riesgos potenciales.
Tratamiento del riesgo	Desarrollar estrategias para mitigar, transferir, aceptar o evitar los riesgos identificados.
Seguimiento y revisión	Monitorear los riesgos de forma continua y evaluar la efectividad de las acciones tomadas.
Registro e informe del riesgo	Documentar los riesgos y las acciones implementadas, garantizando la trazabilidad y la comunicación clara de los resultados.

Nota. Esta tabla presenta los componentes clave del proceso de gestión de riesgos en ECOTEC, basados en los principios establecidos por la ISO 31000:2018.

5.6.1. Generalidades

La gestión del riesgo en la Universidad ECOTEC se concibe como un proceso integrador y transversal, aplicado a todas las unidades académicas, administrativas y tecnológicas. Su propósito es fortalecer la gobernanza institucional y proteger los entornos virtuales y físicos de aprendizaje. Este proceso se basa en un enfoque estructurado, adaptativo y continuo que involucra a todos los niveles y actores de la institución.

Tabla 35.

Objetivos Clave del Proceso de Gestión de Riesgos en ECOTEC

Objetivo	Descripción
Apoyo a la toma de decisiones	Facilita la toma de decisiones estratégicas y operativas, especialmente en áreas como tecnologías educativas, protección de datos personales, continuidad académica y gestión de plataformas internas.
Alineación con objetivos institucionales	Se alinea con los objetivos estratégicos de ECOTEC, como la excelencia educativa, innovación tecnológica, calidad en los servicios y seguridad de la información.
Dinámica, iterativa y adaptable	El sistema de gestión de riesgos se mantiene dinámico, iterativo y adaptable, permitiendo su revisión constante ante nuevas amenazas, cambios normativos o tecnológicos.
Participación activa	Fomenta la participación activa de las partes interesadas (estudiantes, docentes, personal técnico, proveedores y autoridades regulatorias), garantizando la mejora continua del sistema.

Nota. Esta tabla resume los objetivos clave del proceso de gestión de riesgos en ECOTEC, alineados con los principios establecidos por la norma ISO 31000:2018, con un enfoque en la toma de decisiones, la alineación con los objetivos estratégicos y la mejora continua.

5.6.2. Comunicación y consulta

Estos ejes fundamentales son esenciales para la implementación y sostenibilidad del sistema de gestión de riesgos en la organización, cuyo propósito es garantizar que todas las personas y entidades involucradas comprendan claramente los riesgos que pueden afectar a la institución, y participen activamente en su tratamiento mediante acciones preventivas, correctivas y de mejora continua. Este enfoque asegura la proactividad de la institución en la gestión de riesgos, facilitando una respuesta oportuna ante los mismos.

El proceso comunicacional será transversal a todas las etapas del sistema, abarcando desde la identificación, análisis y valoración de los riesgos, hasta su tratamiento, seguimiento, revisión y documentación. La participación activa de los diferentes niveles organizacionales y de las partes interesadas externas fortalecerá tanto la legitimidad como la eficacia del sistema de gestión de riesgos, favoreciendo un enfoque inclusivo que asegura una comprensión integral del proceso en toda la universidad.

Canales y métodos de comunicación

Se dispondrá de diversos medios de comunicación para facilitar la circulación de la información relacionada con la gestión de riesgos dentro de la universidad. Los canales y métodos incluyen:

- ✓ Comunicados institucionales oficiales vía correo electrónico interno.
- ✓ Reuniones técnicas periódicas en cada unidad académica y administrativa.
- ✓ Informes de seguimiento de riesgos generados por el Comité de Seguridad Informática.

- ✓ Boletines digitales de cultura preventiva, accesibles desde el portal institucional.
- ✓ Foros y espacios de consulta en plataformas virtuales de aprendizaje (Moodle).
- ✓ Talleres presenciales y capacitaciones periódicas, especialmente dirigidas a personal TIC, autoridades y docentes.
- ✓ Circulares impresas en áreas estratégicas como laboratorios, salas de servidores y oficinas administrativas.
- ✓ Paneles informativos y pantallas digitales en puntos de alta circulación dentro del campus.

Responsables de la comunicación

A continuación, se detallan las áreas y roles responsables de la comunicación dentro del sistema de gestión de riesgos:

Tabla 36.

Canales y Métodos de Comunicación en la Gestión de Riesgos

Área / Rol	Responsabilidad Específica
Dirección de Tecnologías de la Información	Coordinar la emisión de alertas técnicas y actualizaciones de seguridad.
Comité de Gestión de Riesgos	Elaborar los informes técnicos y difundir las conclusiones de análisis y evaluación.
Departamento de Comunicación Institucional	Asegurar la coherencia de los mensajes institucionales y su adecuada difusión externa.
Unidades Académicas	Informar a docentes y estudiantes sobre protocolos y medidas ante riesgos detectados.
Personal administrativo	Canalizar consultas y observaciones hacia los equipos técnicos.

Nota. Esta tabla presenta los canales y métodos de comunicación utilizados en ECOTEC para facilitar la circulación de la información relacionada con la gestión de riesgos, promoviendo la participación activa de la comunidad.

Etapas de la comunicación dentro del sistema de riesgos

La comunicación será clave en cada fase del proceso de gestión de riesgos. A continuación, se presenta cómo se gestionará la comunicación en cada etapa:

Tabla 37.

Responsables de la Comunicación en la Gestión de Riesgos

Área / Rol	Responsabilidad Específica
Dirección de Tecnologías de la Información	Coordinar la emisión de alertas técnicas y actualizaciones de seguridad.
Comité de Gestión de Riesgos	Elaborar los informes técnicos y difundir las conclusiones de análisis y evaluación.
Departamento de Comunicación Institucional	Asegurar la coherencia de los mensajes institucionales y su adecuada difusión externa.
Unidades Académicas	Informar a docentes y estudiantes sobre protocolos y medidas ante riesgos detectados.
Personal administrativo	Canalizar consultas y observaciones hacia los equipos técnicos.

Nota. Esta tabla describe las áreas y roles responsables de la comunicación dentro del sistema de gestión de riesgos, asegurando la correcta transmisión de la información relevante a todas las partes involucradas.

Consulta a partes interesadas

La consulta regular se realizará con actores relevantes del entorno interno (estudiantes, docentes, administrativos, directivos) y externo (proveedores tecnológicos, organismos reguladores, comunidad académica), mediante encuestas, focus groups, buzones virtuales y comités mixtos. esto permitirán recoger percepciones sobre amenazas emergentes, brechas operativas y oportunidades de mejora.

5.6.3. Alcance, contexto y criterios

5.6.3.1. Generalidades

Esta sección establece las bases fundamentales para comprender el entorno en el que se implementará el sistema de gestión del riesgo. Su correcta formulación permite establecer límites claros, identificar las amenazas y oportunidades, así como definir criterios de actuación acordes al funcionamiento real de la institución**.**

5.6.3.2. Definición del alcance

El alcance del sistema de gestión de riesgos abarcará todos los procesos relacionados con la seguridad de los entornos virtuales de aprendizaje y los sistemas informáticos internos de la universidad. Este enfoque garantiza una cobertura integral de los componentes críticos que sostienen la operación académica y administrativa en ECOTEC.

Componentes incluidos en el alcance:

Figura 5.

Componentes del Sistema de Gestión de Riesgos en ECOTEC

Nota. Esta ilustración muestra los principales componentes involucrados en la gestión de riesgos en ECOTEC, destacando las plataformas digitales, infraestructura tecnológica, sistemas de almacenamiento de datos, conectividad y seguridad de redes internas, así como la atención a incidentes informáticos. Estos elementos son clave para garantizar la seguridad y continuidad operativa dentro de la universidad.

Este alcance se aplicará a todas las unidades de ECOTEC que intervienen directa o indirectamente en el diseño, operación, soporte, monitoreo y mejora de los entornos virtuales, abarcando tanto el ámbito estratégico como operativo de la universidad. Las áreas clave involucradas serán:

- ✓ Dirección de Tecnología.
- ✓ Dirección Académica Virtual.
- ✓ Dirección de Planificación Estratégica.
- ✓ Dirección Administrativa y Financiera.
- ✓ Dirección Jurídica (para soporte regulatorio y cumplimiento).
- ✓ Departamento de Seguridad Informática.

Perspectiva Temporal, Espacial y Organizacional

La implementación del sistema de gestión de riesgos se llevará a cabo en tres fases durante un periodo inicial de 12 meses, con revisión semestral para garantizar su efectividad y adaptabilidad a los cambios. Esta implementación se aplicará espacialmente en los campus físicos y entornos digitales de la universidad, asegurando su integración en todas las áreas de la institución.

Desde una perspectiva organizacional, el sistema impactará en los niveles estratégicos (alta dirección), tácticos (jefaturas de área) y operativos (técnicos y personal de soporte), promoviendo un enfoque colaborativo en todos los niveles.

Recursos y Requerimientos

ECOTEC cuenta con recursos humanos capacitados en seguridad informática, así como herramientas de monitoreo básicas, servidores institucionales y protocolos de respuesta ante incidentes. Sin embargo, para asegurar la viabilidad y sostenibilidad del sistema de gestión de riesgos, será necesario reforzar los siguientes aspectos clave:

1. Adquisición de plataformas para la gestión centralizada de riesgos digitales, lo que permitirá una gestión más eficiente y controlada de los riesgos cibernéticos.
2. Diseño de un plan de capacitación continua para el personal técnico y los usuarios finales, garantizando que todos los involucrados tengan las habilidades necesarias para operar y proteger los entornos virtuales de manera efectiva.

Estas iniciativas fortalecerán la implementación y asegurarán que el sistema de gestión de riesgos sea sostenible y eficaz a largo plazo, en línea con la misión de ECOTEC de proporcionar una educación de calidad en un entorno digital seguro y confiable.

Procedimiento para la Generación de Procedimientos

El procedimiento para la generación de procedimientos es un componente esencial en la implementación de un sistema de gestión de riesgos estructurado, ya que asegura que todos los procesos sean documentados, evaluados y gestionados de manera efectiva y coherente. Este procedimiento debe seguir un ciclo claro que permita la creación, revisión, y mejora continua de todos los procedimientos de gestión de riesgos.

Objetivos del Procedimiento

1. Establecer un enfoque estandarizado para la creación de nuevos procedimientos dentro del sistema de gestión de riesgos.
2. Garantizar que los procedimientos sean coherentes con los principios establecidos por la norma ISO 31000 y con los objetivos institucionales de ECOTEC.
3. Asegurar que todos los procedimientos sean claros, accesibles y comprendidos por los miembros clave de la organización.

Fases del Procedimiento para la Generación de Procedimientos

El siguiente procedimiento describe las etapas clave para la creación, implementación y evaluación de nuevos procedimientos de gestión de riesgos en la Universidad ECOTEC, asegurando que cada uno se alinee con los principios de la ISO 31000:2018 y con los objetivos institucionales de la universidad.

Tabla 38.

Procedimiento para la Generación de Procedimientos en la Gestión de Riesgos de ECOTEC

1. Identificación de la Necesidad de un Procedimiento	Comité de Gestión de Riesgos	Identificar áreas donde sea necesario establecer un procedimiento de gestión de riesgos. Esto puede ser a raíz de incidentes, análisis de riesgos, o cambios normativos.
2. Definición del Propósito y Alcance del Procedimiento	Dirección de Tecnología y Dirección Académica Virtual	Definir el objetivo específico del procedimiento, su alcance dentro de la organización, las partes interesadas involucradas, y los riesgos que se abordarán.
3. Desarrollo del Procedimiento	Responsable del área (dependiendo del riesgo a gestionar)	Redactar el procedimiento, que debe incluir: objetivos y metas, estrategias y acciones específicas, roles y responsabilidades,

		recursos necesarios, e indicadores de rendimiento.
4. Revisión y Aprobación del Procedimiento	Comité de Gestión de Riesgos, junto con los responsables de cada área	Someter el procedimiento a una revisión detallada para asegurar su coherencia con los estándares de ISO 31000 y con las necesidades de ECOTEC. Se obtiene aprobación institucional.
5. Implementación del Procedimiento	Área operativa correspondiente	Poner en marcha el procedimiento dentro de la institución, asegurando que todos los miembros relevantes reciban la formación adecuada y los recursos necesarios.
6. Monitoreo y Evaluación del Procedimiento	Comité de Gestión de Riesgos y Dirección Administrativa	Monitorear la ejecución del procedimiento, evaluando su eficacia, identificando áreas de mejora y tomando las acciones correctivas necesarias.
7. Revisión y Mejora Continua	Comité de Gestión de Riesgos	Revisión periódica del procedimiento para asegurar que se mantenga actualizado frente a cambios en el contexto institucional, amenazas emergentes y avances en las mejores prácticas de gestión de riesgos.

Nota. Esta tabla describe las fases clave en la creación y gestión de procedimientos para la gestión de riesgos en ECOTEC, alineadas con los estándares de la norma **ISO 31000:2018**, garantizando un enfoque estructurado y adaptable.

5.6.3.3. Contextos Externo e Interno

Contexto Externo

La gestión de riesgos en ECOTEC se lleva a cabo en un entorno complejo, dinámico y sujeto a múltiples factores externos que pueden influir directamente en la seguridad de sus entornos virtuales de aprendizaje y la protección de sus sistemas informáticos. Para

comprender de manera más efectiva estos factores, se emplea el modelo de análisis PESTEL, que permite identificar y evaluar los elementos clave que configuran el entorno institucional.

Tabla 39.

Análisis PESTEL del Contexto Externo de ECOTEC

Factor PESTEL	Descripción del Contexto
Político	Las políticas educativas nacionales y las reformas en el sistema de educación superior influyen en los requerimientos tecnológicos y regulatorios de la universidad. Asimismo, existen riesgos relacionados con cambios en normativas de protección de datos y ciberseguridad.
Económico	Factores como inflación, recortes presupuestarios y fluctuaciones en los costos de los servicios tecnológicos afectan la capacidad de inversión en herramientas y sistemas de protección digital.
Social	Las crecientes demandas estudiantiles en cuanto a accesibilidad, conectividad y flexibilidad educativa aumentan la presión sobre los entornos virtuales, exigiendo respuestas rápidas ante incidentes informáticos y ciberataques.
Tecnológico	La innovación tecnológica constante exige que la universidad se adapte rápidamente a nuevas herramientas y se proteja de amenazas emergentes como ransomware o brechas de datos que puedan comprometer la seguridad digital.
Ambiental	Eventos climáticos extremos pueden interrumpir la conectividad o dañar infraestructuras físicas, afectando la continuidad de la educación virtual y la operación de los servicios tecnológicos de la universidad.
Legal	Las normativas ecuatorianas relacionadas con la protección de datos personales, la propiedad intelectual y la educación virtual imponen estrictas obligaciones que la universidad debe cumplir rigurosamente para evitar multas y sanciones.

Nota. Esta tabla resume el análisis PESTEL del contexto externo en el que ECOTEC opera, identificando los factores políticos, económicos, sociales, tecnológicos, ambientales y legales que afectan la gestión de riesgos en la institución.

Partes Interesadas Externas Relevantes para la Universidad ECOTEC

Las partes interesadas externas juegan un papel crucial en la gestión de riesgos de ECOTEC, ya que influyen directamente o indirectamente en las decisiones estratégicas y operativas de la universidad. Por lo tanto, su participación debe ser tomada en cuenta al planificar, gestionar y evaluar los riesgos asociados a los sistemas digitales institucionales.

Tabla 40.

Partes Interesadas Externas de ECOTEC y su Impacto en la Gestión de Riesgos

Parte Interesada	Descripción de la Influencia
Consejo de Educación Superior (CES)	Regula y establece los lineamientos para la educación superior en Ecuador, lo que influye en los requisitos tecnológicos y académicos de la universidad.
Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT)	Impone normativas y directrices que afectan la gestión educativa y las plataformas de aprendizaje, además de definir los estándares de calidad educativa.
Proveedores de servicios tecnológicos y plataformas de aprendizaje	Aportan las herramientas tecnológicas y plataformas educativas que permiten la operación de los entornos virtuales, siendo clave para la protección digital y seguridad de la información.
Empresas con convenios de prácticas profesionales	Facilitan oportunidades de prácticas profesionales, lo que implica la necesidad de gestionar los riesgos laborales y las condiciones de seguridad en estos entornos.
Comunidad educativa (familias, sociedad en general)	La comunidad educativa incluye a los estudiantes, padres y otros miembros de la sociedad que dependen de la calidad educativa y seguridad de los sistemas de ECOTEC.
Entidades reguladoras en protección de datos	Organismos como la Superintendencia de Protección de Datos establecen normativas para asegurar el cumplimiento de regulaciones de protección de datos y la seguridad cibernética.

Nota. Esta tabla identifica las partes interesadas externas que tienen un impacto directo o indirecto en la gestión de riesgos de ECOTEC, particularmente en lo que respecta a los sistemas digitales y la protección de datos. La inclusión de estas partes en el proceso de gestión de

riesgos es fundamental para garantizar un enfoque integral y alineado con los principios de la ISO 31000.

Contexto Interno

El contexto interno de ECOTEC está compuesto por los elementos que definen su identidad institucional, estructura funcional y funcionamiento operativo. Estos factores son esenciales para el diseño e implementación de un sistema de gestión de riesgos efectivo, ya que impactan directamente en las capacidades de la universidad para anticipar, gestionar y mitigar riesgos. A continuación, se describen los factores clave identificados:

Tabla 41.

Factores Clave del Contexto Interno en ECOTEC

Factor	Descripción
Estructura organizacional	ECOTEC cuenta con un organigrama jerárquico bien definido que incluye al Rectorado, Vicerrectorados, Direcciones Académicas, Administrativas y Técnicas. Esto permite una distribución clara de roles y responsabilidades, facilitando la gestión del riesgo, especialmente en temas informáticos y digitales.
Cultura organizacional	Se fomenta una cultura de innovación, calidad educativa y responsabilidad institucional. Sin embargo, existen desafíos en la concienciación sobre la importancia de la seguridad digital, lo que requiere reforzar la cultura preventiva en todos los niveles organizacionales.
Recursos disponibles	La universidad cuenta con infraestructura tecnológica avanzada, redes internas, servidores y plataformas virtuales, junto con personal técnico capacitado. No obstante, se identifican necesidades en cuanto a herramientas de ciberseguridad, sistemas de monitoreo continuo y formación especializada.
Estrategia institucional	El Plan Estratégico de ECOTEC prioriza el fortalecimiento de la educación digital y la gestión de calidad. Este enfoque representa una oportunidad clave para consolidar un sistema de gestión de riesgos que no solo mitigue amenazas, sino que también agregue valor y sostenibilidad a la universidad.

Nota. En esta tabla se muestran los factores en el contexto interno en ECOTEC.

Partes interesadas internas

Las partes interesadas internas son aquellos actores clave dentro de ECOTEC que, debido a su rol en los procesos institucionales, impactan directamente en la gestión de riesgos. Las principales partes interesadas internas identificadas son:

- ✓ Rector y Vicerrectores: Responsables de la toma de decisiones estratégicas y la supervisión general de los procesos institucionales.
- ✓ Dirección de Tecnología: Encargada de gestionar la infraestructura tecnológica y las plataformas digitales utilizadas en la universidad.
- ✓ Dirección Académica Virtual: Gestiona los entornos virtuales de aprendizaje y asegura la calidad educativa en el ámbito digital.
- ✓ Dirección Administrativa y Financiera: Responsable de la gestión financiera y administrativa, incluyendo la asignación de recursos para la gestión de riesgos.
- ✓ Coordinaciones de Carreras: Facilitan la integración de la gestión de riesgos dentro de las actividades académicas y operativas de cada facultad.
- ✓ Estudiantes, docentes y personal administrativo: Todos los miembros de la comunidad universitaria tienen un papel activo en la gestión de riesgos, desde la adopción de buenas prácticas hasta la participación en la capacitación y comunicación.

Interacción y Coordinación

La interacción entre estas partes interesadas es fundamental para la eficacia de los procesos institucionales. A su vez, esta interacción genera riesgos asociados a su operación. Es esencial establecer mecanismos de comunicación, coordinación y evaluación de riesgos que permitan anticipar, mitigar y tratar cualquier evento que pueda comprometer la seguridad

tecnológica de la universidad. Esto incluye desde la planificación estratégica hasta la gestión operativa de los sistemas digitales y tecnológicos.

5.6.3.4. Definición de los criterios de riesgo

Establecimiento de Parámetros de Valoración

Para garantizar una evaluación objetiva y coherente de los riesgos, se han establecido dos escalas fundamentales: una para probabilidad y otra para impacto, ambas definidas en tres niveles (bajo, medio y alto), con valores asignados del 1 al 3. La combinación de ambas escalas genera una matriz de calor (probabilidad × impacto), que permite clasificar los riesgos en tres niveles de gravedad.

Tabla 42.

Matriz de Calor de Riesgos

Nivel de Riesgo	Interpretación	Acción recomendada
Alto (6-9)	Riesgo **inaceptable**	Requiere **intervención inmediata**
Medio (4-5)	Riesgo **moderado**	Requiere **medidas correctivas**
Bajo (1-3)	Riesgo **aceptable con control**	Mantener los **controles actuales**

Nota. Esta tabla presenta la matriz de calor para clasificar los riesgos de acuerdo con su probabilidad e impacto. La combinación de ambas escalas permite determinar las acciones recomendadas según el nivel de riesgo identificado.

Tabla 43.

Mapa de Calor de Riesgos

	Bajo (1)	**Medio (2)**	**Alto (3)**
Bajo (1)	1	2	3
Medio (2)	2	4	6
Alto (3)	3	6	9

Nota. El mapa de calor permite visualizar de forma rápida los riesgos en función de su probabilidad e impacto. Los valores resultantes determinan las acciones a seguir para cada nivel de riesgo.

Consideraciones Clave

En la determinación de los niveles de riesgo se han considerado los siguientes aspectos esenciales:

- ✓ Cumplimiento normativo: Se ha considerado el marco legal y las regulaciones vigentes que rigen a las instituciones de educación superior, como la Ley de Protección de Datos Personales y otros requisitos regulatorios.
- ✓ Expectativas de las partes interesadas: Los estudiantes, docentes, personal administrativo y proveedores esperan que los riesgos institucionales, especialmente los relacionados con la seguridad digital, sean gestionados de forma eficaz y oportuna.
- ✓ Valores institucionales: ECOTEC mantiene como pilares fundamentales la integridad académica, la excelencia tecnológica y la continuidad operativa. La presencia de riesgos que afecten estos principios justifica una respuesta inmediata y proactiva.

Clasificación de Riesgos Críticos

A partir del análisis de riesgos realizado en el anterior capítulo, se han identificado los siguientes riesgos críticos (con una puntuación de 9 puntos), los cuales presentan una alta probabilidad e impacto significativo sobre la seguridad de los entornos virtuales de aprendizaje y los sistemas informáticos de la universidad. Estos riesgos requieren atención prioritaria y la implementación de planes de acción correctivos y preventivos:

- Errores de los usuarios en equipos de cómputo
- Fuga de información en trabajos móviles (teléfonos)
- Alteración de la información en trabajos móviles
- Robo de dispositivos con acceso a internet
- Corte del suministro eléctrico en servidores externos
- Fallo de servicios de comunicación en servidores externos
- Difusión de software dañino en almacenamiento interno

Cada uno de estos escenarios representa una amenaza significativa para la seguridad de la universidad y requiere acciones inmediatas.

Acciones Preventivas Propuestas para Riesgos Críticos

A continuación, se presentan las acciones preventivas propuestas para los riesgos críticos identificados, con los responsables, costos estimados y plazos de ejecución:

Tabla 44.

Acciones Preventivas para Riesgos Críticos

Riesgo Identificado	Acción Preventiva	Responsable	Costo Estimado (USD)	Plazo de Ejecución

Errores de los usuarios	Capacitación en **ciberseguridad** y manejo seguro de la información	Coordinación TIC y Talento Humano	3500	2 meses
Fuga y alteración de información (móvil)	Encriptación de **datos** y control de acceso a dispositivos móviles	Coordinación TIC	2000	1 mes
Robo de dispositivos	Política de uso de **dispositivos**, **GPS** de seguridad y concienciación del personal	Coordinación Administrativa	2800	2 meses
Corte del suministro eléctrico	Instalación de **UPS** y generador auxiliar en servidores clave	Dirección de Tecnología	6500	3 meses
Fallo de comunicaciones (servidores)	Contrato redundante con segundo proveedor ISP y auditoría de red	Dirección de Tecnología	4000	2 meses
Difusión de software dañino	Actualización de **antivirus** corporativo y monitoreo activo	Coordinación de Seguridad Informática	3000	1 mes

Nota. Esta tabla describe las acciones preventivas propuestas para los riesgos críticos identificados, con los responsables, costos estimados y plazos de ejecución. Estas acciones se diseñan para mitigar los riesgos más significativos que afectan la seguridad de ECOTEC.

Consideraciones Claves para las Acciones Preventivas

Requisitos legales: Las acciones preventivas deben cumplir con la Ley Orgánica de Protección de Datos Personales y las regulaciones del sector educativo relacionadas con la protección de información académica y personal.

Expectativas de las partes interesadas: Estudiantes, docentes y personal administrativo esperan que los sistemas de la universidad sean seguros, accesibles y confiables. Las medidas preventivas son una respuesta al compromiso de ECOTEC para preservar la confianza y asegurar un entorno digital seguro.

Valores organizacionales: Los valores fundamentales de transparencia, responsabilidad y mejora continua guían el tratamiento proactivo de los riesgos, asegurando que la universidad se mantenga a la vanguardia en la gestión de riesgos.

5.6.4. Evaluación del Riesgo

La evaluación del riesgo es un proceso fundamental en la gestión de riesgos, ya que permite clasificar, priorizar y tomar decisiones sobre cómo manejar los riesgos identificados. En el marco de la norma ISO 31000:2018, la evaluación del riesgo implica la comparación de los resultados del análisis de riesgos con los criterios establecidos, con el objetivo de determinar si el riesgo es aceptable o si requiere medidas adicionales. Este proceso contribuye a la toma de decisiones informadas, alineando las acciones de gestión de riesgos con los objetivos estratégicos de la organización.

En el contexto de la Universidad Tecnológica ECOTEC, la evaluación del riesgo busca asegurar que los recursos se asignen de manera eficiente y eficaz, priorizando los riesgos que tienen un mayor impacto en las operaciones y objetivos institucionales. La evaluación debe realizarse de manera periódica y continua, lo que garantiza que el sistema de gestión de riesgos sea adaptable a los cambios en el entorno organizacional y que se pueda reaccionar de manera proactiva ante nuevas amenazas.

5.6.4.1. Generalidades

La evaluación del riesgo es un paso crucial en la gestión de riesgos, conforme a la norma ISO 31000:2018. Este proceso tiene como objetivo evaluar y clasificar los riesgos en función de su probabilidad de ocurrencia y el impacto que podrían tener en los activos, los procesos y los objetivos estratégicos de la organización. Para garantizar su efectividad, la

evaluación debe ser un proceso continuo y actualizado, adaptándose a los cambios en el entorno organizacional y las amenazas emergentes.

En el contexto de la Universidad ECOTEC, la evaluación del riesgo tiene la finalidad de identificar, analizar, valorar y priorizar los riesgos que podrían afectar a la seguridad de los datos, la infraestructura tecnológica y los procesos académicos de la institución. Este enfoque permite tomar decisiones informadas sobre cómo manejar los riesgos, asegurando que los recursos de la universidad se asignen de manera eficiente para minimizar o mitigar los riesgos inaceptables, sin comprometer los objetivos institucionales.

El proceso de evaluación del riesgo debe incluir las siguientes etapas, que permiten un enfoque estructurado y colaborativo, involucrando a todas las partes interesadas:

Tabla 45.

Etapas de la Evaluación del Riesgo en la Universidad ECOTEC

Etapa	Descripción
Identificación del Riesgo	En esta etapa se identifican todos los riesgos potenciales que pueden afectar a la organización, cubriendo tanto amenazas internas como externas. Este paso es fundamental para asegurar que no se omitan riesgos importantes.
Análisis del Riesgo	Consiste en evaluar la probabilidad de que ocurra cada riesgo y el impacto que tendría sobre los activos clave de la universidad. Este análisis permite comprender el contexto de cada amenaza.
Valoración del Riesgo	En esta etapa se comparan los riesgos analizados con los criterios preestablecidos para determinar si el riesgo es aceptable o si necesita medidas adicionales de tratamiento. Se utiliza una matriz de riesgo para clasificar los riesgos en niveles: bajo, medio o alto.
Priorización del Riesgo	A partir de la valoración, se priorizan los riesgos según su nivel de impacto y la probabilidad de que ocurran. Esto permite a la universidad enfocarse en los riesgos más críticos primero, garantizando que los recursos se asignen eficientemente.

Nota. Las etapas mencionadas son fundamentales para realizar una evaluación del riesgo estructurada y eficaz, permitiendo a ECOTEC tomar decisiones informadas y adecuadas para gestionar los riesgos en función de su gravedad y probabilidad de ocurrencia.

5.6.4.2. Identificación del Riesgo

La identificación del riesgo es el primer paso crítico en el proceso de gestión de riesgos y es fundamental para la implementación exitosa de un sistema de gestión basado en la norma ISO 31000:2018. Este proceso permite reconocer y documentar los posibles eventos o situaciones que puedan afectar los objetivos y metas de la organización, especialmente aquellos que impactan directamente en los activos críticos, tales como los sistemas de información, la infraestructura tecnológica y los procesos académicos y operativos de la universidad.

En el caso de la Universidad Tecnológica ECOTEC, la identificación de riesgos no solo está centrada en los problemas inmediatos relacionados con la infraestructura tecnológica, sino que también incluye las vulnerabilidades internas y externas que puedan afectar las actividades académicas, administrativas, la seguridad de la información y la continuidad operativa.

La metodología para identificar los riesgos es sistemática y abarcativa, considerando todos los posibles factores que puedan comprometer el normal funcionamiento de la universidad. Para ello se incorpora la participación activa de todas las partes interesadas, desde la alta dirección hasta el personal técnico y los estudiantes, dado que cada grupo tiene una perspectiva única sobre los posibles riesgos que enfrentan.

El análisis realizado en el capítulo cuatro de esta investigación ya ha identificado diversos riesgos informáticos y operativos que ECOTEC enfrenta, tales como los errores de los usuarios en los equipos de cómputo, la fuga de información en dispositivos móviles, la alteración de información sensible y el robo de dispositivos con acceso a la red interna, entre otros. Estos riesgos, identificados previamente, proporcionan una base sólida para profundizar en su análisis y gestión de acuerdo con los lineamientos de la ISO 31000:2018.

Metodología de Identificación del Riesgo

La identificación de los riesgos en ECOTEC se realizó utilizando una combinación de métodos cualitativos y cuantitativos para obtener una visión integral y precisa de las amenazas potenciales. Esto incluye:

Tabla 46.

Métodos de Identificación de Riesgos en ECOTEC

Método de Identificación	Descripción	Objetivo
Revisión de los riesgos previamente identificados	Análisis de los riesgos ya identificados en el capítulo 4, como errores de los usuarios, fuga de información en dispositivos móviles, y robo de dispositivos.	Validar y actualizar los riesgos según nuevas incidencias y cambios en el entorno.
Análisis de incidentes pasados	Revisión de incidentes previos relacionados con fallos de sistemas, violaciones de seguridad y errores humanos.	Identificar patrones y áreas recurrentes de vulnerabilidad para prevenir futuros eventos adversos.
Análisis de cambios tecnológicos y normativos	Evaluación de los avances en tecnologías y los cambios normativos como la Ley Orgánica de Protección de Datos Personales (LOPDP).	Detectar riesgos emergentes y adaptar el sistema de gestión de riesgos a nuevas plataformas y regulaciones.

Evaluación de la cadena de suministro y proveedores externos	Análisis de riesgos derivados de la dependencia de proveedores externos, como los servicios en la nube o infraestructura tecnológica.	Identificar posibles vulnerabilidades en los servicios prestados y evaluar su impacto en la continuidad operativa.

Nota. Esta tabla resume los métodos clave utilizados por ECOTEC para identificar los riesgos, con el objetivo de gestionar eficazmente las amenazas y vulnerabilidades que podrían comprometer sus activos y operaciones críticas.

Riesgos Identificados

Tabla 47.

Riesgos Identificados en el Proceso de Gestión de Riesgos en ECOTEC

Riesgo Identificado	Descripción
Errores de los usuarios en equipos de cómputo	Uso incorrecto de sistemas informáticos por parte de los usuarios, resultando en pérdida o alteración de datos críticos.
Fuga de información en dispositivos móviles	Acceso no autorizado o pérdida de dispositivos móviles que contienen datos sensibles y confidenciales.
Alteración de la información en dispositivos móviles	Modificación no autorizada de datos en dispositivos móviles, afectando la integridad de la información académica y administrativa.
Robo de dispositivos con acceso a la red interna	Robo de laptops, smartphones o tablets con acceso a datos sensibles, poniendo en riesgo la seguridad de los sistemas.
Corte del suministro eléctrico en servidores externos	Corte de energía que afecte la disponibilidad de servicios clave como la página web y los sistemas académicos.
Fallo de servicios de comunicación en servidores externos	Interrupción de la comunicación debido a fallos en los proveedores de servicios, afectando la transmisión de información.

Difusión de software malicioso en almacenamiento interno	Instalación de malware en los sistemas internos que compromete la seguridad de los datos y servicios.

Nota. Los riesgos identificados en esta tabla provienen del análisis realizado en el capítulo cuatro, donde se evidencian las amenazas que podrían afectar la seguridad, operatividad y reputación de ECOTEC. Estos riesgos servirán como base para las etapas posteriores del proceso de gestión de riesgos, de acuerdo con la norma ISO 31000:2018.

5.6.4.3. Análisis del Riesgo

El análisis del riesgo es un paso fundamental en la gestión de riesgos de acuerdo con la norma ISO 31000:2018. Esta fase permite comprender la naturaleza y el contexto de los riesgos, evaluando su probabilidad de ocurrencia y el impacto potencial sobre los activos críticos de la organización. En este proceso, la Universidad ECOTEC ha identificado los riesgos informáticos que podrían afectar la integridad, disponibilidad y confidencialidad de la información en sus plataformas tecnológicas.

Metodología de Análisis

Para realizar el análisis del riesgo, ECOTEC adopta una metodología cualitativa basada en la valoración de la probabilidad y el impacto de cada riesgo identificado. Utilizando una escala de 1 a 3, se asigna un valor a la probabilidad de que un riesgo ocurra y otro valor al impacto que tendría sobre los activos de la universidad. La combinación de estos dos factores genera un índice de riesgo que permite priorizar las amenazas.

Tabla 48.

Probabilidad e impacto para cada riesgo identificado

Probabilidad (de 1 a 3):	**Bajo (1)**
	Medio (2)
	Alto (3)
Impacto (de 1 a 3):	Bajo (1)
	Medio (2)
	Alto (3)

Nota. Metodología de calificación para cada riesgo identificado en ECOTEC

El cálculo del riesgo es la multiplicación de la probabilidad por el impacto (Riesgo = Probabilidad × Impacto). Este enfoque permite una clasificación de los riesgos en tres niveles:

Tabla 49.

Clasificación de riesgos

Alto (6-9)	**Riesgo inaceptable, requiere intervención inmediata.**
Medio (4-5)	Riesgo moderado, requiere medidas correctivas.
Bajo (1-3)	Riesgo aceptable, mantener los controles actuales.

Nota. Esta tabla resume la clasificación de riesgos en tres niveles

5.6.4.4. Valoración del Riesgo

En el caso específico de los riesgos informáticos, se han identificado diversas amenazas que afectan la seguridad de los datos y sistemas de la universidad. A continuación, se presentan algunos de los riesgos más críticos junto con su análisis:

Tabla 50.

Análisis de Riesgos Informáticos en ECOTEC

Activo	Amenaza	Probabilidad	Impacto	Riesgo (Probabilidad × Impacto)	Nivel de Riesgo	Acción Recomendada
Ordenadores	Errores de los usuarios	Alto (3)	Alto (3)	9	Alto	Capacitación y validación de interfaces
Dispositivos móviles	Fuga de información	Alto (3)	Alto (3)	9	Alto	Implementación de cifrado y control de acceso
Servidores Externos	Corte del suministro eléctrico	Alto (3)	Alto (3)	9	Alto	Implementación de UPS y generador de respaldo
Almacenamiento Interno	Difusión de software dañino	Alto (3)	Alto (3)	9	Alto	Instalación de antivirus y reglas de firewall

Nota. Esta tabla presenta los riesgos informáticos más críticos identificados en la Universidad ECOTEC, basados en la probabilidad e impacto de las amenazas sobre los activos clave de la institución. Las acciones recomendadas se proponen para mitigar y tratar los riesgos de manera efectiva.

Priorización del Riesgo

El análisis de riesgo permite que los responsables de la gestión en ECOTEC prioricen las amenazas que tienen el mayor impacto en los activos críticos de la universidad. En este sentido, los riesgos altos (con un valor de 6-9) deben ser abordados con acciones inmediatas, como actualización de políticas de seguridad, cifrado de información y refuerzo de controles de acceso. Las amenazas que afectan la confidencialidad y disponibilidad de la información,

como la fuga de datos o la alteración de la información en dispositivos móviles, requieren especial atención para evitar un daño significativo.

5.6.5. Tratamiento del Riesgo

5.6.5.1. Generalidades

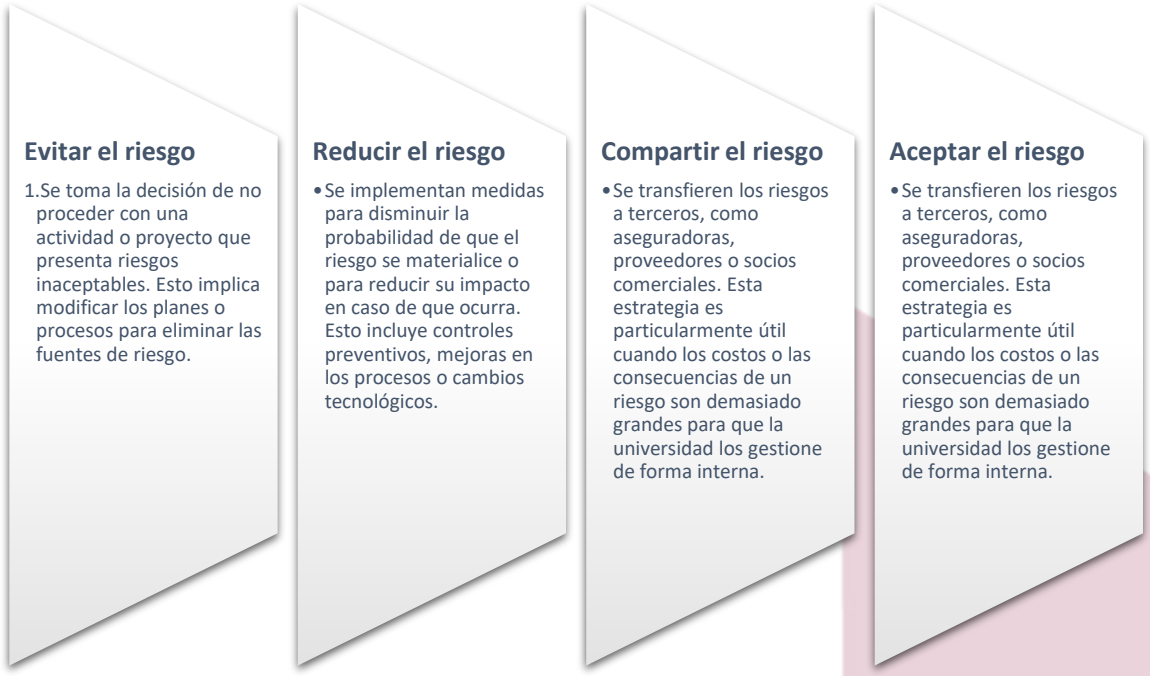
El tratamiento del riesgo es una fase fundamental en la gestión de riesgos según la norma ISO 31000:2018. Durante este proceso, la organización toma decisiones clave sobre cómo manejar los riesgos previamente identificados, con el fin de minimizar los efectos negativos que puedan impactar sus objetivos estratégicos. En términos sencillos, se trata de implementar medidas de control que ayuden a modificar, eliminar o mitigar el riesgo, de acuerdo con su probabilidad y su impacto, mientras se exploran posibles beneficios derivados de riesgos positivos.

En el contexto específico de la Universidad ECOTEC, el tratamiento del riesgo no se limita a una solución puntual, sino que constituye un proceso continuo y dinámico que involucra a todas las áreas de la institución. Desde los sistemas tecnológicos y de infraestructura hasta la gestión académica y administrativa, cada unidad debe alinearse con los objetivos institucionales para garantizar que los riesgos se gestionen de manera integral y eficaz a lo largo de su ciclo de vida. Esto requiere un enfoque sistémico, que no solo contemple la mitigación de los riesgos, sino también la implementación de estrategias que permitan adaptarse a cambios y nuevos desafíos.

Las opciones de tratamiento de riesgos, según la norma ISO 31000:2018, incluyen cuatro estrategias clave:

Figura 6.

Opciones de tratamiento de riegos, conforme ISO31000:2018



Nota. Según la norma ISO 31000:2018, el tratamiento del riesgo implica la implementación de medidas para modificar el riesgo de acuerdo con su probabilidad y su impacto.

El tratamiento del riesgo también debe considerar la priorización de los mismos, basándose en su nivel de gravedad (alto, medio o bajo), el impacto potencial sobre los objetivos de la universidad y los recursos disponibles. Además, cada acción de tratamiento debe ser monitoreada y evaluada para garantizar su efectividad, lo que implica la necesidad de establecer mecanismos de seguimiento y de ajustes periódicos.

5.6.5.2. Selección de las opciones para el tratamiento del riesgo

El tratamiento del riesgo es un paso crucial en la gestión de riesgos, y su correcta selección es vital para garantizar que los riesgos identificados sean manejados de manera

eficaz y alineados con los objetivos estratégicos de la Universidad ECOTEC. Según la norma ISO 31000:2018, existen varias opciones para tratar los riesgos, cada una de las cuales puede adaptarse a las características específicas de la amenaza identificada, su impacto y los recursos disponibles en la universidad.

El tratamiento del riesgo se debe llevar a cabo considerando un enfoque práctico y escalonado, permitiendo tomar decisiones claras sobre cómo gestionar cada tipo de riesgo de acuerdo con su naturaleza y su nivel de gravedad. Las opciones para tratar los riesgos en ECOTEC incluyen:

Tabla 51.

Estrategias de Tratamiento del Riesgo en ECOTEC

Estrategia	Descripción	Aplicación en ECOTEC
Eliminar el Riesgo	Implica la eliminación total del riesgo, evitando por completo la actividad que lo genera. Es viable cuando el riesgo representa una amenaza inaceptable.	Si el riesgo está relacionado con el uso de tecnologías obsoletas o vulnerables, ECOTEC podría optar por actualizar o reemplazar infraestructuras tecnológicas para eliminar la amenaza de ciberataques.
Reducir el Riesgo	Cuando no es posible eliminar el riesgo, se implementan controles para reducir su probabilidad o impacto. Incluye capacitación y nuevas políticas de seguridad.	Si el riesgo es la fuga de información en dispositivos móviles, ECOTEC podría implementar políticas de cifrado y control de acceso para reducir el riesgo de acceso no autorizado a la información.
Compartir el Riesgo	Se transfiere el riesgo a un tercero cuando la universidad no tiene la capacidad de gestionarlo por sí sola, utilizando seguros o externalización de servicios.	Si el riesgo está relacionado con la pérdida de datos debido a fallos en los sistemas externos o en la nube, ECOTEC podría compartir el riesgo con proveedores tecnológicos a través de contratos de seguridad.

Aceptar el Riesgo	Aceptar el riesgo cuando el costo de mitigarlo es mayor que el impacto potencial, o cuando el riesgo tiene baja probabilidad y bajo impacto en los objetivos de la universidad.	Si el riesgo es la caída menor de la red que no interrumpe servicios críticos, ECOTEC podría optar por aceptar el riesgo, monitoreando continuamente la situación para intervenir si es necesario.

Nota. Las estrategias de tratamiento del riesgo deben adaptarse a las circunstancias específicas de ECOTEC, con el objetivo de proteger sus activos críticos y garantizar la continuidad de sus operaciones académicas, administrativas y tecnológicas.

Tabla 52.

Estrategias de tratamiento del riesgo según ISO 31000:2018

Estrategia de Tratamiento	Descripción	Aplicación en ECOTEC
Eliminar el Riesgo	Eliminar la actividad o proceso que origina el riesgo, modificando o suspendiendo su ejecución.	**Actualización de sistemas obsoletos:** Sustituir equipos de computación antiguos que no cumplen con los estándares de seguridad, eliminando así el riesgo de ciberataques debido a vulnerabilidades tecnológicas.
Reducir el Riesgo	Implementar controles para disminuir la probabilidad o el impacto del riesgo.	**Control de acceso y cifrado:** Implementación de políticas de seguridad, como cifrado en dispositivos móviles y autenticación multifactorial, para reducir el riesgo de fuga de información a través de móviles (ej., pérdida o robo).
Compartir el Riesgo	Transferir el riesgo a un tercero, ya sea mediante seguros, acuerdos contractuales o externalización de servicios.	**Contratar seguros de ciberseguridad:** Adquirir seguros para proteger los sistemas clave de la universidad, como los servidores externos, frente a eventos de robo de datos o daños por ciberataques.
Aceptar el Riesgo	Asumir el riesgo cuando no es práctico mitigarlo, o cuando el costo de mitigarlo es mayor que el impacto del riesgo.	**Aceptación de fallos menores en la red interna:** Aceptar los riesgos de pequeñas caídas en la red interna o fallos en los servicios no críticos, como errores menores en la red de Wi-Fi, que no afecten la operación académica.

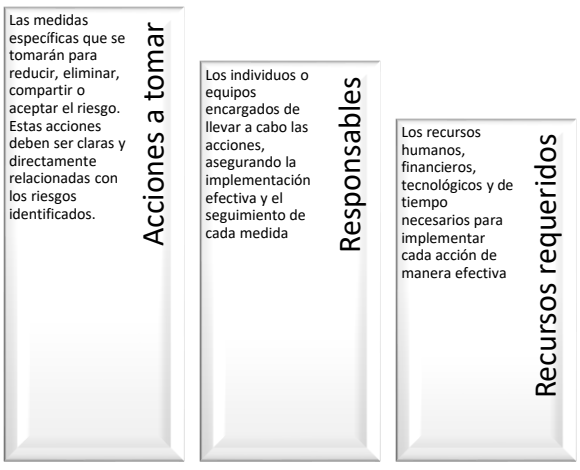
Nota. Las estrategias de tratamiento han sido adaptadas a los riesgos específicos identificados en ECOTEC, centrados principalmente en la protección de datos, seguridad de la información y protección contra ciberataques, asegurando que las acciones sean viables y eficaces en el contexto institucional de la universidad.

5.6.5.3. Preparación e implantación de los planes de tratamiento del riesgo

La preparación e implementación de planes de tratamiento del riesgo es una fase crítica dentro de la gestión de riesgos. Según la norma ISO 31000:2018, estos planes deben ser específicos, detallados y alineados con los objetivos estratégicos de la organización. El objetivo principal de estos planes es mitigar o eliminar los riesgos previamente identificados mediante acciones específicas y concretas. Los planes deben ser documentados y contener información detallada sobre las acciones a tomar, los responsables de implementarlas, los recursos necesarios para llevar a cabo las medidas, y los plazos establecidos para cada acción. Elementos clave de un plan de tratamiento del riesgo:

Figura 7.

Elementos clave para un plan de tratamiento del riesgo



Nota. Ilustración que muestra elementos clave de un plan de tratamiento del riesgo

A continuación, se presenta la estructura de los planes de tratamiento de riesgos en la Universidad ECOTEC, utilizando los riesgos informáticos previamente identificados:

Tabla 53.

Plan de Tratamiento de Riesgos en ECOTEC

Riesgo Identificado	Acción a Tomar	Responsables	Recursos Requeridos	Plazo Establecido
Errores de los usuarios	Capacitación en seguridad informática y validación de interfaces.	Dirección TIC, Departamento Académico	Recursos para formación, software de simulación, tiempos para capacitación.	2 meses
Fuga de información en dispositivos móviles	Implementación de políticas de cifrado y control de acceso.	Dirección TIC, Departamento de Seguridad	Licencias de software de cifrado, recursos humanos para implementación.	1 mes
Corte del suministro eléctrico en servidores externos	Instalación de UPS y generador de respaldo.	Departamento de Infraestructura	Equipos de UPS, generadores, recursos para instalación.	3 meses
Difusión de software dañino en almacenamiento interno	Instalación de antivirus y reglas de firewall.	Departamento TIC	Software antivirus, reglas de firewall, personal para configuración.	1 mes

Nota. Esta tabla resume el plan de tratamiento de riesgos en ECOTEC, destacando las acciones específicas que se tomarán para mitigar los riesgos identificados en el capítulo 4, con los responsables, recursos necesarios y plazos establecidos para garantizar una implementación efectiva.

5.6.6. Seguimiento y Revisión.

En el marco de la gestión de riesgos de la Universidad Tecnológica ECOTEC, es fundamental garantizar que los riesgos identificados y tratados sean monitoreados y revisados de manera continua. El tratamiento de los riesgos no termina con la implementación de las medidas correctivas, sino que requiere un proceso constante de evaluación y ajuste para asegurar que las acciones sean efectivas y adecuadas frente a cualquier cambio en el entorno o en las circunstancias internas de la institución.

A continuación, se presenta una tabla con las medidas de seguimiento y revisión adoptadas por ECOTEC para cada riesgo identificado. Cada medida está acompañada de los responsables, los plazos de revisión establecidos y los indicadores de medición que permitirá evaluar su eficacia en la gestión de los riesgos a lo largo del tiempo.

Tabla 54.

Seguimiento y Revisión de los Riesgos en ECOTEC

Riesgo Identificado	Acción de Seguimiento y Revisión	Responsables	Plazo de Revisión	Medición y Evaluación
Errores de los usuarios	Capacitación continua y pruebas de simulación sobre seguridad y uso adecuado de sistemas.	Dirección TIC, Departamento Académico	Mensual	Evaluación de la efectividad de las capacitaciones.
Fuga de información en dispositivos móviles	Monitoreo de políticas de cifrado y control de acceso, con auditorías periódicas.	Dirección TIC, Departamento de Seguridad	Trimestral	Verificación de accesos no autorizados y revisión de políticas.
Corte del suministro eléctrico en	Monitoreo de UPS y generadores, pruebas de funcionamiento.	Departamento de Infraestructura	Semestral	Inspección física y evaluación del tiempo de respuesta ante fallos.

servidores externos				
Difusión de software dañino en almacenamiento interno	Actualización y auditoría de antivirus, otorgando un seguimiento a incidentes previos.	Departamento TIC	Mensual	Reporte de incidencias de software malicioso y actualización de antivirus.
Acceso no autorizado a la red	Chequeo de los accesos, auditoría de red y análisis de puntos desprotegidos en el sistema.	Dirección TIC, Departamento de Seguridad	Semestral	Informe sobre accesos no autorizados y control de red.
Robo de dispositivos con acceso a la red	Revisión y actualización de controles de acceso físico y seguro, instauración de sistema de alarmas.	Departamento de Infraestructura	Trimestral	Inspección de equipos y sistemas de seguridad instalados.
Interrupciones en la conectividad de la red	Revisión de la infraestructura de la red, seguimiento de proveedores de servicio, y verificación de fallos.	Departamento de Tecnología, Proveedores Externos	Mensual	Reportes de caídas de red y análisis de las causas.

Nota. La tabla muestra las medidas de seguimiento y revisión adoptadas por la Universidad ECOTEC para los riesgos informáticos más relevantes, con sus responsables, plazos de revisión y los mecanismos de medición y evaluación para asegurar la efectividad de las acciones tomadas. Las acciones están alineadas con los principios establecidos por la norma ISO 31000:2018, orientadas a mejorar continuamente la gestión de los riesgos identificados.

5.6.7. Registro e Informe

La gestión de riesgos en la Universidad ECOTEC requiere un enfoque integral de comunicación y monitoreo directo, donde la información sobre los riesgos identificados, las medidas adoptadas y los resultados obtenidos se mantengan accesibles y sean fácilmente

comprendidos por todas las partes interesadas. De acuerdo con la norma ISO 31000:2018, el proceso de registro e informe es esencial para asegurar que los riesgos sean gestionados de manera continua y eficaz.

5.6.7.1. Medios de comunicación

Los siguientes métodos de comunicación se aplicarán en ECOTEC para garantizar que la información sobre los riesgos identificados, las medidas adoptadas para mitigar los riesgos y las conclusiones de las evaluaciones sean accesibles para todos los actores relevantes:

Tabla 55.

Medios de comunicación que utilizará ECOTEC para garantizar información de riesgos identificados

Método de Comunicación	Descripción	Objetivo
Publicación del Mapa de Riesgos	El mapa visual de riesgos actualizado y accesible mediante de plataformas internas a través de la plataforma institucional.	Proveer una representación concisa de los riesgos críticos y sus medidas de mitigación para toda la comunidad universitaria.
Uso de Correos Electrónicos Institucionales	Distribución de informes periódicos sobre riesgos, medidas y actualizaciones por medio de los correos electrónicos institucionales.	Mantener a la comunidad académica y administrativa informada sobre la gestión de riesgos y medidas adoptadas.
Publicación de Riesgos en Descriptivos de Cargos	Inclusión de riesgos asociados a las actividades en los descriptivos de cargos de los empleados y servidores.	Garantizar que cada miembro del personal se informe de los riesgos en su área de trabajo y las medidas preventivas.
Carteleras Informativas en el Campus	Asignación de carteleras estratégicas en el campus universitario con infografías informativas sobre los riesgos y de cada medida preventiva.	Brindar información de los riesgos y las óptimas prácticas de prevención a estudiantes, docentes y personal administrativo.

Socialización con el Personal	Reuniones periódicas con el personal de áreas críticas para socializar sobre riesgos y medidas de mitigación.	Fomentar la participación activa del personal en la gestión de riesgos y garantizar el entendimiento de sus responsabilidades.
Reuniones con Proveedores y Partes Externas	Reuniones periódicas con los proveedores clave para evaluar los riesgos asociados a cada servicio contratado.	Gestionar los riesgos derivados de proveedores externos y garantizar el cumplimiento de las normas de seguridad.
Inspección de Cumplimiento	Inspecciones continuas en áreas operativas para verificar que todas las medidas de mitigación se estén implementando adecuadamente.	Asegurar que las medidas de mitigación sean efectivas y que los controles de seguridad estén operando correctamente.

Nota. Esta tabla proporciona una visión clara y organizada de los métodos de comunicación que ECOTEC utilizará para gestionar la información sobre riesgos dentro de la institución.

5.6.7.2. Cronograma De Actividades Para La Implementación De Procesos De Mejora Ante Los Riesgos Detectados

Para garantizar la efectiva implementación de las medidas de mitigación de riesgos, se establecerá un cronograma detallado de actividades. Este cronograma permitirá la planificación adecuada de las tareas y garantizará que se cumplan los plazos establecidos para la implementación de medidas preventivas y correctivas.

Tabla 56.

Cronograma de actividades para la implementación de procesos de mejora ante riesgos detectados

Actividad	Responsables	Fecha de Ejecución
Reunión de presentación del proyecto y evaluación de riesgos	Alta Dirección, Gerencia de Logística, Equipo Consultor	ene-26

Obtención del presupuesto para la implementación de la Norma ISO 31000 y procesos acordes a la misma	Alta Dirección, Gerencia Financiera, Equipo Consultor	feb-26
Difusión de procedimientos de administración y manejo de riesgos	Alta Dirección, Gerencia de Logística, Equipo Consultor, Colaboradores del área logística	mar-26
Establecimiento de equipos de implementación para unidades de transporte	Área de Logística, Equipo Consultor	abr-26
Instalación y pruebas de equipos y sistemas de gestión de riesgos	Área de Sistemas, Área de Logística, Equipo Consultor	Mayo 2026 - Junio 2026
Evaluación de efectividad del sistema y proceso implementado	Sistema de Gestión Integral, Auditores Externos, Equipo Consultor	Julio 2026 - Agosto 2026
Mantenimiento del Sistema de Gestión Integrado bajo la Norma ISO 31000	Gerencia del Sistema Integrado de Gestión	Septiembre 2026 - Diciembre 2026

Nota. El cronograma presentado es una planificación provisional para el año 2026, con el objetivo de implementar y mantener el sistema de gestión de riesgos en la Universidad ECOTEC conforme a la norma ISO 31000:2018. Las fechas y responsabilidades pueden estar sujetas a ajustes según la disponibilidad de recursos y la evolución del proceso de implementación.

5.6.8. Auditoría Interna

La auditoría interna es una herramienta esencial dentro del proceso de gestión de riesgos que permite verificar la efectividad y el cumplimiento de las políticas y procedimientos establecidos en el sistema de gestión de riesgos. Esta actividad proporciona una evaluación imparcial de los controles internos, asegurando que las medidas adoptadas para mitigar los riesgos sean efectivas y estén nivelados con los objetivos estratégicos de la universidad.

5.6.8.1. Objetivos

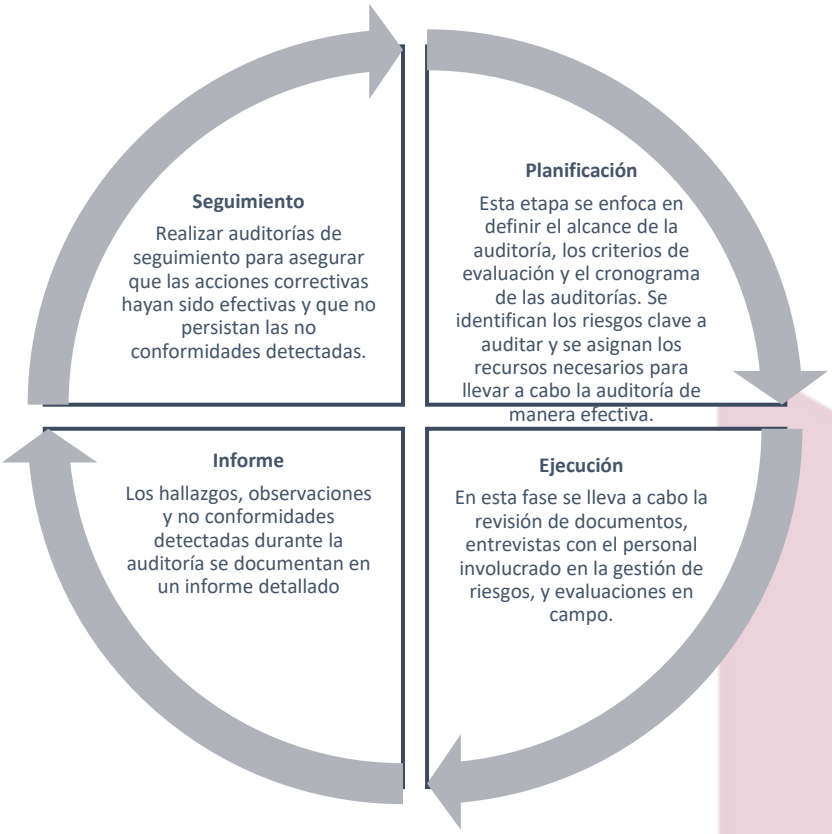
- ✓ Verificar que el sistema esté funcionando correctamente, alineado con los riesgos identificados.
- ✓ Asegurar que los recursos asignados para la gestión de riesgos sean suficientes y se utilicen adecuadamente.
- ✓ Corroborar si las acciones correctivas y preventivas son efectivas en la mitigación de los riesgos.
- ✓ Asegurar que la alta dirección y el personal operativo estén comprometidos con la gestión de riesgos y participen continuamente en las actualizaciones del sistema.

5.6.8.2. Procesos de Auditoría Interna

El proceso de auditoría interna para la gestión de riesgos en ECOTEC se desarrolla en varias etapas esenciales:

Figura 8.

Procesos de auditoría interna para gestión de riesgos en ECOTEC



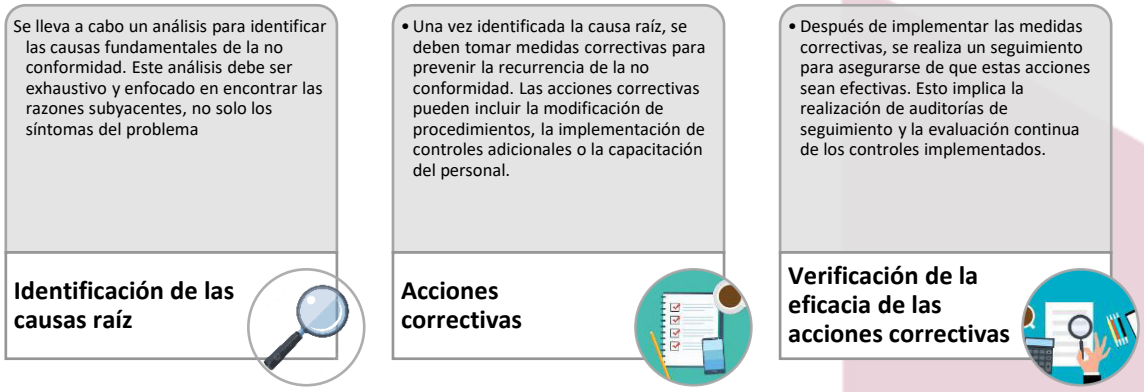
Nota. La ilustración muestra el proceso iterativo que debe desarrollar ECOTEC para optimizar sus procesos a través de la auditoría interna

5.6.8.3. No Conformidades y Acciones Correctivas

Cuando se localiza una, no conformidad en el sistema de gestión de riesgos, es esencial tomar acciones correctivas para asegurar que el riesgo se mitigue adecuadamente (revisar anexo 4). El proceso de gestión de no conformidades se desarrolla en tres etapas clave:

Figura 9.

Pasos para la detección de una no conformidad y su gestión en ECOTEC



Nota. En la presente ilustración, muestra los pasos para la detección de una no conformidad, desde la identificación, hasta su gestión correctiva.

Capítulo 6

6. Conclusiones y Aplicaciones

6.1. Conclusiones Generales

El trabajo realizado a lo largo de esta investigación nos ha permitido analizar y abordar de manera integral la gestión de riesgos informáticos en la Universidad Tecnológica ECOTEC. Este estudio es fundamental para la identificación y evaluación de los riesgos asociados a la protección de datos personales, así como la implementación de un manual alineado con la norma ISO 31000:2018. A través de la evaluación de los sistemas tecnológicos y las políticas institucionales existentes nos ha permitido identificar oportunidades de mejora y fortalecer los procesos de seguridad, siempre con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de los datos sensibles de la comunidad educativa.

Uno de los aspectos más importantes que se destaca es la necesidad de adaptar los procesos de seguridad a los estándares internacionales, lo cual no solo contribuye a la protección de los datos, sino que también posiciona a ECOTEC como una institución comprometida con las mejores prácticas en cuanto a la gestión de riesgos. La implementación de un Plan Director de Seguridad (PDS) y el establecimiento de medidas correctivas y preventivas en los procesos tecnológicos, administrativos y académicos reflejan un paso importante hacia la modernización y la protección integral de la institución.

6.2. Conclusiones Específicas

6.2.1. Análisis del Cumplimiento de los Objetivos de la Investigación

La propuesta realizada, nos ha permitido un análisis exhaustivo del cumplimiento de los objetivos establecidos al inicio del estudio, evidenciando el progreso y las áreas de mejora en la gestión de riesgos informáticos en la Universidad ECOTEC. Los objetivos se logran de manera satisfactoria, especialmente en términos de la implementación de un manual de gestión de riesgos alineado con los estándares internacionales de la norma ISO 31000:2018. Este logro no solo considera la evaluación de los riesgos informáticos, sino también establecer protocolos claros que contribuyen a mejorar la seguridad de la información. La realización de una matriz de riesgos, la creación de procedimientos específicos y la formación continua del personal han sido claves para alcanzar los objetivos planteados. En términos generales, la investigación tiene un impacto positivo en el fortalecimiento de los procesos internos relacionados con la seguridad de datos, lo que se refleja en la mejora de las medidas de protección y control dentro de la institución.

6.2.2. Contribución a la Gestión Empresarial

La creación de un Manual de Gestión de Riesgos tiene un impacto relevante en la gestión empresarial de la Universidad ECOTEC. Al crear una estructura clara para la identificación, evaluación y tratamiento de los riesgos informáticos, la institución fortalece su capacidad para abordar los riesgos de manera proactiva. Además, al alinearse con la normativa ISO 31000:2018, nos ha permitido estandarizar los procesos de gestión de riesgos, lo que contribuye a una mayor eficiencia en la toma de decisiones y en la asignación de recursos, especialmente en áreas clave como los sistemas tecnológicos y la infraestructura de

seguridad. Este enfoque integral facilita la creación de un entorno organizacional más seguro, aumentando la confianza de los estudiantes, docentes y personal administrativo en la institución. A su vez, la propuesta del plan estratégico de seguridad nos ha alineado la gestión de riesgos con los objetivos institucionales, asegurando que la universidad continúe cumpliendo con los requisitos legales y normativos, manteniendo su competitividad en el entorno empresarial.

6.2.3. Contribución a Nivel Académico

A nivel académico la creación del Manual de Gestión de Riesgos es una experiencia enriquecedora, ya que nos ha permitido adquirir una comprensión más profunda sobre la importancia de la seguridad de la información en el ámbito educativo. Este proceso tan sensible cómo la protección de los datos no solo es crucial para el buen funcionamiento de los procesos académicos, sino también para garantizar la integridad y privacidad de la información de estudiantes, docentes y personal administrativo. Además, trabajar con la norma ISO 31000:2018 nos ha proporcionado un marco metodológico claro y estructurado para identificar, evaluar y tratar los riesgos informáticos, lo que ha reforzado el aprendizaje sobre la gestión de riesgos en entornos educativos. La creación de políticas claras sobre protección de datos y el uso de tecnologías seguras ha sido una valiosa oportunidad para comprender la relevancia de la ciberseguridad en el contexto académico. Esta experiencia también ha reforzado la necesidad de sensibilizar y capacitar a la comunidad educativa en prácticas de protección de datos, lo que contribuye significativamente a fomentar una cultura organizacional de seguridad.

6.2.4. Contribución a nivel personal

A nivel personal, este proyecto nos ha proporcionado una valiosa experiencia en la aplicación práctica de conocimientos adquiridos a lo largo de la formación académica. La investigación no solo nos ha permitido consolidar una comprensión profunda de la gestión de riesgos, sino que también ha facilitado el desarrollo de habilidades clave en áreas como la evaluación de riesgos, la implementación de medidas correctivas y preventivas, y la gestión de la seguridad de la información. La colaboración con diversos departamentos y la interacción con expertos en el área han enriquecido la experiencia personal, permitiendo una visión más amplia sobre cómo las decisiones tomadas en el ámbito de la seguridad impactan directamente en el funcionamiento organizacional. Además, la posibilidad de aplicar la normativa ISO 31000:2018 en un entorno real creando una oportunidad única para afianzar competencias en la gestión de riesgos y ha reforzado el compromiso con la mejora continua, tanto a nivel profesional como personal. Este proyecto ha marcado un hito en la culminación de esta maestría y a nivel profesional, consolidando un enfoque práctico para abordar los desafíos de seguridad en las organizaciones modernas.

6.3. Limitaciones a la Investigación

Esta investigación presenta algunas limitaciones que deben ser tomadas en cuenta al momento de evaluar los resultados y las conclusiones alcanzadas. La primera limitación está relacionada con la disponibilidad y el acceso a información confidencial y sensible, debido a la naturaleza de los datos tratados por la universidad, hubo restricciones en cuanto a la cantidad de información específica a la que se pudo acceder, lo que nos ha limitado la

capacidad de realizar un análisis más detallado de ciertos aspectos del tratamiento de datos. A pesar de los esfuerzos por obtener datos completos, las políticas institucionales de privacidad y protección de información restringieron el alcance de algunas áreas clave del estudio.

Otra limitación es el tiempo disponible para llevar a cabo la investigación, aunque se realizaron esfuerzos considerables para completar todas las fases del proyecto, el tiempo limitado en el proceso de recopilación de datos y en la implementación de las soluciones propuestas afectó la posibilidad de realizar un seguimiento más extenso y evaluar los resultados de las acciones implementadas a largo plazo. De haber tenido un período de tiempo más extenso, se podrían haber monitoreado los impactos de las medidas de seguridad y verificado la eficacia de las estrategias aplicadas a lo largo del tiempo.

A pesar de estas limitaciones, la investigación ha logrado sentar las bases para la mejora continua en la gestión de riesgos y la seguridad de la información en ECOTEC, proporcionando una propuesta sólida para avanzar hacia una mayor protección y cumplimiento normativo en el futuro.

7. Referencias bibliográficas

Asamblea Nacional del Ecuador. (2010). *Ley Orgánica de Educación Superior (LOES)*. https://www.asambleanacional.gob.ec

Asamblea Nacional del Ecuador. (2019). *Ley Orgánica de Protección de Datos Personales (LOPDP)*. https://www.asambleanacional.gob.ec

Asamblea Nacional del Ecuador. (2021). *Reglamento de la Ley Orgánica de Protección de Datos Personales (R-LOPDP)*. https://www.gob.ec/web/datos-personales

Castañeda, F. (2020). *La gestión de riesgos en las instituciones educativas: Un enfoque práctico*. Editorial Universitaria.

Comisión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales*. Diario Oficial de la Unión Europea.

Foro Económico Mundial. (2020). *Informe Global de Riesgos 2020*. Recuperado de https://www.weforum.org/reports/the-global-risks-report-2020

González, P., & Pérez, J. (2018). *Tratamiento de datos personales en entornos digitales*. Editorial Jurídica Latinoamericana.

Hillson, D. (2004). Effective risk management: Some essential elements. *International Journal of Project Management, 22*(1), 49-55. https://doi.org/10.1016/j.ijproman.2003.03.006

International Organization for Standardization (ISO). (2009). *ISO Guide 73:2009 Risk management – Vocabulary*. https://www.iso.org/standard/44651.html

International Organization for Standardization (ISO). (2018). *ISO 31000:2018 Risk management – Guidelines*. https://www.iso.org/standard/65694.html

International Organization for Standardization (ISO), & International Electrotechnical Commission (IEC). (2019). *ISO/IEC 31010:2019 Risk management – Risk assessment techniques*. https://www.iso.org/standard/65657.html

ISO. (2018). *ISO 31000:2018 Risk management – Guidelines*. International Organization for Standardization. https://www.iso.org/standard/65694.html

Pinna, M. (2020). *Gestión de riesgos: Estrategias y modelos aplicados en las organizaciones*. Editorial Planeta.

Universidad Tecnológica ECOTEC. (2025). *Normas y reglamentos internos*. Universidad ECOTEC.

Universidad Tecnológica ECOTEC. (2025). *Plan Estratégico Institucional (PEI)*. Universidad ECOTEC.

8. Anexos

Anexo 1. Procedimiento Normalizado del Trabajo.

Creación de Procedimientos Normalizados de Trabajo para la Gestión de Riesgos en los Entornos Virtuales de la Universidad Tecnológica ECOTEC

Código: PNT-GR-VIRT-001

Versión: 1

Fecha de emisión: Julio 2025

Aprobado por: Joaquín Hernández Alvarado, Ph.D. - Rector

Campus ECOTEC, Km 13.5 Vía a la Costa, Samborondón, Ecuador

1. Introducción

La presente normativa tiene como finalidad establecer un marco metodológico claro, consistente y práctico para la creación de Procedimientos Normalizados de Trabajo (PNT) aplicables a la gestión de riesgos de los entornos virtuales de aprendizaje y los sistemas informáticos de la Universidad Tecnológica ECOTEC. Se busca garantizar la seguridad de los activos de información, la continuidad operativa y la protección de los datos de toda la comunidad educativa.

2. Propósito

Definir los lineamientos, criterios y buenas prácticas para el diseño, aprobación, revisión, implementación y actualización de los procedimientos normalizados de trabajo que apoyen la gestión de riesgos en los entornos digitales de la universidad.

3. Alcance

Este procedimiento aplica a todas las áreas académicas, administrativas y de apoyo que utilicen plataformas virtuales, recursos digitales y sistemas de información dentro del ámbito de la Universidad Tecnológica ECOTEC.

4. Principios Rectores

Enfoque preventivo

Mejora continua

Transparencia y responsabilidad

Participación colaborativa

Cumplimiento normativo

Estos principios se alinean con la misión institucional de garantizar calidad, seguridad y resiliencia.

5. Objetivos

Promover la cultura de prevención y gestión de riesgos.

Estandarizar la documentación y control de los procedimientos.

Garantizar la integridad, disponibilidad y confidencialidad de la información.

6. Responsabilidades

La Alta Dirección de la Universidad será la responsable de la aprobación de los PNT. Cada unidad deberá designar un responsable para su aplicación, seguimiento y control. Además, se establecerán roles específicos según el organigrama institucional para garantizar la rendición de cuentas y la efectividad del sistema.

ROL	RESPONSABILIDAD
RECTORÍA	Aprobación final de los PNT y supervisión de su debida implementación
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Diseñar, implementar y mantener los PNT de seguridad de sistemas y entornos virtuales
COORDINACIONES ACADÉMICAS	Garantizar la difusión y el respectivo cumplimiento de los PNT en sus facultades designadas
RESPONSABLES DE PROCESOS	Aplicar los PNT en sus actividades diarias y notificar hallazgos
UNIDAD DE SEGURIDAD INFORMÁTICA	Supervisión en el cumplimiento de los PNT y proponer mejorías y actualizaciones

COMUNIDAD UNIVERSITARIA EN GENERAL	Conocer y aplicar los PNT aprobados para garantizar la seguridad de la información

7. Revisión y Aprobación

Este procedimiento será revisado anualmente o cuando existan cambios significativos en el contexto normativo o tecnológico. La aprobación corresponderá al Rector de la Universidad Tecnológica ECOTEC y al Comité Central de Gestión de Riesgos.

8. Procedimiento

La creación de nuevos PNT deberá contemplar las siguientes fases: análisis de necesidades, diseño preliminar, revisión técnica, validación de responsables, aprobación formal y difusión. Todo cambio deberá documentarse mediante un control de cambios y comunicarse a la comunidad universitaria.

9. Anexos

Plantilla para reporte de incidentes

Fecha del incidente: _____

Descripción del incidente: _____

Impacto: _____

Responsable de la gestión: _____

Acciones correctivas: _____

Seguimiento: _____

Matriz de riesgos priorizados

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	TRATAMIENTO PROPUESTO	RESPONSABLE
ORDENADORES	Errores de usuario	Alta (3)	Alta (3)	9	Capacitación, refuerzo de contraseñas	Unidad de TI
TRABAJOS MÓVILES (TELÉFONOS)	Fuga de información	Alta (3)	Alta (3)	9	Doble autenticación, encriptación	Seguridad Informática
DISPOSITIVOS CON DATOS	Robo	Alta (3)	Alta (3)	9	Trazabilidad, monitoreo, bloqueo remoto	Responsable de Inventario TI
SERVIDORES EXTERNOS	Corte de suministro eléctrico	Alta (3)	Alta (3)	9	UPS, generador de respaldo	Infraestructura TI
ALMACENAMIENTO INTERNO	Difusión de software dañino	Alta (3)	Alta (3)	9	Antivirus, segmentación de red	Seguridad Informática
WIFI	Denegación de servicio	Medio (2)	Alto (3)	6	Segmentación, control de acceso	Red y Comunicaciones

Mapa de calor de riesgos

	IMPACTO BAJO (1)	IMPACTO PROMEDIO (2)	IMPACTO ALTO (3)
PROBABILIDAD ALTA (3)	Medio (3)	Alto (6)	Crítico (9)
PROBABILIDAD PROMEDIO (2)	Bajo (2)	Medio (4)	Alto (6)
PROBABILIDAD BAJA (1)	Bajo (1)	Bajo (2)	Medio (3)

Normas y leyes pertinentes.

- Ley Orgánica de Protección de Datos Personales (Ecuador)
- Reglamento interno de seguridad ECOTEC
- ISO 31000:2018

Anexo 2 . Plan de auditoría interna en Ecotec

Formato de Plan de Auditoría Interna en ECOTEC	
Norma ISO 31000:2018 - Gestión de Riesgos	
Elemento	**Descripción**
Objetivos de la Auditoría:	1. Evaluar la eficacia del sistema de gestión de riesgos. 2. Comprobar la asignación y uso adecuado de los recursos en gestión de riesgos. 3. Verificar la implementación y efectividad de las acciones correctivas. 4. Involucrar a la alta dirección y a todos los niveles operativos en la gestión y actualización continua del sistema de riesgos.
Alcance de la Auditoría	Evaluación del sistema de gestión de riesgos implementado en ECOTEC, con enfoque en los procesos clave de gestión de riesgos identificados, incluidos los riesgos informáticos, operacionales y estratégicos.
Criterios de Auditoría:	- Cumplimiento de la norma ISO 31000:2018 en la identificación, evaluación y tratamiento de riesgos. - Revisión de políticas y procedimientos internos relacionados con la gestión de riesgos. - Evaluación del grado de implementación y seguimiento de las medidas de mitigación propuestas.
Responsables de la Auditoría:	Equipo de Auditoría Interna: Personal especializado de ECOTEC con formación en normas ISO 31000:2018.
Métodos de Auditoría:	1. Revisión de documentos y registros relacionados con la gestión de riesgos. 2. Entrevistas con responsables de áreas clave en la gestión de riesgos. 3. Inspecciones in situ de los controles implementados para mitigar los riesgos identificados.
Cronograma:	- **Inicio de la Auditoría:** [Fecha] - **Finalización de la Auditoría:** [Fecha] - **Informe Final:** [Fecha]
Informe de Auditoría:	El informe de auditoría se entregará al Comité de Gestión de Riesgos, incluyendo los hallazgos, observaciones y propuestas de mejora.
Seguimiento de Acciones Correctivas:	Las acciones correctivas deberán ser verificadas por los auditores internos a los 3, 6 y 12 meses según el nivel de riesgo identificado.

Evaluación de Resultados:	- Revisión de los resultados del tratamiento de los riesgos identificados y evaluación de la efectividad de las medidas correctivas implementadas.

Fecha	**Hora**	**Auditor**	**Área**	**Departamento**	**Proceso**	**Función**	**Auditado**	**Conformidad**	**No Conformidad / Observación**
[Fecha]	[Hora]	[Nombre Auditor]	[Área Auditada]	[Departamento]	[Proceso Evaluado]	[Función Auditada]	[Nombre Auditado]	[Conformidad]	[Descripción de la No Conformidad o Observación]
[Fecha]	[Hora]	[Nombre Auditor]	[Área Auditada]	[Departamento]	[Proceso Evaluado]	[Función Auditada]	[Nombre Auditado]	[Conformidad]	[Descripción de la No Conformidad o Observación]
[Fecha]	[Hora]	[Nombre Auditor]	[Área Auditada]	[Departamento]	[Proceso Evaluado]	[Función Auditada]	[Nombre Auditado]	[Conformidad]	[Descripción de la No Conformidad o Observación]

Firma auditor líder _____ Firma auditor: _____

Anexo 3 . Formato de no conformidades y acciones correctivas

Formato de No Conformidades y Acciones Correctivas
Descripción de variables:
1. Identificador: Un código único para cada no conformidad (por ejemplo, NC-001, NC-002, etc.).
2. Fecha de Identificación: Fecha en que se detectó la no conformidad.
3. Departamento/Área: El área o departamento relacionado con la no conformidad.
4. Descripción de la No Conformidad: Breve descripción del problema o no conformidad encontrada.
5. Causa Raíz: Identificación de la causa que originó la no conformidad (por ejemplo, falta de capacitación, fallos en el sistema, etc.).
6. Acción Correctiva Propuesta: Acción recomendada para solucionar la no conformidad.
7. Responsable: Persona o área encargada de implementar la acción correctiva.
8. Plazo para Implementación: Fecha límite para completar la acción correctiva.
9. Fecha de Implementación: Fecha en que la acción correctiva fue efectivamente implementada.
10. Evidencia de Implementación: Documentación o pruebas que demuestren que la acción correctiva se ha implementado (por ejemplo, listado de contraseñas actualizadas, reporte de capacitación, etc.).
11. Estado: Indicación del estado de la acción correctiva (abierto, en progreso, cerrado).
12. Comentarios Adicionales: Cualquier información relevante o actualizaciones sobre la acción correctiva.
Para completar el formato, los siguientes pasos son los más importantes:
1. Identificación clara de las no conformidades a medida que se detectan, lo que permite un seguimiento efectivo.
2. Responsable designado que se hace cargo de cada acción correctiva para asegurar que se lleve a cabo en tiempo y forma.
3. Prueba de cumplimiento mediante la sección de "Evidencia de Implementación", donde se adjuntan pruebas tangibles de que la corrección fue implementada correctamente.
4. Monitoreo continuo del estado de cada acción correctiva para asegurar que la no conformidad se resuelva completamente.

Identificador	Fecha de Identificación	Departamento/Área	Descripción de la No Conformidad	Causa Raíz	Acción Correctiva Propuesta	Responsable	Plazo para Implementación	Fecha de Implementación	Evidencia de Implementación	Estado	Comentarios Adicionales
NC-001	1/9/2025	Departamento de TI	Fuga de información en la red	Contraseñas débiles	Reforzar políticas de seguridad y actualizar contraseñas	Jefe de TI	30/9/2025	30/9/2025	Listado de contraseñas actualizadas	Cerrado	Se implementó autenticación multifactor

NC-002	2/9/2025	Departamento Académico	Errores en la gestión de matrícula	Falta de formación en el sistema	Capacitación del personal y validación de datos de matrícula	Coordinador Académico	15/10/2025	12/10/2025	Certificados de capacitación	En progreso	Se han capacitado 75% del personal
NC-003	5/9/2025	Seguridad	Fallo en el sistema de videovigilancia	Hardware defectuoso	Sustitución de cámaras y mejora del sistema de monitoreo	Jefe de Seguridad	20/10/2025	20/10/2025	Informe de instalación de nuevas cámaras	Abierto	Se está en proceso de compra de equipos

Firma auditor

Firma auditor lider

Anexo 4. Consentimiento informado a estudiantes para el tratamiento de datos

CONSENTIMIENTO INFORMADO ESTUDIANTES

CONSENTIMIENTO INFORMADO PARA EL TRATAMIENTO DE DATOS PERSONALES Y USO DE IMAGEN UNIVERSIDAD TECNOLÓGICA ECOTEC

Yo, ……, con cédula de ciudadanía N.º… ,

estudiante de la Universidad Tecnológica ECOTEC, declaro haber sido informado/a sobre el tratamiento de mis datos personales, conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP), y en relación con los siguientes aspectos:

1. **Tratamiento obligatorio de datos personales**

Autorizo el tratamiento de mis datos personales (identificativos, académicos, de contacto, financieros y de salud si aplica) por parte de la Universidad, para las siguientes finalidades:

Proceso de admisión, matrícula, gestión académica, administrativa y financiera. Gestión de plataformas educativas y correo institucional.

Evaluaciones, tutorías, seguimiento académico y actividades complementarias. Cumplimiento de obligaciones legales y reglamentarias.

Este tratamiento es obligatorio para mantener mi vínculo académico con la institución.

2. **Tratamiento opcional – uso de imagen y voz**

Conforme a la normativa vigente, el uso de mi imagen, voz o grabaciones para fines institucionales y de difusión requiere mi consentimiento expreso y específico.

Marque si autoriza el siguiente tratamiento opcional:

☐ Autorizo a la Universidad ECOTEC a usar mi imagen y/o voz en redes sociales institucionales (Facebook, Instagram, YouTube, etc.)

☐ Autorizo el uso de mi imagen y/o voz en la página web oficial de la Universidad

☐ Autorizo el uso de mi imagen en materiales internos (boletines, eventos, murales digitales) Este consentimiento es voluntario. No afecta mi condición de estudiante.

3. Videovigilancia

Fui informado/a que las instalaciones de la Universidad cuentan con sistemas de videovigilancia con fines de seguridad institucional. Estos sistemas operan bajo lo establecido

en la LOPDP. La existencia de cámaras está debidamente señalizada mediante cartelería visible en los accesos al campus.

4. **Información adicional sobre protección de datos**

Responsable del tratamiento: Universidad Tecnológica ECOTEC

Finalidad del tratamiento: Académica, administrativa, institucional y de difusión (cuando aplique)

Plazo de conservación: Durante la vigencia de la relación académica y los plazos legales aplicables

Ejercicio de derechos: Acceso, rectificación, oposición, supresión y portabilidad. Contacto del delegado de Protección de Datos: [correo electrónico institucional] Fecha: dd/mm/aa

Firma del estudiante: CI:

Anexo 5. Acuerdo de confidencialidad y tratamiento de datos personales para trabajadores

ACUERDO DE CONFIDENCIALIDAD Y TRATAMIENTO DE DATOS PERSONALES PARA TRABAJADORES

Entre la Universidad Tecnológica ECOTEC y el/la trabajador/a En la ciudad de Guayaquil, a de de 2025, comparecen por una parte la Universidad Tecnológica ECOTEC, representada por el Dr. Joaquín Hernández Alvarado, en su calidad de Rector, a quien en adelante se denominará "LA INSTITUCIÓN"; y por otra parte el/la señor/a con cédula de ciudadanía N° , en calidad de trabajador/a, a quien en adelante se denominará "EL/LA FIRMANTE"; quienes libre y voluntariamente acuerdan lo siguiente:

PRIMERA: Objeto del Acuerdo

Este acuerdo tiene por objeto establecer los términos y condiciones bajo los cuales EL/LA FIRMANTE se compromete a respetar la confidencialidad, integridad, disponibilidad y legalidad del tratamiento de datos personales y otra información sensible o reservada a la que tenga acceso en virtud de su relación laboral con LA INSTITUCIÓN.

SEGUNDA: Finalidad y uso de los datos del firmante

LA INSTITUCIÓN informa a EL/LA FIRMANTE que recopilará y tratará sus datos personales con la finalidad de gestionar la relación laboral, procesos administrativos, control de acceso, cumplimiento de obligaciones legales, seguridad institucional y comunicación interna. Los datos serán tratados de forma confidencial.

TERCERA: Datos a los que accede

Datos personales y académicos de estudiantes.
Datos laborales y personales de docentes y personal administrativo. Información contable, financiera y contractual.
Registros audiovisuales provenientes de sistemas de videovigilancia.

CUARTA: Obligación de Confidencialidad

No divulgar, copiar, modificar ni utilizar para fines personales o externos la información a la que tenga acceso.
Mantener la confidencialidad incluso una vez finalizada su relación con LA INSTITUCIÓN.
Cumplir con la LOPDP y las políticas institucionales. QUINTA: Medidas de Seguridad
Usar contraseñas seguras.
No almacenar información en dispositivos no autorizados. Respetar protocolos de uso de plataformas digitales y servidores. SEXTA: Conservación de datos personales del firmante

Los datos serán conservados durante la vigencia del contrato laboral y hasta cinco (5) años posteriores a su finalización.

SÉPTIMA: Ejercicio de derechos del firmante

EL/LA FIRMANTE podrá ejercer sus derechos ante el Delegado de Protección de Datos (DPD), por correo: [correo institucional], o en la Dirección Jurídica de LA INSTITUCIÓN.

OCTAVA: Vigencia del acuerdo

Este acuerdo estará vigente durante la relación laboral y por cinco (5) años posteriores a su finalización.

Dr. Joaquín Hernández Alvarado

Rector – Universidad Tecnológica ECOTEC

Nombre del/la Firmante:

Firma CI.

Anexo 6. Contrato de encargo de tratamiento de datos personales

CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS PERSONALES

Entre:

RESPONSABLE DEL TRATAMIENTO:

Nombre: Universidad ECOTEC RUC: 1791339207001

Dirección: Km. 13.5 Vía a la Costa, Guayaquil, Ecuador Representante Legal: Dra. María Fernanda Vargas – Rectora Correo electrónico: rectorado@ecotec.edu.ec

Teléfono: (04) 3700 100

ENCARGADO DEL TRATAMIENTO:

Nombre: IMGroup S.A. RUC: 0998765432001

Dirección: Av. Francisco de Orellana, Centro Empresarial Colón, Guayaquil Representante Legal: Ing. Juan Carlos Zambrano

Correo electrónico: jczambrano@imgroup.ec Teléfono: (04) 2200 500

IDENTIFICACIÓN DEL ENCARGADO DE LOS DATOS DENTRO DE LA EMPRESA:

Nombre: Lcda. Gabriela Morales

Cargo: Responsable de Protección de Datos Correo: privacidad@imgroup.ec

OBJETO DEL CONTRATO

Este contrato regula el acceso y tratamiento de los datos personales proporcionados por la Universidad ECOTEC a IMGroup para la ejecución del servicio de gestión de nómina y administración de personal.

Duración del contrato

Vigencia de 12 meses, renovable automáticamente si no existe notificación de terminación con al menos 30 días de anticipación.

Naturaleza del contrato

Relación de prestación de servicios en la cual IMGroup actúa como encargado del tratamiento de datos personales exclusivamente para el cumplimiento del servicio pactado.
Finalidad del tratamiento

El encargado utilizará los datos personales para procesar la nómina, elaborar contratos laborales, afiliar al personal al IESS y elaborar reportes para el Ministerio de Trabajo. Tipo de datos personales tratados

Datos identificativos (nombres, cédula, correo), laborales (cargo, fecha de ingreso), económicos (sueldo, cuenta bancaria), y sensibles (afiliación al IESS, licencias médicas). Obligaciones del responsable de tratamiento: ECOTEC, como responsable del tratamiento, debe garantizar que los encargados cuenten con las condiciones técnicas, jurídicas y organizativas necesarias para cumplir con la normativa vigente. También debe supervisar, auditar y asegurar el cumplimiento continuo del tratamiento por parte de estos terceros.

Subcontratación: Se establece que el encargado no podrá subcontratar el tratamiento de datos sin previa autorización expresa, escrita y específica por parte de ECOTEC. En caso de aprobarse, el subencargado deberá cumplir con las mismas obligaciones contractuales.

Transferencia internacional de datos: En los casos en que el tratamiento implique la transferencia internacional de datos (por ejemplo, uso de servicios en la nube), se exige que el país receptor cuente con un nivel adecuado de protección reconocido por la autoridad competente o que se suscriban cláusulas contractuales tipo que aseguren dicha protección.

Ejercicio de derechos: Los contratos establecen que los encargados deben asistir a ECOTEC en la gestión de solicitudes de derechos de los titulares (acceso, rectificación, eliminación, oposición, entre otros), sin que puedan responder directamente al titular salvo autorización expresa.

Comunicación de brechas de seguridad: Se obliga al encargado a notificar a ECOTEC de forma inmediata, y no más allá de 72 horas, cualquier incidente o brecha de seguridad que afecte datos personales. Asimismo, debe colaborar en la mitigación del riesgo y en la documentación del evento conforme a lo establecido en el plan de respuesta institucional.

Tratar los datos conforme a las instrucciones del responsable. No usarlos para fines propios ni comunicarlos sin autorización. Implementar medidas de seguridad adecuadas.

Garantizar confidencialidad del personal que accede a los datos. Suprimir los datos al finalizar el contrato.

Colaborar en el ejercicio de derechos de los titulares.

Firmas

En constancia de conformidad, las partes firman el presente contrato en dos ejemplares de igual tenor, en la ciudad de Guayaquil, a los días del mes de de 2025.

Por la Universidad ECOTEC

Firma: Nombre: Dra. María Fernanda Vargas Cargo: Rectora C.I.: 0900000000
Por IMGroup S.A.

Firma: Nombre: Ing. Juan Carlos Zambrano Cargo: Gerente General

C.I.: 0911111111