Maestría en

Nombre Maestría

Trabajo de investigación previo a la obtención del título de

Magíster en Gestión de Riesgo

AUTORES:

Daici Nelva Alberca Colala

Jefferson Eduardo Curay Valdiviezo

Israel Espinoza Rueda

Jorge Antonio Soria Tamayo

Ángel Alejandro Tenemaza Castillo

Nefer Paulette Velasco Holguin

TUTORES:

David G. Benavides Gutiérrez

Paloma Manzano Martínez

Enrique Molina Suarez

"Propuesta de elaboración de un manual de la Norma ISO 31000 para la Gestión de Riesgos en el Instituto Superior Universitario Campus Sur-Campus Matriz"

Quito, abril del 2025

Certificación de autoría

Nosotros, **Daici Nelva Alberca Colala, Jefferson Eduardo Curay Valdiviezo, Israel Espinoza Rueda, Jorge Antonio Soria Tamayo, Ángel Alejandro Tenemaza Castillo, Nefer Paulette Velasco Holguin**, 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:
DAICI NELVA ALBERCA COLALA
Validar únicamente con FirmaEC

Firma del graduando
Daici Nelva Alberca Colala

Firmado electrónicamente por:
JEFFERSON EDUARDO CURAY VALDIVIEZO
Validar únicamente con FirmaEC

Firma del graduando
Jefferson Eduardo Curay Valdiviezo

Firmado electrónicamente por:
ISRAEL ESPINOZA RUEDA
Validar únicamente con FirmaEC

Firma del graduando
Israel Espinoza Rueda

Firmado electrónicamente por:
JORGE ANTONIO SORIA TAMAYO
Validar únicamente con FirmaEC

Firma del graduando
Jorge Antonio Soria Tamayo

Firmado electrónicamente por:
ANGEL ALEJANDRO TENEMAZA CASTILLO
Validar únicamente con FirmaEC

Firma del graduando
Ángel Alejandro Tenemaza Castillo

Firmado electrónicamente por:
NEFER PAULETTE VELASCO HOLGUIN
Validar únicamente con FirmaEC

Firma del graduando
Nefer Paulette Velasco Holguin

Autorización de Derechos de Propiedad Intelectual

Nosotros, **Daici Nelva Alberca Colala, Jefferson Eduardo Curay Valdiviezo, Israel Espinoza Rueda, Jorge Antonio Soria Tamayo, Ángel Alejandro Tenemaza Castillo, Nefer Paulette Velasco Holguin**, en calidad de autores del trabajo de investigación titulado **"Propuesta de elaboración de un manual de la Norma ISO 31000 para la Gestión de Riesgos en el Instituto Superior Universitario Compu Sur-Campus Matriz"**, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, julio 2025

Firmado electrónicamente por:
DAICI NELVA ALBERCA COLALA
Validar únicamente con FirmaEC

Firma del graduando
Daici Nelva Alberca Colala

Firmado electrónicamente por:
JEFFERSON EDUARDO CURAY VALDIVIEZO
Validar únicamente con FirmaEC

Firma del graduando
Jefferson Eduardo Curay Valdiviezo

Firmado electrónicamente por:
ISRAEL ESPINOZA RUEDA
Validar únicamente con FirmaEC

Firma del graduando
Israel Espinoza Rueda

Firmado electrónicamente por:
JORGE ANTONIO SORIA TAMAYO
Validar únicamente con FirmaEC

Firma del graduando
Jorge Antonio Soria Tamayo

Firmado electrónicamente por:
ANGEL ALEJANDRO TENEMAZA CASTILLO
Validar únicamente con FirmaEC

Firma del graduando
Ángel Alejandro Tenemaza Castillo

Firmado electrónicamente por:
NEFER PAULETTE VELASCO HOLGUIN
Validar únicamente con FirmaEC

Firma del graduando
Nefer Paulette Velasco Holguin

Aprobación de dirección y coordinación del programa

Nosotros, **Paloma Manzano Martínez/ David G. Benavides Gutiérrez**, declaramos que los graduandos: **Daici Nelva Alberca Colala, Jefferson Eduardo Curay Valdiviezo, Israel Espinoza Rueda, Jorge Antonio Soria Tamayo, Ángel Alejandro Tenemaza Castillo, Nefer Paulette Velasco Holguin** 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 10:32:54 +02'00'

Paloma Manzano Martínez

Directora de la Maestría en Gestión de riesgos

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

David G. Benavides Gutiérrez

Coordinador Maestría en Gestión de riesgos

DEDICATORIA

A mis padres, por ser el pilar de mi vida. Gracias por enseñarme con su ejemplo el valor del esfuerzo, la honestidad y la perseverancia. Su apoyo incondicional, incluso en los momentos más difíciles, ha sido la luz que me ha guiado a seguir adelante y a nunca rendirme.

A mis hermanos, compañeros de vida y motivación constante. Su confianza en mí, sus palabras de aliento y esa complicidad que solo los hermanos conocen, me han impulsado a superarme día tras día.

A mi abuela por su amor incondicional en los últimos años. Ella se ha convertido en un ejemplo de vida y en mi mayor inspiración para seguir adelante cada día con honestidad y carácter.

Este proyecto no solo es un logro académico, sino también el reflejo de los valores que me han inculcado desde siempre: responsabilidad, amor por el conocimiento y la firme creencia de que todo es posible con dedicación y corazón.

Con profundo cariño, les dedico este trabajo que lleva parte de ustedes en cada página.

Jefferson Curay.

A Dios por otorgarme la perseverancia para mantenerme firme en el camino del aprendizaje, sin esa constancia no habría sido posible culminar una meta muy importante.

A mi familia que siempre me apoya en todos mis retos a lo largo del tiempo, gracias por enseñarme el valor del trabajo constante y la dignidad del esfuerzo, por mostrarme que los sueños se conquistan con determinación y que los obstáculos son solo oportunidades para fortalecerse. Cada página de este trabajo refleja los valores que ustedes sembraron en mí.

Finalmente, dedico este logro a mí ser, por no rendirse ante las adversidades, por las horas invertidas, los sacrificios realizados y la disciplina mantenida hasta el final. Este trabajo representa no solo la culminación de un proyecto académico, sino también un testimonio de que la constancia y la pasión pueden transformar los desafíos en triunfos significativos.

Jorge Soria.

Quiero agradecer:

Dedico principalmente a Dios, por darme la fuerza necesaria para culminar esta meta.

A mi padre, madre por sus consejos, cariño, amor, apoyo incondicional, a mi hijo quien es mi pilar fundamental para poder culminar con éxitos la maestría., este triunfo es de todos.

Un sincero agradecimiento a mis compañeros del proyecto de titulación ya que cada uno de ustedes ha contribuido con sus conocimientos para realizar este trabajo.

Me gustaría agradecer a la Universidad Internacional del Ecuador por abrirme las puertas y brindarme la oportunidad de avanzar en mis estudios profesional, s los docentes de la maestría que han aportado con sus conocimientos y experiencia en mi formación profesional.

Alejandro Tenemaza.

A mis padres Edwin (+) y Anita (+) por darme la vida, no caminaron mucho conmigo, pero sé que desde arriba me cuidan en cada paso que doy.

A mis abuelitos Elías (+) y Anita que han sido como mis padres, me acogieron desde muy niño, me han enseñado todos los principios y valores que me han permitido ser una buena persona y me han apoyado en toda mi formación académica para ser profesional. Este crecimiento académico es justamente para aumentar el orgullo que sienten.

A mi compañera de vida Yadi que me ha dado un hijo hermoso, es una esposa y madre sin igual. De igual manera ha sido constante en su apoyo sentimental, logístico y técnico para el adecuado desarrollo de esta maestría.

A mi hijo Edwin Israel por ser esa motivación extra que siempre se necesita para tomar decisiones en favor de la superación personal y familiar. Todo esfuerzo que se hace será para mejorar su futuro.

Israel Espinoza R.

En primer lugar, quiero agradecer a Dios por ser mi guía, mi fuerza y mi refugio en cada paso de este camino, por darme la sabiduría, la fe y la fortaleza para culminar este logro.

A mi amado esposo, Marvi Viteri por su amor incondicional, su paciencia infinita y su apoyo constante, que fueron fundamentales para alcanzar esta meta.

A mis padres, Paul Velasco y Katty Holguín por su ejemplo de esfuerzo y sacrificio, por enseñarme el valor de la educación y por ser mi motor e inspiración en cada etapa de mi vida.

A mis hermanos, Génesis Velasco y Paul Velasco por su amor inmenso, sus oraciones y por ser la raíz de la familia que me sostiene y me impulsa a seguir adelante.

A mis abuelos, por su amor inmenso, por cuidarme desde pequeña, sus oraciones y por ser la raíz de la familia que me sostiene y me impulsa a seguir adelante.

Nefer Velasco Holguín.

Dedico este logro a mis padres, cuyo amor y dedicación han sido las fuerzas que han guiado mi vida. A mi querido padre, que ya no está físicamente con nosotros, pero cuya sabiduría y fortaleza siguen resonando en lo más profundo de mi corazón. Su ejemplo de trabajo arduo y

perseverancia ha sido una fuente de inspiración constante. Cada desafío que he enfrentado ha sido moldeado por las valiosas lecciones que me enseñó, y su recuerdo me impulsa a seguir adelante con determinación y coraje.

A mi adorada madre, el faro que ilumina mi camino. Su amor incondicional y tu apoyo constante han sido mi refugio en los momentos de incertidumbre. Gracias por creer en mí, incluso cuando yo dudaba de mis propias capacidades. Su sacrificio y dedicación han hecho posible que hoy me encuentre aquí, logrando un sueño que compartíamos y que siempre llevaremos en nuestros corazones.

A mis hermanos, mis cómplices en esta travesía. Cada uno de ustedes ha aportado risas, apoyo y un sentido de pertenencia que ha hecho de mi vida algo verdaderamente especial. Juntos hemos creado recuerdos que atesoro profundamente, y su aliento me ha dado fuerzas en los momentos más difíciles. No hay nada como saber que siempre puedo contar con ustedes.

Con todo mi cariño y gratitud,

Daici Nelva Alberca Colala

AGRADECIMIENTOS

Agradecemos profundamente al Instituto Tecnológico Superior Compu Sur (ITECSUR) por la apertura brindada, por compartir su valiosa información y permitirnos realizar un análisis que contribuya a fortalecer su gestión de riesgos. Su disposición y colaboración han sido fundamentales para el desarrollo de este trabajo.

Extendemos también nuestro sincero agradecimiento a nuestros compañeros de clase, quienes con sus ideas, experiencias y compromiso han enriquecido este proceso académico. Ha sido un verdadero privilegio compartir este camino con personas tan dedicadas y solidarias.

Finalmente, expresamos nuestra gratitud a nuestros profesores, cuyas enseñanzas, guía y motivación nos han permitido adquirir los conocimientos necesarios para enfrentar con responsabilidad y criterio los desafíos profesionales. Su aporte ha sido clave para transformar este proyecto en una experiencia de crecimiento académico y personal.

A todos ustedes, gracias por ser parte de este proceso.

RESUMEN

El presente trabajo tiene como objetivo diseñar e implementar un modelo de gestión de riesgos basado en la norma ISO 31000:2018 en el Instituto Tecnológico Superior Compu Sur (ITECSUR) enfocado en la protección de datos personales y la seguridad de la información. En un contexto donde las instituciones educativas ecuatorianas enfrentan crecientes desafíos frente a amenazas cibernéticas y marcos legales más estrictos, como la Ley Orgánica de Protección de Datos Personales del Ecuador (2021), se identificó la necesidad de establecer un sistema estructurado de identificación, evaluación, tratamiento y monitoreo de riesgos. La investigación se desarrolló bajo un enfoque correctivo y preventivo, proponiendo la elaboración de un manual técnico que permita al Instituto cumplir con la normativa vigente, fortalecer la cultura institucional de seguridad de la información y reducir la exposición a brechas de seguridad. Se abordo como alcance del sistema de gestión el proceso crítico de gestión de información académica y la consideración de activos tecnológicos, análisis de riesgos y controles aplicables, estableciendo acciones correctivas y preventivas bajo los principios de la norma ISO 31000. El resultado final proporciona una hoja de ruta para que ITECSUR mejore su gobernanza de riesgos académicos, tecnológicos, legales-normativos, administrativos y reputacionales.

Palabras Claves: Gestión de riesgos, protección de datos personales, gestión académica, concientización, comunidad educativa, ISO 31000:2018

ABSTRACT

This study aims to design and implement a risk management model based on the ISO 31000:2018 standard at the Instituto Tecnológico Superior Compu Sur (ITECSUR), focused on personal data protection and information security. In a context where Ecuadorian educational institutions face growing challenges from cyber threats and increasingly strict legal frameworks—such as the Organic Law on Personal Data Protection of Ecuador (2021)—the need was identified to establish a structured system for identifying, assessing, treating, and monitoring risks. The research was developed under a corrective and preventive approach, proposing the creation of a technical manual that enables the institution to comply with current regulations, strengthen its institutional culture of information security, and reduce its exposure to security breaches. The scope of the management system addressed the critical process of academic information management, including the consideration of technological assets, risk analysis, and applicable controls, establishing corrective and preventive actions aligned with the principles of ISO 31000. The outcome provides a roadmap for ITECSUR to enhance its governance of academic, technological, regulatory, administrative, and reputational risks.

Keywords: Risk management, personal data protection, academic management, awareness, educational community, ISO 31000:2018

TABLA DE CONTENIDOS (Índice)

LISTA DE TABLAS

LISTA DE FIGURAS (Índice de figuras)

Capítulo 1:

Introducción

En la actualidad, las instituciones de educación superior enfrentan desafíos crecientes frente a la transformación digital y el uso intensivo de tecnologías para gestionar información académica, administrativa y personal. Esta realidad conlleva una exposición constante a riesgos asociados al manejo de datos, tales como accesos no autorizados, pérdida de información o vulneraciones a la privacidad, que pueden afectar la operación institucional y la confianza de su comunidad educativa.

La gestión de riesgos permite anticipar y reducir el impacto de eventos no deseados, garantizando la continuidad de las actividades y la protección de los recursos críticos. En este contexto, resulta fundamental contar con un sistema estructurado que permita identificar, evaluar, tratar y monitorear los riesgos que afectan el entorno educativo. Asimismo, el cumplimiento de marcos normativos como la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP), vigente desde 2021, obliga a las instituciones a adoptar medidas que garanticen la seguridad y el uso legítimo de los datos personales.

El presente trabajo propone el diseño e implementación de un modelo de gestión de riesgos basado en la norma internacional ISO 31000:2018 aplicado al Instituto Tecnológico Superior Compu Sur (ITECSUR). Este modelo tiene como finalidad fortalecer la protección de datos personales, mejorar la seguridad de la información y cumplir con los requerimientos legales vigentes.

El proyecto parte del reconocimiento del problema sobre la ausencia en el instituto de contar con un sistema formal y organizado que permita gestionar adecuadamente los riesgos tecnológicos e institucionales en el tratamiento de la información. Por ello, el objetivo principal es establecer una propuesta clara, práctica y adaptable a través de manuales y análisis de su situación actual.

1. PLANTEAMIENTO DEL PROBLEMA E IMPORTANCIA DEL ESTUDIO

1.1. Definición del proyecto

El presente proyecto tiene como finalidad diseñar un manual de implementación de un sistema de gestión integral de riesgos basado en la norma ISO 31000:2018 para el Instituto Tecnológico Superior Compu Sur (ITECSUR). El modelo propuesto busca abordar los riesgos institucionales en sus diferentes dimensiones: académica, tecnológica, legal, normativa, administrativa y reputacional, con un enfoque preventivo y correctivo que permita fortalecer la resiliencia de la organización frente a eventos no deseados.

La iniciativa surge como respuesta a la falta de un modelo formal y estructurado para la identificación, evaluación, tratamiento y monitoreo de riesgos dentro de ITECSUR. Esta carencia incrementa la exposición de la institución a impactos que pueden afectar la continuidad de sus operaciones, la calidad de sus servicios y la confianza de su comunidad educativa.

Con este manual se busca generar una guía a la institución de una herramienta que mejore su gobernanza, optimice la toma de decisiones frente a escenarios de riesgo, y

contribuya a mitigar impactos que pudieran comprometer su operación, reputación o cumplimiento regulatorio.

1.2. Naturaleza o tipo de proyecto

Este es un proyecto de diseño ya que se basa en el diseño de la normativa internacional ISO 31000 y en regulaciones nacionales de datos personales para la toma de decisiones. Además, es un proyecto preventivo, pues propone el diseño de estructuras y medidas orientadas a gestionar eficazmente los riesgos de seguridad de la información.

1.3. Objetivos

1.3.1. Objetivo general

- Desarrollar un modelo de la norma ISO 31000 en el Instituto Tecnológico Superior Compu Sur para la gestión de riesgos académicos, tecnológicos, legales, normativos, administrativos y reputacionales que se identifiquen.

1.3.2. Objetivo especifico

- Identificar los activos de información críticos y los roles involucrados en el tratamiento de datos personales dentro de ITECSUR.
- Analizar los riesgos existentes relacionados con la gestión y tratamiento de datos, evaluando su probabilidad, impacto y controles actuales.
- Proponer controles y medidas de seguridad acordes al nivel de riesgo detectado, alineados con los principios de la norma ISO 31000.
- Definir un plan de acción que facilite la implementación progresiva del modelo de gestión de riesgos propuesto.

1.3.3. Justificación e importancia del trabajo de investigación

En Ecuador, el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) en 2021 ha establecido un marco legal que obliga a las organizaciones, incluidas las instituciones educativas, a implementar medidas técnicas y organizativas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que manejan. Sin embargo, estudios recientes indican que muchas instituciones aún enfrentan desafíos en la implementación efectiva de estas medidas, debido a limitaciones en infraestructura tecnológica y capacitación del personal. Álvarez-Carrión, J. A., & Hernández-Sotomayor, G. P. (2024).

Además, el panorama de ciberseguridad en el país es preocupante. Ecuador se posiciona como el tercer país con mayores amenazas cibernéticas en América Latina, con un incremento del 8% en los ataques cibernéticos semanales durante el año 2023. Estos ataques incluyen tácticas como el ransomware, phishing avanzado y ataques a infraestructuras críticas, afectando sectores clave como el educativo. Goberna, R. (2024).

Frente a este contexto, la implementación de un modelo de gestión de riesgos basado en la norma ISO 31000 se presenta como una necesidad imperante para las instituciones educativas. Este modelo proporciona un enfoque estructurado para identificar, evaluar y mitigar los riesgos desde un enfoque integral.

El desarrollo de este proyecto no solo busca cumplir con las disposiciones legales vigentes, sino también fomentar una cultura organizacional orientada hacia la seguridad de la

información, promoviendo la confianza entre los miembros de la comunidad educativa y asegurando la continuidad de las operaciones académicas en un entorno digital seguro.

Capítulo 2
La Organización

2. PERFIL DE LA ORGANIZACIÓN.

2.1. NOMBRE, ACTIVIDADES, MERCADOS SERVIDOS Y PRINCIPALES CIFRAS

2.1.1. Nombre de la empresa

Instituto Tecnológico Superior Compu Sur

2.1.2. Misión, visión, valores

Misión

Formar profesionales de niveles técnico, tecnológico, superior universitario y/o de posgrado con carácter humanista, científico, de pensamiento autocrítico, innovador y emprendedor, con criterios de formación autodidacta y principios de trabajo orientados al servicio, a través de un enfoque de calidad, mejoramiento continuo y con capacidad para generar estrategias en beneficio del desarrollo.

Visión

Ser una institución académica, investigativa y de vinculación con la sociedad de referencia nacional, líder en la formación de profesionales de niveles técnico, tecnológico, superior universitario y/o de posgrado con vocación de servicio, integralidad y excelencia.

Valores institucionales

1.Libertad académica.

2. Transversalidad de la investigación básica.

3. Autonomía institucional responsable.

4. No discriminación.

5. Pluralidad.

6. Protección frente a los actos de violencia.

7. Inviolabilidad del espacio académico.

8. Prohibición de la censura.

9. Protección y prevención frente a acciones u omisiones de terceros.

10. Educación en derechos humanos.

11. Acceso a la información, Internet y a otras tecnologías.

12. Cooperación y diálogo inclusivo.

13. Implementación de acciones afirmativas.

2.1.3. Actividades, marcas, productos y servicios

Como parte de las actividad y servicios de la institución se consideran las siguientes categorías de productos a sus estudiantes.

2.1.3.1.Actividades

El Instituto Tecnológico Superior Universitario Compu Sur (ITECSUR) desarrolla diversas actividades académicas y complementarias, entre las que se destacan:

- **Formación técnica y tecnológica**: Ofrece programas de nivel técnico y tecnológico superior en áreas como salud, tecnología, derecho, administración, educación y seguridad ciudadana.
- **Educación continua**: Proporciona cursos de profesionalización, seminarios, talleres y programas de formación complementaria para el desarrollo profesional de la comunidad educativa.

- **Investigación y vinculación**: Participa en proyectos de investigación y mantiene una revista científica institucional para la difusión del conocimiento.
- **Servicios en línea**: Dispone de plataformas digitales como campus virtual, biblioteca virtual y correo institucional para facilitar el acceso a recursos académicos.

2.1.3.2.Marcas

ITECSUR utiliza su nombre institucional como marca principal en todas sus actividades y servicios. Además, cuenta con logotipos y distintivos visuales que representan su identidad corporativa en medios digitales, impresos y eventos institucionales.

Figura 1

Logo ITECSUR

Fuente: *ITECSUR.*

2.1.3.3. Productos o servicios

Los principales productos o servicios que ofrece ITECSUR incluyen:

- **Programas académicos**: Carreras de nivel técnico y tecnológico superior en diversas modalidades (presencial, en línea e híbrida), tales como:

- Técnico Superior en Enfermería.
- Tecnología Superior en Desarrollo Infantil Integral.
- Tecnología Superior en Asistencia Jurídica.
- Tecnología Superior en Rehabilitación Física.
- Tecnología Superior en Estética Integral.
- Tecnología Superior en Control de Incendios y Operaciones de Rescate.
- Tecnología Superior en Administración.
- Tecnología Superior en Desarrollo de Software.
- Tecnología Superior en Ciberseguridad.
- Tecnología Superior en Seguridad Ciudadana y Orden Público.
- Tecnología Superior en Emergencias Médicas.

- **Educación continua**: Ofrece programas de profesionalización, estudios paralelos, seminarios y cursos especializados para el fortalecimiento de competencias en diversas áreas.
- **Servicios digitales**: Proporciona acceso a plataformas como el campus virtual, biblioteca virtual y correo institucional para apoyar el proceso de enseñanza-aprendizaje.

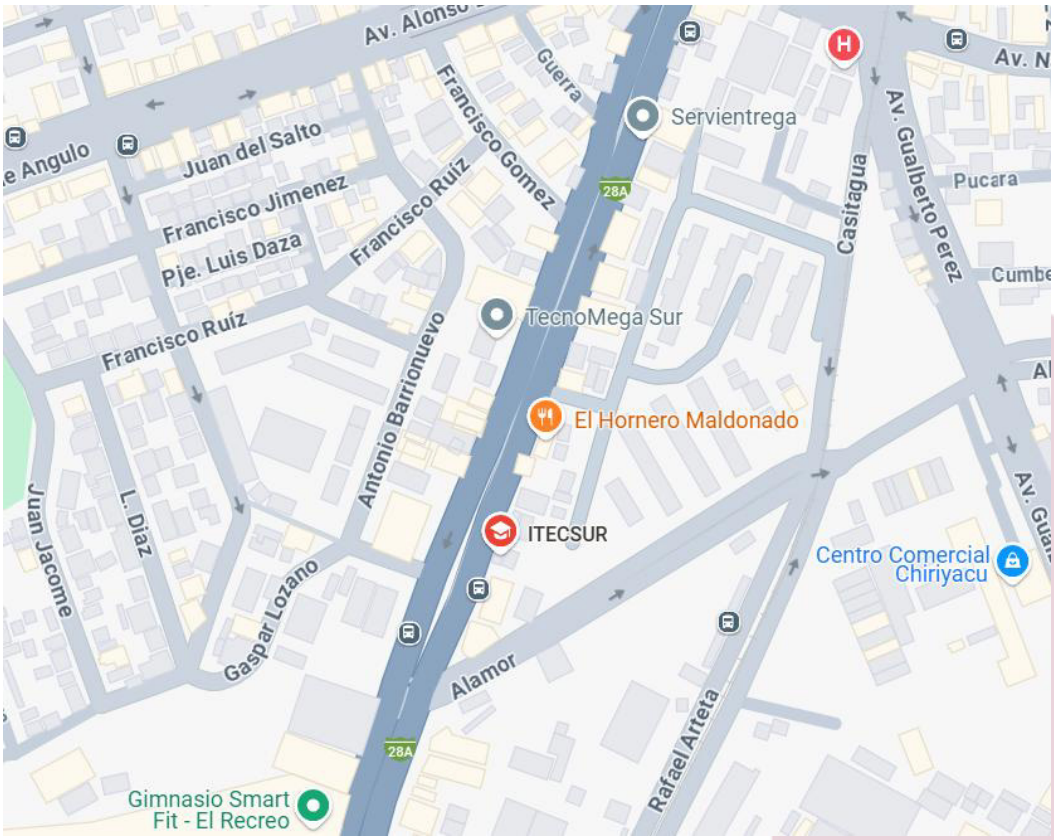
2.1.3.4. Ubicación de la sede

Se cuenta con una Sede Matriz en el sur, el primer edificio ubicado en la Av. Maldonado y Gil Martin y en la Av. Maldonado y Alamor, el segundo es un edificio propio de la institución de cinco pisos donde funcionan armónicamente sus espacios y frente a este, se

cuenta con un edificio alquilado (compuesto por cuatro pisos, en el cual se trabajan específicamente aulas y laboratorios pequeños).

Figura 2

Ubicación de ITECSUR



Fuente: *Google Maps*.

2.1.3.5. Ubicación de las operaciones

Sede Matriz: Av. Maldonado y Gil Martin.

Figura 3

Ubicación de operaciones ITECSUR

Fuente: *Google maps*

2.1.3.6. Propiedad y forma jurídica

La propiedad y forma jurídica de la institución es: Sociedad con personería jurídica, considerando:

- Sector: Privado

- Estado actual: Abierto
- Provincia: Pichincha
- Cantón: Quito

2.1.3.7. Mercados servidos o ubicación de sus actividades de negocio

El Instituto Tecnológico Superior Compu Sur (ITECSUR) desarrolla sus actividades académicas y administrativas principalmente en las siguientes ubicaciones físicas dentro del territorio ecuatoriano:

- Provincia de Pichincha:
    - Campus de estudio y edificio administrativo Matriz: Quito, sector centro-norte.
    - Campus de estudio Shyris: Quito, sector norte.
    - Campus de estudio Villaflora: Quito, sector sur.
- Provincia de Guayas:
    - Campus Guayaquil: Ciudad de Guayaquil, sector norte.

En cada uno de estos campus, ITECSUR ofrece programas de educación técnica y tecnológica superior en modalidades presencial, en línea e híbrida, proporcionando servicios académicos de formación profesional, educación continua y vinculación con la sociedad.

Además, gracias a su oferta académica en modalidad virtual (en línea), la institución amplía su alcance a todo el territorio nacional, permitiendo el acceso a sus programas a estudiantes ubicados en distintas provincias del Ecuador.

ITECSUR orienta sus servicios educativos principalmente a los siguientes segmentos:

- Estudiantes de nivel técnico y tecnológico superior: jóvenes y adultos que buscan una

formación profesional con alta empleabilidad en áreas como salud, tecnología, educación, derecho, administración, seguridad y emergencias.

- Profesionales que buscan actualización académica: mediante programas de educación continua, cursos de certificación y especialización que fortalecen habilidades específicas en distintas disciplinas.
- Egresados de bachillerato: que desean acceder a programas de tercer nivel con reconocimiento oficial y rápida inserción laboral.
- Sector productivo y sociedad en general: a través de programas de vinculación con la sociedad y proyectos de investigación que promueven el desarrollo social, económico y tecnológico.

La institución, a través de sus modalidades presencial, híbrida y virtual, atiende un mercado diversificado que incluye tanto estudiantes de zonas urbanas de Quito y Guayaquil como estudiantes de otras ciudades y provincias que optan por programas en modalidad en línea.

2.1.3.8. Tamaño de la organización

El Instituto Tecnológico Superior Compu Sur (ITECSUR) cuenta actualmente con:

- 5 campus: Matriz (Quito) + Shyris, Villaflora, Valle de Los Chillos (todos en Pichincha) + Guayaquil (Guayas).
- 5191 estudiantes matriculados en sus distintos programas de formación técnica y tecnológica superior.
- 33 profesores que integran la plantilla académica regular.

Con base en esta información, se considera que ITECSUR es una organización educativa de tamaño grande, dado que:

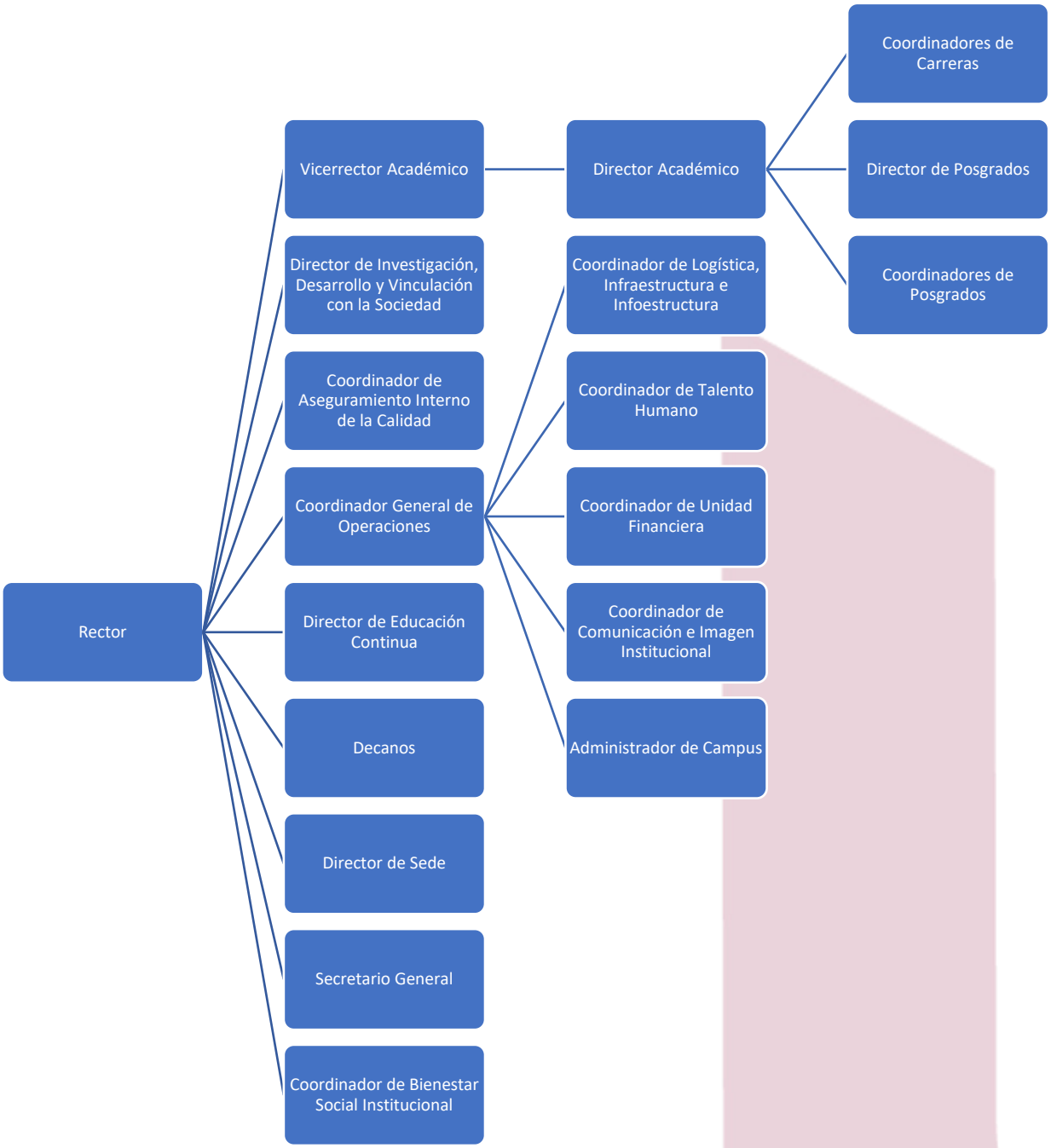
- Según estándares de categorización educativa en Ecuador y Latinoamérica, una institución con más de 2000 estudiantes matriculados y múltiples campus físicos se clasifica como institución grande.
- Su operación en varias provincias (Pichincha y Guayas) y su modalidad mixta (presencial, en línea e híbrida) también respaldan esta clasificación.

Esta dimensión permite a ITECSUR tener una cobertura nacional y un impacto significativo en la formación de talento humano técnico y tecnológico en el país.

La Estructura en Organigrama dando cumplimiento del Reglamento Interno y fuentes institucionales, el organigrama funcional simplificado es el siguiente:

Figura 4

Organigrama de la estructura organizacional de Itecsur.



Fuente: Elaborado por equipo técnico

2.1.3.9. Información sobre empleados y otros trabajadores

El Instituto Tecnológico Superior Compu Sur (ITECSUR) cuenta con un equipo humano comprometido con la calidad educativa y el desarrollo institucional. A continuación, se presenta una caracterización general del personal con base en datos disponibles y estimaciones:

Distribución por tipo de contrato

Tipo de trabajador	Cantidad estimada	Porcentaje (%)
Docentes con contrato fijo	48	15.58%
Docentes con contrato temporal	173	56.17%
Personal administrativo fijo	78	25.32%
Personal técnico (TI, soporte)	6	1.95%
Personal de servicios operativos	3	0.97%
Total estimado	308	100%

Distribución por sexo

Sexo	Porcentaje estimado (%)
Masculino	45%
Femenino	55%

Distribución por grupo etario

Grupo de edad	Porcentaje estimado (%)
Menores de 30 años	22%
Entre 30 y 45 años	51%
Mayores de 45 años	27%

Dentro de la estructura de ITECSUR, los siguientes cargos directivos también cumplen funciones operativas:

- Rector: Dirección institucional y representación legal.
- Vicerrector Académico: Coordinación general académica.
- Director Académico: Supervisión del cuerpo docente y de los programas educativos.
- Directores de Posgrado, Educación Continua, y Decanos: Ejercen funciones de gestión y docencia en sus áreas respectivas.

Adicionalmente, varios directores y coordinadores (por ejemplo, en áreas de investigación, calidad, operaciones y comunicación) tienen participación activa en la toma de decisiones estratégicas y en la ejecución operativa.

2.1.3.10. Procesos claves relacionados con el objetivo propuesto

Para el diseño e implementación del manual del modelo de gestión de riesgos basado en la norma ISO 31000, es fundamental identificar aquellos procesos que son críticos para la identificación de riesgos integrales dentro del ciclo de vida académico y administrativo de la institución.

Estos procesos no solo sustentan la actividad educativa principal de ITECSUR, sino que también representan áreas clave donde existen riesgos asociados al tratamiento de información sensible, por lo que deben ser analizados, evaluados y controlados como parte del sistema de gestión de riesgos.

A continuación, se detallan los procesos claves:

Tabla 1

Procesos claves del negocio de la institución identificados

Proceso clave	Descripción
Proceso de admisión y matrícula	Inicia con la inscripción del estudiante interesado, evaluación de requisitos, validación de documentos y culmina con la matrícula formal en el sistema académico.
Gestión de la vida estudiantil	Abarca el seguimiento al rendimiento académico, registro de asistencia, evaluación continua, atención a necesidades de bienestar estudiantil y tutorías.
Ejecución de programas académicos	Incluye la planificación, diseño y ejecución de las mallas curriculares por parte de los docentes y coordinadores de carrera en cada ciclo académico.
Evaluación y calificación	Aplicación de instrumentos de evaluación y registro de calificaciones en el sistema académico, conforme a lo establecido por los reglamentos internos.
Gestión de prácticas preprofesionales y vinculación	Organización, control y seguimiento de actividades que permiten a los estudiantes aplicar sus conocimientos en contextos reales.
Proceso de titulación	Gestión de requisitos de egreso, trabajo final o proyecto integrador, trámites administrativos y obtención del título de tercer nivel tecnológico.
Seguimiento a graduados	Recopilación de información de egresados para evaluar la pertinencia de la oferta académica y el impacto en el entorno laboral.

Fuente: Instituto Tecnológico Superior Compu Sur

Adicionalmente para el diseño e implementación de la norma ISO 31000 en ITECSUR, los procesos clave incluyen procesos transversales como los siguientes:

- **Protección de Datos Personales:** Manejo y resguardo de la información personal de estudiantes y personal, en cumplimiento con normativas de privacidad.

- **Seguridad de la Información:** Implementación de medidas para proteger la integridad y confidencialidad de los datos institucionales.
- **Investigación y Desarrollo:** Conducción de proyectos de investigación que requieren manejo seguro de datos sensibles.

2.1.3.11. Principales cifras, ratios y números que definen a la empresa

ITECSUR es un instituto tecnológico privado que no publica sus finanzas al no contar con esa obligación por su ente regulador, sin embargo, el detalle en relación a sus datos institucionales y números que definen al instituto son:

- Año de fundación: 1994.
- Tipo de institución: Instituto Superior Universitario técnico-tecnológico, acreditado por SENESCYT.
- Número de carreras de tercer nivel: 13 carreras entre presencial, online e híbridas.
- Cantidad aproximada de estudiantes: Alrededor de 3000 estudiantes en 2025.

2.1.3.12. Modelo de negocio

ITECSUR opera bajo un modelo educativo que combina la formación técnica y tecnológica con servicios de educación continua. Ofrece programas académicos en diversas facultades, incluyendo Salud, Seguridad Ciudadana, Derecho y Administración, Educación y Tecnología. Además, proporciona cursos de capacitación y certificaciones para profesionales y público en general, contribuyendo al desarrollo profesional y comunitario.

2.1.3.13. Grupos de interés internos y externos

Internos:

- Estudiantes: Beneficiarios directos de los programas educativos.
- Docentes: Responsables de impartir conocimientos y guiar el aprendizaje.
- Personal Administrativo: Encargados de la gestión operativa y administrativa de la institución.

Externos:

- Graduados: Egresados que mantienen vínculo con la institución a través de programas de seguimiento y actualización.
- Entidades Reguladoras: Organismos gubernamentales que supervisan el cumplimiento de normativas educativas y de protección de datos.
- Sociedad en General: Comunidad que se beneficia de los servicios educativos y proyectos de vinculación social de ITECSUR.

2.1.3.14. Otros datos de interés

- Normativas Institucionales: ITECSUR cuenta con un conjunto de reglamentos que rigen aspectos como seguimiento a graduados, formación y capacitación de profesores, relaciones interinstitucionales, prácticas preprofesionales, investigación y desarrollo, selección de personal académico, aseguramiento interno de la calidad, otorgamiento de becas y acompañamiento a estudiantes.
- Publicaciones Académicas: La institución edita revistas científicas como "InnDev" y la "Revista Ecuatoriana de Derecho y Administración", que difunden investigaciones en diversas áreas del conocimiento.

- Compromiso Ambiental: Implementa políticas de gestión ambiental, manejo de desechos y residuos, y promueve buenas prácticas ambientales dentro de la comunidad educativa.

Capítulo 3
Manual Documento de seguridad

3.1.Análisis de Riesgos.

3.1.1. Identificación de la organización y de sus centros de trabajo.

Organización: Instituto Tecnológico Superior Compu Sur - 1792902630001.

Centro de trabajo: Campus matriz - Av. Pedro Vicente Maldonado y Alamor.

Otras sucursales fuera del alcance:

- Sucursal Adamus.
- Cede norma Luna.
- Campus Norte.
- Campus Valle de los Chillos.

3.1.2. Representante legal y Responsable de seguridad.

Representante legal: Erazo Luna Andrés Mauricio.

Responsables de seguridad:

Seguridad digital: Ing. Jorge Muzo.

Seguridad física: Servicio contratado del proveedor Grunseg.

3.1.3. Actividades de la organización.

La institución se dedica a la educación de tercer nivel, destinado a la formación básica en una disciplina o a la capacitación para el ejercicio de una profesión. Corresponden a este nivel el grado de tecnólogo, licenciado y los títulos profesionales universitarios o politécnicos, que son equivalentes, incluido las actividades de escuelas.

3.1.4. Tratamientos de la organización y sus riesgos.

El tratamiento de datos identificado en talleres conjuntos con la institución es:

Tabla 2

Tratamiento de la organización y sus riesgos

Tratamientos de datos	Riesgo asociado
Datos del historial académico de estudiantes	Divulgación no autorizada de calificaciones u observaciones personales
	Acceso indebido por personal no autorizado
	Pérdida de información por fallos en el sistema o eliminación accidental
Datos de facturación de estudiantes	Uso fraudulento de información financiera
	Pérdida de confidencialidad por mal manejo de archivos digitales o físicos
Datos laborales de estudiantes	Uso indebido en procesos de selección u otras decisiones sin consentimiento
	Exposición no autorizada en procesos internos
Datos de identificación y contacto para matriculación y carnetización	Suplantación de identidad
	Divulgación no autorizada de datos personales
Fotos de estudiantes para carnetización	Uso no autorizado en redes o material institucional
Datos personales sensibles de estudiantes (ej. discapacidad, salud, orientación)	Discriminación por parte de terceros o personal interno
	Divulgación sin consentimiento expreso
Datos de bienestar estudiantil	Pérdida de confidencialidad por falta de medidas de seguridad
	Uso no ético de información en procesos de evaluación o intervención
Fotos de estudiantes para campañas de marketing	Publicación sin consentimiento
	Asociación no deseada a la imagen institucional

Videovigilancia de personal administrativo, docentes y estudiantes en aulas y pasillos	Uso indebido de grabaciones para fines disciplinarios o sin autorización
	Vulneración del derecho a la privacidad
Datos socioeconómicos de estudiantes	Estigmatización o discriminación
	Divulgación indebida a terceros
Datos de identificación y contacto del personal	Suplantación de identidad
Fotos del personal	Publicación sin autorización
Datos personales sensibles del personal (ej. salud, afiliaciones)	Discriminación laboral
	Acceso no autorizado por personal no autorizado
Datos laborales del personal (currículum	Modificación no autorizada de información profesional
	Uso indebido en redes o medios institucionales sin consentimiento
Datos médicos del personal con dependencia	Discriminación o vulneración de derechos laborales
Datos biométricos del personal	Suplantación de identidad mediante copias biométricas
Videovigilancia del personal en aulas y pasillos	Monitorización indebida del desempeño laboral
Datos contractuales y legales (firmas, antecedentes, etc.)	Filtración de información confidencial legal
Datos contractuales y legales	Discriminación o uso inapropiado en procesos internos

Fuente: Instituto Tecnológico Superior Compu Sur

3.1.5. Consentimientos y notas informativas.

INSTITUTO TECNOLÓGICO SUPERIOR COMPU SUR (ITECSUR)

RUC: 1792902630001.

Dirección: Campus matriz - Av. Pedro Vicente Maldonado y Alamor.

Página web: https://itecsur.edu.ec

Yo,

Nombres y apellidos: _____

Cédula de identidad: _____

Correo electrónico: _____

Teléfono: _____

En calidad de: ☐ Estudiante ☐ Investigador

del Instituto Tecnológico Superior Compu Sur (ITECSUR), expreso mi consentimiento libre, específico, informado e inequívoco para que ITECSUR, en calidad de responsable del tratamiento, realice el tratamiento de mis datos personales conforme a lo dispuesto en la Ley Orgánica de Protección de Datos Personales del Ecuador.

---

1. Finalidad del tratamiento

Mis datos personales serán tratados para las siguientes finalidades:

- Gestionar los procesos de admisión, matrícula, control académico y titulación.
- Administrar mi participación en programas de bienestar estudiantil, investigación y actividades de vinculación con la sociedad.
- Cumplir con obligaciones legales ante organismos de control educativo nacionales.
- Gestionar el acceso a plataformas educativas, bibliotecas virtuales, correo institucional y otros servicios digitales del centro.

2. Base legal del tratamiento

Este consentimiento se otorga conforme a lo establecido en los artículos 7, 8, 9, 10, 11 y 12 de la Ley Orgánica de Protección de Datos Personales del Ecuador, y en cumplimiento del principio de licitud, transparencia, finalidad y proporcionalidad.

3. Tratamiento de la imagen personal (Opcional)

El Instituto podrá utilizar mi imagen (fotografía o video) exclusivamente para fines de comunicación institucional y promoción educativa en sus medios oficiales (página web, redes sociales, material promocional), siempre que yo otorgue mi consentimiento explícito.

Marque la opción que corresponda:

☐ Autorizo el uso de mi imagen para fines institucionales descritos.

☐ No autorizo el uso de mi imagen.

4. Plazo de conservación

Mis datos personales serán conservados durante la vigencia de mi relación académica con el Instituto y, posteriormente, durante los plazos de prescripción legal aplicables para cumplir obligaciones administrativas y legales.

5. Derechos del titular de los datos

Como titular de mis datos personales, reconozco que tengo derecho a:

- Acceder a mi información personal.
- Rectificar datos incorrectos.
- Solicitar la supresión de mis datos cuando haya perdido la finalidad.
- Oponerme al tratamiento.
- Revocar el presente consentimiento en cualquier momento.

Para ejercer mis derechos, podré contactar al Responsable del Tratamiento a través del correo: info@itecsur.edu.ec.

---

6. Destino de la información

Mi imagen no será utilizada con fines distintos a los aquí descritos ni será cedida a terceros sin mi autorización, salvo por obligación legal.

Fecha de firma: ___ / ___ / 202__

Lugar: Quito, Ecuador

Firma del titular: _____

Firma del responsable institucional: _____

Nombre: _____

Cargo: _____

3.2. Registro de Actividades de Tratamiento.

3.2.1. Grupos de información.

Este apartado tiene como objetivo identificar y clasificar los diferentes grupos de información manejados por ITECSUR.

Grupos de Información:

- Información Académica de Estudiantes:
    - Descripción: Datos relacionados con el rendimiento académico de los estudiantes, incluyendo calificaciones, asistencias, registros de matrículas y participación en actividades académicas.
    - Ejemplos: Historial académico, actas de calificaciones, registros de asistencia, certificados de estudios, inscripciones a cursos o programas.
- Información Personal de Estudiantes:
    - Descripción: Datos personales de identificación y contacto recopilados de los estudiantes para su gestión académica, administrativa y de servicios institucionales.
    - Ejemplos: Nombres completos, números de cédula, direcciones, números de teléfono, correos electrónicos, fecha de nacimiento, información socioeconómica.
- Información Personal de Colaboradores:
    - Descripción: Datos personales y laborales de los trabajadores de la institución (docentes, personal administrativo, técnico y operativo) necesarios para la

gestión de la relación laboral o contractual.

- Ejemplos: Nombres completos, números de cédula, direcciones, correos electrónicos, teléfonos de contacto, currículum vitae, contratos laborales, historial laboral, evaluaciones de desempeño.

- Información Financiera:
  - Descripción: Datos relacionados con transacciones financieras, pagos de matrículas, nóminas y presupuestos institucionales.
  - Ejemplos: Registros de pagos, estados financieros, información bancaria.
- Información de Investigación:
  - Descripción: Datos generados a partir de proyectos de investigación llevados a cabo por la institución.
  - Ejemplos: Resultados de investigaciones, publicaciones científicas, datos experimentales.
- Información Administrativa:
  - Descripción: Documentación relacionada con la gestión y operación interna de la institución.
  - Ejemplos: Políticas institucionales, procedimientos administrativos, actas de reuniones.
- Información de Videovigilancia:
  - Descripción: Imágenes y grabaciones de video captadas por cámaras de seguridad en las instalaciones del Instituto para fines de protección y control de

accesos.

- Ejemplos: Grabaciones de aulas, pasillos, accesos principales, áreas comunes.

- Información de Bienestar Estudiantil:
  - Descripción: Datos relacionados con servicios de apoyo psicológico, asistencial o de salud dirigidos a estudiantes.
  - Ejemplos: Reportes de bienestar, atenciones de trabajo social, solicitudes de asistencia económica.
- Información Legal y Contractual:
  - Descripción: Documentación y datos relacionados con procesos legales, convenios interinstitucionales y documentación contractual relevante.
  - Ejemplos: Contratos de colaboración, convenios de prácticas profesionales, pólizas de seguros.

3.2.2. Sistemas de tratamiento y niveles de seguridad.

La información sobre sistemas de tratamiento y niveles de seguridad por grupo de información se detalla a continuación:

Tabla 3

Grupos de Información, Sistema de tratamiento, Tipo de Soporte y Nivel de seguiradad.

Grupo de Información	Sistema de tratamiento	Tipo de soporte	Nivel de seguridad
Información Académica de Estudiantes	Plataforma académica virtual, sistemas de calificaciones, registros físicos de notas.	Mixto (digital+ físico)	Alto

Información Personal de Estudiantes	Sistemas de gestión estudiantil (CRM académico), archivos físicos de matrícula.	Mixto (digital+ físico)	Alto
Información Personal de Colaboradores	Sistema de Recursos Humanos, archivos de contratos físicos.	Mixto (digital+ físico)	Alto
Información Financiera	Sistema de facturación y pagos institucional, respaldos bancarios físicos.	Mixto (digital+ físico)	Medio
Información de Investigación	Repositorios digitales, publicaciones, documentos de respaldo físico de proyectos	Digital	Medio
Información Administrativa	Sistemas administrativos digitales (document management system) y archivo físico institucional	Mixto (digital+ físico)	Medio
Información de Videovigilancia	Sistema de cámaras IP, servidores de almacenamiento de video	Digital	Bajo
Información de Bienestar Estudiantil	Sistema de gestión de servicios estudiantiles, documentos físicos de atención	Mixto (digital+ físico)	Alto
Información Legal y Contractual	Sistema de gestión documental legal, archivo físico de contratos	Mixto (digital+ físico)	Alto

Fuente**:** Instituto Tecnológico Superior Compu Sur

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

Los datos relacionales a las finalidades de tratamiento de datos personales se detallan a continuación.

Tabla 4

Finalidades, categorías de datos, de interesados y destinatarios

Grupo de Información	Finalidad del Tratamiento	Categorías de Datos	Categorías de Interesados	Destinatarios o terceros
Información Académica de Estudiantes	Gestión del historial académico, matrícula, asistencia, calificaciones	Datos académicos	Estudiantes	Autoridades educativas, plataformas académicas
Información Personal de Estudiantes	Identificación, comunicación institucional, gestión administrativa y matrícula	Datos identificativos y de contacto	Estudiantes	Área académica, administrativa y proveedores TI
Información Personal de Colaboradores	Administración de personal, gestión de contratos, contacto institucional	Datos identificativos, laborales y de contacto	Docentes, administrativos, operativos	Área de talento humano, plataformas de gestión laboral
Información Financiera	Facturación, pagos, control tributario, gestión contable	Datos financieros y bancarios	Estudiantes, personal	Área financiera, bancos, SRI
Información de Investigación	Desarrollo de proyectos de investigación, publicaciones, divulgación científica	Datos académicos, datos de investigación	Estudiantes, docentes, investigadores	Revistas científicas, plataformas de investigación
Información Administrativa	Gestión de procesos internos, actas,	Datos administrativos y de gestión	Personal administrativo	Entidades de control (cuando aplique)

	procedimientos administrativos			
Información de Videovigilancia	Seguridad física, control de accesos, monitoreo de instalaciones	Datos de imagen y video	Estudiantes, colaboradores, visitantes	Área de seguridad institucional, proveedores de CCTV
Información de Bienestar Estudiantil	Apoyo psicológico, asistencial o económico	Datos de salud, datos socioeconómicos	Estudiantes	Área de Bienestar Estudiantil, médicos
Información Legal y Contractual	Gestión de contratos, convenios interinstitucionales, cumplimiento legal laboral	Datos legales y contractuales	Personal, proveedores	Área legal, asesorías externas

Fuente: Instituto Tecnológico Superior Compu Sur

3.2.4. Encargados de los Tratamientos

Encargados del tratamiento:

Tabla 5

Registro de encargados de tratamiento

Prestador de Servicio	Tipo de Servicio	Localidad	Observaciones
Telconet	Empresa de soporte informático y mantenimiento de servidores	Ecuador	Acceso a información almacenada en servidores y bases de datos sobre datos de facturación
Grunseg	Mantenimiento de infraestructura física	Ecuador	Accede a información de dispositivos de acceso físico y dispositivos de videovigilancia
Moodle	Empresa de plataforma virtual de clases	Australia	Cuentan con acceso a la información académica de los estudiantes en la plataforma virtual de estudios

Prestador de Servicio	Tipo de Servicio	Localidad	Observaciones
EOS	Empresa de hosting	Ecuador	Cuentan con acceso a la información que los estudiantes e interesados registran a través de la página web de consultas.
Microsoft	Empresa de sistemas virtuales en la nube y mailing	Estados Unidos	Cuentan con acceso a la información compartida por estudiantes por correo electrónico y la información respaldada en Sharepoint y OneDrive.

Fuente: Instituto Tecnológico Superior Compu Sur

3.3. Registro de Dispositivos (Dispositivos digitales)

Los dispositivos tipo hardware dentro del instituto se configuran de manera similar considerando los siguientes tipos de dispositivos:

Tabla 6

Registro de dispositivos

Etiqueta	Activo de información	Cantidad	Tipo de activo de información	S.O. Marca	Clasificación	Responsable del activo
ITECSUR-HARD-01	Servidor de sistema de finanzas (ERP)	2	Hardware	Microsoft Server 2016	Alto	Coordinador de Logística, Infraestructura e Infoestructura
ITECSUR-HARD-02	Servidor de Active Directory	2	Hardware	Microsoft Server 2016	Alto	Coordinador de Logística, Infraestructura e Infoestructura

ITECSUR-HARD-03	Servidores de Backups institucionales	1	Hardware	Microsoft Server 2016	Alto	Coordinador de Logística, Infraestructura e Infoestructura
ITECSUR-HARD-04	Servidor de Control de Acceso Físico	1	Hardware	Ubuntu Server LTS	Alto	Administrador de Campus
ITECSUR-HARD-05	Cámaras de grabación	28	Hardware	Ubuntu Server LTS	Alto	Coordinador de Logística, Infraestructura e Infoestructura
ITECSUR-HARD-06	Cintas y dispositivos externos de almacenamiento de video	2	Hardware	No aplica	Alto	Coordinador de Logística, Infraestructura e Infoestructura
ITECSUR-HARD-07	Servidor de Base de Datos Académica	1	Hardware	Debian 12	Alto	Coordinador de Logística, Infraestructura e Infoestructura
ITECSUR-HARD-08	Servidor de sistema de videovigilancia	1	Hardware	Microsoft Server 2016	Alto	Coordinador de Logística, Infraestructura e Infoestructura
ITECSUR-PC-01	PCs Administrativa	6	Hardware	Windows 10	Medio	Secretaría Académica
ITECSUR-PC-02	PCs Financiera	2	Hardware	Windows 10	Medio	Coordinador de Unidad Financiera

ITECSUR-PORT-01	Portátil del Área Académica	2	Hardware	Windows 10	Medio	Director Académico
ITECSUR-PORT-02	Portátil de Docentes	24	Hardware	Windows 10	Medio	Coordinador de Vinculación
ITECSUR-MOV-01	Móvil Corporativo de Talento Humano	2	Hardware	Android 14	Medio	Coordinador de Talento Humano
ITECSUR-MOV-02	Móvil Corporativo de Área Financiera	2	Hardware	Android 14	Medio	Coordinador de Unidad Financiera
ITECSUR-MOV-03	Móvil Propio (BYOD) usado por docentes	34	Hardware	Android 14, Android 12, Android 11	Medio	Personal Autorizado (Política de BYOD)

Fuente: Instituto Tecnológico Superior Compu Sur

3.4. Registro de Sistemas de información (Software, seguridad, etc.).

El registro de los activos de información relacionados a los tratamientos de información es:

Tabla 7

Registro de sistemas de información

Etiqueta	Activo de información	Descripción	Clasificación	Medidas de control
ITECSUR-APP-01	Sistema Académico virtual	Servicio tipo SaaS Moodle (Licenciado)	Alto	Control de accesos basado en roles y privilegios mínimos; Respaldos cifrados y verificados periódicamente; Actualización y parchado del sistema y aplicaciones; Gestión de vulnerabilidades y escaneo periódico; Criptografía en almacenamiento y transmisión (AES-256, TLS 1.2+); Registro y monitoreo de eventos de

				seguridad; Evaluación contractual de SLA en seguridad y privacidad; Cifrado extremo a extremo de los datos; Ubicación del almacenamiento en región segura; Gestión de identidades y autenticación fuerte (MFA);
ITECSUR-APP-02	Sistema de Finanzas	Microsoft Server 2016 (Licenciado)	Alto	Control de accesos basado en roles y privilegios mínimos; Respaldos cifrados y verificados periódicamente; Actualización y parchado del sistema y aplicaciones; Gestión de vulnerabilidades y escaneo periódico; Segmentación de red y firewall de perímetro; Auditoría de accesos privilegiados; Cifrado de bases de datos financieras; Política de retención y eliminación segura de información
ITECSUR-APP-03	Página web institucional	Servicio tipo SaaS (Contratado)	Alto	Respaldos cifrados y verificados periódicamente; Actualización y parchado del sistema y aplicaciones; Gestión de vulnerabilidades y escaneo periódico; Criptografía en almacenamiento y transmisión (AES-256, TLS 1.2+); Registro y monitoreo de eventos de seguridad; Evaluación contractual de SLA en seguridad y privacidad; Cifrado extremo a extremo de los datos; Ubicación del almacenamiento en región segura;
ITECSUR-APP-04	Software ofimático	Licenciado	Alto	Actualización y parchado de aplicaciones
ITECSUR-APP-05	Plataforma de respaldos y almacenamiento de información	Servicio tipo SaaS Microsoft (Licenciado)	Medio	Control de accesos basado en roles y privilegios mínimos; Respaldos cifrados y verificados periódicamente; Actualización y parchado del sistema y aplicaciones; Gestión de vulnerabilidades y escaneo periódico; Criptografía en almacenamiento y transmisión (AES-256, TLS 1.2+); Registro y monitoreo de eventos de

				seguridad; Evaluación contractual de SLA en seguridad y privacidad; Cifrado extremo a extremo de los datos; Ubicación del almacenamiento en región segura; Gestión de identidades y autenticación fuerte (MFA);
ITECSUR-APP-06	Servicio de correo institucional	Servicio tipo SaaS Microsoft (Licenciado)	Medio	Control de accesos basado en roles y privilegios mínimos; Respaldos cifrados y verificados periódicamente; Actualización y parchado del sistema y aplicaciones; Gestión de vulnerabilidades y escaneo periódico; Criptografía en almacenamiento y transmisión (AES-256, TLS 1.2+); Registro y monitoreo de eventos de seguridad; Evaluación contractual de SLA en seguridad y privacidad; Cifrado extremo a extremo de los datos; Ubicación del almacenamiento en región segura; Gestión de identidades y autenticación fuerte (MFA);
ITECSUR-APP-07	Sistema Firewall	Sophos (Licenciado)	Alto	Control de accesos basado en roles y privilegios mínimos; Respaldos cifrados y verificados periódicamente; Actualización y parchado del sistema y aplicaciones; Gestión de vulnerabilidades y escaneo periódico; Criptografía en almacenamiento y transmisión (AES-256, TLS 1.2+); Registro y monitoreo de eventos de seguridad
ITECSUR-APP-08	Sistema IDS/IPS	Sophos (Licenciado)	Alto	Control de accesos basado en roles y privilegios mínimos; Respaldos cifrados y verificados periódicamente; Actualización y parchado del sistema y aplicaciones; Gestión de vulnerabilidades y escaneo periódico; Criptografía en almacenamiento y transmisión (AES-256, TLS 1.2+);

				Registro y monitoreo de eventos de seguridad
ITECSUR-APP-09	Licencias de antivirus de equipos PCs	Kaspersky Licenciado, pero instalación individual sin consola	Medio	Actualización y parchado de aplicaciones
ITECSUR-APP-10	Sistema de Gestión de Backups	Servicio tipo SaaS Veeam Backup (Licenciado)	Alto	Control de accesos basado en roles y privilegios mínimos; Respaldos cifrados y verificados periódicamente; Actualización y parchado del sistema y aplicaciones; Gestión de vulnerabilidades y escaneo periódico; Criptografía en almacenamiento y transmisión (AES-256, TLS 1.2+); Registro y monitoreo de eventos de seguridad
ITECSUR-APP-11	Sistema de Control de Acceso	Licenciado	Alto	Actualización y parchado de aplicaciones; Respaldos cifrados y verificados periódicamente;
ITECSUR-APP-12	Sistema de Grabación y Monitoreo de Cámaras	Licenciado	Alto	Actualización y parchado de aplicaciones; Respaldos cifrados y verificados periódicamente;
ITECSUR-APP-13	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Licenciado	Alto	Actualización y parchado de aplicaciones; Respaldos cifrados y verificados periódicamente;
ITECSUR-APP-14	Herramientas de teleconferencia (Zoom, meet)	Licenciado	Medio	Actualización y parchado de aplicaciones
ITECSUR-APP-15	VPN institucional	Licenciado son sistema Firewall	Alto	Actualización y parchado de aplicaciones

ITECSUR-APP-16	Active Directory	Microsoft Server 2016 (Licenciado)	Alto	Control de accesos basado en roles y privilegios mínimos; Respaldos cifrados y verificados periódicamente; Actualización y parchado del sistema y aplicaciones; Gestión de vulnerabilidades y escaneo periódico; Registro y monitoreo de eventos de seguridad

Fuente: Instituto Tecnológico Superior Compu Sur

3.5.Registro de personal.

3.5.1. Con acceso a Datos.

Tabla 8

Personal con Acceso a datos

Rol del Personal	Participación en el Tratamiento de Datos
Vicerrector Académico	Apoya la supervisión académica. Accede a información de alto nivel y coordina políticas sobre tratamiento de datos.
Director Académico	Accede y supervisa datos académicos de estudiantes y docentes. Responsable del cumplimiento académico y controles.
Coordinadores de Carreras	Acceden a datos académicos y personales de estudiantes. Aplican controles dentro de su carrera.
Director de Posgrados	Accede y gestiona datos de estudiantes y docentes de programas de posgrado. Participa en controles.
Coordinadores de Posgrados	Acceden a datos académicos y personales de estudiantes de posgrado. Manejan procesos administrativos.
Director de Investigación, Desarrollo y Vinculación con la Sociedad	Accede a datos de estudiantes, docentes y externos para gestión de proyectos. Responsable de manejo ético de la información.
Coordinador de Aseguramiento Interno de la Calidad	Accede a datos estadísticos y reportes de evaluación. Apoya en el análisis institucional con controles de confidencialidad.
Coordinador de Bibliotecas	Accede a registros de préstamos y datos de contacto de estudiantes. Aplica controles básicos.
Secretario General	Accede a información legal y administrativa de toda la comunidad. Responsable de integridad documental.
Coordinador de Bienestar Social Institucional	Accede a datos sensibles de estudiantes. Responsable de confidencialidad y tratamiento adecuado.
Director de Educación Continua	Accede a datos personales de estudiantes externos o egresados. Maneja procesos administrativos y promocionales.

Decanos	Supervisan el tratamiento de datos en sus respectivas facultades. Pueden acceder a datos y garantizar controles.
Director de Sede	Coordina las operaciones de una sede. Puede acceder a información general de estudiantes y personal.
Coordinador de Talento Humano	Accede a datos personales, contractuales y financieros del personal. Responsable del tratamiento seguro.
Coordinador de Unidad Financiera	Accede a datos financieros de estudiantes y empleados. Responsable del tratamiento y confidencialidad.
Coordinador de Comunicación e Imagen Institucional	Accede a imágenes y datos públicos para fines promocionales. Responsable del consentimiento.
Docentes	Acceden a datos académicos, personales de identificación, asistencia, evaluaciones y resultados académicos de los estudiantes. Responsables de garantizar la confidencialidad y el tratamiento seguro de la información educativa.

Fuente: Instituto Tecnológico Superior Compu Sur

3.5.2. Sin acceso a Datos

Tabla 9

Personal sin Acceso a datos

Rol del Personal	Participación en el Tratamiento de Datos
Coordinador General de Operaciones	No accede
Coordinador de Logística, Infraestructura e Infraestructura	No accede
Personal externo de limpieza y cafetería	No accede

Fuente: Instituto Tecnológico Superior Compu Sur

3.5.3. Accesos Físicos

Se detalla la siguiente información sobre el acceso a las ubicaciones físicas.

Tabla 10

Aspectos físicos

Cargo	Ubicación física a la que accede	Justificación del acceso
Rector	Oficinas administrativas superiores	Supervisión general de las operaciones institucionales.

Vicerrector Académico	Oficinas académicas, salas de reuniones	Gestión académica institucional y toma de decisiones.
Director Académico	Oficinas académicas, centro de coordinación docente	Supervisión del proceso educativo y coordinación con coordinadores de carrera.
Coordinadores de Carreras	Oficinas de coordinación de carrera	Gestión directa de los programas de estudios y atención a estudiantes.
Director de Posgrados	Oficina de posgrados	Gestión académica de programas de cuarto nivel.
Coordinadores de Posgrados	Oficina de posgrados	Ejecución y coordinación académica-administrativa de los programas de posgrado.
Director de Investigación, Desarrollo y Vinculación	Oficina de proyectos	Gestión de actividades de investigación y vinculación con la sociedad.
Coordinador de Aseguramiento Interno de la Calidad	Oficina de calidad institucional	Monitoreo de procesos académicos y administrativos.
Coordinador General de Operaciones	Instalaciones operativas, salas técnicas	Supervisión de infraestructura y soporte institucional.
Coordinador de Bibliotecas	Biblioteca institucional	Gestión de recursos bibliográficos y servicios de información.
Secretario General	Oficina administrativa	Gestión de documentos oficiales y archivos institucionales.
Coordinador de Bienestar Social Institucional	Oficinas de atención estudiantil	Atención a estudiantes en temas de salud, becas y asistencia.
Director de Educación Continua	Aulas y salas de capacitación	Gestión de programas externos y cursos abiertos.
Decanos	Oficinas de facultad	Supervisión académica de programas tecnológicos.
Director de Sede	Dirección general del campus	Gestión administrativa de la sede correspondiente.
Coordinador de Logística, Infraestructura e Infoestructura	Salas técnicas, data center, oficinas administrativas	Supervisión de dispositivos y sistemas de seguridad.
Coordinador de Talento Humano	Oficinas de RRHH	Gestión de expedientes laborales y administrativos del personal.
Coordinador de Unidad Financiera	Área financiera y tesorería	Gestión contable, presupuestaria y financiera.
Coordinador de Comunicación e Imagen Institucional	Área de diseño y medios institucionales	Gestión de campañas de comunicación y marketing.
Administrador de Campus	Instalaciones generales, áreas comunes	Supervisión de condiciones operativas y de infraestructura.

Fuente: Instituto Tecnológico Superior Compu Sur

3.6. Registro de prestadores de servicio.

Actualmente ITECSUR cuenta con profesionales que prestan servicios bajo requerimientos y contratos con alcances definidos para los procesos a continuación que detallan profesionales con acceso a Datos Catalogados y sin acceso a Datos Catalogados.

3.6.1. Prestadores de Servicio con Acceso a Datos Catalogados

Tabla 11

Prestadores de servicio con acceso a datos catalogados

Prestador de Servicio	Tipo de Servicio	Acceso a Datos Catalogados	Observaciones
Soporte de impresoras	Personal que se dirige a las instalaciones de ITECSUR para dar soporte a los equipos de impresión.	Si	Acceden a la información de los documentos que tienen problema de impresión, pero la información se almacena en la impresora de ITECSUR y el proveedor no cuenta con la obtención de datos del instituto.
Técnicos de soporte de PCs	Personal técnico que se dirige a las instalaciones de ITECSUR para dar mantenimiento a los equipos portátiles y de escritorio del instituto	Si	Acceden a la información de los equipos de los docentes y personal administrativo para el mantenimiento, pero la información queda almacenada en los equipos de ITECSUR.

Fuente: Instituto Tecnológico Superior Compu Sur

3.6.2. Prestadores de Servicio sin Acceso a Datos Catalogados

Tabla 12

Prestadores de servicio sin acceso a datos catalogados

Prestador de Servicio	Tipo de Servicio	Acceso a Datos Catalogados	Observaciones
Capacitadores y seminaristas	Personal externo que da charlas académicas de nuevos temas de experiencia	No	Son los encargas de dar capacitaciones en las instalaciones del instituto según se requiera
Guardias de seguridad	Personal que cuida las instalaciones por incidentes con visitantes.	No	Son los encargados del cuidado de las instalaciones.

Prestador de Servicio	Tipo de Servicio	Acceso a Datos Catalogados	Observaciones
Personal de limpieza	Personal contratado para la limpieza de las instalaciones académicas.	No	Son los encargados de la limpieza de las instalaciones.

Fuente: Instituto Tecnológico Superior Compu Sur

3.7.Sistemas de captación de imágenes y audio.

Tabla 13

Sistemas de captación de imágenes

Elemento	Cámaras de seguridad IP
Número de cámaras	28 cámaras de seguridad distribuidas en las áreas clave del edificio, cada aula, pasillos, oficinas, departamentos y parqueadero.
Zonas de influencia	- Entradas y salidas del edificio. - Pasillos principales en cada piso. - Biblioteca y áreas de estudio. - Parqueadero y accesos exteriores. - Escaleras.
Sistema de tratamiento y almacenamiento	- Grabación en servidores locales con almacenamiento de 30 días. - Sistema de respaldo en la nube con acceso restringido. - Monitoreo en tiempo real desde la planta baja supervisada por el guardia de seguridad del edificio.
Usuarios autorizados	- Personal de seguridad del instituto. - Administrador de Tics. - Dirección administrativa bajo solicitud específica.

Nota: No se maneja respaldos de audio solo de video conferencia.
Fuente: *Instituto Tecnológico Superior Compu Sur*

3.8.Dispositivos y medidas de seguridad

3.8.1. Análisis de las medidas de seguridad de los dispositivos

Como parte del análisis de las medidas de seguridad en dispositivos del instituto se analizan las herramientas de Firewall, IDS/IPS, Antivirus, Backups, Control de acceso físico, VPN, Plataforma Educativa:

Tabla 14

Dispositivos y medidas de seguridad

Activo de información	Control de seguridad	Análisis

Sistema Académico virtual	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Sistema Académico virtual	Respaldo de configuración	Cumple: Cuenta con respaldos por su modalidad SaaS.
Sistema Académico virtual	Monitoreo de actividad	Parcial: Se monitorea la infraestructura por el proveedor Saas, pero no se tiene monitoreo de los logs del aplicativo.
Sistema Académico virtual	Actualización de software	Cumple: Cuenta con actualizaciones por su modalidad SaaS.
Sistema Académico virtual	Reglas de contraseñas	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.
Sistema Académico virtual	Bloqueo automático de sesión	Cumple: La sesión en la plataforma se cierra tras 5 minutos de inactividad.
Sistema Académico virtual	Gestión de vulnerabilidades	Cumple: Cuenta con ejercicios de vulnerabilidades por su modalidad SaaS.
Sistema Académico virtual	Control de cambios	Cumple: Cuenta con control de cambios por su modalidad SaaS
Sistema Académico virtual	Doble factor de autenticación	Falla: No se cuenta con un doble factor de autenticación configurado.
Sistema de Finanzas	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Sistema de Finanzas	Respaldo de configuración	Parcial: Respaldos automáticos generados, pero sin ejecución de pruebas de integridad.
Sistema de Finanzas	Monitoreo de actividad	Parcial: Se monitorea la actividad de usuarios, pero no se revisa periódicamente.

Sistema de Finanzas	Gestión de vulnerabilidades	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.
Sistema de Finanzas	Actualización de software	Parcial: No se aplican parches de forma programada.
Sistema de Finanzas	Sincronización de hora NTP	Falla: No sincronizado con servidor NTP.
Sistema de Finanzas	Reglas de contraseñas	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.
Sistema de Finanzas	Bloqueo automático de sesión	Falla: No existe cierre de sesión tras inactividad.
Sistema de Finanzas	Control de cambios	Falla: No existe un procedimiento formal documentado.
Página web institucional	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening.
Página web institucional	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Página web institucional	Gestión de vulnerabilidades	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.
Página web institucional	Respaldo de configuración	Parcial: Respaldos automáticos generados, pero sin ejecución de pruebas de integridad.
Página web institucional	Monitoreo de actividad	Falla: No se monitorea cambios generados en la página web.
Página web institucional	Actualización de software	Parcial: No se aplican parches de forma programada para el servidor de página web del proveedor.
Página web institucional	Sincronización de hora NTP	Falla: No sincronizado con servidor NTP.
Página web institucional	Control de cambios	Falla: No existe un procedimiento formal documentado. Su proveedor genera los cambios por solicitudes por correo.

Software ofimático	Actualización de software	Parcial: No se aplican actualizaciones de manera manual en los equipos que ingresan a mantenimiento.
Plataforma de respaldos y almacenamiento de información	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening en el tenant.
Plataforma de respaldos y almacenamiento de información	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Plataforma de respaldos y almacenamiento de información	Respaldo de configuración	Cumple: Cuenta con respaldos por su modalidad SaaS.
Plataforma de respaldos y almacenamiento de información	Monitoreo de actividad	Cumple: Cuenta con un tenant con el monitoreo de la aplicación y usuarios por el modelo SaaS.
Plataforma de respaldos y almacenamiento de información	Actualización de software	Cumple: Cuenta con actualizaciones por su modalidad SaaS.
Plataforma de respaldos y almacenamiento de información	Reglas de contraseñas	Cumple: Cuenta con políticas de actualización y contraseñas robustas.
Plataforma de respaldos y almacenamiento de información	Bloqueo automático de sesión	Falla: No existe cierre de sesión tras inactividad.
Plataforma de respaldos y almacenamiento de información	Control de cambios	Cumple: Cuenta con control de cambios por su modalidad SaaS.
Plataforma de respaldos y almacenamiento de información	Doble factor de autenticación	Falla: No se cuenta con un doble factor de autenticación configurado.
Servicio de correo institucional	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening en el tenant.
Servicio de correo institucional	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.

Servicio de correo institucional	Respaldo de configuración	Cumple: Cuenta con respaldos por su modalidad SaaS.
Servicio de correo institucional	Monitoreo de actividad	Cumple: Cuenta con un tenant con el monitoreo de la aplicación y usuarios por el modelo SaaS.
Servicio de correo institucional	Actualización de software	Cumple: Cuenta con actualizaciones por su modalidad SaaS.
Servicio de correo institucional	Reglas de contraseñas	Cumple: Cuenta con políticas de actualización y contraseñas robustas.
Servicio de correo institucional	Bloqueo automático de sesión	Falla: No existe cierre de sesión tras inactividad.
Servicio de correo institucional	Control de cambios	Cumple: Cuenta con control de cambios por su modalidad SaaS.
Servicio de correo institucional	Fuga de información	Parcial: Se cuenta con reglas de DLP y SPAM por defecto.
Servicio de correo institucional	Doble factor de autenticación	Falla: No se cuenta con un doble factor de autenticación configurado.
Sistema Firewall	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening.
Sistema Firewall	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Sistema Firewall	Respaldo de configuración	Parcial: Se tiene un respaldo de la configuración anterior de Firewall, pero no es periódica.
Sistema Firewall	Monitoreo de actividad	Falla: No se cuenta con un monitoreo permanente de los logs del equipo Firewall.
Sistema Firewall	Actualización de software	Falla: No se han realizado actualizaciones del firmware del aplicativo.
Sistema Firewall	Sincronización de hora NTP	Falla: No sincronizado con servidor NTP.

Sistema Firewall	Reglas de contraseñas	Cumple: Cuenta con políticas de actualización y contraseñas robustas.
Sistema Firewall	Bloqueo automático de sesión	Cumple: Las sesiones remotas se bloquea tras 5 minutos de inactividad.
Sistema Firewall	Control de cambios	Falla: No existe un procedimiento formal documentado.
Sistema IDS/IPS	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening.
Sistema IDS/IPS	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Sistema IDS/IPS	Respaldo de configuración	Parcial: Se tiene un respaldo de la configuración anterior de Firewall, pero no es periódica.
Sistema IDS/IPS	Monitoreo de actividad	Falla: No se cuenta con un monitoreo permanente de los logs del equipo Firewall.
Sistema IDS/IPS	Actualización de software	Falla: No se han realizado actualizaciones del firmware del aplicativo.
Sistema IDS/IPS	Sincronización de hora NTP	Falla: No sincronizado con servidor NTP.
Sistema IDS/IPS	Reglas de contraseñas	Cumple: Cuenta con políticas de actualización y contraseñas robustas.
Sistema IDS/IPS	Bloqueo automático de sesión	Cumple: Las sesiones remotas se bloquea tras 5 minutos de inactividad.
Licencias de antivirus de equipos PCs	Configuración segura (Hardening)	Falla: Modulo de protección no configurable de forma masiva o políticas.
Licencias de antivirus de equipos PCs	Gestión de privilegios de acceso	Parcial: Acceso restringido a personal autorizado por contraseña del software.

Licencias de antivirus de equipos PCs	Respaldo de configuración	Falla: No se respalda la configuración al ser por equipo.
Licencias de antivirus de equipos PCs	Monitoreo de actividad	Falla: No se cuenta con una consola centralizada para obtener los logs de alertas.
Licencias de antivirus de equipos PCs	Actualización de software	Falla: La actualización es manual equipo por equipo.
Licencias de antivirus de equipos PCs	Sincronización de hora NTP	Falla: No sincronizado con servidor NTP.
Licencias de antivirus de equipos PCs	Reglas de contraseñas	Falla: La contraseña de instalación de antivirus no se ha actualizado.
Licencias de antivirus de equipos PCs	Control de cambios	Falla: No existe un procedimiento formal documentado.
Sistema de Gestión de Backups	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening.
Sistema de Gestión de Backups	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Sistema de Gestión de Backups	Monitoreo de actividad	Cumple: Cuenta con un tenant con el monitoreo de la aplicación y usuarios por el modelo SaaS.
Sistema de Gestión de Backups	Actualización de software	Cumple: Cuenta con actualizaciones por su modalidad SaaS.
Sistema de Gestión de Backups	Reglas de contraseñas	Cumple: Cuenta con políticas de actualización y contraseñas robustas.
Sistema de Gestión de Backups	Bloqueo automático de sesión	Falla: No existe cierre de sesión tras inactividad.
Sistema de Gestión de Backups	Control de cambios	Cumple: Cuenta con control de cambios por su modalidad SaaS.
Sistema de Control de Acceso	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening.
Sistema de Control de Acceso	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.

Sistema de Control de Acceso	Respaldo de configuración	Parcial: Respaldos automáticos generados, pero sin ejecución de pruebas de integridad.
Sistema de Control de Acceso	Monitoreo de actividad	Parcial: Se monitorea la actividad de usuarios, pero no se revisa periódicamente.
Sistema de Control de Acceso	Gestión de vulnerabilidades	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.
Sistema de Control de Acceso	Actualización de software	Falla: No se han realizado actualizaciones del sistema.
Sistema de Control de Acceso	Sincronización de hora NTP	Falla: No sincronizado con servidor NTP.
Sistema de Control de Acceso	Reglas de contraseñas	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.
Sistema de Control de Acceso	Bloqueo automático de sesión	Falla: No existe cierre de sesión tras inactividad.
Sistema de Control de Acceso	Control de cambios	Falla: No existe un procedimiento formal documentado.
Sistema de Grabación y Monitoreo de Cámaras	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening.
Sistema de Grabación y Monitoreo de Cámaras	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Sistema de Grabación y Monitoreo de Cámaras	Respaldo de configuración	Parcial: Respaldos automáticos generados, pero sin ejecución de pruebas de integridad.
Sistema de Grabación y Monitoreo de Cámaras	Monitoreo de actividad	Parcial: Se monitorea la actividad de usuarios, pero no se revisa periódicamente.
Sistema de Grabación y Monitoreo de Cámaras	Gestión de vulnerabilidades	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.
Sistema de Grabación y Monitoreo de Cámaras	Actualización de software	Falla: No se han realizado actualizaciones del sistema.

Sistema de Grabación y Monitoreo de Cámaras	Sincronización de hora NTP	Falla: No sincronizado con servidor NTP.
Sistema de Grabación y Monitoreo de Cámaras	Reglas de contraseñas	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.
Sistema de Grabación y Monitoreo de Cámaras	Bloqueo automático de sesión	Falla: No existe cierre de sesión tras inactividad.
Sistema de Grabación y Monitoreo de Cámaras	Control de cambios	Falla: No existe un procedimiento formal documentado.
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening.
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Respaldo de configuración	Parcial: Respaldos automáticos generados, pero sin ejecución de pruebas de integridad.
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Monitoreo de actividad	Parcial: Se monitorea la actividad de usuarios, pero no se revisa periódicamente.
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Gestión de vulnerabilidades	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Actualización de software	Falla: No se han realizado actualizaciones del sistema.
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Sincronización de hora NTP	Falla: No sincronizado con servidor NTP.
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Reglas de contraseñas	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.

Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Bloqueo automático de sesión	Falla: No existe cierre de sesión tras inactividad.
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Control de cambios	Falla: No existe un procedimiento formal documentado.
Herramientas de teleconferencia (Zoom, meet)	Gestión de privilegios de acceso	Parcial: Acceso restringido a personal autorizado por contraseña del software.
Herramientas de teleconferencia (Zoom, meet)	Respaldo de configuración	Falla: No se respalda la configuración al ser por equipo.
Herramientas de teleconferencia (Zoom, meet)	Monitoreo de actividad	Falla: No se cuenta con una consola centralizada para obtener los logs de alertas.
Herramientas de teleconferencia (Zoom, meet)	Actualización de software	Falla: La actualización es manual equipo por equipo.
VPN institucional	Gestión de privilegios de acceso	Parcial: Acceso restringido a personal autorizado por contraseña del software.
VPN institucional	Monitoreo de actividad	Cumple: Se generan los logs de actividad en el equipo Firewall.
VPN institucional	Actualización de software	Falla: La actualización es manual equipo por equipo.
VPN institucional	Reglas de contraseñas	Parcial: Política existe, pero no aplica históricos ni complejidad.
VPN institucional	Bloqueo automático de sesión	Cumple: Se bloquea tras 5 minutos de inactividad.
Active Directory	Configuración segura (Hardening)	Falla: No se ha aplicado política institucional de hardening.
Active Directory	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.

Active Directory	Respaldo de configuración	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.
Active Directory	Monitoreo de actividad	Parcial: Se monitorea, pero no se revisa periódicamente.
Active Directory	Actualización de software	Parcial: No se aplican parches de forma programada.
Active Directory	Sincronización de hora NTP	Falla: No sincronizado con servidor NTP.
Active Directory	Reglas de contraseñas	Parcial: Política existe, pero no aplica históricos ni complejidad.
Active Directory	Bloqueo automático de sesión	Cumple: Se bloquea tras 5 minutos de inactividad.
Active Directory	Control de cambios	Falla: No existe un procedimiento formal documentado.
Servidor de sistema de finanzas (ERP)	Respaldos de configuración	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.
Servidor de sistema de finanzas (ERP)	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Servidor de sistema de finanzas (ERP)	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Servidor de sistema de finanzas (ERP)	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
Servidor de sistema de finanzas (ERP)	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
Servidor de sistema de finanzas (ERP)	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.
Servidor de sistema de finanzas (ERP)	Instalación de software	Cumple: Se realiza un control de instalación para el personal autorizado/administrador.

Servidor de sistema de finanzas (ERP)	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.
Servidor de sistema de finanzas (ERP)	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.
Servidor de sistema de finanzas (ERP)	Bloqueo automático de sesión	Cumple: Bloqueo del equipo tras 5 minutos de inactividad.
Servidor de sistema de finanzas (ERP)	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
Servidor de sistema de finanzas (ERP)	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Servidor de sistema de finanzas (ERP)	Protección contra software malicioso	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.
Servidor de Active Directory	Respaldos de configuración	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.
Servidor de Active Directory	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Servidor de Active Directory	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Servidor de Active Directory	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
Servidor de Active Directory	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
Servidor de Active Directory	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.

Servidor de Active Directory	Instalación de software	Cumple: Se realiza un control de instalación para el personal autorizado/administrador.
Servidor de Active Directory	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.
Servidor de Active Directory	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.
Servidor de Active Directory	Bloqueo automático de sesión	Cumple: Bloqueo del equipo tras 5 minutos de inactividad.
Servidor de Active Directory	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
Servidor de Active Directory	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Servidor de Active Directory	Protección contra software malicioso	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.
Servidores de Backups institucionales	Respaldos de configuración	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.
Servidores de Backups institucionales	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Servidores de Backups institucionales	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Servidores de Backups institucionales	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
Servidores de Backups institucionales	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.

Servidores de Backups institucionales	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.
Servidores de Backups institucionales	Instalación de software	Cumple: Se realiza un control de instalación para el personal autorizado/administrador.
Servidores de Backups institucionales	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.
Servidores de Backups institucionales	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.
Servidores de Backups institucionales	Bloqueo automático de sesión	Cumple: Bloqueo del equipo tras 5 minutos de inactividad.
Servidores de Backups institucionales	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
Servidores de Backups institucionales	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Servidores de Backups institucionales	Protección contra software malicioso	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.
Servidor de Control de Acceso Físico	Respaldos de configuración	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.
Servidor de Control de Acceso Físico	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Servidor de Control de Acceso Físico	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Servidor de Control de Acceso Físico	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.

Servidor de Control de Acceso Físico	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
Servidor de Control de Acceso Físico	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.
Servidor de Control de Acceso Físico	Instalación de software	Cumple: Se realiza un control de instalación para el personal autorizado/administrador.
Servidor de Control de Acceso Físico	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.
Servidor de Control de Acceso Físico	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.
Servidor de Control de Acceso Físico	Bloqueo automático de sesión	Cumple: Bloqueo del equipo tras 5 minutos de inactividad.
Servidor de Control de Acceso Físico	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
Servidor de Control de Acceso Físico	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Servidor de Control de Acceso Físico	Protección contra software malicioso	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.
Cámaras de grabación	Gestión de privilegios de acceso	Cumple: Se cuenta con control de acceso para personal autorizado.
Cámaras de grabación	Gestión de vulnerabilidades	Falla: No se han realizado pruebas de vulnerabilidades del firmware de los equipos.
Cámaras de grabación	Actualización de software	Falla: No se han realizado actualizaciones de firmware.

Cintas y dispositivos externos de almacenamiento de video	Cifrado de información	Falla: Los equipos no cuentan con cifrado de almacenamiento de información o protección por contraseña.
Servidor de Base de Datos Académica	Respaldos de configuración	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.
Servidor de Base de Datos Académica	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Servidor de Base de Datos Académica	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Servidor de Base de Datos Académica	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
Servidor de Base de Datos Académica	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
Servidor de Base de Datos Académica	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.
Servidor de Base de Datos Académica	Instalación de software	Cumple: Se realiza un control de instalación para el personal autorizado/administrador.
Servidor de Base de Datos Académica	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.
Servidor de Base de Datos Académica	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.
Servidor de Base de Datos Académica	Bloqueo automático de sesión	Cumple: Bloqueo del equipo tras 5 minutos de inactividad.
Servidor de Base de Datos Académica	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.

Servidor de Base de Datos Académica	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Servidor de Base de Datos Académica	Protección contra software malicioso	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.
Servidor de sistema de videovigilancia	Respaldos de configuración	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.
Servidor de sistema de videovigilancia	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Servidor de sistema de videovigilancia	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Servidor de sistema de videovigilancia	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
Servidor de sistema de videovigilancia	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
Servidor de sistema de videovigilancia	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.
Servidor de sistema de videovigilancia	Instalación de software	Cumple: Se realiza un control de instalación para el personal autorizado/administrador.
Servidor de sistema de videovigilancia	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.
Servidor de sistema de videovigilancia	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.
Servidor de sistema de videovigilancia	Bloqueo automático de sesión	Cumple: Bloqueo del equipo tras 5 minutos de inactividad.

Servidor de sistema de videovigilancia	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
Servidor de sistema de videovigilancia	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Servidor de sistema de videovigilancia	Servidor de Base de Datos Académica	Servidor de Base de Datos Académica
PCs Administrativa	Respaldos de configuración	Parcial: No se cuenta con procedimiento de respaldos del equipo, pero se respaldan carpetas del equipo.
PCs Administrativa	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
PCs Administrativa	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
PCs Administrativa	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
PCs Administrativa	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
PCs Administrativa	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.
PCs Administrativa	Instalación de software	Cumple: Se realiza un control de instalación para el personal autorizado/administrador.
PCs Administrativa	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.
PCs Administrativa	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.
PCs Administrativa	Bloqueo automático de sesión	Falla: No se bloquea el dispositivo por inactividad.

PCs Administrativa	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
PCs Administrativa	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
PCs Administrativa	Protección contra software malicioso	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.
PCs Financiera	Respaldos de configuración	Parcial: No se cuenta con procedimiento de respaldos del equipo, pero se respaldan carpetas del equipo.
PCs Financiera	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
PCs Financiera	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
PCs Financiera	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
PCs Financiera	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
PCs Financiera	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.
PCs Financiera	Instalación de software	Cumple: Se realiza un control de instalación para el personal autorizado/administrador.
PCs Financiera	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.
PCs Financiera	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.

PCs Financiera	Bloqueo automático de sesión	Falla: No se bloquea el dispositivo por inactividad.
PCs Financiera	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
PCs Financiera	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
PCs Financiera	Protección contra software malicioso	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.
Portátil del Área Académica	Respaldos de configuración	Parcial: No se cuenta con procedimiento de respaldos del equipo, pero se respaldan carpetas del equipo.
Portátil del Área Académica	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Portátil del Área Académica	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Portátil del Área Académica	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
Portátil del Área Académica	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
Portátil del Área Académica	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.
Portátil del Área Académica	Instalación de software	Cumple: Se realiza un control de instalación para el personal autorizado/administrador.
Portátil del Área Académica	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.

Portátil del Área Académica	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.
Portátil del Área Académica	Bloqueo automático de sesión	Falla: No se bloquea el dispositivo por inactividad.
Portátil del Área Académica	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
Portátil del Área Académica	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Portátil del Área Académica	Protección contra software malicioso	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.
Portátil de Docentes	Respaldos de configuración	Parcial: No se cuenta con procedimiento de respaldos del equipo, pero se respaldan carpetas del equipo.
Portátil de Docentes	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Portátil de Docentes	Gestión de privilegios de acceso	Cumple: Acceso restringido a personal autorizado.
Portátil de Docentes	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
Portátil de Docentes	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
Portátil de Docentes	Actualización de software	Parcial: Se realizan actualizaciones de manera manual.
Portátil de Docentes	Instalación de software	Falla: Los docentes tienen privilegios para instalar programas sin control previo.

Portátil de Docentes	Sincronización de hora NTP	Falla: No se sincroniza con el servidor NTP.
Portátil de Docentes	Regla de contraseñas	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.
Portátil de Docentes	Bloqueo automático de sesión	Falla: No se bloquea el dispositivo por inactividad.
Portátil de Docentes	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
Portátil de Docentes	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Portátil de Docentes	Protección contra software malicioso	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.
Móvil Corporativo de Talento Humano	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Móvil Corporativo de Talento Humano	Gestión de privilegios de acceso	Falla: No se cuentan con mecanismos MDM para el control de accesos.
Móvil Corporativo de Talento Humano	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
Móvil Corporativo de Talento Humano	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
Móvil Corporativo de Talento Humano	Actualización de software	Falla: No se cuenta con un procedimiento de actualización de estos dispositivos.
Móvil Corporativo de Talento Humano	Instalación de software	Falla: No se cuenta con control de instalación de aplicaciones.

Móvil Corporativo de Talento Humano	Regla de contraseñas	Falla: No se cuentan con mecanismos MDM para el control de accesos.
Móvil Corporativo de Talento Humano	Bloqueo automático de sesión	Falla: No se cuenta con control de bloqueo de dispositivo.
Móvil Corporativo de Talento Humano	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
Móvil Corporativo de Talento Humano	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Móvil Corporativo de Talento Humano	Protección contra software malicioso	Falla: No se cuenta con un software de protección de software malicioso.
Móvil Corporativo de Área Financiera	Configuración segura	Falla: No se ha aplicado política institucional de hardening.
Móvil Corporativo de Área Financiera	Gestión de privilegios de acceso	Falla: No se cuentan con mecanismos MDM para el control de accesos.
Móvil Corporativo de Área Financiera	Gestión de vulnerabilidades	Falla: No se cuenta con una revisión periódica de vulnerabilidades.
Móvil Corporativo de Área Financiera	Monitoreo de actividad	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.
Móvil Corporativo de Área Financiera	Actualización de software	Falla: No se cuenta con un procedimiento de actualización de estos dispositivos.
Móvil Corporativo de Área Financiera	Instalación de software	Falla: No se cuenta con control de instalación de aplicaciones.
Móvil Corporativo de Área Financiera	Regla de contraseñas	Falla: No se cuentan con mecanismos MDM para el control de accesos.
Móvil Corporativo de Área Financiera	Bloqueo automático de sesión	Falla: No se cuenta con control de bloqueo de dispositivo.

Móvil Corporativo de Área Financiera	Control de cambios	Falla: No se cuenta con un procedimiento de control de cambios documentado.
Móvil Corporativo de Área Financiera	Fuga de información	Falla: No se cuenta con un software para el control de fuga de información o DLP.
Móvil Corporativo de Área Financiera	Protección contra software malicioso	Falla: No se cuenta con un software de protección de software malicioso.
Móvil Propio (BYOD) usado por docentes	Configuración segura	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Gestión de privilegios de acceso	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Gestión de vulnerabilidades	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Monitoreo de actividad	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Actualización de software	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Instalación de software	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Regla de contraseñas	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Bloqueo automático de sesión	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Control de cambios	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Fuga de información	Falla: No se cuenta con controles o políticas de dispositivos BYOD.
Móvil Propio (BYOD) usado por docentes	Protección contra software malicioso	Falla: No se cuenta con controles o políticas de dispositivos BYOD.

Fuente: Instituto Tecnológico Superior Compu Sur

3.8.2. Propuesta de mejora de las medidas de seguridad

En relación con las oportunidades de mejora identificados en los dispositivos de seguridad antes mencionados, tenemos:

Tabla 15

Propuesta de mejora

Activo de información	Análisis	Plan de acción	Prioridad de remediación
Sistema Académico virtual	Parcial: Se monitorea la infraestructura por el proveedor Saas, pero no se tiene monitoreo de los logs del aplicativo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Sistema Académico virtual	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En	Alta

		caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
Sistema Académico virtual	Falla: No se cuenta con un doble factor de autenticación configurado.	Implementar un doble factor de autenticación para el acceso al sistema SaaS.	Media
Sistema de Finanzas	Parcial: Respaldos automáticos generados, pero sin ejecución de pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Sistema de Finanzas	Parcial: Se monitorea la actividad de usuarios, pero no se revisa periódicamente.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Sistema de Finanzas	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema de Finanzas	Parcial: No se aplican parches de forma programada.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema de Finanzas	Falla: No sincronizado con servidor NTP.	Establecer un control de sincronización con el	Media

		servidor NTP para los dispositivos.	
Sistema de Finanzas	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	Alta
Sistema de Finanzas	Falla: No existe cierre de sesión tras inactividad.	Configurar políticas de tiempo de inactividad y	Media

		bloqueo automático en los dispositivos.	
Sistema de Finanzas	Falla: No existe un procedimiento formal documentado de control de cambios.	Establecer un procedimiento documental para el control de cambios con ambientes de pruebas y producción.	Media
Página web institucional	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Página web institucional	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Página web institucional	Parcial: Respaldos automáticos generados, pero sin ejecución de pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Página web institucional	Falla: No se monitorea cambios generados en la página web.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Página web institucional	Parcial: No se aplican parches de forma programada para el servidor de página web del proveedor.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Página web institucional	Falla: No sincronizado con servidor NTP.	Establecer un control de sincronización con el servidor NTP para los dispositivos.	Media

Página web institucional	Falla: No existe un procedimiento formal documentado. Su proveedor genera los cambios por solicitudes por correo.	Establecer un procedimiento documental para el control de cambios con ambientes de pruebas y producción. Se debe considerar los roles del proveedor en el proceso.	Media
Software ofimático	Parcial: No se aplican actualizaciones de manera manual en los equipos que ingresan a mantenimiento.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Plataforma de respaldos y almacenamiento de información	Falla: No se ha aplicado política institucional de hardening en el tenant.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Plataforma de respaldos y almacenamiento de información	Falla: No existe cierre de sesión tras inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media
Plataforma de respaldos y almacenamiento de información	Falla: No se cuenta con un doble factor de autenticación configurado.	Implementar un doble factor de autenticación para el acceso al sistema SaaS.	Media
Servicio de correo institucional	Falla: No se ha aplicado política institucional de hardening en el tenant.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Servicio de correo institucional	Falla: No existe cierre de sesión tras inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media

Servicio de correo institucional	Parcial: Se cuenta con reglas de DLP y SPAM por defecto.	Robustecer el sistema SaaS con la configuración de reglas DLP y los registros públicos de correo como: DKIM, DMARK y SPF.	Alta
Servicio de correo institucional	Falla: No se cuenta con un doble factor de autenticación configurado.	Implementar un doble factor de autenticación para el acceso al sistema SaaS.	Media
Sistema Firewall	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Sistema Firewall	Parcial: Se tiene un respaldo de la configuración anterior de Firewall, pero no es periódica.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Sistema Firewall	Falla: No se cuenta con un monitoreo permanente de los logs del equipo Firewall.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Sistema Firewall	Falla: No se han realizado actualizaciones del firmware del aplicativo.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema Firewall	Falla: No sincronizado con servidor NTP.	Establecer un control de sincronización con el servidor NTP para los dispositivos.	Media
Sistema Firewall	Falla: No existe un procedimiento formal documentado de	Establecer un procedimiento documental para el control de cambios con	Media

	control de cambios.	ambientes de pruebas y producción.	
Sistema IDS/IPS	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Sistema IDS/IPS	Parcial: Se tiene un respaldo de la configuración anterior de Firewall, pero no es periódica.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Sistema IDS/IPS	Falla: No se cuenta con un monitoreo permanente de los logs del equipo Firewall.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Sistema IDS/IPS	Falla: No se han realizado actualizaciones del firmware del aplicativo.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema IDS/IPS	Falla: No sincronizado con servidor NTP.	Establecer un control de sincronización con el servidor NTP para los dispositivos.	Media
Licencias de antivirus de equipos PCs	Falla: Modulo de protección no configurable de forma masiva o políticas.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Licencias de antivirus de equipos PCs	Parcial: Acceso restringido a personal autorizado por contraseña del software.	Implementar una consola de antivirus centralizada para la gestión de activación, actualización y protección de software antimalware.	Alta
Licencias de antivirus de equipos PCs	Falla: No se respalda la	Configurar respaldos automáticos y	Media

	configuración al ser por equipo.	verificación periódica de su integridad.	
Licencias de antivirus de equipos PCs	Falla: No se cuenta con una consola centralizada para obtener los logs de alertas.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Licencias de antivirus de equipos PCs	Falla: La actualización es manual equipo por equipo.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Licencias de antivirus de equipos PCs	Falla: No sincronizado con servidor NTP.	Establecer un control de sincronización con el servidor NTP para los dispositivos.	Media
Licencias de antivirus de equipos PCs	Falla: La contraseña de instalación de antivirus no se ha actualizado.	Implementar una consola de antivirus centralizada para la gestión de activación, actualización y protección de software antimalware.	Alta
Licencias de antivirus de equipos PCs	Falla: No existe un procedimiento formal documentado de control de cambios.	Establecer un procedimiento documental para el control de cambios con ambientes de pruebas y producción.	Media
Sistema de Gestión de Backups	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Sistema de Gestión de Backups	Falla: No existe cierre de sesión tras inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media
Sistema de Control de Acceso	Falla: No se ha aplicado política	Aplicar políticas de configuración segura y auditoría de cambios.	Media

	institucional de hardening.		
Sistema de Control de Acceso	Parcial: Respaldos automáticos generados, pero sin ejecución de pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Sistema de Control de Acceso	Parcial: Se monitorea la actividad de usuarios, pero no se revisa periódicamente.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Sistema de Control de Acceso	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema de Control de Acceso	Falla: No se han realizado actualizaciones del sistema.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema de Control de Acceso	Falla: No sincronizado con servidor NTP.	Establecer un control de sincronización con el servidor NTP para los dispositivos.	Media
Sistema de Control de Acceso	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales.	Alta

		Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
Sistema de Control de Acceso	Falla: No existe cierre de sesión tras inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media
Sistema de Control de Acceso	Falla: No existe un procedimiento formal documentado de control de cambios.	Establecer un procedimiento documental para el control de cambios con ambientes de pruebas y producción.	Media
Sistema de Grabación y Monitoreo de Cámaras	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Sistema de Grabación y Monitoreo de Cámaras	Parcial: Respaldos automáticos generados, pero	Configurar respaldos automáticos y verificación periódica de su integridad.	Media

	sin ejecución de pruebas de integridad.		
Sistema de Grabación y Monitoreo de Cámaras	Parcial: Se monitorea la actividad de usuarios, pero no se revisa periódicamente.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Sistema de Grabación y Monitoreo de Cámaras	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema de Grabación y Monitoreo de Cámaras	Falla: No se han realizado actualizaciones del sistema.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema de Grabación y Monitoreo de Cámaras	Falla: No sincronizado con servidor NTP.	Establecer un control de sincronización con el servidor NTP para los dispositivos.	Media
Sistema de Grabación y Monitoreo de Cámaras	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en	Alta

		diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
Sistema de Grabación y Monitoreo de Cámaras	Falla: No existe cierre de sesión tras inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media
Sistema de Grabación y Monitoreo de Cámaras	Falla: No existe un procedimiento formal documentado de control de cambios.	Establecer un procedimiento documental para el control de cambios con ambientes de pruebas y producción.	Media
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Parcial: Respaldos automáticos generados, pero sin ejecución de pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Sistema de Gestión Académica y	Parcial: Se monitorea la actividad de	Establecer herramientas de monitoreo continuo	Alta

Plataforma Educativa (BECAS TEC)	usuarios, pero no se revisa periódicamente.	y análisis de logs para detectar anomalías.	
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Falla: No se han realizado ejercicios de gestión de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Falla: No se han realizado actualizaciones del sistema.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Falla: No sincronizado con servidor NTP.	Establecer un control de sincronización con el servidor NTP para los dispositivos.	Media
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Parcial: Existe política de complejidad, pero no de caducidad o cambio periódico.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas	Alta

		cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Falla: No existe cierre de sesión tras inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media
Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Falla: No existe un procedimiento formal documentado de control de cambios.	Establecer un procedimiento documental para el control de cambios con ambientes de pruebas y producción.	Media
Herramientas de teleconferencia (Zoom, meet)	Parcial: Acceso restringido a personal autorizado por contraseña del software.	Revisar políticas de acceso, aplicar controles de autenticación y fortalecer la seguridad de credenciales.	Alta
Herramientas de teleconferencia (Zoom, meet)	Falla: No se respalda la configuración al ser por equipo.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Herramientas de teleconferencia (Zoom, meet)	Falla: No se cuenta con una consola centralizada para obtener los logs de alertas.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Herramientas de teleconferencia (Zoom, meet)	Falla: La actualización es manual equipo por equipo.	Implementar un proceso regular de actualización y parches de seguridad	Alta

		para reducir vulnerabilidades.	
VPN institucional	Parcial: Acceso restringido a personal autorizado por contraseña del software.	Establecer un acceso a VPN por credenciales de Active Directory.	Alta
VPN institucional	Falla: La actualización es manual equipo por equipo.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
VPN institucional	Parcial: Política existe, pero no aplica históricos ni complejidad.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación	Alta

		en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
Active Directory	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Active Directory	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Active Directory	Parcial: Se monitorea, pero no se revisa periódicamente.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Active Directory	Parcial: No se aplican parches de forma programada.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Active Directory	Falla: No sincronizado con servidor NTP.	Establecer un control de sincronización con el servidor NTP para los dispositivos.	Media

Active Directory	Parcial: Política existe, pero no aplica históricos ni complejidad.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	Alta
Active Directory	Falla: No existe un procedimiento formal documentado de	Establecer un procedimiento documental para el control de cambios con	Media

	control de cambios.	ambientes de pruebas y producción.	
Servidor de sistema de finanzas (ERP)	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Servidor de sistema de finanzas (ERP)	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Servidor de sistema de finanzas (ERP)	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de sistema de finanzas (ERP)	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Servidor de sistema de finanzas (ERP)	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de sistema de finanzas (ERP)	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para sincronización de los equipos.	Media

Servidor de sistema de finanzas (ERP)	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	Alta
Servidor de sistema de finanzas (ERP)	Falla: No se cuenta con un procedimiento de control de	Establecer un procedimiento de control de cambios documentado para la gestión de servidores en	Media

	cambios documentado.	ambiente de pruebas y luego el paso a producción.	
Servidor de sistema de finanzas (ERP)	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
Servidor de sistema de finanzas (ERP)	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de Active Directory	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Servidor de Active Directory	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Servidor de Active Directory	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de Active Directory	Falla: No se cuenta con una aplicación de monitoreo	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta

	continuo de los logs del equipo.		
Servidor de Active Directory	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de Active Directory	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para sincronización de los equipos.	Media
Servidor de Active Directory	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15	Alta

		minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
Servidor de Active Directory	Falla: No se cuenta con un procedimiento de control de cambios documentado.	Establecer un procedimiento de control de cambios documentado para la gestión de servidores en ambiente de pruebas y luego el paso a producción.	Media
Servidor de Active Directory	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
Servidor de Active Directory	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidores de Backups institucionales	Parcial: Respaldos manuales, pero no se validan las	Configurar respaldos automáticos y verificación periódica de su integridad.	Media

	pruebas de integridad.		
Servidores de Backups institucionales	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Servidores de Backups institucionales	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidores de Backups institucionales	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Servidores de Backups institucionales	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidores de Backups institucionales	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para sincronización de los equipos.	Media
Servidores de Backups institucionales	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de	Alta

		contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
Servidores de Backups institucionales	Falla: No se cuenta con un procedimiento de control de cambios documentado.	Establecer un procedimiento de control de cambios documentado para la gestión de servidores en ambiente de pruebas y luego el paso a producción.	Media
Servidores de Backups institucionales	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
Servidores de Backups institucionales	Parcial: Se cuenta con la licencia de antivirus instalada, pero	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta

	no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.		
Servidor de Control de Acceso Físico	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Servidor de Control de Acceso Físico	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Servidor de Control de Acceso Físico	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de Control de Acceso Físico	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Servidor de Control de Acceso Físico	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de Control de Acceso Físico	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para sincronización de los equipos.	Media

Servidor de Control de Acceso Físico	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	Alta
Servidor de Control de Acceso Físico	Falla: No se cuenta con un procedimiento de control de	Establecer un procedimiento de control de cambios documentado para la gestión de servidores en	Media

	cambios documentado.	ambiente de pruebas y luego el paso a producción.	
Servidor de Control de Acceso Físico	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
Servidor de Control de Acceso Físico	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Cámaras de grabación	Falla: No se han realizado pruebas de vulnerabilidades del firmware de los equipos.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Cámaras de grabación	Falla: No se han realizado actualizaciones de firmware.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Cintas y dispositivos externos de almacenamiento de video	Falla: Los equipos no cuentan con cifrado de almacenamiento de información o protección por contraseña.	Implementación de almacenamiento de información cifrada en los dispositivos	Media

Servidor de Base de Datos Académica	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Servidor de Base de Datos Académica	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Servidor de Base de Datos Académica	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de Base de Datos Académica	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Servidor de Base de Datos Académica	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de Base de Datos Académica	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para sincronización de los equipos.	Media
Servidor de Base de Datos Académica	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras	Alta

		minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
Servidor de Base de Datos Académica	Falla: No se cuenta con un procedimiento de control de cambios documentado.	Establecer un procedimiento de control de cambios documentado para la gestión de servidores en ambiente de pruebas y luego el paso a producción.	Media
Servidor de Base de Datos Académica	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta

Servidor de Base de Datos Académica	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de sistema de videovigilancia	Parcial: Respaldos manuales, pero no se validan las pruebas de integridad.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Servidor de sistema de videovigilancia	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Servidor de sistema de videovigilancia	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de sistema de videovigilancia	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Servidor de sistema de videovigilancia	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Servidor de sistema de videovigilancia	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para	Media

		sincronización de los equipos.	
Servidor de sistema de videovigilancia	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	Alta
Servidor de sistema de videovigilancia	Falla: No se cuenta con un procedimiento	Establecer un procedimiento de control de cambios	Media

	de control de cambios documentado.	documentado para la gestión de servidores en ambiente de pruebas y luego el paso a producción.	
Servidor de sistema de videovigilancia	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
PCs Administrativa	Parcial: No se cuenta con procedimiento de respaldos del equipo, pero se respaldan carpetas del equipo.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
PCs Administrativa	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
PCs Administrativa	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
PCs Administrativa	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
PCs Administrativa	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta

PCs Administrativa	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para sincronización de los equipos.	Bajo
PCs Administrativa	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	Alta

PCs Administrativa	Falla: No se bloquea el dispositivo por inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media
PCs Administrativa	Falla: No se cuenta con un procedimiento de control de cambios documentado.	Establecer un procedimiento de actualización y mantenimiento de los equipos de usuarios.	Bajo
PCs Administrativa	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
PCs Administrativa	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
PCs Financiera	Parcial: No se cuenta con procedimiento de respaldos del equipo, pero se respaldan carpetas del equipo.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media

PCs Financiera	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
PCs Financiera	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
PCs Financiera	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
PCs Financiera	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
PCs Financiera	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para sincronización de los equipos.	Bajo
PCs Financiera	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas	Alta

		mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
PCs Financiera	Falla: No se bloquea el dispositivo por inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media
PCs Financiera	Falla: No se cuenta con un procedimiento de control de cambios documentado.	Establecer un procedimiento de actualización y mantenimiento de los equipos de usuarios.	Bajo
PCs Financiera	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
PCs Financiera	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta

	consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.		
Portátil del Área Académica	Parcial: No se cuenta con procedimiento de respaldos del equipo, pero se respaldan carpetas del equipo.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Portátil del Área Académica	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Portátil del Área Académica	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Portátil del Área Académica	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Portátil del Área Académica	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Portátil del Área Académica	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para sincronización de los equipos.	Bajo

Portátil del Área Académica	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	Alta
Portátil del Área Académica	Falla: No se bloquea el dispositivo por inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media

Portátil del Área Académica	Falla: No se cuenta con un procedimiento de control de cambios documentado.	Establecer un procedimiento de actualización y mantenimiento de los equipos de usuarios.	Bajo
Portátil del Área Académica	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
Portátil del Área Académica	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Portátil de Docentes	Parcial: No se cuenta con procedimiento de respaldos del equipo, pero se respaldan carpetas del equipo.	Configurar respaldos automáticos y verificación periódica de su integridad.	Media
Portátil de Docentes	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Portátil de Docentes	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta

Portátil de Docentes	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Portátil de Docentes	Parcial: Se realizan actualizaciones de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Portátil de Docentes	Falla: No se sincroniza con el servidor NTP.	Establecer la sincronización con el servidor NTP para sincronización de los equipos.	Bajo
Portátil de Docentes	Parcial: Se cuenta con políticas de complejidad para usuarios logueados pero no de caducidad y cambio.	La organización establece que todas las contraseñas utilizadas para acceder a sus sistemas de información deben tener una longitud mínima de 12 caracteres y deben incluir al menos tres de los siguientes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales. Está prohibido el uso de contraseñas débiles o comunes, las cuales serán bloqueadas mediante un sistema de detección basado en diccionarios de contraseñas inseguras. Las contraseñas deberán renovarse cada 90 días y no podrá reutilizarse ninguna de las últimas cinco utilizadas. En	Alta

		caso de cinco intentos fallidos de autenticación en un periodo de 15 minutos, la cuenta será bloqueada automáticamente, y solo podrá ser desbloqueada por el administrador del sistema mediante verificación de identidad.	
Portátil de Docentes	Falla: No se bloquea el dispositivo por inactividad.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media
Portátil de Docentes	Falla: No se cuenta con un procedimiento de control de cambios documentado.	Establecer un procedimiento de actualización y mantenimiento de los equipos de usuarios.	Bajo
Portátil de Docentes	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
Portátil de Docentes	Parcial: Se cuenta con la licencia de antivirus instalada, pero no con una consola por lo que los logs no se respaldan y las actualizaciones se realizan de manera manual.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta

Móvil Corporativo de Talento Humano	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Móvil Corporativo de Talento Humano	Falla: No se cuentan con mecanismos MDM para el control de accesos.	Implementación de políticas para control de acceso en dispositivos móviles o la implementación de una herramienta MDM para el control remoto.	Alta
Móvil Corporativo de Talento Humano	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Móvil Corporativo de Talento Humano	Falla: No se cuenta con una aplicación de monitoreo continuo de los logs del equipo.	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta
Móvil Corporativo de Talento Humano	Falla: No se cuenta con un procedimiento de actualización de estos dispositivos.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Móvil Corporativo de Talento Humano	Falla: No se cuenta con control de instalación de aplicaciones.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Móvil Corporativo de Talento Humano	Falla: No se cuentan con mecanismos MDM para el control de accesos.	Implementación de políticas para control de acceso en dispositivos móviles o la implementación de una herramienta MDM para el control remoto.	Alta
Móvil Corporativo de Talento Humano	Falla: No se cuenta con	Configurar políticas de tiempo de inactividad y	Media

	control de bloqueo de dispositivo.	bloqueo automático en los dispositivos.	
Móvil Corporativo de Talento Humano	Falla: No se cuenta con un procedimiento de control de cambios documentado.	Establecer un procedimiento de actualización y mantenimiento de los equipos de usuarios.	Bajo
Móvil Corporativo de Talento Humano	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
Móvil Corporativo de Talento Humano	Falla: No se cuenta con un software de protección de software malicioso.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Móvil Corporativo de Área Financiera	Falla: No se ha aplicado política institucional de hardening.	Aplicar políticas de configuración segura y auditoría de cambios.	Media
Móvil Corporativo de Área Financiera	Falla: No se cuentan con mecanismos MDM para el control de accesos.	Implementación de políticas para control de acceso en dispositivos móviles o la implementación de una herramienta MDM para el control remoto.	Alta
Móvil Corporativo de Área Financiera	Falla: No se cuenta con una revisión periódica de vulnerabilidades.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Móvil Corporativo de Área Financiera	Falla: No se cuenta con una aplicación de monitoreo	Establecer herramientas de monitoreo continuo y análisis de logs para detectar anomalías.	Alta

	continuo de los logs del equipo.		
Móvil Corporativo de Área Financiera	Falla: No se cuenta con un procedimiento de actualización de estos dispositivos.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Móvil Corporativo de Área Financiera	Falla: No se cuenta con control de instalación de aplicaciones.	Implementar un proceso regular de actualización y parches de seguridad para reducir vulnerabilidades.	Alta
Móvil Corporativo de Área Financiera	Falla: No se cuentan con mecanismos MDM para el control de accesos.	Implementación de políticas para control de acceso en dispositivos móviles o la implementación de una herramienta MDM para el control remoto.	Alta
Móvil Corporativo de Área Financiera	Falla: No se cuenta con control de bloqueo de dispositivo.	Configurar políticas de tiempo de inactividad y bloqueo automático en los dispositivos.	Media
Móvil Corporativo de Área Financiera	Falla: No se cuenta con un procedimiento de control de cambios documentado.	Establecer un procedimiento de actualización y mantenimiento de los equipos de usuarios.	Bajo
Móvil Corporativo de Área Financiera	Falla: No se cuenta con un software para el control de fuga de información o DLP.	Implementar reglas de bloqueo web para evitar fuga de información y la instalación de software DLP para prevenir la fuga de información.	Alta
Móvil Corporativo de Área Financiera	Falla: No se cuenta con un software de protección de	Implementar un proceso regular de actualización y parches de seguridad	Alta

	software malicioso.	para reducir vulnerabilidades.	
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo

	dispositivos BYOD.		
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo
Móvil Propio (BYOD) usado por docentes	Falla: No se cuenta con controles o políticas de dispositivos BYOD.	Establecer políticas BYOD para la gestión de los riesgos asociados.	Bajo

Fuente: *Instituto Tecnológico Superior Compu Sur*

3.9.Puestos de trabajo

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

Como análisis de los puestos de trabajo de los docentes se toma como muestra los puestos de trabajo de los profesores que manejan información de los estudiantes en su ciclo de aprendizaje. Se debe considerar que los docentes manejan un solo tipo de configuración.

Tabla 16

Puestos de trabajo

Puesto de trabajo	Control de seguridad	Análisis
Docente	Antivirus actualizado y activo	Parcialmente: Cuenta con antivirus instalados, sin embargo, las firmas no han sido actualizado en el último mes al no contar con una consola administrada.
Docente	Configuración segura (Hardening)	Falla: No se cuenta con una plantilla institucional para aplicar configuraciones seguras en los equipos.
Docente	Restricción de instalación de software	Falla: Los docentes tienen privilegios para instalar programas sin control previo.
Docente	Uso de cuentas de usuario no privilegiadas	Falla: Los docentes suelen operar con cuentas de administrador local para la instalación de software para sus clases.
Docente	Actualizaciones automáticas del sistema operativo	Parcialmente: Se cuenta con una versión estable de sistema operativo, sin embargo, el equipo no ha descargado y actualizado los parches del último mes.
Docente	Acceso a red institucional con autenticación segura	Parcialmente: Implementado a través de WiFi institucional, sin embargo, se conectan por contraseña de SSID.
Docente	Bloqueo automático de pantalla por inactividad	Falla: No se establece un bloqueo tras un periodo de tiempo de inactividad.
Docente	Uso de credenciales	Parcialmente: Se cuenta con una política para contraseñas robustas, sin embargo, no se establecen las recomendaciones totales como cambio cada 3 meses, uso obligatorio de caracteres especiales o histórico de no uso de contraseñas.
Docente	Escritorio y pantalla limpia	Falla: En los escritorios y puestos de trabajo de los profesores se pueden visualizar documentos de estudiantes en carpetas y papeles con información para recordar.
Docente	Prohibición de uso de dispositivos USB no autorizados	Falla: No se encuentra bloqueado en los equipos de los profesores para uso de dispositivos externos.

Docente	Formación en ciberseguridad básica	Parcialmente: Han recibido una capacitación de Ciberseguridad, sin embargo, no se ha realizado una en el último año o se tiene una planificación de capacitación.

Fuente: Instituto Tecnológico Superior Compu Sur

Tabla 17

Propuesta de mejora

Docente	Antivirus actualizado y activo	Parcialmente: Cuenta con antivirus instalados, sin embargo, las firmas no han sido actualizadas en el último mes.	1.- Revisar y actualizar política de actualización automática de antivirus. 2.- Monitoreo mensual de estado de firmas a través de consola centralizada.	Coordinador de TI / Coordinador Académico	Media
Docente	Configuración segura (Hardening)	Falla: No se cuenta con una plantilla institucional para aplicar configuraciones seguras en los equipos.	1.- Crear plantilla de configuración segura. 2.- Aplicar hardening en todos los dispositivos docentes.	Coordinador de TI / Coordinador Académico	Alta
Docente	Restricción de instalación de software	Falla: Los docentes tienen privilegios para instalar programas sin control previo.	1.- Implementar control de instalaciones con software autorizado. 2.- Eliminar privilegios de instalación libre.	Coordinador de TI / Coordinador Académico	Alta
Docente	Uso de cuentas de usuario no privilegiadas	Falla: Los docentes suelen operar con cuentas de administrador local para la instalación de software para sus clases.	1.- Eliminar cuentas con privilegios de administrador. 2.- Configurar perfiles estándar para docentes.	Coordinador de TI / Coordinador Académico	Alta
Docente	Actualizaciones	Parcialmente: Se cuenta con una versión estable de sistema	1.- Configurar actualizaciones	Coordinador de TI /	Media

	automáticas del sistema operativo	operativo, sin embargo, el equipo no ha descargado y actualizado los parches del último mes.	automáticas. 2.- Verificar cumplimiento trimestralmente.	Coordinador Académico	
Docente	Copia de seguridad de archivos académicos	Falla: No existe política de respaldo automático de archivos académicos.	1.- Crear política institucional de respaldo automático de archivos académicos. 2.- Incluir almacenamiento seguro en la nube.	Coordinador de TI / Coordinador Académico	Alta
Docente	Acceso a red institucional con autenticación segura	Parcialmente: Implementado a través de WiFi institucional, sin embargo, se conectan por contraseña de SSID.	1.- Implementar autenticación de red basada en usuarios y contraseñas individuales. 2.- Reforzar seguridad de WiFi institucional.	Coordinador de TI / Coordinador Académico	Media
Docente	Bloqueo automático de pantalla por inactividad	Falla: No se establece un bloqueo tras un periodo de tiempo de inactividad.	1.- Establecer un control de bloqueo por GPO tras 5 minutos de inactividad.	Coordinador de TI / Coordinador Académico	Baja
Docente	Uso de credenciales	Parcialmente: Se cuenta con política para contraseñas robustas, sin embargo, no se aplican totalmente.	1.- Implementar rotación de contraseñas cada 90 días. 2.- Aplicar políticas obligatorias de complejidad.	Coordinador de TI / Coordinador Académico	Media
Docente	Escritorio y pantalla limpia	Falla: Se visualizan documentos de estudiantes en escritorios y papeles visibles.	1.- Implementar política de escritorio limpio. 2.- Sensibilización a docentes sobre protección de datos.	Coordinador de TI / Coordinador Académico	Alta

Docente	Prohibición de uso de dispositivos USB no autorizados	Falla: No se encuentra bloqueado el uso de dispositivos externos en equipos de profesores.	1.- Bloquear puertos USB o usar soluciones de control de dispositivos. 2.- Solo permitir USBs corporativos certificados.	Coordinador de TI / Coordinador Académico	Alta
Docente	Formación en ciberseguridad básica	Parcialmente: Han recibido capacitación, pero no hay actualización anual ni planificación futura.	1.- Planificar capacitaciones anuales de ciberseguridad. 2.- Registrar la asistencia y evaluación de conocimientos.	Coordinador de TI / Coordinador Académico	Media

Fuente: *Instituto Tecnológico Superior Compu Sur*

3.9.2. Acuerdo de confidencialidad

En relación con el acuerdo de confidencialidad que los colaboradores del instituto deben firmar se cuenta con el siguiente ejemplo.

Entre:

INSTITUTO TECNOLÓGICO SUPERIOR COMPU SUR (ITECSUR)

RUC: 1792902630001.

Dirección: Campus matriz - Av. Pedro Vicente Maldonado y Alamor.

Representado por: Erazo Luna Andrés Mauricio.

Correo institucional: info@itecsur.edu.ec.

En calidad de Responsable legal, conforme al artículo 5 de la Ley Orgánica de Protección de Datos Personales.

Y:

Nombre del trabajador: _____

Cédula de identidad: _____

Correo electrónico: _____

Cargo: Docente

Departamento / Coordinación: _____

ACUERDAN lo siguiente:

---

1. Actividad de tratamiento de acceso

El trabajador, en el ejercicio de sus funciones como colaborador de ITECSUR, accederá a información personal y académica de estudiantes, como calificaciones, historial académico, datos de contacto, asistencia, entre otros. Este tratamiento se realiza únicamente con fines educativos, administrativos y de seguimiento académico, en cumplimiento de los fines institucionales.

---

2. Obligación de confidencialidad

El trabajador se compromete a mantener en absoluta confidencialidad toda la información personal, académica y administrativa a la que tenga acceso por motivo de su cargo. Esta obligación se extiende incluso después de finalizada la relación laboral con ITECSUR.

---

3. Obligación de cumplimiento de medidas de seguridad

El colaborador se obliga a:

- Utilizar contraseñas seguras y proteger el acceso a sus dispositivos de trabajo.
- No compartir información sensible por medios no autorizados.
- Cifrar o proteger documentos que contengan datos personales cuando sean transportados o almacenados.
- Informar de inmediato a la institución en caso de pérdida, acceso no autorizado o vulneración de datos.

---

4. Consecuencias de vulnerar las obligaciones

La infracción de cualquiera de estas obligaciones podrá dar lugar a:

- Sanciones administrativas o disciplinarias internas.
- Acciones legales por parte de la institución.
- Responsabilidad civil, penal o administrativa conforme a lo dispuesto en la LOPDP.

---

5. Finalidad y uso de la recogida de los datos del trabajador por parte de la organización

ITECSUR recopilará y tratará los datos personales del trabajador con la finalidad de gestionar su vinculación laboral, cumplimiento de obligaciones contractuales y verificación de su idoneidad para el acceso a información sensible.

---

6. Tiempo de almacenamiento de sus datos

Los datos del trabajador serán conservados mientras dure la relación laboral y, posteriormente, durante el tiempo necesario para el cumplimiento de obligaciones legales o contractuales.

---

7. Ejercicio de derechos del trabajador

El trabajador podrá ejercer sus derechos **de** acceso, rectificación, actualización, eliminación, oposición, portabilidad y suspensión del tratamiento, enviando su solicitud a:

Correo de contacto para derechos de protección de datos**:** info@itecsur.edu.ec.

---

8. Datos del Delegado de Protección de Datos (DPD)

Nombre del DPD: _____

Correo electrónico: _____

Teléfono de contacto: _____

---

9. Tratamiento de datos por sistemas de videovigilancia

El trabajador queda informado de que las aulas, pasillos y áreas administrativas cuentan con cámaras de videovigilancia instaladas con fines de seguridad institucional y control interno. Las grabaciones serán tratadas de acuerdo con la LOPDP, y no serán utilizadas con fines disciplinarios salvo autorización legal o judicial.

---

10. Consentimiento para uso de imagen en redes sociales y página web institucional

De forma adicional, y de manera libre, específica, informada e inequívoca, el trabajador puede otorgar su consentimiento para que su imagen (fotografías o videos) sea utilizada por el Instituto Tecnológico Superior Compu Sur (ITECSUR) con fines institucionales, promocionales o de comunicación en medios digitales como redes sociales, página web, boletines electrónicos o material institucional.

☐ ACEPTO el uso de mi imagen conforme a los fines antes descritos.

☐ NO ACEPTO el uso de mi imagen para estos fines.

Nota: En caso de aceptar, el trabajador podrá revocar este consentimiento en cualquier momento mediante solicitud enviada al correo electrónico de contacto: info@itecsur.edu.ec.

Quito, Ecuador

Fecha: ___ / ___ / 202__

FIRMAS:

Firma del trabajador

Erazo Luna Andrés Mauricio.

Representante Legal ITECSUR.

Firma del responsable institucional

3.10. Encargado del tratamiento

3.10.1. Contrato de encarga de tratamiento

a) RESPONSABLE DEL TRATAMIENTO

INSTITUTO TECNOLÓGICO SUPERIOR COMPU SUR (ITECSUR)

RUC: 1792902630001.

Dirección: Campus matriz - Av. Pedro Vicente Maldonado y Alamor.

Representado por: Erazo Luna Andrés Mauricio.

Correo institucional: info@itecsur.edu.ec.

b) ENCARGADO DEL TRATAMIENTO

GRUNSEG CIA. LTDA.

RUC: 1792016576001.

Dirección: C Lote 35 Oe4d Vicente Rocafuerte.

Correo electrónico: info@grunseg.com.

Representante Legal: Grunauer Solines Ernesto Rafael.

c) DELEGADO DE PROTECCIÓN DE DATOS (DPD) DEL RESPONSABLE

Nombre: _____

Correo: _____

Teléfono:_____

---

2. OBJETO DEL CONTRATO

El presente contrato tiene por objeto regular los términos y condiciones bajo los cuales GRUNSEG, en calidad de Encargado del Tratamiento, accederá y tratará los datos personales necesarios para prestar los servicios de control de acceso físico a instalaciones, monitoreo de

cámaras de seguridad y gestión de respaldo de grabaciones, conforme a las instrucciones del Responsable del Tratamiento (ITECSUR).

---

3. DURACIÓN

El presente contrato tendrá una duración de un (1) año, contado a partir de la fecha de firma, prorrogable automáticamente por iguales períodos, salvo notificación en contrario de alguna de las partes con al menos 30 días de antelación.

---

4. NATURALEZA DEL TRATAMIENTO

El Encargado del Tratamiento únicamente podrá acceder y procesar datos personales en virtud del presente contrato, y no podrá utilizarlos para fines propios ni transferirlos a terceros, salvo autorización expresa del Responsable del Tratamiento o exigencia legal.

---

5. FINALIDAD DEL TRATAMIENTO

Los datos personales serán tratados exclusivamente para:

- Controlar y registrar el ingreso y salida de personal y visitantes al campus.
- Monitorear en tiempo real las áreas comunes y aulas mediante cámaras de seguridad.
- Almacenar y respaldar de forma segura las grabaciones de video.
- Atender requerimientos legales o internos relacionados con seguridad física institucional.

---

6. TIPO DE DATOS PERSONALES TRATADOS

- Imágenes y videos de personas captadas por cámaras.
- Información de identificación en sistemas de acceso (nombres, cédula, hora de entrada/salida).
- Información de contacto para autorizaciones o reportes de procesos de seguridad.

---

7. INSTRUCCIONES PARA EL TRATAMIENTO

GRUNSEG se compromete a:

- Tratar los datos personales conforme a lo establecido en este contrato y en las instrucciones escritas del Responsable.
- No utilizar los datos para fines distintos a los aquí previstos.
- No conservar copias de los datos una vez finalizada la relación contractual.
- No subcontratar el servicio sin autorización previa y por escrito del Responsable.

---

8. CATEGORÍAS DE INTERESADOS

Los datos personales tratados corresponden a:

- Estudiantes
- Docentes
- Personal administrativo
- Visitantes y terceros que ingresen a las instalaciones de ITECSUR

---

9. OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

El Encargado deberá:

- Aplicar medidas de seguridad técnicas y organizativas adecuadas.
- Garantizar la confidencialidad, integridad y disponibilidad de la información.
- Asegurar que su personal esté capacitado y comprometido con la protección de datos.
- Colaborar con el Responsable en la atención de solicitudes de derechos de los titulares.
- Notificar al Responsable cualquier incidente de seguridad dentro de un plazo máximo de 48 horas.
- Permitir revisiones tipo auditoria de los procesos cuando se requiera considerando una notificación previa de 30 días.

---

10. OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

ITECSUR se compromete a:

- Proveer al Encargado las instrucciones necesarias por escrito.
- Verificar periódicamente el cumplimiento de las medidas de seguridad aplicadas.
- Informar al Encargado sobre cualquier cambio normativo que afecte el tratamiento de datos personales.
- Facilitar la gestión de derechos de los titulares.

---

11. MEDIDAS ANTE BRECHAS DE SEGURIDAD

En caso de una violación de la seguridad que implique destrucción, pérdida, alteración o acceso no autorizado a los datos personales tratados, el Encargado deberá notificar al Responsable dentro de un plazo máximo de 48 horas, detallando lo descrito en el reglamento de ley:

- Naturaleza de la brecha
- Datos afectados
- Posibles consecuencias
- Medidas adoptadas o propuestas

---

12. ACUERDO DE FINALIZACIÓN DE LA RELACIÓN

Al término del contrato, el Encargado deberá:

- Devolver o destruir de forma segura todos los datos personales tratados, en función de la instrucción del Responsable.
- Certificar por escrito la destrucción de la información, de ser el caso.
- No conservar copias salvo disposición legal expresa.

---

13. SUBCONTRATACIÓN

El Encargado no podrá subcontratar con terceros el acceso, tratamiento o almacenamiento de los datos personales objeto de este contrato sin la previa autorización expresa, específica y por escrito del Responsable del Tratamiento.

En caso de que se autorice la subcontratación, el subencargado deberá asumir las mismas obligaciones de protección de datos establecidas en este contrato, formalizando a su vez un contrato que regule su relación conforme a los requisitos de la Ley Orgánica de Protección de Datos Personales del Ecuador.

El Encargado será plenamente responsable frente al Responsable por el incumplimiento de las obligaciones por parte del subencargado.

---

14. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

No se realizará ninguna transferencia internacional de datos personales fuera del territorio ecuatoriano salvo que:

- Exista un consentimiento previo, expreso e informado del Responsable del Tratamiento o del titular de los datos, conforme a lo previsto en la Ley Orgánica de Protección de Datos Personales.
- El país de destino proporcione un nivel de protección de datos personales adecuado y reconocido oficialmente.
- Se firmen las cláusulas contractuales tipo o mecanismos que garanticen la protección de los datos, de acuerdo con los lineamientos de la Autoridad de Protección de Datos del Ecuador.

En caso de requerirse una transferencia internacional, el Encargado deberá solicitar autorización previa por escrito al Responsable, adjuntando la documentación de respaldo que garantice la protección adecuada de los datos.

15. FIRMA DE CONFORMIDAD

Ambas partes declaran haber leído y comprendido el contenido del presente contrato, y se obligan a cumplir lo establecido, de conformidad con la Ley Orgánica de Protección de Datos Personales del Ecuador.

Por el Responsable del Tratamiento

Firma: _____

Nombre: _____

Cargo: _____

Fecha: _____

Por el Encargado del Tratamiento (GRUNSEG)

Firma: _____

Nombre: _____

Cargo: _____

Fecha: _____

3.11. Análisis Web

El Instituto Tecnológico Superior Compu Sur (ITECSUR), comprometido con la transparencia, la seguridad de la información y la mejora continua de su presencia digital, realiza periódicamente revisiones de su sitio web institucional, evaluando el cumplimiento de las mejores prácticas internacionales de Ciberseguridad.

3.11.1. Análisis, configuración y Política de cookies

Como parte de su presencia digital el instituto tecnológico cuenta con una página web no segura con el siguiente link: https://itecsur.edu.ec/autoridades-itecsur/, como resultados del análisis del portal tenemos:

- Uso de servicio con certificado digital con las siguientes configuraciones:
    - Protocolos TLS 1.3, TLS 1.2, TLS 1.1 y TLS 1.0 habilitados.
- No se identifica la configuración de las siguientes cabeceras de seguridad en la página web:
    - Strict-transport-security.
    - Content-security-policy.
    - X-Frame-Options.
    - X-Content-Type-Options.
    - Referrer-policy.
    - Permissions-policy.

El sitio web de ITECSUR emplea cookies para optimizar la experiencia del usuario, analizar datos estadísticos de navegación y ofrecer contenidos personalizados. Dentro de la política de cookies se establece que:

- Se utilizan cookies propias y de terceros para recopilar datos estadísticos de navegación.
- El usuario no tiene la opción de aceptar, rechazar o configurar las cookies al ingresar al sitio y se plantea un inconveniente.
- ITECSUR garantiza que los datos recopilados son tratados conforme a la legislación

vigente en materia de protección de datos, sin embargo, no están especificados de una forma clara de cómo se van a manejar sus datos conforme lo especificado dentro del aviso legal sobre el tratamiento de datos personales.

Recomendación: Se debe implementar las siguientes configuraciones sobre su página web:

- Implementar un banner de cookies (pop-up inicial) que permita:
  - Aceptar todas las cookies.
  - Rechazar todas las cookies (excepto las estrictamente necesarias).
  - Configurar preferencias específicas.
- Publicar una Política de Cookies independiente, con el detalle de:
  - Tipología de cookies.
  - Finalidad específica de cada cookie.
  - Base legal para su uso.
  - Forma del cliente para revocar el consentimiento.

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

El sitio de ITECSUR pone a disposición varios formularios para facilitar la comunicación y participación:

- **Formulario de Contacto:** No posee un formulario preestablecido para consultas generales y solicitudes de información, se agregan números de contacto para la comunicación directa, WhatsApp 096 367 0206 y el mail info@itecsur.edu.ec. Adicionalmente se habilita un chatbot en la página web para la atención de dudas.

Recomendación: Se debe manejar un canal único de información para poder mantener esos datos de manera centralizada puesto que se crearía una mejor base estadística y desde ahí se debería direccionar hacía los puntos focales de acuerdo con la depuración de datos, ya que se puede masificar y colapsar dicho correo si no se cuentan con las medidas de seguridad informáticas adecuadas. Adicionalmente no se visualiza un mecanismo que permita que los titulares de Datos personales puedan garantizar sus derechos a nivel web.

El formulario debe considerar los campos de aceptación de política de privacidad y la explicación previa del uso de los datos enviados.

- **Newsletter:** Posee una casilla en la cual se registran datos personales para suscripción a boletines informativos sobre actividades académicas, eventos y noticias institucionales.

  Recomendación: Se debe implementar una guía o previa lectura y aceptación clara sobre el tratamiento de los datos provistos en dicho formulario, permitiendo al usuario tomar una decisión informada. La actual redacción solo informa, pero no solicita consentimiento específico.

- **Trabaja con Nosotros:** Formulario disponible para la recepción de hojas de vida y postulaciones a vacantes disponibles en el siguiente link: https://phpclusters-122936-0.cloudclusters.net/trabajaconnosotros.

Recomendación: Se debe unificar la denominación en todo el documento, las finalidades del tratamiento son demasiado generales. Se recomienda detallar específicamente cada propósito (académico, administrativo, marketing, investigación, etc.) permitiendo que los titulares

puedan dar consentimiento específico para cada finalidad. Adicionalmente se debe diferenciar entre datos personales ordinarios y datos personales sensibles, especificando las medidas adicionales para estos últimos. Como control complementario se debe especificar los países o destinatarios de posibles transferencias internacionales y las garantías aplicables.

- **Formulario de Registro:** Formulario disponible para la inscripción en programas académicos, cursos y eventos institucionales disponible en el siguiente link: https://docs.google.com/forms/d/e/1FAIpQLSeunmoi-r9codtVaLqNRkOE8CKCqpvMhQdAVpeflcIk4A1V6g/viewform.

Recomendación: Se debe añadir un campo introductorio que explique por qué es importante proteger los datos personales, en un lenguaje cercano. Adicionalmente se debe separar cada tema de forma clara en subtítulos claros para lector como: "Responsable del tratamiento" "Finalidad del tratamiento" "Tipos de datos recopilados".

3.11.3. Avisos legales

ITECSUR dispone del aviso legal de datos descrito por su proveedor de plataforma de servicio en la nube Moodle, pero no están fácilmente accesible desde la página web de ITECSUR sino desde la página principal de su proveedor en el siguiente link https://moodle.com/es/aviso-de-privacidad/:

- Aviso de Privacidad: Existe, pero no está visible en las páginas del sitio solo desde la página de la plataforma de su proveedor.

Para dar cumplimiento a las disposiciones legales y buenas prácticas se deben implementar los siguientes controles en avisos legales:

1. Aviso o Política de Privacidad (Obligatorio): Este documento debe ser claro, específico y accesible, explicando:

- Qué datos personales se recolectan (nombre, correo, IP, cookies, etc.).
- Finalidad del tratamiento de datos (por ejemplo, envío de newsletters, análisis de tráfico).
- Base legal que justifica el tratamiento (consentimiento, cumplimiento contractual, interés legítimo, etc.).
- Derechos del titular (acceso, rectificación, cancelación, oposición, portabilidad, limitación y retiro del consentimiento).
- Plazo de conservación de los datos.
- Medidas de seguridad aplicadas.
- Transferencias internacionales o a terceros (incluyendo prestadores de servicios como Google, Meta, etc.).
- Datos del responsable del tratamiento (nombre del responsable, correo de contacto, etc.).

2. Términos y Condiciones de Uso (Obligatorio): Regula la relación entre la plataforma y el usuario. Incluye:

- Normas de uso del sitio web.
- Responsabilidades del usuario y del titular del sitio.
- Limitaciones de responsabilidad.
- Condiciones de registro.

- Legislación aplicable y jurisdicción (Ecuador).
- Procedimientos para modificar las condiciones.

3. Política de Propiedad Intelectual (Obligatorio): Debe contemplar:

- Derechos de autor sobre textos, informes, investigaciones, imágenes, logos, etc.
- Restricciones de uso y reproducción del contenido.
- Instrucciones para reportar infracciones o solicitar uso de material.

4. Política de Cookies (Obligatorio): Debe indicar:

- Tipos de cookies utilizadas (técnicas, analíticas, de terceros, etc.).
- Finalidad de cada una.
- Cómo deshabilitarlas.
- Enlace al banner de consentimiento o configuración de cookies.

5. Formularios de recolección de información (Recomendado): Debe incluir:

- Una casilla de verificación que el usuario marque voluntariamente.
- Texto que indique claramente para qué se usarán sus datos.
- Un enlace al aviso de privacidad.

6. Formulario de ejercicio de derechos ARCO-POL (Recomendado): Se debe incluir un formulario o mecanismo para que el usuario pueda:

- Acceder a sus datos.
- Rectificarlos.
- Cancelarlos o eliminarlos.
- Oponerse al tratamiento.

Solicitar portabilidad o limitar el tratamiento.

7. Política de Seguridad de la información (Recomendado): Aunque no es obligatorio publicarla, la LOPDP exige que las organizaciones implementen y documenten medidas de seguridad para proteger los datos. Algunas empresas optan por compartir un resumen público para reforzar la confianza.

3.12. Medidas de seguridad

Es esencial establecer políticas y medidas sólidas para asegurar el uso seguro de los navegadores web, especialmente en un entorno educativo donde los recursos de seguridad avanzados como CASB (Cloud Access Security Broker) o DLP (Data Loss Prevention) no están disponibles. Adicionalmente se debe considerar que la web es una fuente de amenazas como malware que pueden afectar los activos de información de la organización.

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

Los navegadores web son herramientas fundamentales en el ámbito educativo, facilitando el acceso a recursos de aprendizaje, plataformas de gestión académica y servicios en la nube. Sin embargo, su uso también conlleva riesgos significativos:

- Acceso a sitios maliciosos: Los estudiantes y el personal pueden, inadvertidamente, visitar sitios web que albergan malware o intentan realizar ataques de phishing.
- Descarga de archivos no seguros: La descarga de contenido desde fuentes no verificadas puede introducir software malicioso en los sistemas institucionales.
- Vulnerabilidades del navegador: Navegadores desactualizados o mal configurados pueden ser explotados por atacantes para comprometer la seguridad del sistema.

- Fugas de información: Sin herramientas de DLP, existe el riesgo de que información sensible sea compartida o extraída sin autorización.

Las medidas de seguridad recomendadas para la implementación de controles en ITECSUR son:

1. Actualización y Configuración Segura de Navegadores:

- Mantener los navegadores del personal y utilizado por los estudiantes actualizados. Se debe asegurar de que todos los navegadores utilizados estén en su versión más reciente para corregir vulnerabilidades conocidas.
- Deshabilitar funciones innecesarias: Desactivar complementos, extensiones o funciones que no sean esenciales para reducir la superficie de ataque.
- Configurar políticas de seguridad: Utilizar políticas de grupo (GPO) para establecer configuraciones de seguridad que permitan la actualización de los navegadores de manera automática o en su defecto establecer un control periódico de actualización manual por el personal técnico.

2. Implementación de Filtros de Contenido Web

- Utilizar servicios de DNS seguros: Configurar la red para utilizar servicios como OpenDNS o Google Public DNS, que ofrecen filtrado de contenido y protección contra sitios maliciosos.
- Bloqueo de categorías de sitios: Establecer políticas para bloquear categorías de sitios web no relacionadas con actividades académicas, como juegos, redes sociales o contenido para adultos.

- Bloqueo de páginas de exfiltración de información para los colaboradores administrativos: Establecer reglas que bloqueen sitios web que permiten la fuga de información como: Wetransker, Dropbox, Protonmail, etc.

3. Uso de Extensiones de Seguridad en Navegadores

- Instalar extensiones de bloqueo de scripts: Herramientas como NoScript o ScriptSafe permiten controlar la ejecución de scripts en las páginas web, reduciendo el riesgo de ataques XSS o drive-by downloads.
- Bloqueadores de anuncios y rastreadores: Instalar extensiones como uBlock Origin ayudan a bloquear anuncios maliciosos y rastreadores que pueden comprometer la privacidad y seguridad del usuario.
- Regla de análisis de archivos descargados: Configurar el software de seguridad endpoint para la revisión de análisis malicioso de todos los archivos descargados.

3.12.2. Hosting y servidores

Ante la presencia de reiterados fallos en la plataforma académica ROMAGMK por citar algunos, incompatibilidad con navegadores, retraso en actividades, pocas bases de configuración, las autoridades tomaron la decisión de migrar a una mejor opción y hoy en día se cuenta con una plataforma de tipo MOODLE manejada por conecti.me un proveedor de servicio dedicado a la implementación, personalización y evolución de Entornos Virtuales de Aprendizaje radicado en Brasil con su base de operaciones.

Entre las principales medidas aplicadas se incluyen:

- Ordenadores personalizados y redes específicas para actividades

administrativas y docentes.

- Autenticación de dos factores (2FA).
- Auditorias de extensiones y complementos para los ordenadores y navegadores preestablecidos con el fin de minimizar el nivel de exposición al navegar en la web.
- Sistemas de detección de correos sospechosos o spam.
- Protocolos de cifrado para el envío y recepción de correos.

Adicionalmente a las medidas tomadas por ITECSUR se realiza un análisis independiente entre hosting y servidores al mantener controles diferentes en la gestión tecnológica.

3.12.2.1. Medidas de seguridad

Hosting Web (Tercerizado): El servicio de hosting se gestiona por un proveedor externo que aloja el sitio web institucional, correo institucional, LMS (como Moodle), entre otros. Aunque el control directo puede ser limitado a los acuerdos contractuales, se deben aplicar y exigir medidas de seguridad específicas a nivel de los portales web:

- Uso obligatorio de certificados SSL/TLS válidos (HTTPS).
- Deshabilitar listados de directorios y módulos innecesarios.
- Configurar encabezados HTTP seguros:
    - Strict-transport-security.
    - Content-security-policy.
    - X-Frame-Options.

- X-Content-Type-Options.
- Referrer-policy.
- Permissions-policy.

- Validar que el proveedor realiza actualizaciones regulares del CMS (WordPress, Joomla, Moodle, etc.) y sus plugins.
- Aplicar pruebas periódicas de análisis de vulnerabilidades web y Pentesting.
- Uso de autenticación multifactor (MFA) en el panel de administración del hosting.
- Control de cuentas administrativas: mínimo número de usuarios con privilegios altos.
- Hay que asegurar que el proveedor realiza backups automáticos diarios.
- Validar que exista un proceso para recuperación ante desastres accesible y probado.
- Solicitar al proveedor servicios de Web Application Firewall (WAF) básico si está disponible.
- Configurar filtros anti-spam y antivirus en los servicios de correo asociados al hosting.

Para el caso de los servidores administrados en materia web ITECSUR debe implementar las siguientes medidas:

a) Infraestructura segura

- Mantener el sistema operativo actualizado y aplicar parches de seguridad de forma

controlada.

- Configuración de firewall local (iptables, UFW, Windows Firewall) con políticas de "deny by default".
- Segmentación de red para separar servidores internos del tráfico público.
    - Para el control de segmentación para los servicios públicos se debe establecer el control de DMZ en la segmentación.

b) Seguridad en la red

- Monitorizar el tráfico con herramientas de usuarios que se conecten a las redes del personal o estudiantes.
- Establecer reglas de detección de amenazas con un IDS/IPS para los segmentos productivos.
- Evitar servicios innecesarios expuestos a internet (como SSH o RDP).

c) Gestión de usuarios y accesos

- Deshabilitar cuentas de administrador predeterminadas y aplicar principio de mínimo privilegio en los servicios públicos.
- Uso de autenticación por llaves SSH (no contraseñas).
- Registros de auditoría habilitados y protegidos contra alteración.

d) Resiliencia y continuidad

- Implementar sistemas de respaldo locales y remotos (incrementales y completos).
- Pruebas regulares de restauración de servicios críticos.
- Documentar y probar un plan de recuperación ante incidentes.

3.12.2.2. Prestadores de servicio

Actualmente el proveedor identificado en la gestión de hosting es:

- Hosting: EOS – Ecuador.
- Proveedor de soporte y servicios TI: Soporte IT Informático Servicios de IT.

Como controles de la gestión de los prestadores de servicio ITECSUR debe considerar:

- Solicitar a EOS y proveedores TI la entrega formal de su Política de privacidad y el procedimiento de atención de brechas de seguridad.
- Formalizar cláusulas de protección de datos en los contratos de prestación de servicios externos, según la Ley Orgánica de Protección de Datos Personales (LOPDP).
- Establecer las cláusulas contractuales de cumplimiento sobre regulaciones locales, código de ética, salud y seguridad ocupacional, continuidad de negocio, confidencialidad y secreto profesional, garantías, competencias del personal técnico, responsables del contrato, cesión y subcontrato, protección de propiedad intelectual, declaración de conflictos de interés, cláusulas de terminación, conformidad, seguridad de la información y datos personales.
- Establecer indicadores de servicio conocidos como SLA y medirlos de manera mensual para conocer que los objetivos en la prestación del servicio se cumplan. En caso de incumplir con los SLA establecer cláusulas de multas a nivel contractual como un numeral de Penalizaciones y niveles de servicio.

3.12.2.3. Gestores de correo electrónico

Actualmente ITECSUR cuenta con la implementación de controles desde la suite de Microsoft Office 365 y herramientas complementarias como Veeam Backup para mitigar riesgos identificados en el servicio de correo electrónico. Sin embargo, cabe destacar que la solución de correo es accesible desde equipos corporativos como dispositivos personales BYOD.

3.12.2.4. Medidas de seguridad

Actualmente, el Instituto Tecnológico cuenta con la suite de Microsoft 365 como solución de productividad y colaboración, y con la herramienta Bream Backup como respaldo y control de los servicios de correo electrónico. Estas herramientas proporcionan un conjunto robusto de medidas de seguridad:

a) Seguridad ofrecida por Microsoft 365

- Autenticación multifactor (MFA): disponible en planes comerciales, protege el acceso a cuentas de usuarios.
- Protección contra malware y spam: mediante Microsoft Defender for Office 365, en planes que lo incluyen.
- Cifrado de correos electrónicos: utilizando S/MIME o Microsoft Purview Message Encryption.
- Control de acceso basado en roles (RBAC): gestión granular de privilegios.
- Auditoría y registro de actividades: seguimiento de inicios de sesión, modificaciones en archivos, etc.
- Protección contra suplantación de identidad (anti-phishing): integrada en

Exchange Online Protection.

- Almacenamiento en la nube con redundancia geográfica (OneDrive, SharePoint).

b) Seguridad ofrecida por Bream Backup

- Respaldo automatizado de buzones y archivos asociados.
- Restauración granular de correos o carpetas.
- Protección frente a eliminación accidental o ataques ransomware.
- Cifrado en tránsito y en reposo de los respaldos.
- Políticas de retención personalizables.

Adicionalmente a las herramientas implementadas por ITECSUR se deben considerar la implementación de los siguientes controles identificados:

- Implementación de un CASB (Cloud Access Security Broker): para monitoreo y control de aplicaciones en la nube.
- Solución de DLP (Prevención de Pérdida de Datos): para evitar fuga de datos sensibles por correo o almacenamiento en nube.
- Gestión de dispositivos (MDM): control de dispositivos móviles y estaciones que acceden a los servicios de M365.
- Segmentación de acceso y monitoreo con SIEM externo.
- Clasificación automática de datos confidenciales.
- Complementar bloqueo web en los equipos de los docentes para el manejo de datos personales.

3.12.2.5. Prestadores de servicio

Al ser Microsoft un proveedor de servicios bajo modelo SaaS en correo electrónico, ITECSUR debe reconocer que existe un modelo compartido de responsabilidad. La empresa gestiona la seguridad de la infraestructura, pero la institución es responsable de la configuración, gestión de acceso y protección de los datos.

Los controles y exigencias hacia Microsoft como proveedor deben ser:

- SLAs claros y exigibles sobre disponibilidad, recuperación ante desastres y tiempo de respuesta ante incidentes.
- Certificaciones de cumplimiento: exigir que Microsoft mantenga certificaciones como ISO 27001, SOC 2, GDPR, etc.
- Auditorías externas: acceso a informes de auditoría y cumplimiento.
- Control sobre ubicación de los datos: saber dónde están alojados y que exista opción de soberanía de datos.
- Notificaciones ante incidentes: cláusulas contractuales que obliguen a informar incidentes de seguridad o brechas.
- Compatibilidad con herramientas de terceros de ciberseguridad.
- Acuerdo de confidencialidad y protección de datos: conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador.
- Acceso a logs y registros en caso de investigación interna o legal.

Capítulo 4

4.1. Descripción de lo que es un Plan Director de Seguridad y los beneficios para la empresa.

4.1.1. Check List PDS

Tabla 18

Check list PDS

NIVEL	ALCANCE	CONTROL	
A	PRO	**Analizar la situación actual de la empresa,** Analizas detalladamente la situación actual de la empresa para poder acometer un Plan Director de Seguridad.	X
A	PRO	**Alinear el PDS con la estrategia de la empresa.** Tienes en cuenta la estrategia empresarial en su conjunto a la hora de diseñar el Plan Director de Seguridad.	X
A	PRO	**Definir los proyectos a ejecutar.** Estableces y defines en detalle las acciones concretas para alcanzar los niveles de seguridad deseados.	X
A	PRO	**Clasificar y priorizar los proyectos.** Agrupas y clasificas las acciones a ejecutar con el fin de priorizar aquellas que nos proporcionen mayores beneficios en relación a su coste.	

B	PRO	**Aprobar el PDS.** Apruebas y publicas la versión definitiva del PDS.
A	PRO	**Ejecución del PDS** Pones en marcha los proyectos acordados para alcanzar los objetivos de ciberseguridad definidos.
A	PRO	**Certificación en seguridad.** Consideras la implantación de un proceso de certificación que acredite el sistema de gestión de la seguridad de tu empresa

Fuente: *Instituto Tecnológico Superior Compu Sur*

4.1.2. Análisis de la situación actual de la empresa.

Para realizar el análisis de la situación actual de la empresa cuando se encuentre en una situación crítica derivada de varias deficiencias estructurales, estratégicas y tecnológicas podemos destacar:

Un modelo de gestión limitado está definido cómo opera la empresa con un modelo administrativo tradicional, aún con muchos procesos manuales y una falta de automatización. Al no existir herramientas tecnológicas tan robustas que puedan soportar la toma de decisiones a una escala macro y tampoco enfrentar una trazabilidad de operación.

Desarticulación estratégica dentro de todo hay un nivel evidente de desconexiones entre el nivel administrativo-gerencial y el mando operativo puesto que los objetivos no se encuentran definidos o a su vez alineados a una estrategia integral para el desarrollo futuro lo

cual dificulta de cierta forma la ejecución sincrónica de proyectos en pro de una mejora continua en los procesos.

Hay una brecha tecnológica un tanto significativa que ha sido identificada principalmente una carencia de tecnología sólida en ciertas áreas qué sería el tema de captación de alumnos, atención al cliente, logística o finanzas. Todo esto abarca una falta en los sistemas interconectados lo que nos priva de mantener actualizada a tiempo real y con disponibilidad inmediata la información de igual manera el tema de la trazabilidad a futuro con los indicadores los cuales son necesarios para la mejora continua.

Dentro del ámbito cultural podemos destacar como toda organización reactiva la cual mantiene un enfoque un poco sesgado de lo éticamente correcto que en este caso vendría siendo la prevención, más bien ha existido una gestión enfocada directamente en la resolución de problemas al instante sin esclarecer un plan como mecanismo de mejora e innovación.

En lo que conocemos cómo oportunidades de transformación nos enfocaremos dentro de cada una de las limitaciones inherentes al rol de negocio de la institución existe por parte de los altos mandos una predisposición para mejorar, lo que abre un abanico de posibilidades para la implementación de herramientas tecnológicas accesibles puesto que la educación en el país no es tan rentable o al menos ese es su objetivo y en el futuro se pueda implementar para qué tengo un impacto positivo dentro de sus procesos, como es el caso del presente documento.

4.1.3. Plan estratégico en materia tecnológica

Dentro del plan estratégico en materia tecnológica realizaremos un cronograma modificable con tiempos y actividades que sea considerado importante para la toma de

decisiones y la mejora de la eficiencia operativa para medir de una manera mucho más clara los procesos.

4.1.3.1. Diagnóstico e infraestructura 1-2 MESES

Se realizará un levantamiento de necesidades tecnológicas de acuerdo a las áreas de interés, se debe realizar una auditoría de la infraestructura tecnológica actual y determinar las limitaciones y las prioridades en cuanto a hardware software conectividad seguridad y otros factores involucrados dentro de la conformación de la parte tecnológica.

4.1.3.2. Digitalización de procesos clave 3-6 MESES

El mejoramiento del sistema ERP que maneja actualmente la institución y que permite integrar de manera óptima las ventas, inventario, adquisiciones y finanzas dentro del plano administrativo así también enfocaremos la digitalización del proceso de atención al cliente mediante un CRM, adicionalmente se buscará la automatización del área financiera para todo el conglomerado de reportes.

4.1.3.3. Capacitación y cultura digital 4-8 MESES

Se sugiere la implementación de un dashboard de indicadores clave ya sea en plataformas como power BI o Google data studio, esto deberá ir de la mano con las rutinas de revisión semanal y mensual de los KPIs.

4.1.3.4. Optimización y escalabilidad 10-12 MESES

Para una evaluación de impacto de todas las herramientas que se van a ir implementando a lo largo del plan estratégico y las que actualmente ya se están usando en pos

de realizar un ajuste y mejoras en concordancia con la retroalimentación en diferido que se realizan las juntas de la parte gerencial.

Y, por último, pero no menos importante se debe preparar el terreno para la integración de herramientas tecnológicas nuevas como la inteligencia artificial la automatización avanzada, entre otras.

4.1.3.5. Qué tipo de resultado podríamos esperar:

Cómo la reducción de proceso administrativo disminuiría a futuro en aproximadamente un 25 a 40%.

Se estima también una visibilidad del estado operativo, administrativo y financiero de la organización enfocado a la mejora continua.

Dentro de la calidad que recibe un cliente desde el momento de su ingreso hasta su atención se debe guiar por medio de automatizaciones y seguimientos estructurados conforme la complejidad de su requerimiento.

También se busca impulsar la generación de una cultura orientada hacia el manejo de datos y el mejoramiento dentro de sus actividades laborales diarias.

4.2. Verificación de controles.

Tabla 19

Verificación 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?*	*SI han definido su política empresarial dentro de sus estatutos y reglamentos como el de SSO que se socializa al ingreso y cada año.*	*Departamento TICs*	*17/5/2025*
ID_0002	*¿La política de seguridad de la información se revisa periódicamente?*	*SI existe una revisión que se la realiza anualmente y en este caso conforme la LOPDP fue actualizada de forma reciente.*	*Departamento TICs*	*17/5/2025*
ID_0003	*¿Se han definido las responsabilidades en materia de seguridad de la información?*	*SI se mantiene un registro de las personas encargadas en este caso el departamento de TIC´s.*	*Departamento TICs*	*17/5/2025*
ID_0004	*¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?*	*NO*		
ID_0005	*¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la organización? (Confidencialida*	*SI se aplican de manera uniforme para cualquier persona u organización por parte del departamento Legal.*	*Departamento de Talento Humano*	*17/5/2025*

	d, propiedad intelectual, etc.).			
ID_0006	*¿Se dispone de un inventario de activos?*	*SI de modo que aún no se encuentra completo ya que hemos detectado falencias.*	*Departamento de Talento Humano*	*17/5/2025*
ID_0007	*¿Se ha definido quien es el responsable de los activos?*	*SI el asistente de TTHH se encarga de dichos activos*	*Departamento Administrativo/Finenciero*	*17/5/2025*
ID_0008	*¿Se comprueban las referencias de todos los candidatos a empleo?*	*SI siempre y cuando se cuente con la autorización por parte del postulante.*	*Departamento de Talento Humano*	*17/5/2025*
ID_0009	*¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?*	*SI se encuentran en lugares a los que no pueden acceder normalmente los usuarios o personal administrativo -docentes.*	*Departamento Administrativo/Finenciero*	*17/5/2025*
ID_0010	*¿Los equipos TIC críticos de la organización están ubicados en salas de CPD?*	*NO*		
ID_0011	*¿Se han definido y documentado los procedimientos operacionales TIC?*	*NO*		

ID_0012	*¿Las copias se seguridad se realizan regularmente de acuerdo con la política de backup establecida?*	*SI de acuerdo con un cronograma que se encuentra en reestructuración por parte del departamento de TIC´s.*	*Departamento TICs*	*17/5/2025*
ID_0013	*¿Se verifica regularmente la correcta realización de las copias se seguridad?*	*SI acorde con los estándares ofrecidos por los prestadores de servicios.*	*Departamento TICs*	*17/5/2025*
ID_0014	*¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?.*	*SI por parte de TIC´s se realiza mensualmente un mantenimiento preventivo acompañado de su revisión.*	*Departamento TICs*	*17/5/2025*
ID_0015	*¿Se registran las actividades de los administradores y operadores de sistema?*	*NO*		
ID_0016	*¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?.*	*SI se encuentra especificado en la tabla de asignaciones de accesos y autorizaciones .*	*Departamento TICs*	*17/5/2025*
ID_0017	*¿Se ha definido, documentado e implantado un proceso formal para la*	*NO*		

	asignación de contraseñas?			
ID_0018	*¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?*	*SI constantese recomienda el cambio de clave cada 3-4 meses para mantener la seguridad de la información.*	*Departamento TICs*	*17/5/2025*
ID_0019	*¿Los usuarios se aseguran de proteger los equipos desatendidos? (Ej. bloqueando o cerrando la sesión?*	*SI con protectores de pantalla y cada oficina posee barreras físicas y vigilancia continua ya que son separaciones de vidrio.*	*Departamento TICs*	*17/5/2025*
ID_0020	*¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?*	*SI en cada ordenador o acceso a plataformas o páginas web educativas se cuenta con accesos personales.*	*Departamento TICs*	*17/5/2025*
ID_0021	*¿Se controla la instalación de software en sistemas en producción?*	*SI ya que todo programa debe contar con autorización tanto para descargo, ingreso y posterior instalación.*	*Departamento TICs*	*17/5/2025*
ID_0022	*¿Existe un proceso formal para la gestión*	*NO*		

	de las vulnerabilidades técnicas de los sistemas en uso?	
ID_0023	*¿Se ha definido, documentado e implantado un proceso formal para la gestión de los incidentes de seguridad?*	*NO*
ID_0024	*¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?*	*NO*
ID_0025	*¿Se han definido, documentado e implantado planes de continuidad de negocio?*	*NO*
ID_0026	*¿Los planes de continuidad de negocio se revisan y prueban formalmente?*	*NO*
ID_0027	*¿Todos los requisitos relevantes de carácter legal se mantienen identificados?*	*NO*
ID_0028	*¿Se han implementado procedimientos para asegurar el cumplimiento de los requisitos relevantes de carácter legal?*	*NO*

ID_0029	*¿Se han establecido e implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?*	*NO*		
ID_0030	*¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?*	*SI el departamento de TIC´s se encarga de forma trimestral o de acuerdo a las especificaciones técnicas brindadas por el proveedor.*	*Departamento TICs*	*17/5/2025*

Fuente: *Instituto Tecnológico Superior Compu Sur*

4.3. Inventario de activos.

Tabla 20

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	Servidores Sistema Académico	Sistema Académico virtual que gestiona procesos educativos.	Coordinador de Tecnologías Educativas	Servidor (físico)	Sala de CPD1	Sí
ID_0003	Servidores Sistema de Finanzas	Sistema para la gestión financiera institucional.	Director Financiero.	Servidor (físico)	Sala de CPD2	Sí

ID_0004	Servidores Software ofimático	Servidor que aloja software de ofimática usado por el personal.	Jefe de TI	Servidor (físico)	Sala de CPD1	No
ID_0005	Página web institucional	Portal web oficial con información institucional.	Responsable de Comunicaciones	Activo lógico	Alojamiento externo (hosting)	Sí
ID_0006	Plataforma de respaldos y almacenamiento de información	Sistema para respaldar y almacenar información crítica.	Administrador de Sistemas	Servidor (físico)	Sala de CPD2	Sí
ID_0007	Servicio de correo institucional	Plataforma de correo electrónico institucional.	Administrador de Sistemas	Activo lógico	Nube (proveedor externo)	Sí
ID_0008	Sistema Firewall	Sistema de protección perimetral de red.	Administrador de Seguridad de la Información	Dispositivo de red	Sala de CPD1	Sí
ID_0009	Sistema IDS/IPS	Sistema de detección y prevención de intrusos.	Administrador de Seguridad de la Información	Dispositivo de red	Sala de CPD1	Sí
ID_0010	Licencias de Antivirus (Kaspersky)	Sistema de protección contra software malicioso en estaciones y servidores.	Administrador de Seguridad de la Información	Activo lógico	Nube / Estaciones locales	Sí
ID_0011	Sistema de Gestión de Backups (Veeam Backup)	Plataforma de gestión, automatización y recuperación de copias de seguridad.	Administrador de Sistemas	Activo lógico	Sala de CPD2	Sí

ID_0012	Sistema de Control de Acceso	Sistema para gestión de acceso físico a instalaciones mediante credenciales electrónicas.	Jefe de Seguridad Física / TI	Dispositivo de red	Instalaciones físicas	Sí
ID_0013	Sistema de Grabación y Monitoreo de Cámaras	Sistema de videovigilancia para monitoreo y grabación de áreas institucionales.	Jefe de Seguridad Física	Dispositivo de red	Centro de Monitoreo / Sala de CPD	Sí
ID_0014	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Plataforma en línea para la administración académica, becas y contenidos educativos.	Coordinador de Tecnologías Educativas	Activo lógico	Nube / Sala de CPD	Sí
ID_0015	Herramientas de Teleconferencia (Zoom, Meet)	Herramientas para reuniones virtuales y colaboración remota.	Coordinador de TI	Activo lógico	Nube	No
ID_0016	VPN Institucional	Sistema de red privada virtual para acceso seguro a recursos internos.	Administrador de Seguridad de la Información	Activo lógico	Sala de CPD1 / Nube	Sí
ID_0017	Active Directory (Microsoft Server 2016)	Servicio de directorio para gestión de identidades, permisos y autenticación.	Administrador de Sistemas	Servidor (físico)	Sala de CPD1	Sí

ID_0018	Móvil(es)	Dispositivos móviles usados por personal institucional.	Jefe de TI	Dispositivo móvil	Institución / Remoto	No
ID_0019	Ordenadores e incluso algún servidor	Estaciones de trabajo y servidores de escritorio en uso.	Jefe de TI	Hardware	Oficinas / CPD	Sí
ID_0020	Dispositivos móviles con datos y apps	Móviles con acceso a apps corporativas y datos sensibles.	Jefe de TI	Dispositivo móvil	Uso personal/institucional	Sí
ID_0021	Ordenadores y conexión a Internet	Equipos de cómputo con acceso a red institucional o pública.	Jefe de TI	Hardware / Activo lógico	Oficinas	Sí
ID_0022	Dispositivos móviles para telefonía y datos	Dispositivos móviles para llamadas y acceso a datos móviles.	Jefe de TI	Dispositivo móvil	Uso externo	No
ID_0023	Herramientas comerciales de gestión	Aplicaciones empresariales (ERP, CRM, etc.)	Administrador de Sistemas	Activo lógico	Nube / CPD	Sí
ID_0024	Conexión a Internet con wifi	Infraestructura de red inalámbrica institucional.	Administrador de Redes	Dispositivo de red	Institución	Sí
ID_0025	Herramientas para empresas en la nube	Soluciones SaaS corporativas (Google Workspace, Microsoft 365).	Administrador de Sistemas	Activo lógico	Nube	Sí
ID_0026	E-administración	Plataformas gubernamentales o institucionale	Responsable Administrativo	Activo lógico	Nube	Sí

	s para trámites digitales.

Fuente: *Instituto Tecnológico Superior Compu Sur*

4.4.Análisis de Riesgos

Tabla 21

Análisis de riesgo

AMENAZAS / ACTIVOS	Ordenadores administrativos y de biblioteca	Terminales móviles	Conexión a Internet junto con wifi	Ordenadores y conexión a Internet	Dispositivos móviles para telefonía y datos	Soluciones tecnológicas	Página web	Ordenadores y servidores	Conexión a Internet con wifi	Dispositivos móviles con datos y apps	Herramienta(s) comercial(es) de gestión	Página web / tienda online y redes	Herramientas para empresas en la nube	E-administración para su relación con las AAPP
Fuego	Sí	Sí	No	Sí	Sí	No	No	Sí	No	Sí	No	No	No	No
Daños por agua	Sí	Sí	No	Sí	Sí	No	No	Sí	No	Sí	No	No	No	No
Desastres naturales	Sí	Sí	No	Sí	Sí	No	No	Sí	No	Sí	No	No	No	No
Fuga de información	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Introducción de falsa información	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Alteración de la información	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Corrupción de la información	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Destrucción de información	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Intercepción de información (escucha)	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Corte del suministro eléctrico	Sí	No	Sí	Sí	No	No	Sí	Sí	Sí	No	Sí	Sí	Sí	No
Condiciones inadecuadas de temperatura o humedad	Sí	Sí	No	Sí	Sí	No	No	Sí	No	Sí	No	No	No	No
Fallo de servicios de comunicaciones	Sí	No	Sí	Sí	No	No	Sí	Sí	Sí	No	Sí	Sí	Sí	No
Interrupción de otros servicios y suministros esenciales	Sí	No	Sí	Sí	No	No	Sí	Sí	Sí	No	Sí	Sí	Sí	No
Desastres industriales	Sí	Sí	No	Sí	Sí	No	No	Sí	No	Sí	No	No	No	No
Degradación de los soportes de almacenamiento de la información	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Difusión de software dañino	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Errores de mantenimiento / actualización de programas (software)	Sí	No	No	Sí	No	No	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Errores de mantenimiento / actualización de equipos (hardware)	Sí	No	No	Sí	No	No	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Caída del sistema por sobrecarga	Sí	No	Sí	Sí	No	No	Sí	Sí	Sí	No	Sí	Sí	Sí	No
Pérdida de equipos	Sí	Sí	No	Sí	Sí	No	No	Sí	No	Sí	No	No	No	No
Indisponibilidad del personal	No	No	No	No	No	No	Sí	No	No	No	Sí	Sí	Sí	Sí
Abuso de privilegios de acceso	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Acceso no autorizado	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Errores de los usuarios	Sí	No	No	Sí	No	No	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Errores del administrador	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Errores de configuración	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Denegación de servicio	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Robo	Sí	Sí	No	Sí	Sí	No	No	Sí	No	Sí	No	No	No	No
Extorsión	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Ingeniería social	No	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Fuente: *Instituto Tecnológico Superior Compu Sur*

4.5. Clasificación y Priorización.

Tabla 22

Evaluación de riesgos

Amenaza	Activo	Probabilidad	Impacto	Riesgo (P x I)	Color de Riesgo
Fuga de información	Sistema Académico Virtual (Moodle)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Sistema Académico Virtual (Moodle)	Medio (2)	Alto (3)	6	
Errores del administrador	Sistema Académico Virtual (Moodle)	Alto (3)	Alto (3)	9	
Denegación de servicio	Sistema Académico Virtual (Moodle)	Medio (2)	Alto (3)	6	
Robo	Sistema Académico Virtual (Moodle)	Medio (2)	Medio (2)	4	
Extorsión	Sistema Académico Virtual (Moodle)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Sistema Académico Virtual (Moodle)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Sistema Académico Virtual (Moodle)	Bajo (1)	Medio (2)	2	
Errores de configuración	Sistema Académico Virtual (Moodle)	Medio (2)	Medio (2)	4	
Fuga de información	Sistema de Finanzas (Microsoft Server 2016)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Sistema de Finanzas (Microsoft Server 2016)	Medio (2)	Alto (3)	6	
Errores del administrador	Sistema de Finanzas (Microsoft Server 2016)	Alto (3)	Alto (3)	9	
Denegación de servicio	Sistema de Finanzas (Microsoft Server 2016)	Medio (2)	Alto (3)	6	
Robo	Sistema de Finanzas (Microsoft Server 2016)	Medio (2)	Medio (2)	4	
Extorsión	Sistema de Finanzas (Microsoft Server 2016)	Medio (2)	Medio (2)	4	

Acceso no autorizado	Sistema de Finanzas (Microsoft Server 2016)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Sistema de Finanzas (Microsoft Server 2016)	Bajo (1)	Medio (2)	2	
Errores de configuración	Sistema de Finanzas (Microsoft Server 2016)	Medio (2)	Medio (2)	4	
Fuga de información	Página Web Institucional (SaaS contratado)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Página Web Institucional (SaaS contratado)	Medio (2)	Alto (3)	6	
Errores del administrador	Página Web Institucional (SaaS contratado)	Alto (3)	Alto (3)	9	
Denegación de servicio	Página Web Institucional (SaaS contratado)	Medio (2)	Alto (3)	6	
Robo	Página Web Institucional (SaaS contratado)	Medio (2)	Medio (2)	4	
Extorsión	Página Web Institucional (SaaS contratado)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Página Web Institucional (SaaS contratado)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Página Web Institucional (SaaS contratado)	Bajo (1)	Medio (2)	2	
Errores de configuración	Página Web Institucional (SaaS contratado)	Medio (2)	Medio (2)	4	
Fuga de información	Software Ofimático	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Software Ofimático	Medio (2)	Alto (3)	6	
Errores del administrador	Software Ofimático	Alto (3)	Alto (3)	9	
Denegación de servicio	Software Ofimático	Medio (2)	Alto (3)	6	
Robo	Software Ofimático	Medio (2)	Medio (2)	4	
Extorsión	Software Ofimático	Medio (2)	Medio (2)	4	
Acceso no autorizado	Software Ofimático	Alto (3)	Alto (3)	9	
Pérdida de equipos	Software Ofimático	Bajo (1)	Medio (2)	2	
Errores de configuración	Software Ofimático	Medio (2)	Medio (2)	4	

Fuga de información	Plataforma de Respaldos y Almacenamiento (SaaS / Microsoft)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Plataforma de Respaldos y Almacenamiento (SaaS / Microsoft)	Medio (2)	Alto (3)	6	
Errores del administrador	Plataforma de Respaldos y Almacenamiento (SaaS / Microsoft)	Alto (3)	Alto (3)	9	
Denegación de servicio	Plataforma de Respaldos y Almacenamiento (SaaS / Microsoft)	Medio (2)	Alto (3)	6	
Robo	Plataforma de Respaldos y Almacenamiento (SaaS / Microsoft)	Medio (2)	Medio (2)	4	
Extorsión	Plataforma de Respaldos y Almacenamiento (SaaS / Microsoft)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Plataforma de Respaldos y Almacenamiento (SaaS / Microsoft)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Plataforma de Respaldos y Almacenamiento (SaaS / Microsoft)	Bajo (1)	Medio (2)	2	
Errores de configuración	Plataforma de Respaldos y Almacenamiento (SaaS / Microsoft)	Medio (2)	Medio (2)	4	
Fuga de información	Servicio de Correo Institucional (SaaS Microsoft)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Servicio de Correo Institucional (SaaS Microsoft)	Medio (2)	Alto (3)	6	
Errores del administrador	Servicio de Correo Institucional (SaaS Microsoft)	Alto (3)	Alto (3)	9	
Denegación de servicio	Servicio de Correo Institucional (SaaS Microsoft)	Medio (2)	Alto (3)	6	

Robo	Servicio de Correo Institucional (SaaS Microsoft)	Medio (2)	Medio (2)	4	
Extorsión	Servicio de Correo Institucional (SaaS Microsoft)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Servicio de Correo Institucional (SaaS Microsoft)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Servicio de Correo Institucional (SaaS Microsoft)	Bajo (1)	Medio (2)	2	
Errores de configuración	Servicio de Correo Institucional (SaaS Microsoft)	Medio (2)	Medio (2)	4	
Fuga de información	Sistema Firewall (Sophos)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Sistema Firewall (Sophos)	Medio (2)	Alto (3)	6	
Errores del administrador	Sistema Firewall (Sophos)	Alto (3)	Alto (3)	9	
Denegación de servicio	Sistema Firewall (Sophos)	Medio (2)	Alto (3)	6	
Robo	Sistema Firewall (Sophos)	Medio (2)	Medio (2)	4	
Extorsión	Sistema Firewall (Sophos)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Sistema Firewall (Sophos)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Sistema Firewall (Sophos)	Bajo (1)	Medio (2)	2	
Errores de configuración	Sistema Firewall (Sophos)	Medio (2)	Medio (2)	4	
Fuga de información	Sistema IDS/IPS (Sophos)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Sistema IDS/IPS (Sophos)	Medio (2)	Alto (3)	6	
Errores del administrador	Sistema IDS/IPS (Sophos)	Alto (3)	Alto (3)	9	

Denegación de servicio	Sistema IDS/IPS (Sophos)	Medio (2)	Alto (3)	6	
Robo	Sistema IDS/IPS (Sophos)	Medio (2)	Medio (2)	4	
Extorsión	Sistema IDS/IPS (Sophos)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Sistema IDS/IPS (Sophos)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Sistema IDS/IPS (Sophos)	Bajo (1)	Medio (2)	2	
Errores de configuración	Sistema IDS/IPS (Sophos)	Medio (2)	Medio (2)	4	
Fuga de información	Licencias de Antivirus (Kaspersky)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Licencias de Antivirus (Kaspersky)	Medio (2)	Alto (3)	6	
Errores del administrador	Licencias de Antivirus (Kaspersky)	Alto (3)	Alto (3)	9	
Denegación de servicio	Licencias de Antivirus (Kaspersky)	Medio (2)	Alto (3)	6	
Robo	Licencias de Antivirus (Kaspersky)	Medio (2)	Medio (2)	4	
Extorsión	Licencias de Antivirus (Kaspersky)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Licencias de Antivirus (Kaspersky)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Licencias de Antivirus (Kaspersky)	Bajo (1)	Medio (2)	2	
Errores de configuración	Licencias de Antivirus (Kaspersky)	Medio (2)	Medio (2)	4	
Fuga de información	Sistema de Gestión de Backups (Veeam Backup)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Sistema de Gestión de Backups (Veeam Backup)	Medio (2)	Alto (3)	6	
Errores del administrador	Sistema de Gestión de Backups (Veeam Backup)	Alto (3)	Alto (3)	9	
Denegación de servicio	Sistema de Gestión de Backups (Veeam Backup)	Medio (2)	Alto (3)	6	

Robo	Sistema de Gestión de Backups (Veeam Backup)	Medio (2)	Medio (2)	4	
Extorsión	Sistema de Gestión de Backups (Veeam Backup)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Sistema de Gestión de Backups (Veeam Backup)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Sistema de Gestión de Backups (Veeam Backup)	Bajo (1)	Medio (2)	2	
Errores de configuración	Sistema de Gestión de Backups (Veeam Backup)	Medio (2)	Medio (2)	4	
Fuga de información	Sistema de Control de Acceso	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Sistema de Control de Acceso	Medio (2)	Alto (3)	6	
Errores del administrador	Sistema de Control de Acceso	Alto (3)	Alto (3)	9	
Denegación de servicio	Sistema de Control de Acceso	Medio (2)	Alto (3)	6	
Robo	Sistema de Control de Acceso	Medio (2)	Medio (2)	4	
Extorsión	Sistema de Control de Acceso	Medio (2)	Medio (2)	4	
Acceso no autorizado	Sistema de Control de Acceso	Alto (3)	Alto (3)	9	
Pérdida de equipos	Sistema de Control de Acceso	Bajo (1)	Medio (2)	2	
Errores de configuración	Sistema de Control de Acceso	Medio (2)	Medio (2)	4	
Fuga de información	Sistema de Grabación y Monitoreo de Cámaras	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Sistema de Grabación y Monitoreo de Cámaras	Medio (2)	Alto (3)	6	
Errores del administrador	Sistema de Grabación y Monitoreo de Cámaras	Alto (3)	Alto (3)	9	

Denegación de servicio	Sistema de Grabación y Monitoreo de Cámaras	Medio (2)	Alto (3)	6	
Robo	Sistema de Grabación y Monitoreo de Cámaras	Medio (2)	Medio (2)	4	
Extorsión	Sistema de Grabación y Monitoreo de Cámaras	Medio (2)	Medio (2)	4	
Acceso no autorizado	Sistema de Grabación y Monitoreo de Cámaras	Alto (3)	Alto (3)	9	
Pérdida de equipos	Sistema de Grabación y Monitoreo de Cámaras	Bajo (1)	Medio (2)	2	
Errores de configuración	Sistema de Grabación y Monitoreo de Cámaras	Medio (2)	Medio (2)	4	
Fuga de información	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Medio (2)	Alto (3)	6	
Errores del administrador	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Alto (3)	Alto (3)	9	
Denegación de servicio	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Medio (2)	Alto (3)	6	
Robo	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Medio (2)	Medio (2)	4	
Extorsión	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Bajo (1)	Medio (2)	2	
Errores de configuración	Sistema de Gestión Académica y Plataforma Educativa (BECAS TEC)	Medio (2)	Medio (2)	4	
Fuga de información	Herramientas de Teleconferencia (Zoom, Meet)	Alto (3)	Alto (3)	9	

Fallo de servicios de comunicaciones	Herramientas de Teleconferencia (Zoom, Meet)	Medio (2)	Alto (3)	6	
Errores del administrador	Herramientas de Teleconferencia (Zoom, Meet)	Alto (3)	Alto (3)	9	
Denegación de servicio	Herramientas de Teleconferencia (Zoom, Meet)	Medio (2)	Alto (3)	6	
Robo	Herramientas de Teleconferencia (Zoom, Meet)	Medio (2)	Medio (2)	4	
Extorsión	Herramientas de Teleconferencia (Zoom, Meet)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Herramientas de Teleconferencia (Zoom, Meet)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Herramientas de Teleconferencia (Zoom, Meet)	Bajo (1)	Medio (2)	2	
Errores de configuración	Herramientas de Teleconferencia (Zoom, Meet)	Medio (2)	Medio (2)	4	
Fuga de información	VPN Institucional	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	VPN Institucional	Medio (2)	Alto (3)	6	
Errores del administrador	VPN Institucional	Alto (3)	Alto (3)	9	
Denegación de servicio	VPN Institucional	Medio (2)	Alto (3)	6	
Robo	VPN Institucional	Medio (2)	Medio (2)	4	
Extorsión	VPN Institucional	Medio (2)	Medio (2)	4	
Acceso no autorizado	VPN Institucional	Alto (3)	Alto (3)	9	
Pérdida de equipos	VPN Institucional	Bajo (1)	Medio (2)	2	
Errores de configuración	VPN Institucional	Medio (2)	Medio (2)	4	
Fuga de información	Active Directory (Microsoft Server 2016)	Alto (3)	Alto (3)	9	
Fallo de servicios de comunicaciones	Active Directory (Microsoft Server 2016)	Medio (2)	Alto (3)	6	
Errores del administrador	Active Directory (Microsoft Server 2016)	Alto (3)	Alto (3)	9	

Denegación de servicio	Active Directory (Microsoft Server 2016)	Medio (2)	Alto (3)	6	
Robo	Active Directory (Microsoft Server 2016)	Medio (2)	Medio (2)	4	
Extorsión	Active Directory (Microsoft Server 2016)	Medio (2)	Medio (2)	4	
Acceso no autorizado	Active Directory (Microsoft Server 2016)	Alto (3)	Alto (3)	9	
Pérdida de equipos	Active Directory (Microsoft Server 2016)	Bajo (1)	Medio (2)	2	
Errores de configuración	Active Directory (Microsoft Server 2016)	Medio (2)	Medio (2)	4	
Fuego	móvil(es)	Medio (2)	Medio (2)	4	
Fuego	ordenadores e incluso algún servidor	Medio (2)	Alto (3)	6	
Fuego	dispositivos móviles con datos y apps	Bajo (1)	Medio (2)	2	
Daños por agua	ordenadores y conexión a Internet	Medio (2)	Alto (3)	6	
Daños por agua	ordenadores e incluso algún servidor	Medio (2)	Alto (3)	6	
Daños por agua	dispositivos móviles con datos y apps	Bajo (1)	Medio (2)	2	
Fuga de información	dispositivos móviles para telefonía y datos	Alto (3)	Alto (3)	9	
Fuga de información	una página web sencilla	Medio (2)	Alto (3)	6	
Fuga de información	ordenadores e incluso algún servidor	Alto (3)	Alto (3)	9	
Fuga de información	dispositivos móviles con datos y apps	Alto (3)	Alto (3)	9	
Fuga de información	herramientas comerciales de gestión	Alto (3)	Alto (3)	9	
Fuga de información	página web / tienda online y redes	Alto (3)	Alto (3)	9	
Fuga de información	herramientas para empresas en la nube	Alto (3)	Alto (3)	9	
Fuga de información	e-administración	Alto (3)	Alto (3)	9	
Corte del suministro eléctrico	ordenadores y conexión a Internet	Medio (2)	Alto (3)	6	
Corte del suministro eléctrico	ordenadores e incluso algún servidor	Medio (2)	Alto (3)	6	

Corte del suministro eléctrico	conexión a Internet con wifi	Medio (2)	Alto (3)	6	
Corte del suministro eléctrico	herramientas comerciales de gestión	Bajo (1)	Alto (3)	3	
Corte del suministro eléctrico	página web / tienda online y redes	Bajo (1)	Alto (3)	3	
Corte del suministro eléctrico	herramientas para empresas en la nube	Bajo (1)	Alto (3)	3	

Fuente: *Instituto Tecnológico Superior Compu Sur*

Tabla 23

Registro, clasificación y priorización de iniciativas

REGISTRO, CLASIFICACIÓN Y PRIORIZACIÓN DE INICIATIVAS

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión
IN_0001	Fuga de información.	Controlar el acceso a los datos, utilizar software de prevención de pérdida de datos (DLP), actualizar los sistemas y software regularmente, mantener copias de seguridad y capacitar a los empleados en seguridad informática	Responsable de seguridad	Organizativa	1000,00 $	1 mes	3 meses
IN_0002	Fallo de servicios de comunicaciones	Realizar revisiones periódicas de equipos, software y hardware para detectar y solucionar problemas antes de que causen fallos.	Responsable de comunicaciones .	Técnica	800,00 $	2 meses	2 mes

IN_0003	Errores del administrador	Simplificar y estandarizar los procesos administrativos ayuda a reducir la complejidad y, por lo tanto, el riesgo de errores.	Departamento administrativo	Organizativa	1500,00 $	1 mes	2 meses
IN_0004	Denegación de servicio.	La implementación de sistemas de seguridad como firewalls y sistemas de detección de intrusiones, la utilización de redes de entrega de contenido (CDNs) y la configuración de la infraestructura para soportar picos de tráfico.	Departamento TICs	Técnica	500,00 $	2 meses	3 meses
IN_0005	Acceso no autorizado	La implementación de políticas de contraseñas seguras, el uso de autenticación multifactor y actualizaciones periódicas de software para corregir vulnerabilidades	Departamento TICs	Técnica	1000,00 $	1 mes	0 2 meses
IN_0006	Fuego	Mantener la instalación eléctrica en buen estado, evitar sobrecarga en los contactos, no usar cables dañados y tener cuidado con materiales inflamables.	Departamento TICs	Técnica	1000,00 $	2 meses	3 meses
IN_0007	Daños por agua	Inspeccionar regularmente las areas propensas a filtrado sellando las entradas y salidas de agua, y el uso de sensores de agua.	Departamento TICs	Técnica	900,00 $	1 mese	3 meses

IN_0008	Corte del suministro eléctrico	Utilizar dispositivos de protección con sistema de Alimentación Ininterrumpida (SAI) o UPS (Uninterruptible Power Supply) es esencial para proporcionar energía de respaldo durante un corte, permitiendo guardar datos y apagar la computadora de forma segura	Departamento TICs	Técnica	700,00 $	2 mese	3 meses

Fuente: *Instituto Tecnológico Superior Compu Sur*

4.6. Check List PDS.

Tabla 24

Check list

NIVEL	ALCANCE	CONTROL	
A	PRO	**Analizar la situación actual de la empresa,** Analizas detalladamente la situación actual de la empresa para poder acometer un Plan Director de Seguridad.	X
A	PRO	**Alinear el PDS con la estrategia de la empresa.** Tienes en cuenta la estrategia empresarial en su conjunto a la hora de diseñar el Plan Director de Seguridad.	X
A	PRO	**Definir los proyectos a ejecutar.** Estableces y defines en detalle las acciones concretas para alcanzar los niveles de seguridad deseados.	X
A	PRO	**Clasificar y priorizar los proyectos.** Agrupas y clasificas las acciones a ejecutar con el fin de priorizar aquellas que nos proporcionen mayores beneficios en relación a su coste.	X
B	PRO	**Aprobar el PDS.** Apruebas y publicas la versión definitiva del PDS.	

A	PRO	**Ejecución del PDS** Pones en marcha los proyectos acordados para alcanzar los objetivos de ciberseguridad definidos.
A	PRO	**Certificación en seguridad.** Consideras la implantación de un proceso de certificación que acredite el sistema de gestión de la seguridad de tu empresa

Fuente: *Instituto Tecnológico Superior Compu Sur*

Una vez que se ha realizado un análisis exhaustivo de los activos de la empresa, las amenazas que se presentan dentro y fuera de ella, las afectaciones que podrían tener los activos frente a estas amenazas y la evaluación de riesgos de la empresa, nos ayudaron para determinar los proyectos y acciones a realizar dentro del Plan Director de Seguridad.

El Plan Director de Seguridad se consolidará gracias a la clasificación de los proyectos con el fin de priorizar aquellas actividades que nos proporcionen mayores beneficios en relación a su coste. La empresa logrará reducir los riesgos a los que está expuesta hasta unos niveles aceptables, garantizando la continuidad del negocio

Capítulo 5

Propuesta de implementación de un sistema de gestión basado en la norma ISO 31000:2018 en el Instituto Superior Tecnológico Compu Sur sede matriz.

5.1. Objeto y campo de aplicación

Este manual tiene como objeto establecer un modelo de gestión del riesgo basado en la norma ISO 31000:2018, con el objetivo de su implementación en el Instituto Tecnológico Superior Compu Sur (ITECSUR), con énfasis en la protección de datos personales, seguridad de la información, y continuidad operativa.

Los objetivos específicos complementarios son:

- Documentar un sistema de gestión de riesgos para la identificación, análisis y evaluación de los riesgos relacionados con el tratamiento de datos personales e infraestructuras tecnológicas críticas en ITECSUR.
- Documentar medidas de tratamiento del riesgo que fortalezcan los controles técnicos, administrativos y legales existentes, asegurando la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento con la Ley Orgánica de Protección de Datos Personales (LOPDP) para el instituto educativo.

El alcance del sistema de gestión de riesgos aplica para los procesos de tratamiento de información académica de los estudiantes en la infraestructura tecnológica del instituto, considerando: la recopilación, registro, almacenamiento, uso, transmisión, modificación, conservación y eliminación de datos académicos de los estudiantes del Instituto Tecnológico Superior Compu Sur (ITECSUR), desde su ingreso hasta su egreso institucional. Se incluye

como parte del tratamiento de información registros como: historial académico, calificaciones, matrículas, asistencia, asignaturas cursadas, observaciones pedagógicas, procesos de evaluación, prácticas preprofesionales y proyectos de titulación.

5.2. Referencias Normativas

Este manual toma como referencia los siguientes marcos:

- Norma ISO 31000:2018 – Gestión del riesgo. Principios y directrices.
- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27701:2019 – Gestión de la privacidad de la información.
- Reglamento de Protección de Datos Institucional de ITECSUR.
- Adicionalmente el manual considera la evaluación de cumplimiento de los siguientes reglamentos de cumplimiento obligatorios del instituto:
- Constitución de la República del Ecuador.
- Código Orgánico Administrativo (COA).
- Ley de Seguridad Social.
- Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP).
- Reglamento de la LOPDP.
- Normas técnicas de ciberseguridad del Ministerio de Telecomunicaciones
- Ley Orgánica de Educación Superior (LOES).
- Ley Orgánica de Educación Intercultural (LOEI).
- Código de Trabajo.
- Normativa Técnica del MINTEL (Ministerio de Telecomunicaciones).

- Reglamentos del Consejo de Educación Superior (CES).
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

5.3. Términos y definiciones

Los términos y definiciones adoptados de la norma ISO 31000:2018 y aplicables al proyecto son:

- **Riesgo:** efecto de incertidumbre sobre los objetivos.
- **Administración/gestión de riesgos:** actividades coordinadas para dirigir y controlar la organización con relación a los riesgos.
- **Parte interesada:** persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.
- **Fuente de riesgos:** elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.
- **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias.
- **Consecuencia:** resultado de un evento que afecta a los objetivos.
- **Probabilidad:** posibilidad de que algo suceda.
- **Control:** medida que mantiene y/o modifica un riesgo.

5.4. Principios

5.4.1. Integrada

La gestión del riesgo en el Instituto Tecnológico Superior Compu Sur (ITECSUR) se tomará como una práctica transversal a todos los procesos institucionales, con un enfoque principal en aquellos relacionados con el tratamiento de información académica del alcance

del sistema y a sus procesos de apoyo. Este enfoque responde al principio fundamental de la norma ISO 31000:2018 que establece que la gestión del riesgo debe estar integrada en todas las estructuras, operaciones y decisiones de la organización.

5.4.1.1. Cultura de conciencia de riesgo

Uno de los elementos clave para la integración efectiva del sistema de gestión es la concienciación, comunicación y capacitación del equipo directivo sobre la importancia de identificar, evaluar y mitigar los riesgos en todas las etapas del ciclo académico. Los directivos de ITECSUR han demostrado un compromiso activo con el fortalecimiento de las capacidades institucionales, promoviendo una cultura orientada a la prevención y la mejora continua. Esta cultura se fomentará mediante la planificación de campañas de comunicación, talleres de capacitaciones específicos y reuniones periódicas de revisión de riesgos.

5.4.1.2. Procesos integrados

La gestión del riesgo será incorporada en los procesos académicos como parte de su estructura y documentación. Adicionalmente la toma de decisiones se ejecutará bajo metodologías que respondan a la gestión de riesgos y apetitos definidos por las autoridades de la institución.

5.4.1.3.Responsabilidad compartida

La implementación del sistema de gestión del riesgo no es responsabilidad exclusiva de un área o equipo, sino que se establece como un objetivo compartido por las partes interesadas del instituto. Para ello se han definido los siguientes roles y responsabilidades:

Tabla 25

Roles y Responsabilidades

Rol / Cargo	Responsabilidad en la gestión de riesgos
Rector y Vicerrector Académico	Revisar y validar las políticas institucionales y aprobar planes de tratamiento del riesgo según su apetito.
Coordinador de TI / Seguridad de la Información	Desarrollar las políticas e implementar los controles técnicos, monitoreo y respaldo de sistemas críticos, según aplique.
Coordinadores de carrera y Directores Académicos	Identificar riesgos en el ciclo académico y aplicar medidas correctivas en su ámbito.
Docentes	Garantizar el adecuado manejo de la información académica de los estudiantes.
Personal Administrativo	Cumplir con los procedimientos establecidos para el tratamiento seguro de la información.
Área de Bienestar Estudiantil	Gestionar con confidencialidad los datos sensibles de estudiantes.

Fuente: *Instituto Tecnológico Superior Compu Sur*

5.4.1.4. Apoyo de los sistemas de información

Para facilitar la integración del modelo, ITECSUR dispone de una infraestructura tecnológica que aporta al sistema de gestión. Se han implementado sistemas internacionales de calidad como: el Sistema Académico Virtual (Moodle), la plataforma de gestión de becas y titulación, los repositorios documentales y las plataformas de respaldo y correo institucional.

5.4.2. Estructurada y exhaustiva

La gestión del riesgo en ITECSUR se implementará para seguir un enfoque estructurado y exhaustivo, lo que permite que los resultados obtenidos sean coherentes, repetibles y comparables a lo largo del tiempo y entre diferentes procesos institucionales. Para su enfoque se establecen las siguientes etapas de gestión.

5.4.2.1. Identificación del riesgo

Se realizará un levantamiento y clasificación de los activos de información críticos para los procesos del alcance y la identificación de posibles eventos que puedan afectar negativamente el cumplimiento de los objetivos institucionales. En esta fase se consideran:

- Riesgos tecnológicos (fallas en plataformas académicas, ataques informáticos,

indisponibilidad de sistemas).

- Riesgos legales (incumplimientos de la LOPDP, uso indebido de datos).
- Riesgos operacionales (errores en la gestión académica, accesos no autorizados, fuga de información).
- Riesgos reputacionales (filtración de datos sensibles, fallos en la atención al estudiante).

5.4.2.2. Apoyo de los sistemas de información

Para facilitar la integración del modelo, ITECSUR dispone de una infraestructura tecnológica que aporta al sistema de gestión. Se han implementado sistemas internacionales de calidad como: el Sistema Académico Virtual (Moodle), la plataforma de gestión de becas y titulación, los repositorios documentales y las plataformas de respaldo y correo institucional.

5.4.2.3. Monitoreo y revisión

La gestión del riesgo es un proceso dinámico y continuo para lo cual se debe establecer mecanismos de verificación de planes de acción y la identificación de nuevos riesgos o cambios existentes para los ajustes respectivos. Se deben establecer revisiones semestrales o ante cambios significativos con la generación de actas sobre la toma de decisión al Comité respectivo.

5.4.3. Adaptativa

El sistema de gestión del instituto se establecerá como sistema adaptativo, es decir, capaz de cambiar y responder de forma ágil a los nuevos paradigmas del entorno operativo, tecnológico, normativo y social que afectan a su funcionamiento académico y administrativo.

Las herramientas a utilizar serán el establecimiento de monitoreo anuales de cambios significativos en los entornos operativos institucionales relacionados a la normativa educativa

y de los marcos normativos nacionales e internacionales aplicables al instituto. Adicionalmente se establecerán revisiones semestrales del cumplimiento o actualización de objetivos estratégicos a través de indicadores establecidos y un análisis FODA.

5.4.4. Inclusiva

La gestión del riesgo en ITECSUR se enfocará en el principio de inclusividad, lo que implica la participación activa de las partes interesadas internas y externas. Como paso inicial se identificarán a las partes interesadas y sus requerimientos operativos o legales que debe dar cumplimiento el sistema de gestión. Adicionalmente se establecerán los responsables y canales de comunicación oficiales para cada parte interesa que permitirá una correcta inclusión.

5.4.5. Dinámica

El enfoque dinámico del sistema preparará a los procesos de gestión a la adaptación en el tiempo para responder a cambios en el entorno operativo y ajustes a nuevos paradigmas. Para la gestión se establecerán procesos de control de cambios que permitan la identificación temprana de nuevos escenarios de riesgos antes no identificados. Adicionalmente se establecerá un principio equilibrado de maestro de documentación que asegure que la información le pertenezca al instituto y no a las personas.

5.4.6. Mejor información disponible

El sistema de gestión tomará en cuenta que la información para la toma de decisiones sea la más pertinente, confiable, actualizada y útil. Para asegurar la mejor información disponible, se toma en cuenta:

- Obtención de información histórica.

- Información actualizada.
- Proyecciones y expectativas futuras.

Para el desarrollo de información se asignarán responsables según aplique y se garantizará la disponibilidad de la información a quien se requiera.

5.4.7. Factores humanos y culturales

Uno de los pilares fundamentales de la implementación del sistema son los factores humanos y culturales para la gestión del riesgo, en ese sentido el instituto tiene identificados las posibilidades de errores humanos, la resistencia al cambio, falta de compromiso o la baja conciencia del personal al riesgo, para ello se establecerán mecanismos como:

- Cultura de apertura y participación: Se establecerá una cultura de confianza para el personal y las partes interesadas de manera que los usuarios del sistema se sientan habilitados para comunicar preocupaciones, incidentes o debilidades que consideren desde su punto de vista y experiencia en la gestión de riesgos o implementación de planes de acción.
- Formación innovadora y adaptativa: Se establecerá niveles de formación y capacitación para el personal y partes interesadas considerando que cada grupo de trabajo tiene diferentes medios para la captación de su atención. Principalmente se deberá establecer mecanismos de formación para personal administrativo, personal operativo-académico y autoridades para llegar con escenarios y ejemplos de riesgo personalizados. Adicionales los mecanismos de aprendizaje se enfocarán en talleres prácticos y complementos de presentaciones teóricas.

- Liderazgo empático y comprometido: Para la implementación del sistema de gestión se reforzará al personal el compromiso de las autoridades con la implementación del sistema de gestión a través de su participación y acompañamiento. Adicionalmente a abrir espacios de escucha activa ante las inquietudes que surjan en la implementación del sistema, controles o planes de acción que surjan de su ejecución.

5.4.8. Mejora continua

Se establece el ciclo PDCA (Planificar-Hacer-Verificar-Actuar) para revisar la implementación del modelo ISO 31000. Los mecanismos en las etapas de verificación y mejora continua se establecerán considerando:

- Establecer un ejercicio anual de auditoría interna con personal independiente al sistema de gestión o una auditoría externa del sistema de gestión.
- Establecer ejercicios semestrales de revisión por las autoridades para conocer el avance de implementación y operación del sistema de gestión.
- Establecer procedimiento de cumplimiento para las políticas y procesos del alcance del sistema para su revisión anual por la primera línea.

5.5. Marco de referencia

5.5.1. Generalidades

El marco de referencia establecerá las bases para la implementación del sistema de gestión de riesgos en el instituto ITECSUR, asegurando que se integre a todos los procesos organizacionales.

Para asegurar la implementación del sistema, los procesos de gestión del riesgo se alinean con los objetivos estratégicos institucionales definidos en el artículo 8 de su normativa interna y con las estrategias operativas del artículo 10, promoviendo una cultura organizacional.

Para el establecimiento del marco de referencia, los principios que orientan la implementación del sistema de gestión de riesgos son:

- Integración transversal: La gestión de riesgo deberá estar presentes en todas las áreas y niveles del instituto. Considerando los procesos críticos como los procesos de apoyo.
- Adaptabilidad: El sistema deberá responder a las necesidades presentes y futuras del instituto, apoyando su capacidad de anticipación y resiliencia.
- Inclusividad: La implementación del sistema deberá considerar la participación de todas las partes interesadas identificadas.
- Dinamismo y mejora continua: El sistema deberá evolucionar y mejorar a través de procesos de autoevaluación, retroalimentación y aprendizaje institucional.
- Ética, valores y derechos humanos: La gestión del riesgo deberá promover el respeto a los principios fundamentales del pluralismo, la equidad y la cultura democrática como foco central del instituto.

Las siguientes políticas se establecerán para asegurar la implementación del sistema de gestión. Las políticas se encuentran alineados al cumplimiento de objetivos institucionales y estrategias definidas por el instituto.

Tabla 26

Políticas, Objetivos y Estrategias

Política	Objetivos institucionales y estrategias
La implementación del sistema de gestión de riesgos se basa en los principios establecidos en la norma ISO 31000 y sus principios de integración, estructuración, personalización, dinamismo y participación.	(OB 2) Fomentar el espíritu científico y la actualización permanente con una visión estratégica que responda a la educación superior basada en los más altos estándares nacionales e internacionales.
El Rectorado y las autoridades del instituto se comprometen a la implementación del sistema de gestión de riesgos garantizando su respaldo para la implementación, mantenimiento y mejora continua del marco de gestión para dar cumplimiento a las normativas vigentes.	(E 7) Adaptabilidad a las necesidades presentes y futuras.
Integrar la gestión de riesgos en la planificación y ejecución de proyectos de investigación y vinculación, así como en los procesos transversalmente en la organización.	(E 10) Gestión de proyectos de investigación, innovación, desarrollo y vinculación con la sociedad que promuevan el desarrollo de la matriz productiva, la prestación de servicios de calidad, la preservación del medio ambiente, la recuperación efectiva ante desastres naturales o antrópicos y otros que coadyuven a la solución de problemas que afecten las comunidades.
Fomentar una cultura de prevención, resiliencia y responsabilidad compartida a su personal y estudiantes orientada a la gestión de riesgos.	(OB 1) Formar profesionales cualificados y socialmente responsables, capaces de adaptarse a las necesidades actuales y futuras de la sociedad.

Fuente: *Instituto Tecnológico Superior Compu Sur*

5.5.2. Liderazgo y compromiso

El liderazgo y compromiso institucional son esenciales para el éxito del sistema de gestión de riesgos en el Instituto Tecnológico Superior Compu Sur (ITECSUR), para ello las

autoridades del instituto, en conjunto con los líderes académicos y administrativos deben participar en la promoción, comunicación, respaldo e implementación de la gestión del riesgo como parte integral de la cultura organizacional.

Para asegurar el liderazgo y compromiso en la implementación del sistema se establece los siguientes lineamientos asociados al sistema de gestión.

5.5.3. Integración

La integración de la gestión de riesgos en ITECSUR constituye un objetivo principal para asegurar su eficacia, sostenibilidad y alineación con los objetivos institucionales. De acuerdo con la norma ISO 31000:2018, la gestión del riesgo no debe ser una actividad aislada o reactiva, sino un proceso transversal, continuo y coherente, presente en todas las áreas, niveles y decisiones del instituto.

ITECSUR incorporará la gestión del riesgo en sus procesos institucionales desde la planificación estratégica y la formulación de políticas institucionales, hasta las actividades diarias que se desarrollan en los procesos académicos, administrativos, tecnológicos, investigativos y de vinculación con la sociedad.

La cultura y procesos de la gestión de riesgos será parte integral de los siguientes procesos y actividades institucionales:

- Planificación Estratégica: La gestión de riesgos se integrará para dar cumplimiento a los objetivos de largo plazo, la sostenibilidad del modelo educativo, la transformación digital, la gobernanza institucional y el cumplimiento normativo.

- La planificación operativa anual: La gestión de riesgos se integrará para la identificación y evaluación de riesgos operativos en la ejecución de proyectos, uso de recursos, programas académicos, procesos de evaluación y control interno.
- La gestión de proyectos y actividades específicas: La gestión de riesgos se integrará en la implementación de nuevas iniciativas o proyectos que contemple sus impactos potenciales, beneficiarios, responsables y medidas de mitigación.
- La toma de decisiones diaria: La gestión de riesgos se integrará a través de la cultura en los responsables de procesos para que consideren variables de riesgo al autorizar compras, implementar nuevas herramientas digitales, manejar datos personales, contratar servicios o gestionar reclamos.

Este enfoque permite que la gestión del riesgo no dependa exclusivamente de un equipo de gestión, sino que se convierta en una responsabilidad compartida por toda la comunidad educativa.

Para que esta integración sea efectiva se requiere generar un proceso de capacitación y cultura en el instituto, considerando:

- Capacitaciones periódicas sobre la norma ISO 31000: Se establecerá un plan de capacitación anual para los diferentes niveles de autoridades, personal y comunidad educativa para el refuerzo de conceptos de riesgo, controles, medidas preventivas y protocolos institucionales.
- Sesiones de concientización y sensibilización: Se establecerán sesiones para

docentes, personal administrativo y estudiantes sobre cómo sus decisiones cotidianas pueden generar, reducir o trasladar riesgos relacionados a cumplimiento normativas, buenas prácticas y manejo de datos personales.

- Guías y manuales operativos: Se establecerá una cultura de documentación del conocimiento que incluyan criterios de gestión del riesgo aplicados a procesos específicos (ej. manejo de datos, uso de plataformas, atención al usuario).
- Ejercicios prácticos o simulacros: Se establecerá los espacios para mejora continua con la simulación de escenarios de crisis especialmente en temas relacionados con ciberseguridad, continuidad operativa y protección de información.

5.5.4. Diseño

En el marco de la implementación de la gestión de riesgos bajo la norma ISO 31000:2018, lo que constituye como diseño es una etapa fundamental para organizar que dicho proceso se adapte de una manera efectiva dentro de la estructura, la cultura organizacional y los objetivos estratégicos que posee el ITECSUR. Dentro de este apartado se aborda la forma en la que se van a estructurar ciertos elementos clave dentro del sistema de gestión del riesgo, asegurando su alineación con la misión educativa, la mejora continua de la calidad académica y la sostenibilidad institucional.

En el transcurso de esta fase se establecerán los componentes procesos recursos responsabilidades y mecanismos de integración que son básicos y fundamentales para que la gestión del riesgo se convierte en una práctica transversal y sistemática en la organización.

En lo que respecta a un diseño bien estructurado va a permitir a dicha institución el anticiparse a posibles eventos que puedan afectar la continuidad académica la seguridad de la comunidad educativa la reputación institucional Y el cumplimiento de los objetivos estratégicos lo que fortalecerá su capacidad de resistencia frente a contextos cambiantes y desafíos emergentes.

5.5.4.1.Comprensión de la organización y su contexto

Para implementar una gestión de riesgos es importante comprender a fondo el contexto en el que opera la institución. Este análisis permite identificar los factores que pueden influir positiva o negativamente en la capacidad del instituto para alcanzar sus objetivos estratégicos y operativos, y establecer los criterios adecuados para la identificación, evaluación y tratamiento del riesgo.

A continuación, se presenta un análisis FODA aplicado al contexto operativo de ITECSUR para identificar factores relevantes que influyen en su sistema de gestión de riesgos:

Tabla 27

Análisis FODA

Fortalezas	**Oportunidades**
- Compromiso institucional con la calidad educativa y la innovación. - Cultura organizacional orientada a valores y derechos humanos. - Procesos académicos estructurados y programas con pertinencia regional. - Implementación de procesos de autoevaluación y mejora continua.	- Avances tecnológicos aplicables al entorno académico. - Vinculación creciente con el sector productivo y entidades públicas. - Reformas normativas que promueven la protección de datos y la ciberseguridad. - Acceso a programas de capacitación docente y redes educativas.
Debilidades	**Amenazas**

- Recursos limitados para la actualización tecnológica de última generación. - Brechas en la capacitación continua del personal sobre gestión del riesgo. - Dependencia de proveedores tecnológicos externos y/o extranjeros. - Escasa cultura de reporte de incidentes o vulnerabilidades.	- Amenazas cibernéticas a la infraestructura digital educativa. - Cambios normativos que exigen rápida adaptación institucional. - Riesgos asociados a desastres naturales o interrupciones del servicio. - Presiones sociales, económicas o políticas que afectan la estabilidad.

Fuente: *Instituto Tecnológico Superior Compu Sur*

Otro enfoque principal para la comprensión del instituto es la definición de su propósito definido como: La formación de profesionales cualificados, socialmente responsables y adaptables, mediante un modelo educativo inclusivo, orientado a la innovación, la justicia social y el desarrollo sostenible. Este propósito se articula con su compromiso con los derechos humanos, la diversidad cultural, la paz, la democracia y la vinculación con la sociedad, guiando su estrategia académica, tecnológica y de gestión.

Para la correcta comprensión del instituto se debe tener en cuenta a las partes interesadas que influyen o son influenciadas por el sistema de gestión del riesgo en ITECSUR, considerando:

- Estudiantes: Son los principales beneficiarios de un entorno educativo seguro, inclusivo y tecnológicamente confiable.
- Docentes: Son los actores clave en la implementación de medidas y buenas prácticas de seguridad y gestión de riesgos. Adicionalmente de ser eje principal en la operación institucional académica.

- Personal administrativo: Son los responsables de la ejecución de procesos críticos para la gestión de datos personales, matrículas, procesos de talento humano y administración de la tecnología.
- Autoridades institucionales: Son los encargados del liderazgo estratégico, la toma de decisiones y asignación de recursos.
- Entes reguladores (CES, CACES, SENESCYT, Superintendencia de Datos Personales): Son los encargados de supervisar el cumplimiento de estándares de calidad, normativa educativa y protección de datos.
- Proveedores tecnológicos y aliados externos: Son los aliados que aportan servicios o herramientas que pueden generar o mitigar riesgos.
- Sociedad y comunidades locales: Son los destinatarios de los proyectos de vinculación y servicios del instituto.

5.5.4.2. Articulación del compromiso con la gestión del riesgo

El Instituto Tecnológico Superior Compu Sur (ITECSUR) manifiesta su compromiso institucional con la gestión del riesgo a través de una política formal que define el propósito, los principios y la importancia estratégica de la gestión del riesgo en su modelo de gobernanza y operación. ITECSUR establece su Política de Gestión de Riesgos como un documento institucional de referencia, orientado a:

- Proteger la misión y los objetivos institucionales frente a eventos que puedan afectar su cumplimiento.
- Promover una cultura organizacional proactiva, participativa y responsable frente

al riesgo.

- Garantizar la seguridad de la comunidad académica, la continuidad de los servicios y la protección de los datos personales e institucionales.
- Cumplir con las normativas vigentes, tanto en el ámbito educativo como en el tecnológico y de protección de la información.

Adicionalmente la política contempla los siguientes elementos clave:

- Propósito institucional: Fortalecer la toma de decisiones informadas, anticipar amenazas y minimizar impactos que puedan comprometer la misión educativa del instituto.
- Ámbito de aplicación: Aplica a todas las unidades, procesos, niveles y miembros de la comunidad institucional.
- Principios rectores:
    - Integración transversal del riesgo en la planificación y operaciones.
    - Responsabilidad compartida y participación activa de todas las partes interesadas.
    - Mejora continua basada en evidencia, aprendizaje y retroalimentación.
    - Cumplimiento ético y legal, con enfoque en derechos, diversidad y sostenibilidad.
- Roles y responsabilidades: Define las funciones del equipo directivo, las áreas operativas, los coordinadores de carrera y los responsables de procesos tecnológicos y académicos.

- Compromiso de recursos: La institución asignará el soporte humano, tecnológico y económico necesario para implementar y mantener el sistema de gestión del riesgo.
- Revisión periódica: La política será evaluada al menos una vez al año o se actualizará de manera requerida conforme a los resultados del sistema, cambios significativos y el contexto institucional normativo.

Para que esta política tenga un impacto efectivo y pueda ser conocida por las partes interesadas, ITECSUR implementará una estrategia de comunicación interna, incluyendo:

- La publicación y mantenimiento de la política en el portal institucional público e intranet.
- Inclusión en los manuales de inducción del personal docente y administrativo.
- Jornadas informativas y capacitaciones específicas sobre el contenido de la política y su aplicación práctica para el nuevo personal y nuevos estudiantes.
- Inclusión de implementación y seguimiento del sistema en las reuniones de planificación, seguimiento y evaluación institucional.
- Elaboración de materiales de divulgación adaptados a distintos públicos (infografías, cápsulas audiovisuales, trípticos digitales).

Esta estrategia tiene como objetivo que todos los miembros del instituto comprendan el propósito de la política, su rol dentro del sistema y las implicaciones de una gestión de riesgos efectiva.

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

ITECSUR establecerá una estructura funcional dentro de su sistema de gestión de riesgos para la asignación de responsabilidades en todos los niveles jerárquicos, desde las autoridades hasta el personal operativo, considerando:

- Autoridades (Rectorado y Dirección Académica)
- Rol: Máxima autoridad en la gestión del riesgo institucional.
- Responsabilidades:
    - Aprobar la política de gestión de riesgos.
    - Asignar recursos necesarios para la implementación del sistema.
    - Promover la cultura institucional del riesgo.
    - Supervisar el desempeño del sistema y su alineación con los objetivos estratégicos.
    - Evaluar los resultados del sistema de gestión al menos una vez al año.
- Comité o Unidad de Gestión de Riesgos
- Rol: Órgano técnico y operativo responsable de coordinar la implementación y mantenimiento del sistema.
- Responsabilidades:
    - Diseñar, aplicar y actualizar metodologías para la identificación, evaluación y tratamiento del riesgo.
    - Asesorar a las unidades organizativas para la implementación del sistema.

- Consolidar informes de riesgos y presentarlos a las autoridades.
- Coordinar actividades de capacitación y sensibilización en los diferentes niveles del instituto.

- Coordinadores de Carreras y Responsables de Áreas
- Rol: Gestores operativos del riesgo en sus respectivas unidades.
- Responsabilidades:
  - Identificar riesgos asociados a sus procesos.
  - Aplicar controles y monitorear los riesgos relevantes.
  - Reportar incidentes o vulnerabilidades al comité o unidad de gestión de riesgos.
  - Asegurar el cumplimiento de procedimientos de seguridad y normativas.
- Personal Docente y Administrativo
- Rol: Colaboradores directos en la ejecución de acciones preventivas y correctivas.
- Responsabilidades:
  - Aplicar buenas prácticas y procedimientos seguros en sus funciones.
  - Notificar riesgos, incidentes o situaciones irregulares.
  - Participar en capacitaciones institucionales sobre gestión del riesgo.
  - Resguardar información y recursos de acuerdo con las políticas internas.
- Estudiantes
- Rol: Usuarios del sistema institucional con deberes en el autocuidado y uso responsable de plataformas y servicios.

- Responsabilidades:
    - Acatar normas de conducta digital y seguridad.
    - Reportar incidentes que afecten su seguridad académica o tecnológica.
    - Participar en jornadas informativas o de formación preventiva.

5.5.4.4.Asignación de recursos

Reconociendo que la gestión de riesgos no es una actividad puntual sino un proceso continuo y transversal requerido por el instituto, ITECRUS establece los mecanismos que garantizan que los recursos necesarios estén disponibles y sean utilizados de manera eficiente para la prevención, mitigación, monitoreo y tratamiento de los riesgos institucionales.

ITECSUR asegurará un presupuesto institucional asignado al sistema de gestión del riesgo, que permita asegurar:

- La adquisición y mantenimiento de herramientas tecnológicas de gestión de riesgos (software de análisis, plataformas de monitoreo, respaldo de información, entre otros).
    - Contar con sistemas de información institucionales seguros y auditables.
    - Integrar herramientas para la gestión de riesgos y continuidad operativa (matrices de riesgo digitales, dashboards de monitoreo, etc.).
    - Respaldar información crítica con soluciones de almacenamiento seguro y recuperación ante desastres.
    - Fortalecer la infraestructura tecnológica educativa, minimizando los riesgos operativos derivados de su uso masivo.

- La documentación actualizada del sistema: políticas, procedimientos, instructivos y registros.

- La contratación de consultorías especializadas o auditorías externas, cuando se requiera evaluar el sistema desde una perspectiva independiente.
- La implementación de planes de acción correctiva, derivados de auditorías, revisiones internas o incidentes registrados.
- La ejecución de eventos formativos, simulacros, y jornadas de sensibilización, capacitación y comunicación para los diferentes niveles institucionales y necesidades de la organización.
    - Principios de gestión de riesgos según ISO 31000.
    - Identificación y evaluación de riesgos.
    - Cultura organizacional de prevención.
    - Gestión de incidentes, ciberseguridad y protección de datos personales.
    - Uso de herramientas de registro y monitoreo.

Este presupuesto debe ser revisado anualmente como parte del Plan Operativo Anual (POA), el retorno de inversión y ajustados según los cambios en el contexto de riesgo y los nuevos requerimientos institucionales.

5.5.4.5.Establecimiento de la comunicación y consulta

De acuerdo con ISO 31000:2018 ITECSURA establecerá un proceso de comunicación bidireccional que será estructurada y adaptada a cada público, asegurando la transparencia y fomentando la participación consciente. Además, los procesos para la consulta permitirán

incorporar la experiencia, el conocimiento local y las percepciones de los diversos actores para enriquecer la toma de decisiones.

ITECSUR desarrollará un plan de comunicación integral que contemple las siguientes acciones clave:

- Difusión interna de la política, objetivos y principios del sistema de gestión de riesgos (en forma de carteleras informativas físicas y digitales las cuales estarán en áreas comunes y plataformas internas, capacitaciones y talleres presenciales o virtuales con sesiones diferenciadas de acuerdo a los perfiles y a la temática que se vaya a tratar.)
- Proceso de comunicación para autoridades externas según aplique para el reporte de incidencias o vulnerabilidades relacionadas a datos personales.
- Informes periódicos de avance y desempeño del sistema, dirigidos a directivos, docentes y personal administrativo.
- Capacitación comunicacional a los diferentes niveles institucionales en los que se enseñe cómo reportar incidentes, identificar riesgos y usar los canales establecidos.
- Espacios virtuales y físicos donde los estudiantes y el personal puedan consultar documentación y hacer sugerencias de retroalimentación del sistema de gestión.
- Integración del tema en actividades de inducción y bienvenida a nuevos miembros de la comunidad académica.
- Canales de comunicación abiertas para dar cumplimiento a las obligaciones de

cumplimiento de la ley orgánica de protección de datos personales.

ITECSUR establecerá mecanismos de consulta periódica y participativa para recoger las perspectivas, expectativas y retroalimentación sobre el riesgo de sus principales grupos de interés:

- Encuestas o formularios anónimos para conocer percepciones de riesgo, experiencias con incidentes o nivel de preparación.
- Mesas de diálogo o talleres participativos con docentes, estudiantes y personal técnico como parte de la retroalimentación de las partes interesadas.
- Reuniones con representantes de organismos reguladores, aliados estratégicos o comunidades vinculadas, para evaluar impactos y riesgos compartidos.
- Revisión de buzones de sugerencias, reclamos o alertas, como insumos para el análisis de riesgos emergentes.

Este proceso de consulta fortalecerá la legitimidad del sistema, fomentará la corresponsabilidad y aportará información valiosa para la mejora continua del marco de gestión.

5.5.5. Implementación

La implementación del sistema de gestión de riesgos en ITECSUR representa la fase operativa donde se ejecutan los principios, políticas y procesos definidos en el marco normativo y estratégico.

El proceso de implementación se alinea con los objetivos institucionales garantizando la participación activa de las partes interesadas y permite la incorporación progresiva de una cultura preventiva y resiliente.

ITECSUR ejecutará los procesos de gestión de riesgos conforme a las siguientes etapas fundamentales:

- Identificación del riesgo
    - Se determinarán eventos, condiciones o amenazas que puedan afectar el logro de los objetivos institucionales, académicos o tecnológicos.
    - Se utilizarán herramientas como listas de verificación, entrevistas, análisis de incidentes previos y revisión documental.
- Análisis del riesgo
    - Se evaluará la probabilidad de ocurrencia y el impacto potencial de los riesgos identificados, utilizando escalas definidas en el marco metodológico institucional.
    - Se podrá aplicar análisis cualitativo, semi-cuantitativo o cuantitativo según el tipo de riesgo.
- Evaluación del riesgo
    - Se compararán los niveles de riesgo con los criterios de aceptación establecidos.
    - Se priorizarán los riesgos que requieren tratamiento inmediato, seguimiento o monitoreo especial.

- Tratamiento del riesgo
    - Se definirán las estrategias de respuesta más adecuadas: evitar, mitigar, compartir o aceptar el riesgo.
    - Se diseñarán planes de acción con responsables, recursos asignados y cronogramas definidos.
- Comunicación y consulta
    - Durante todo el proceso, se garantizará la comunicación con las partes interesadas, promoviendo la transparencia y la participación informada.
- Monitoreo y revisión
    - Se hará seguimiento periódico de los riesgos, la efectividad de los controles y el cumplimiento de las acciones implementadas.
    - Se ajustarán las acciones ante cambios contextuales o resultados no esperados.

ITECSUR establecerá un mecanismo de revisión sistemática del marco de implementación, para garantizar su eficacia, sostenibilidad y alineación continua con los objetivos institucionales, considerando:

- Implementar una evaluación anual del desempeño del sistema de gestión de riesgos.
- Revisión anual de políticas y metodologías en función de auditorías, incidentes u observaciones internas y externas o cambios significativos del entorno.
- Actualización de los registros y bases de conocimiento de riesgos y matrices por área o proceso.
- Retroalimentación de la comunidad institucional para reforzar la pertinencia del

sistema.

Este enfoque dinámico y participativo asegura que el marco de gestión no se mantenga estático, sino que evolucione conforme al desarrollo institucional y la participación de sus partes interesadas, la transformación digital, la normativa vigente y las necesidades emergentes.

5.5.6. Valoración

La fase de valoración constituye un componente fundamental para evaluar la eficacia del sistema implementado, verificando si cumple con los objetivos institucionales, si los procesos están funcionando de forma adecuada y si se mantienen alineados al contexto dinámico y a las necesidades de la organización.

Este análisis permite identificar áreas de mejora, ajustar estrategias y mantener la relevancia del sistema ante nuevas amenazas o cambios en el entorno. La valoración, además, fortalece la rendición de cuentas institucional y consolida una cultura de revisión continua.

Para monitorear la efectividad del sistema de gestión de riesgos, ITECSUR establecerá un conjunto de indicadores clave de desempeño (KPIs), orientados a medir:

- Indicadores operativos:
    - Número de riesgos identificados por área/proceso.
    - Porcentaje de riesgos tratados dentro del período planificado.
    - Tiempo promedio de respuesta ante incidentes reportados por nivel de criticidad.
    - Número de incidentes relacionados con protección de datos.

- Indicadores de madurez del sistema:
    - Porcentaje de cumplimiento de las acciones establecidas en los planes de tratamiento.
    - Frecuencia de actualización de las matrices de riesgo.
    - Porcentaje de personal capacitado en gestión de riesgos.
    - Grado de cumplimiento de implementación de políticas internas y controles definidos.

La valoración se desarrollará de forma periódica con revisión anual.

5.5.7. Mejora

Dentro del contexto de implementación progresiva del sistema de gestión de riesgos se resalta la importancia de establecer mecanismos continuos de mejora y adaptación, en los cuales ser reconozca el entorno educativo es dinámico influenciado por cambios tecnológicos sociales normativos y académicos por lo que el sistema debe ser flexible revisado regularmente y sujeto a procesos de realimentación y enmienda.

El objetivo de esta fase será garantizar que dicho sistema no solo responda eficazmente a los riesgos actuales sino que también evolucionan con el tiempo vaya incorporando lecciones aprendidas se corrijan desviaciones y se fortalezca esa cultura institucional para la prevención y la resiliencia a futuro, una de las mejores formas de adaptación será la cual implica revisar de una manera sistemática aquellos resultados de esta gestión en los cuales se evaluará su efectividad y se realizarán todos los ajustes para alinearse

con los objetivos estratégicos el contexto organizacional y las expectativas de las partes interesadas internas y externas.

5.5.7.1.Adaptación

La norma ISO 31000 establece que el marco debe ajustarse conforme evolucionan los objetivos institucionales, el contexto regulatorio, los avances tecnológicos, las expectativas de las partes interesadas o cambios significativos. Un sistema rígido o desactualizado representa un riesgo en sí mismo, ya que impide detectar oportunamente amenazas emergentes o responder con agilidad ante nuevas condiciones.

ITECSUR implementará mecanismos de revisión estructurada del marco de gestión de riesgos, cada vez que se produzcan:

- Cambios organizacionales relevantes, como reestructuraciones, apertura de nuevas carreras, renovación tecnológica o incorporación de nuevas plataformas educativas.
- Modificaciones normativas o legales, especialmente aquellas relacionadas con la educación superior, la protección de datos personales, la ciberseguridad o el uso de tecnologías emergentes.
- Actualización de los objetivos estratégicos o misionales, resultado de procesos de planificación institucional o respuesta a auditorías externas (CES, CACES, etc.).
- Cambios sociales, económicos o ambientales que puedan modificar el perfil de riesgo de la institución (por ejemplo, crisis sanitarias, desastres naturales o transformación digital acelerada).
- Retroalimentación institucional que revele fallas, vacíos o desajustes en el sistema

actual de gestión de riesgos.

Estas revisiones se documentarán mediante informes y reuniones de evaluación que alimenten los procesos de ajuste correctivo y preventivo.

En función de los resultados obtenidos en los procesos de revisión, ITECSUR aplicará ajustes necesarios que pueden incluir:

- Actualización de la política institucional de riesgos y sus principios rectores.
- Rediseño de las metodologías de evaluación y tratamiento de riesgos.
- Contratación de apoyo externo en forma de consultoría.
- Inclusión de nuevas responsabilidades o áreas dentro del sistema.
- Mejora de herramientas tecnológicas o canales de comunicación.
- Redistribución de recursos financieros y humanos para áreas críticas emergentes.
- Revisión de planes de formación y sensibilización, incorporando nuevas temáticas o perfiles de riesgo.

Estos ajustes deberán mantenerse documentados, comunicados y validados por la alta dirección, y ser incorporados en el ciclo de mejora continua institucional.

5.5.7.2.Mejora continua

La mejora continua se integra en el ciclo de vida de la gestión de riesgos mediante la realización sistemática de auditorías, revisiones y análisis de desempeño, así como la implementación de acciones correctivas y preventivas. ITECSUR para la implementación de su sistema de gestión establece los siguientes mecanismos de acción.

Auditorías y revisiones periódicas.

- Planificación de auditorías internas.
  - Se programan auditorías anuales del sistema de gestión de riesgos, coordinadas por la Unidad de Gestión de Riesgos.
- Revisiones de desempeño semestrales
  - Se revisan los KPIs de gestión de riesgos para verificar tendencias, desviaciones y cumplimiento de objetivos anualmente.
  - Se presentan informes anuales del estado del sistema de gestión a las autoridades para la revisión de la Alta Dirección.
- Análisis de resultados y lecciones aprendidas
  - Se documentarán los hallazgos de auditorías y revisiones.
  - Se genera un informe consolidado con recomendaciones para optimizar procesos, fortalecer controles y actualizar metodologías.

Acciones correctivas y preventivas:

- Detección de causas raíz: A partir de las no conformidades o brechas detectadas, se realiza un análisis de causa raíz (5 Porqués o Diagrama de Ishikawa) para identificar el origen de los problemas.
- Definición de acciones correctivas: Se elaborarán planes de acción para corregir desviaciones específicas con la actualización de procedimientos, mejoras en la capacitación, refuerzo de controles tecnológicos o ajustes en la asignación de recursos.
- Prevención de recurrencia: Se diseñan e implementan medidas preventivas asociadas

a riesgos emergentes, garantizando que aprendizajes institucionales se traduzcan en cambios sostenibles y duraderos.

- Seguimiento de acciones: Cada acción correctiva o preventiva contará con un responsable, un cronograma y un mecanismo de verificación de eficacia. La Unidad de Gestión de Riesgos hace un seguimiento mensual hasta la completa resolución, informando los avances al Comité de Dirección.

Integración al ciclo PDCA institucional

Con la mejora continua, ITECSUR cierra el ciclo Planificar–Hacer–Verificar–Actuar (PDCA) de la gestión de riesgos:

- Planificar: Actualizar políticas y planes de tratamiento basados en hallazgos.
- Hacer: Ejecutar las acciones correctivas y preventivas definidas.
- Verificar: Auditorías y revisiones miden la eficacia de los cambios.
- Actuar: Incorporar ajustes adicionales, reforzar la cultura de aprendizaje y reiniciar el ciclo.

Este enfoque garantiza que el sistema de gestión de riesgos se mantenga vivo, respondiendo con agilidad a la realidad institucional y fortaleciendo la resiliencia de ITECSUR.

5.6. Proceso

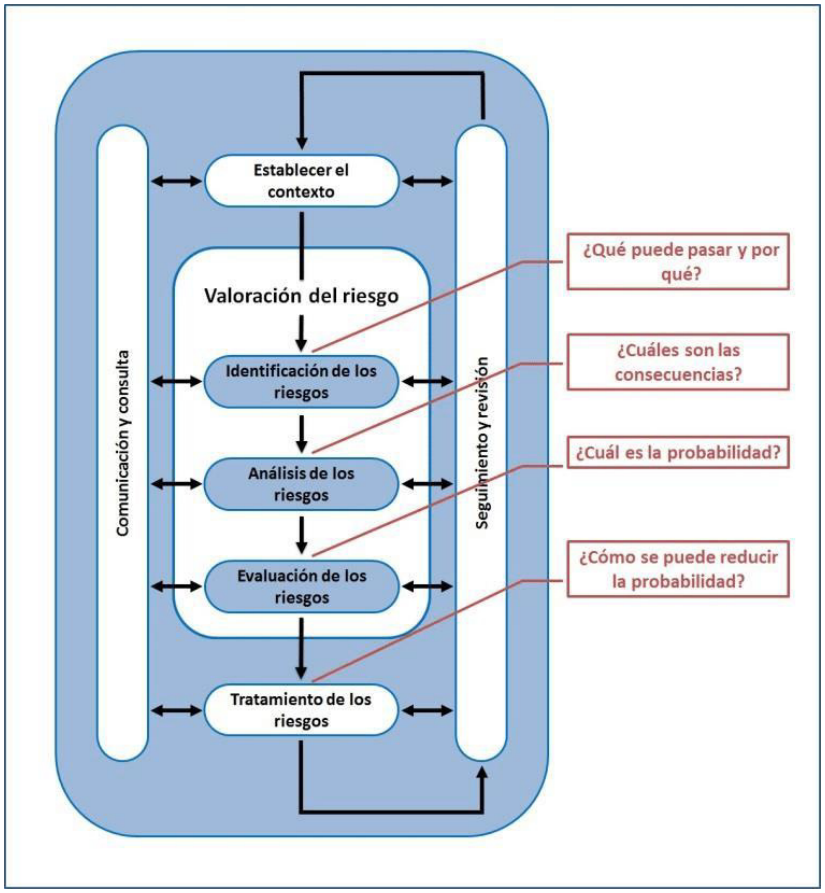
5.6.1. Generalidades

Se puede describir el proceso de gestión de riesgos cómo un ciclo iterativo a lo largo del tiempo que integra y tiene la capacidad de orientar todas las decisiones que se tomen

dentro de la institución en este caso el ITECSUR. Dentro de este enfoque que ven global muchas partes podemos considerar que la gestión de riesgos no va a ser una parte aislada Sino más bien un componente estratégico enmarcado principalmente por la gobernanza la planificación dentro de la institución y todos aquellos procesos académicos y tecnológicos qué son claves dentro del manejo.

Figura 5

Diagrama para la gestión de riesgos bajo ISO3100:2018



Fuente: Valgenesis

5.6.2. Comunicación y Consulta

Características claves dentro del proceso:

Apoyo en la toma de decisiones: Se va a utilizar principalmente en la priorización de ciertas inversiones tecnológicas con el fin de definir y en marcar de manera correcta conforme a la ley orgánica de protección de datos personales las principales políticas de privacidad y la selección de controles en el ámbito de la ciberseguridad no es lo que de cierta forma aportaría de manera objetiva y técnica la toma de decisiones de una mejor manera.

Alineación con los objetivos institucionales: El sistema responde a los objetivos en primera instancia lo que se busca con esto es que por ejemplo se garantice la protección de los datos, la continuidad educativa y el cumplimiento de la normativa nacional en este caso (LOPDP y LOES).

Dinamismo y adaptabilidad: En este caso se estableció un mecanismo de control a modo de revisión periódica mediante el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) lo que ha permitido su adaptación ante las amenazas emergentes dentro de la organización como un ransomware o fugas de datos por parte de colaboradores.

Participación de las partes interesadas: Al momento de articular estos mecanismos se toma en cuenta a los estudiantes, docentes, proveedores y organismos reguladores de tal forma que como organización se garantiza que todas las partes interesadas contemplen los lineamientos y sean parte fundamental pero no vital de la organización.

Mejora continua: Dentro de este paso se busca establecer los mejores indicadores clave como el número de incidentes por trimestre, los niveles de riesgo residual y porcentajes de cumplimiento de los planes de tratamiento que nutren a los diferentes sistemas de retroalimentación para alcanzar el objetivo de este.

Objetivo: Garantizar que la gestión de riesgos sea comprensible para todo el conglomerado, compartida y respaldada por todos los actores institucionales, desde un enfoque bidireccional y adaptado al perfil de los diferentes actores interesados.

Estructura técnica del plan de comunicación:

Difusión estructurada: Por medio del departamento de comunicación se canalizará las mejores estrategias para que se difundan cada una de las políticas y objetivos mediante mails a la parte interna de la organización o a su vez por canales o medios digitales, inducciones institucionales, boletines internos y meets de sensibilización

Sistemas de retroalimentación: Formularios anónimos y confidenciales, buzones digitales especiales para tal fin, mesas de diálogo, talleres de participación en los que se aplicarán estrategias para captar percepciones de riesgo en los involucrados e incidentes que no se han reportado de manera formal.

Comunicación externa regulatoria: Se debe formalizar canales de comunicación con el CES, SENECYT, MINTEL y el comité de protección de datos de la Función de Transparencia y Control Social, incluyendo los reportes de incidentes bajo los esquemas normados.

Roles Definidos:

Rectorado y Vicerrectorado: validación institucional de mensajes críticos.

Unidad de Riesgos y TI: diseño de alertas, informes y estrategias de concienciación.

Direcciones académicas: facilitación del mensaje en sus áreas.

Tabla 28

Guía para la gestión de riesgos

Etapa	Cómo debe ocurrir la comunicación	Responsable primario	Tipo de mensaje a transmitir	Responsable de la respuesta ante incidentes	Ejemplo práctico interno	Ejemplo práctico externo
1.- análisis de riesgos	Comunicación bidireccional entre áreas técnicas (ti, académica y administrativa) para levantar información de activos, amenazas, vulnerabilidades y controles actuales. Se documentan hallazgos y se reporta en la dirección	Coordinador de logística infraestructura p info estructura + directora académica	Reporte de hallazgos de riesgos, listas de activos críticos, vulnerabilidades detectadas y recomendaciones preliminares.	Un comité de seguridad de la información conformado por técnicos del departamento ti	Reunión técnica entre ti y la dirección académica para revisión de accesos de la plataforma moodle.	Envío de informe sobre los hallazgos de vulnerabilidades en regencia de revoluciones control de datos arco.
2.- reducción de riesgos (tratamiento)	Comunicación genérica guion aceptar para decidir controles a implementar, asignar presupuesto ni capacitar a los usuarios finales. Difusión del manual de buenas prácticas.	Vicerrectorado académico + coordinador de talento humano + coordinador de ti	Manual de políticas de seguridad, instructivos de uso de sistemas, directrices de acceso a datos.	Comunicador de logística, infraestructura e infoestructura.	Circular interna explicando nueva política de contraseñas y doble autenticación para los docentes.	Notificación formal a microsoft sobre una implementación de nuevas políticas de acceso en plataformas y en la nube.
3. Respuesta	Comunicación inmediata	Coordinador de	Al leer puertas de	Coordinador general	Mensaje de	Notificación obligatoria

a incidentes	directa y documentada a través de canales oficiales correo chat institucional y telefónica activan protocolos definidos en el plan de respuesta a incidentes	logística infraestructura e infoestructura + administrador de campus conocido como prefecto + seguridad física (grunseg)	incidente comunicados de contención instrucciones para usuarios y visitantes.	de operaciones de cada campus + comité de alta dirección.	emergencia a personal de ti sobre detección de acceso no autorizado.	al regulador (lopdp) guía estudiantes afectados por filtración de datos.
4. Recuperación y continuidad del negocio	Comunicación de seguimiento a usuarios y partes interesadas para informar sobre la restauración de servicios, resultados del análisis post incidente y medidas correctivas. Se incluyen recomendaciones para evitar recurrencia.	Vicerrectorado académico + coordinador del área de comunicación e imagen institucional.	Informe final del incidente, estado de sistemas, cronograma de restauración, medidas de refuerzo.	Comité de seguridad de la información.	Boletín interno con lecciones aprendidas y recordatorio de nuevas prácticas de respaldo.	Comunicado oficial a medios ir a la comunidad estudiantil informando la recuperación de la plataforma académica tras el incidente.

Fuente: *Instituto Tecnológico Superior Compu Sur*

Aspectos clave

Enfoque técnico: cada etapa debe contemplar un nivel de comunicación estructurada usando reportes formales actas registros y un panel de evidencias.

Responsabilidad compartida: el modelo hizo 31000 enfatiza la responsabilidad transversal desde el área de TI pasando por el modelo administrativo hasta las autoridades académicas.

Documentación: todas las acciones comunicativas deben manejar una trazabilidad para auditorías internas y regulatorias en caso de que sean necesarias como por ejemplo la que se realiza por el consejo de educación superior CES.

Canales seguros: se priorizan plataformas seguras con el correo institucional herramientas de control de acceso como la doble verificación.

Ejemplo de flujo real

Interno: el director académico convoca a coordinadores de carrera para informar sobre nuevas directrices de seguridad en la matriz de calificaciones.

Externo: se puede remitir a la agencia de regulación de datos el informe mensual de auditoría de accesos en cumplimiento con la ley orgánica de protección de datos personales.

Integración Transversal: La comunicación no va a verse limitada por la difusión, más bien actuaría como un enlace en cada una de las fases del ciclo de riesgos.

5.6.3. Alcance, Contexto y Criterios

5.6.3.1.Generalidades

Esta etapa establece las directrices para toda decisión de evaluación, tratamiento o monitoreo de riesgos. La solidez que brinda está definida por la relevancia y precisión del modelo que se ha de implementar.

Objetivos técnicos de la etapa:

- Determinar los procesos críticos (académicos, financieros, tecnológicos, legales, etc.)
- Establecer límites claros para evitar una dispersión en el tratamiento de los datos.
- Realizar una alineación sobre el análisis contextual con los intereses institucionales, regulatorios y sociales.

5.6.3.2.Definición del Alcance

Descripción técnica del alcance

- **Procesos incluidos:** De forma cronológica se realizaría la admisión, matrícula, titulación, gestión académica, becas, conectividad, videovigilancia, correo institucional, atención médica y sistemas financieros.
- **Límites temporales:** Revisión anual del sistema; seguimiento semestral hay eventos críticos que pongan en peligro la organización.
- **Límites espaciales:** Campus Matriz.
- **Organizacionales:** Abarcan desde el nivel máximo en este caso el rectorado hasta las unidades ejecutoras del personal administrativo y docente.
- **Recursos disponibles:**
    - Infraestructura física (servidores, UPS, centros de datos).
    - Infraestructura lógica (firewalls, antivirus, plataformas con respaldo en la nube).
    - Recursos humanos: equipo TIC, docentes capacitados, personal administrativo.

- **Brechas detectadas:**
    - Limitación en personal experto en gestión de riesgos digitales.
    - Ausencia de pruebas periódicas de recuperación de datos (DRP).
    - Falta de controles de acceso centralizados para plataformas educativas.

5.6.3.3.Contexto Externo e Interno

Contexto externo (Modelo PESTEL-FODA):

Con relación al análisis FODA que fue presentada en el capítulo anterior vamos a tomarle como el modelo a seguir y dentro de este capítulo se va a incorporar una matriz DAFO con puntos relevantes en cuanto al tratamiento de cada uno de las aristas

Tabla 29

Modelo PESTEL-FODA

FACTORES INTERNOS / FACTORES EXTERNOS	OPORTUNIDADES (O)	AMENAZAS (A)
FORTALEZAS (F) DEBILIDADES (D)	FO (Fortalezas - Oportunidades) DO (Debilidades - Oportunidades)	FA (Fortalezas - Amenazas) DA (Debilidades - Amenazas)
Fortalezas	Oportunidades FO: estrategias ofensivas FO1: potenciar la cultura de calidad Aprovechando avances tecnológicos O1 mediante inversiones en plataformas educativas seguras. FO2: ampliar redes de vinculación para acceder a recursos externos y programas de capacitación. O2, O4	Amenazas FA: estrategias de defensa. FA1: usar la innovación educativa para crear redundancias digitales y planes de contingencia frente a amenazas cibernéticas A1 y desastres de origen natural A3. FA2: apalancar la cultura institucional de

		FO3: integral prácticas de autoevaluación con nuevas normativas de protección de datos O3 para fortalecer el cumplimiento regulatorio	derechos humanos para manejar de forma ética presiones sociales y políticas. FA3: utilizar procesos académicos robustos para responder rápidamente a cambios regulatorios. DA: estrategia de supervivencia.
Debilidades	DO: Estrategias de reorientación. DO1: superar limitaciones tecnológicas gestionando alianzas con proveedores y usando programas de capacitación gratuita. DO2: reducir brechas de capacitación impulsando proyectos de formación continua con apoyo de redes académicas. DO3: disminuir dependencia de proveedores externos mediante acuerdos de transferencia tecnológica y capacitación interna.		DA1: elaborar un plan de contingencia para amenazas cibernéticas y EMERGENCIAS mitigando la falta de recursos tecnológicos. DA2: promover la cultura de reporte de incidentes mediante programas de concienciación para responder a cambios normativos y fortalecer la resiliencia institucional. DA3: diversificar proveedores y desarrollar capacidades internas para reducir vulnerabilidad ante inestabilidad social y económica.

Fuente: *Instituto Tecnológico Superior Compu Sur*

- FO: priorizar inversiones en tecnología educativa segura y en certificaciones de ciberseguridad alineadas con la norma ISO 31000 y LOPDP.
- FA: establecer simulacros de respuesta a incidentes y protocolos de continuidad académica en caso de emergencias.
- DO: ay ya aprovechar convenios interinstitucionales para capacitar al personal

sin costos elevados y reducir la dependencia tecnológica.

- DA: desarrollar campañas internas para fomentar la cultura de notificación de vulnerabilidad y reforzar los canales de comunicación institucional.

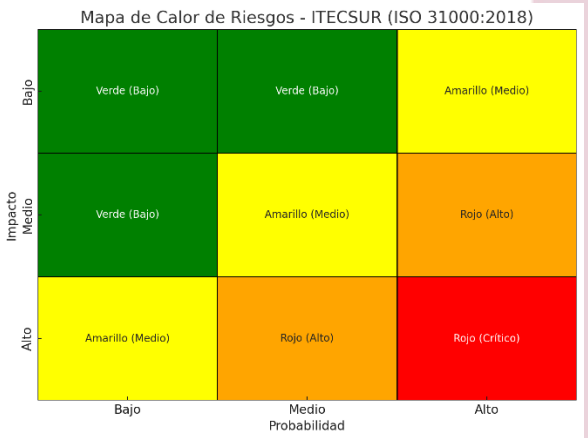
Contexto interno

- Cultura organizacional participativa pero aún reactiva ante incidentes
- Estructura jerárquica con bajo nivel de automatización en algunos procesos
- Falta de un sistema integral de reporte de incidentes por parte de estudiantes
- Interacciones deficientes entre ti, dirección académica y departamento legal lo cual genera vulnerabilidades transversales.

5.6.3.4.Definición de Criterios de Riesgo

Figura 6

Parámetros establecidos (criterios de evaluación de riesgos)



Fuente: Elaboración Propia

- **Probabilidad:**
  - Baja: Menos del 25% (Ocurrencia de una vez al año).

- Media: Del 26 al 50% (Ocurrencia de 2-5 veces al año).
- Alto: Más del 51% (Ocurrencia de más de 5 veces al año).

- **Impacto:**
  - Bajo: sin afectación significativa.
  - Medio: interrupción parcial o pérdida de datos no críticos.
  - Alto: violación de datos personales, parálisis operativa o sanción legal.

Matriz de evaluación de riesgos (Probabilidad x Impacto)

Tabla 30

Criterios de riesgo

Probabilidad x Impacto	Bajo	Medio	Alta
Bajo	Verde-Bajo	Verde-Bajo	Amarillo-Medio
Medio	Verde-Bajo	Amarillo-Medio	Rojo-Alto
Alto	Amarillo-Medio	Rojo-Alto	Rojo-Crítico

Fuente: *Instituto Tecnológico Superior Compu Sur*

Leyenda del Mapa de Calor

- **Verde (Bajo)**: Riesgo aceptable. No se requiere acción adicional más allá del monitoreo estándar.

- **Amarillo (Medio)**: Riesgo tolerable. Requiere supervisión activa y posible mejora de controles.
- **Rojo (Alto)**: Riesgo inaceptable. Requiere tratamiento prioritario y mitigación inmediata.
- **Rojo (Crítico)**: Riesgo extremo. Se debe suspender o rediseñar el proceso afectado hasta su mitigación.

Factores clave en los criterios:

- *Requisitos legales* (LOPDP, ISO/IEC 27701).
- *Expectativas de stakeholders* (estudiantes, padres, reguladores).
- *Valores institucionales* (ética, transparencia, innovación).

Ejemplo práctico:

- *Riesgo:* acceso no autorizado a sistemas de calificaciones.
  - Probabilidad: Alta
  - Impacto: Alto (compromete integridad de datos estudiantiles).
  - Clasificación: **Rojo (crítico)**
  - Tratamiento: Implementar doble factor, revisar logs, redefinir roles de acceso.

Matriz de Evaluación de Riesgos con Ejemplos Reales

Tabla 31

Evaluación de riesgo

Riesgo identificado	Probabilidad	Impacto	Clasificación
Acceso no autorizado a moodle	Alta	Alto	Rojo-crítico

De datos académicos por eliminación accidental	Media	Alto	Rojo-alto
Uso fraudulento de información financiera	Media	Alto	Rojo-alto
Fuga de imágenes sin consentimiento ya sea en marketing o redes sociales	Alta	Media	Rojo-alto
Suplantación de identidad con datos de caracterización	Alta	Alto	Rojo-crítico
Acceso indebido por personal no autorizado	Media	Medio	Amarillo-medio
Monitorización indebida del personal vídeo vigilancia no autorizada	Baja	Alto	Verde-bajo

Fallo en sistema de respaldos	Alta	Alto	Rojo-crítico
No cumplimiento de la lopdp por omisión o controles ineficaces	Media	Alto	Rojo-alto
Falta de control de cambios en software financiero	Alta	Alto	Rojo-crítico
Vulnerabilidad sin parchear un servidor web institucional	Alta	Alto	Rojo-crítico
Falta de doble automática nación en sistemas críticos académicos y financieros	Alta	Alto	Rojo-crítico

Fuente: *Instituto Tecnológico Superior Compu Sur*

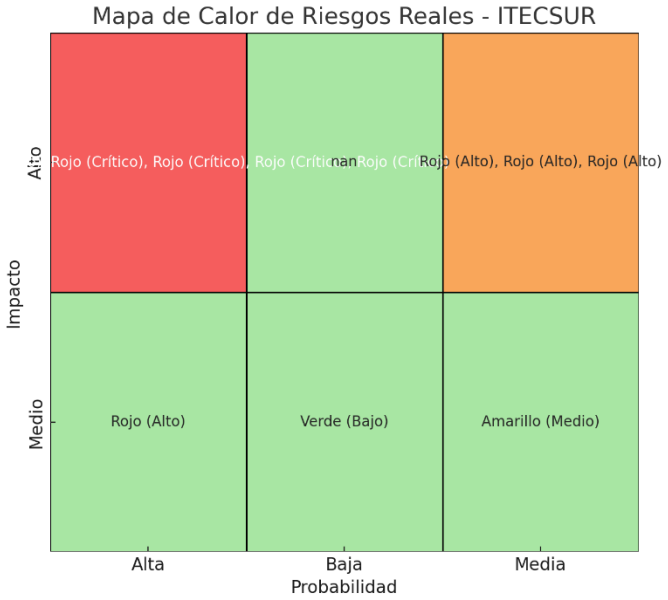
Contexto de resultado de ejemplo

- 9 riesgos clasificados como "Rojo": requieren acciones inmediatas de mitigación.

- 1 riesgo como "Amarillo": monitoreo activo y mejora de controles.
- 1 riesgo como "Verde": mantenido bajo supervisión estándar.

Figura 7

Distribución de riesgos según su probabilidad e impacto.



Fuente: *Instituto Tecnológico Superior Compu Sur*

- Cada celda indica la cantidad de riesgos detectados con una combinación específica de Probabilidad e Impacto.
- Además, dentro de cada celda se muestra la clasificación del riesgo conforme a la norma ISO 31000 como se ha detallado en la matriz anterior.

Este gráfico sirve como una herramienta eficaz para priorizar recursos y diseñar un plan de tratamiento de riesgos proporcional a la criticidad detectada.

5.6.4. Evaluación de riesgo

En el contexto del Instituto Tecnológico Superior Compu Sur (ITECSUR) esta etapa permite identificar y comprender aquellos eventos, amenazas o vulnerabilidades que podrían afectar negativamente el cumplimiento de los objetivos institucionales, especialmente en áreas clave como la calidad educativa, la gestión académica, la seguridad de la información y el cumplimiento normativo.

5.6.4.1.Generalidades

La evaluación del riesgo tiene como propósito central proporcionar información precisa y relevante que permita a los responsables institucionales tomar decisiones informadas sobre cómo gestionar eficazmente los riesgos identificados. Este proceso constituye la base para priorizar acciones, asignar recursos y establecer controles adecuados, garantizando la continuidad académica, administrativa y tecnológica del Instituto Tecnológico Superior Compu Sur (ITECSUR).

Considerando el alcance de procesos académicos se establece los siguientes niveles de impacto y probabilidad como calificación cualitativa y cuantitativa.

Tabla 32

Probabilidad

PROBABILIDAD		
Valor	Tipo	Descripción
1	Baja	Menos del 25% (Ocurrencia de una vez al año).
2	Media	Del 26 al 50% (Ocurrencia de 2-5 veces al año).

3	Alta	Más del 51% (Ocurrencia de más de 5 veces al año).

Fuente: *Instituto Tecnológico Superior Compu Sur*

Tabla 33

Impacto

IMPACTO		
Valor	Tipo	Descripción
1	Bajo	Sin afectación significativa.
2	Medio	Interrupción parcial o pérdida de datos no críticos.
3	Alto	Violación de datos personales, parálisis operativa o sanción legal.

Fuente: *Instituto Tecnológico Superior Compu Sur*

En el caso de ITECSUR, la evaluación de riesgos se realiza considerando los siguientes aspectos fundamentales:

- El origen del riesgo: Se identifican las fuentes o causas potenciales de los eventos que podrían afectar el cumplimiento de los objetivos institucionales.
- Las consecuencias potenciales (Impacto): Se analiza el impacto que tendría la materialización del riesgo en términos académicos, operativos, financieros o reputacionales.
- La probabilidad de ocurrencia: Se estima la frecuencia con la que es probable que el evento de riesgo ocurra, utilizando datos históricos, juicios expertos y tendencias del entorno educativo y tecnológico.
- Los controles existentes: Se consideran las medidas ya implementadas por la

institución para mitigar o prevenir el riesgo, como políticas internas, firewalls, sistemas de respaldo de información, capacitaciones al personal o protocolos de seguridad física y digital.

5.6.4.2.Identificación de riesgos

La identificación de riesgos permite reconocer con anticipación los eventos que podrían afectar el cumplimiento de sus objetivos estratégicos, operativos, académicos, tecnológicos y normativos. Esta fase busca determinar qué podría ocurrir, por qué, y qué consecuencias tendría para la institución, permitiendo actuar de forma preventiva. Para ello, se utilizan diversas herramientas y enfoques complementarios:

- Consulta con expertos internos y externos: Participación de directivos, responsables de áreas, personal de TI, asesores legales, docentes y profesionales externos en sesiones de revisión y análisis de riesgos específicos.
- Revisión de datos históricos: Análisis de registros de incidentes previos, fallos del sistema, auditorías, quejas estudiantiles, problemas de conectividad, interrupciones académicas u otras situaciones que hayan afectado el funcionamiento institucional.
- Talleres participativos y análisis de escenarios: Realización de sesiones grupales con las diferentes áreas del instituto para visualizar situaciones hipotéticas (por ejemplo, caída del sistema académico, filtración de datos personales, paralización por eventos naturales) y evaluar causas y consecuencias posibles.

Como resultado de la revisión antes menciona se identifica el siguiente catálogo de riesgos en el proceso de gestión académica del instituto.

- Riesgos Académicos: Riesgos relacionados con la calidad del proceso de enseñanza-aprendizaje, el desempeño estudiantil y la gestión curricular.
- Riesgo Tecnológico: Riesgos vinculados al uso, disponibilidad, seguridad y actualización de las plataformas tecnológicas y sistemas informáticos.
- Riesgo Legal/Normativo: Riesgos derivados del incumplimiento de leyes, normativas o regulaciones nacionales e internacionales aplicables a la educación superior.
- Riesgo Administrativo: Riesgos asociados a la gestión operativa, financiera y documental del instituto.
- Riesgo reputacional: Riesgos que afectan la imagen pública, la confianza de los estudiantes y la percepción externa de la calidad institucional.

Tabla 34

Tipo de riesgo

Tipo de riesgo	Riesgo Específico
Académico	Deserción estudiantil por desmotivación o problemas económicos
	Retrasos en la entrega de calificaciones
	Falta de actualización curricular frente a demandas del mercado
	Bajo rendimiento académico generalizado
	Falta de docentes especializados en áreas clave
Tecnológico	Caída del sistema de gestión académica
	Fallas en la infraestructura de red del campus
	Acceso no autorizado a plataformas institucionales
	Pérdida de datos por mal uso de respaldos
	Obsolescencia de equipos tecnológicos y software
Legal/Normativo	Incumplimiento de la Ley Orgánica de Protección de Datos Personales

	Sanciones por falta de informes al CES o Senescyt
	No conformidades en auditorías académicas o financieras
	Inadecuado tratamiento de datos personales de estudiantes y docentes
	Falta de contratos o convenios actualizados con docentes externos
	Errores en la gestión de matrículas y registros estudiantiles
	Mala planificación presupuestaria
Administrativo	Baja eficiencia en los procesos de compras públicas
	Desorganización en el archivo documental institucional
	Falta de seguimiento a convenios de cooperación interinstitucional
	Malas opiniones públicas en redes sociales sobre la calidad educativa
	Conflictos internos divulgados externamente
Reputacional	Divulgación de incidentes de seguridad o privacidad
	Resultados negativos en evaluaciones externas o rankings
	Falta de visibilidad institucional frente a otros institutos tecnológicos

Fuente: *Instituto Tecnológico Superior Compu Sur*

5.6.4.3.Análisis de riesgos

El análisis de riesgos se aplica tanto a procesos académicos como administrativos y tecnológicos, considerando las características particulares de la educación superior, los entornos digitales, la protección de datos personales, la infraestructura física y la relación con partes interesadas.

En el contexto del Instituto Tecnológico Superior Compu Sur (ITECSUR), este análisis permite:

- Determinar qué tan probable es que se presenten eventos como fallos en los sistemas académicos, filtración de datos personales o interrupciones operativas.
- Evaluar la gravedad de sus consecuencias en ámbitos como el cumplimiento normativo, la reputación institucional, la seguridad de la información y el bienestar estudiantil.

- Considerar la efectividad de los controles existentes, como protocolos de respaldo, políticas de acceso, formación del personal o infraestructura tecnológica.

Este análisis no solo permite priorizar los riesgos según su criticidad, sino que también guía la toma de decisiones para el tratamiento más adecuado, orientando la asignación de recursos, el diseño de planes de acción y el monitoreo posterior.

Para la consideración de escenarios ajustados de probabilidad e impacto tenemos las siguientes consideraciones.

Tabla 35

Análisis de probabilidad

PROBABILIDAD		
Valor	Tipo	Descripción
1	Baja	* Ocurrencia de una vez al año. * El evento puede ocurrir en otras instituciones educativas, pero en circunstancias muy específicas. * No se tienen alertas históricas sobre la materialización del evento.
2	Media	* Ocurrencia de 2-5 veces al año. * El evento ha ocurrido en otras instituciones educativas. * Se cuentan con alertas o incidencias históricas sobre la materialización del evento en el último año en más de una ocasión.
3	Alta	* Ocurrencia de más de 5 veces al año. * El evento ocurre de manera frecuente en otras instituciones y es un escenario latente. * Se cuentan con alertas o incidencias semestrales históricas sobre la materialización del evento en el último año.

Fuente: *Instituto Tecnológico Superior Compu Sur*

Tabla 36

Análisis de impacto

IMPACTO

Valor	Tipo	Descripción
1	Bajo	* Sin afectación significativa. * Pérdida financiera menor al 2% de la facturación anual. * Pérdida de matrícula de hasta 50 estudiantes. * Interrupción parcial o pérdida de datos no críticos.
2	Medio	* Pérdida financiera entre al 2% al 7% de la facturación anual. * Pérdida de matrícula de entre 50 a 150 estudiantes. * Violación de datos personales, parálisis operativa o sanción legal.
3	Alto	* Pérdida financiera mayor al 7% de la facturación anual. * Pérdida de matrícula superior a 150 estudiantes.

Fuente: *Instituto Tecnológico Superior Compu Sur*

Como resultado del análisis se obtiene la siguiente matriz cualitativa y cuantitativa de riesgos.

Tabla 37

Análisis de riesgo

Probabilidad x Impacto	Baja (1)	Media (2)	Alta (3)
Bajo (1)	Verde-Bajo (1)	Verde-Bajo (2)	Amarillo-Medio (3)
Medio (2)	Verde-Bajo (2)	Amarillo-Medio (4)	Rojo-Alto (6)
Alto (3)	Amarillo-Medio (3)	Rojo-Alto (6)	Rojo-Crítico (9)

Fuente: *Instituto Tecnológico Superior Compu Sur*

5.6.4.4.Valoración de riesgos

Aplicando los criterios antes mencionados se obtiene el siguiente análisis de valoración de riesgos a los eventos antes detallados:

Tabla 38

Valoración de riesgos

		RIESGO			
Tipo de riesgo	**Riesgo Específico**	**Probabilidad (1-3)**	**Impacto (1-3)**	**Probabilidad x Impacto**	**Clasificación de riesgo**
Académico	Deserción estudiantil por desmotivación o problemas económicos	3	1	3	Medio
	Retrasos en la entrega de calificaciones	1	1	1	Bajo
	Falta de actualización curricular frente a demandas del mercado	3	3	9	Crítico
	Bajo rendimiento académico generalizado	3	3	9	Crítico
	Falta de docentes especializados en áreas clave	1	3	3	Medio
Tecnológico	Caída del sistema de gestión académica	1	2	2	Bajo
	Fallas en la infraestructura de red del campus	3	3	9	Crítico
	Acceso no autorizado a plataformas institucionales	2	2	4	Medio
	Pérdida de datos por mal uso de respaldos	3	2	6	Alto
	Obsolescencia de equipos tecnológicos y software	3	3	9	Crítico
Legal/Normativo	Incumplimiento de la Ley Orgánica de Protección de Datos Personales	3	2	6	Alto
	Sanciones por falta de informes al CES o Senescyt	3	3	9	Crítico
	No conformidades en auditorías académicas o financieras	1	3	3	Medio
	Inadecuado tratamiento de datos personales de estudiantes y docentes	3	1	3	Medio
	Falta de contratos o convenios actualizados con docentes externos	2	3	6	Alto
Administrativo	Errores en la gestión de matrículas y registros estudiantiles	1	1	1	Bajo
	Mala planificación presupuestaria	2	3	6	Alto
	Baja eficiencia en los procesos de compras públicas	2	3	6	Alto
	Desorganización en el archivo documental institucional	2	1	2	Bajo
	Falta de seguimiento a convenios de cooperación interinstitucional	2	1	2	Bajo
Reputacional	Malas opiniones públicas en redes sociales sobre la calidad educativa	2	3	6	Alto
	Conflictos internos divulgados externamente	1	2	2	Bajo

Divulgación de incidentes de seguridad o privacidad	2	1	2	Bajo
Resultados negativos en evaluaciones externas o rankings	2	2	4	Medio
Falta de visibilidad institucional frente a otros institutos tecnológicos	1	2	2	Bajo

Fuente: *Instituto Tecnológico Superior Compu Sur*

5.6.5. Tratamiento de riesgo

En esta fase, la organización selecciona e implementa opciones estratégicas y operativas para modificar, reducir, transferir o aceptar los riesgos identificados, alineándose con sus criterios de riesgo y objetivos institucionales.

5.6.5.1.Generalidades

Para el análisis de tratamiento de riesgos se debe contar con una aprobación de las Autoridades del Instituto, considerando el contexto actual con posibles escenarios poco planificados se establece las siguientes estrategias para la gestión de riesgos:

- Riesgos Críticos: Deben darse gestión y reducirlo.
- Riesgos Altos: Deben darse gestión y reducirlo una opción válida es la transferencia del riesgo a terceros.
- Riesgos Medios: Se mantendrán en monitoreo y aceptación.
- Riesgos Bajos: Se mantendrán en aceptación.

5.6.5.2.Selección de las opciones para el tratamiento

Según la definición de las autoridades del instituto se procede a establecer la estrategia de reducción para los siguientes riesgos:

Tabla 39

Clasificación de riesgo

Riesgo especifico	Código de riesgo	Probabilidad x Impacto	Clasificación de riesgo
Falta de actualización curricular frente a demandas del mercado	ITEC_RC001	9	Crítico
Bajo rendimiento académico generalizado	ITEC_RC002	9	Crítico
Fallas en la infraestructura de red del campus	ITEC_RC003	9	Crítico
Obsolescencia de equipos tecnológicos y software	ITEC_RC004	9	Crítico
Sanciones por falta de informes al CES o Senescyt	ITEC_RC005	9	Crítico

Fuente: *Instituto Tecnológico Superior Compu Sur*

Tabla 40

Clasificación de riesgo

Riesgo especifico	Código de riesgo	Probabilidad x Impacto	Clasificación de riesgo
Pérdida de datos por mal uso de respaldos	ITEC_RA001	6	Alto
Incumplimiento de la Ley Orgánica de Protección de Datos Personales	ITEC_RA002	6	Alto
Falta de contratos o convenios actualizados con docentes externos	ITEC_RA003	6	Alto
Mala planificación presupuestaria	ITEC_RA004	6	Alto
Baja eficiencia en los procesos de compras públicas	ITEC_RA005	6	Alto
Malas opiniones públicas en redes sociales sobre la calidad educativa	ITEC_RA006	6	Alto

Fuente: *Instituto Tecnológico Superior Compu Sur*

5.6.5.3.Preparación e implantación de los planes de tratamiento de riesgos

Para una adecuada gestión de los planes de tratamiento de riesgos se asignará un plan de acción con su identificador, titulo, descripción y responsable interno. Adicionalmente se establecerán fechas de priorización y periodos de monitoreo.

Tabla 41

Preparación e implementación de los planes de tratamiento de riesgos

Código de riesgo	Título del plan de acción	Descripción del plan de acción	Responsable del instituto	Tipo de plan de acción	Coste aproximado	Prioridad (Fecha de cierre)	Periodo de monitoreo
ITEC_RC001	Actualización Curricular Continua	Establecer un comité permanente de revisión curricular con participación del sector productivo.	Coordinación Académica	Preventivo	$5.000	2025-12-01	Trimestral
ITEC_RC002	Plan de Refuerzo Académico	Implementar tutorías personalizadas y seguimiento de estudiantes en riesgo académico.	Departamento Académico	Correctivo	$3.000	2025-10-15	Mensual
ITEC_RC003	Mejora de Infraestructura de Red	Modernizar y ampliar la red interna del campus con equipos de respaldo.	Unidad de TI	Correctivo	$10.000	2025-11-30	Mensual
ITEC_RC004	Plan de Renovación Tecnológica	Adquirir nuevos equipos y actualizar licencias de software obsoletas.	Unidad de TI	Preventivo	$15.000	2025-12-15	Semestral
ITEC_RC005	Fortalecimiento del Cumplimiento Regulatorio	Establecer un calendario automatizado de entregables y alertas de cumplimiento ante CES/Senescyt.	Secretaría General	Preventivo	$2.000	2025-09-30	Trimestral
ITEC_RA001	Gestión Segura de Respaldos	Capacitar al personal y automatizar políticas de respaldo con control de integridad.	Unidad de TI	Correctivo	$4.000	2025-08-30	Mensual
ITEC_RA002	Cumplimiento LOPDP	Elaborar políticas y procedimientos para el tratamiento adecuado de datos personales.	Oficial de Protección de Datos	Preventivo	$2.500	2025-09-15	Trimestral
ITEC_RA003	Gestión de Contratos Docentes	Actualizar y centralizar convenios y contratos con mecanismos de revisión periódica.	Dirección Administrativa	Correctivo	$1.500	2025-10-01	Trimestral
ITEC_RA004	Planificación Presupuestaria Responsable	Implementar software de gestión financiera con revisión	Finanzas	Correctivo	$3.000	2025-10-31	Semestral

		participativa de presupuestos.					
ITEC_RA005	Optimización de Compras Públicas	Capacitación en normativas de contratación pública y control cruzado de adquisiciones.	Compras Públicas	Preventivo	$2.000	2025-09-25	Trimestral
ITEC_RA006	Gestión de Reputación Institucional	Monitorear redes sociales y establecer un comité de respuesta ante crisis de imagen.	Comunicación Institucional	Correctivo	$3.500	2025-09-10	Mensual

Fuente: *Instituto Tecnológico Superior Compu Sur*

5.6.6. Seguimiento y revisión

El seguimiento y revisión del sistema de gestión de permite asegurar su efectividad, adaptación y mejora continua en el tiempo. En el caso del Instituto Tecnológico Superior Compu Sur (ITECSUR), este proceso tiene como propósito principal verificar el cumplimiento de los objetivos institucionales, evaluar la eficacia de las medidas de tratamiento implementadas y garantizar la alineación del sistema con los cambios del entorno educativo, legal y tecnológico.

Los objetivos a cumplirse por parte de los procesos de revisión y seguimiento, son:

- Verificar que los riesgos se gestionen según los criterios establecidos.
- Evaluar la eficacia de los controles y planes de tratamiento.
- Detectar desviaciones, incidentes o nuevas amenazas no previstas.
- Actualizar el marco de gestión ante cambios internos o externos.

Las actividades de seguimiento y revisión se realizarán sobre las siguientes actividades:

Tabla 42

Seguimiento y revisión

Actividad	Responsable	Frecuencia	Descripción
Revisión de los indicadores clave de riesgos (KRI)	Coordinador de Gestión de Riesgos / Jefes de área	Trimestral	Evaluación de métricas sobre incidentes, impactos, respuestas implementadas, y desempeño del sistema.
Seguimiento de acciones correctivas y preventivas	Responsable del riesgo / Dirección administrativa	Mensual	Se monitorea el cumplimiento del cronograma de planes de tratamiento, su ejecución y resultados.
Revisión por la alta dirección	Rectorado / Dirección Ejecutiva	Semestral	Evaluación estratégica del sistema de gestión, incluyendo cumplimiento de objetivos, cambios normativos, ajustes presupuestarios y decisiones de mejora.

Fuente: *Instituto Tecnológico Superior Compu Sur*

Como parte del proceso de seguimiento de acciones correctivas y preventivas se establecerá el siguiente formato de evaluación.

Tabla 43

Proceso de seguimiento de acciones correctivas y preventivas

Riesgo especifico	Código de riesgo	Probabilidad x Impacto	Clasificación de riesgo	Nivel de madurez del control y plan de acción	Nivel de riesgo final
Falta de actualización curricular frente a demandas del mercado	ITEC_RC001	9	Crítico		
Bajo rendimiento académico generalizado	ITEC_RC002	9	Crítico		
Fallas en la infraestructura de red del campus	ITEC_RC003	9	Crítico		
Obsolescencia de equipos tecnológicos y software	ITEC_RC004	9	Crítico		
Sanciones por falta de informes al CES o Senescyt	ITEC_RC005	9	Crítico		

Fuente: *Instituto Tecnológico Superior Compu Sur*

Se establece que los niveles de madurez establecerán los siguientes objetivos de reducción de riesgos:

- Control Gestionado: Los procesos o controles están planificados y se asignan un presupuesto requerido de implementación. Reducción del nivel de riesgo del 10%.
- Control Definido: Los procesos o controles están implementados, estandarizados y documentados. Reducción del riesgo del 50%.
- Control Cuantitativamente Gestionado: Los procesos o controles se miden cuantitativamente y se gestionan para alcanzar objetivos específicos. Reducción del riesgo del 75%.
- Control Optimizado: Los procesos o controles se mejoran continuamente a través de la retroalimentación y la innovación. Reducción del riesgo del 90%.

5.6.7. Registro e informe

La gestión de riesgos no solo requiere la identificación, evaluación y tratamiento adecuado de los riesgos, sino también un sistema robusto de registro, supervisión y comunicación continua. Este componente permite garantizar la trazabilidad de las decisiones, verificar la eficacia de las acciones implementadas, y detectar cambios internos o externos que puedan generar nuevos riesgos o modificar los ya identificados.

5.6.7.1.Medios de comunicación

ITECSUR establecerá un sistema de medios y canales de comunicación institucional para documentar, comunicar y archivar toda la información relacionada con la gestión de riesgos. Este sistema incluirá:

- Presentación de informe a las autoridades y dirección en las reuniones semestrales con el detalle del sistema con los siguientes datos:
    - Riesgos identificados y su clasificación.
    - Evaluación de impacto y probabilidad.
    - Planes de tratamiento implementados y en progreso.
    - Responsables y fechas de revisión para planes de acción.
    - KPI del SGR.
- Socialización de resultados de implementación de planes de acción:
    - A través de Informes trimestrales dirigidos a las autoridades y jefes de área.
    - Presentación de resultados en los minutos cívicos mensuales sobre la gestión de los principales riesgos.
    - Publicación de los KPI del SGR en la intranet del personal.
    - Boletines o comunicados internos sobre riesgos emergentes.
- Comunicación con partes externas (cuando corresponda):
    - Reportes a la Senescyt, CES o entes regulatorios en caso de riesgos normativos cuando se requiera.
    - Informes públicos resumidos como parte del portal de transparencia institucional de manera anual en el estatus de rendición de cuentas.
    - Habilitación de canales de atención para recibir alertas o sugerencias desde estudiantes o comunidad.

5.6.7.2.Cronograma de actividades

Con el fin de mantener el sistema actualizado y promover una mejora continua, se establecerá un cronograma institucional que definirá las fechas y responsables para la implementación, monitoreo y revisión de acciones relacionadas con los riesgos identificados. Este cronograma incluirá:

Tabla 44

Cronograma de actividades

Actividad	Responsable	Frecuencia	Fecha	Objetivo
Revisión de riesgos identificados	Coordinador de riesgos	Trimestral	Octubre 2025	Verificar que los riesgos sigan vigentes o detectar cambios en su contexto.
Actualización de planes de tratamiento	Responsables de cada área	Semestral	Diciembre 2025	Ajustar acciones preventivas o correctivas según resultados o nueva información.
Reunión de comité de riesgos	Comité de riesgos institucional	Trimestral	Octubre 2025	Evaluar estado de planes, asignar nuevas responsabilidades y coordinar recursos.
Auditorías internas del sistema de gestión de riesgos	Auditoría interna	Anual	Marzo 2026	Evaluar cumplimiento, eficacia y trazabilidad del sistema.
Reporte consolidado a la Dirección	Coordinación de riesgos	Semestral	Diciembre 2025	Informar a la alta dirección sobre avances, desviaciones y acciones prioritarias.

Fuente: *Instituto Tecnológico Superior Compu Sur*

5.6.8. Auditoría Interna

La auditoría interna dentro del marco de la gestión de riesgos conforme a la norma ISO 31000:2018 es una herramienta fundamental que permite verificar la eficacia, adecuación y aplicabilidad de las acciones implementadas para tratar los riesgos

identificados. Este proceso proporciona una visión objetiva e independiente sobre la correcta ejecución del sistema de gestión y su alineación con los objetivos institucionales.

En el contexto de ITECSUR, la auditoría interna busca garantizar que las medidas adoptadas sean prácticas, sostenibles y contribuyan a reducir o controlar los niveles de riesgo, sin interferir negativamente en los procesos académicos, administrativos o tecnológicos.

5.6.8.1.Objetivos

- Evaluar la eficacia de los planes de tratamiento de riesgos ejecutados por las distintas áreas del instituto, verificando si han logrado mitigar el riesgo conforme a lo planificado.
- Revisar la adecuada documentación, trazabilidad y comunicación de los riesgos, sus controles y resultados, garantizando la transparencia y coherencia con los lineamientos de la ISO 31000.
- Detectar desviaciones, omisiones o riesgos emergentes que no hayan sido gestionados correctamente o que se hayan agravado por cambios internos o externos.
- Proponer recomendaciones de mejora continua, acciones correctivas o ajustes a la estrategia de gestión de riesgos, fomentando la cultura de responsabilidad y cumplimiento en todos los niveles institucionales.

5.6.8.2.Procesos de la Auditoría interna

La auditoría cumplirá con la siguiente estructura metodológica compuesta por las siguientes fases:

Planificación: En esta etapa se define el alcance de la auditoría, especificando los procesos, áreas y riesgos que serán evaluados. Se establecen los criterios de evaluación, que pueden incluir normativas legales, políticas institucionales, lineamientos de ISO 31000 o resultados esperados de planes de acción. Además, se diseña un cronograma de actividades, asignando recursos, auditores y responsables para asegurar el cumplimiento dentro de los tiempos establecidos, con mínimo impacto operativo.

2. Ejecución: Durante esta fase, los auditores internos llevan a cabo la revisión documental (planes de tratamiento, bitácoras de incidentes, actas de comité), realizan entrevistas al personal clave y ejecutan observaciones en terreno para verificar si las acciones implementadas son efectivas, si los controles están funcionando correctamente, y si existe conciencia del riesgo en los actores involucrados. Esta etapa busca identificar buenas prácticas, desviaciones o debilidades en la gestión.

Informe: Con base en la información recolectada, se elabora un informe técnico de auditoría, en el que se documentan los hallazgos relevantes, incluyendo no conformidades, observaciones y oportunidades de mejora. Este informe debe ser claro, verificable y alineado a los objetivos de la auditoría, y será compartido con las autoridades institucionales y responsables de las áreas auditadas.

4. Seguimiento: Una vez entregado el informe, se realiza una verificación del cumplimiento de las acciones correctivas o preventivas recomendadas. Este seguimiento

garantiza que los problemas detectados se resuelvan en tiempo oportuno y que los procesos de riesgo evolucionen hacia una mayor eficacia. Las actividades de seguimiento se integran al ciclo de mejora continua del sistema.

Como resultante del proceso de auditoría interna se contará con el siguiente modelo de informe. Ver ANEXO 2. Modelo de Auditoría Interna.

5.6.8.3.No conformidades y acciones correctivas

En el marco del sistema de gestión de riesgos basado en la norma ISO 31000:2018, las no conformidades se entienden como desviaciones significativas respecto a los criterios, políticas, procedimientos o controles establecidos para gestionar los riesgos. Estas pueden detectarse durante auditorías internas, evaluaciones periódicas, seguimiento de indicadores, o mediante denuncias y retroalimentación de partes interesadas. Parala identificación de no conformidades en el Instituto como proceso interno, se considera:

- Identificación de la causa raíz: Una vez detectada una no conformidad, el primer paso es determinar su causa raíz. Esto implica no solo identificar el efecto inmediato, sino también analizar qué falló en el proceso, sistema, capacitación o cultura organizacional que permitió que ocurriera. Como parte del proceso de ITECSUR se utilizará la herramienta de los “5 porques”.
- Aplicación de acciones correctivas: Una vez comprendida la causa raíz, se diseñan y ejecutan acciones correctivas específicas para corregir el problema y prevenir su recurrencia. Estas acciones pueden incluir:
    - Modificación de procedimientos operativos.

- Refuerzo en capacitaciones o sensibilización.
- Implementación de nuevos controles técnicos o administrativos.
- Reasignación de responsabilidades o funciones.

- Verificación de la eficacia: Una vez implementadas las acciones correctivas, es necesario realizar una verificación de su eficacia, la cual puede incluir:
  - Revisiones de seguimiento.
  - Auditorías específicas al área involucrada.
  - Indicadores de cumplimiento o pruebas de control.
  - Retroalimentación de los usuarios o partes interesadas.

Como resultados de la No Conformidad se contará con el siguiente modelo de informe. Ver ANEXO 4. Modelo de No Conformidades.

Capítulo 6
Conclusiones y Aplicaciones

6.1. Conclusiones generales

El presente estudio identifica la importancia de contar con un manual de implementación de un sistema de gestión de riesgos integral en el Instituto Tecnológico Superior Compu Sur (ITECSUR). La propuesta basada en la norma ISO 31000:2018 responde a la necesidad de estructurar procesos claros de identificación, análisis, tratamiento y monitoreo de riesgos, alineados con las exigencias legales y operativas actuales, con un enfoque en la gestión de riesgos académicos, tecnológicos, legales, normativos, administrativos y reputacionales. La gestión de riesgos no solo mitiga amenazas y vulnerabilidades tecnológicas y operativas, sino que contribuye a fortalecer la gobernanza y la cultura organizacional, enfocada en la comunidad educativa y el cumplimiento de los objetivos estratégicos establecidos por la institución.

6.2. Conclusiones específicas

6.2.1. Análisis del cumplimiento de los objetivos de la investigación

El desarrollo del estudio permite afirmar que se ha cumplido satisfactoriamente con el objetivo general planteado en diseñar un modelo de gestión de riesgos basado en la norma ISO 31000:2018. En el proceso de investigación se identificó los activos críticos de información en ITECSUR, se evaluaron los riesgos asociados a su proceso crítico de gestión académica y se proponen controles técnicos y organizativos adecuados y viables para su implementación por parte del instituto. Además, el manual de implementación desarrollado

constituye una guía práctica que facilita la aplicación del modelo en la realidad operativa de la institución.

6.2.2. Contribución a la gestión empresarial

La propuesta representa una herramienta de gran utilidad para la toma de decisiones estratégicas dentro de la gestión educativa, al ofrecer un marco estructurado para el análisis y mitigación de riesgos. Permite a la institución cumplir con normativas como la ISO 31000:2018, Ley Orgánica de Protección de Datos Personales y enfrentar con mayor preparación amenazas emergentes como ciberataques o fugas de información. También aporta a la eficiencia operativa al reducir la incertidumbre y establecer roles y responsabilidades claras.

6.2.3. Contribución a nivel académico

Desde una perspectiva académica, este proyecto ha sido para el grupo de trabajo una valiosa oportunidad de aplicar metodologías estructuradas y normativas para la gestión de riesgos, específicamente bajo el marco de la norma ISO 31000:2018. El desarrollo del estudio ha permitido al equipo adquirir competencias en el análisis integral de riesgos, la priorización de acciones y la toma de decisiones basadas en procesos sistemáticos y objetivos. Este enfoque contribuye al fortalecimiento del pensamiento crítico y analítico en la resolución de problemas complejos dentro del entorno educativo y profesional. Además, el trabajo realizado constituye una guía práctica que puede servir como referencia para futuras investigaciones sobre la integración de modelos de gestión de riesgos en instituciones de

educación superior y su alineación con el cumplimiento normativo y buenas prácticas internacionales.

6.2.4. Contribución a nivel personal

Para los autores el desarrollo del trabajo de investigación significó un proceso de aprendizaje profundo sobre gestión de riesgos, cumplimiento normativo y planificación estratégica. Permitió el fortalecimiento de competencias técnicas en la identificación de activos de información, análisis de vulnerabilidades, la evaluación de controles, evaluación de riesgos integrales, establecimiento de apetito y estrategias de riesgos, el diseño de planes de mejora y ejecución de procesos de auditoría interna. Adicionalmente fomentó el trabajo en equipo, la toma de decisiones basadas en evidencia e información más fiable y una mayor conciencia sobre la importancia de la gestión de riesgos en todos los ámbitos profesionales.

6.3. Limitaciones a la Investigación

Una de las principales limitaciones encontradas durante el desarrollo de este trabajo fue la falta de información histórica detallada sobre incidentes, riesgos identificados previamente y métricas de gestión en el Instituto Tecnológico Superior Compu Sur (ITECSUR). Esta carencia de datos dificultó el análisis de tendencias propias de la institución y limitó la posibilidad de fundamentar decisiones exclusivamente en su contexto real. Como consecuencia, el diseño de la metodología y la definición de los planes de acción se apoyaron en estándares, guías normativas y tendencias observadas en instituciones educativas similares, más que en la experiencia y datos específicos de ITECSUR.

No obstante, estas limitaciones constituyen una oportunidad para futuros trabajos de investigación e implementación que aborden el seguimiento operativo del modelo, su retroalimentación y su adaptación continua, contribuyendo a fortalecer de manera progresiva la cultura de gestión de riesgos en ITECSUR.

Bibliografía

Álvarez-Carrión, J. A., & Hernández-Sotomayor, G. P. (2024). Protección de datos personales en plataformas educativas digitales en el sistema de educación superior de Ecuador. *MQRInvestigar*, *8*(3), 5324–5339. https://doi.org/10.56048/MQR20225.8.3.2024.5324-5339

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial N.º 459. https://www.registroficial.gob.ec

Betancourt, D. F. (2018, abril 19). *Cómo hacer el análisis FODA (matriz FADO) paso a paso + ejemplo práctico*. Ingenio Empresa. Recuperado el 11 de junio de 2025 de https://www.ingenioempresa.com/matriz-foda

Cedeño Zambrano, R. M., & Morell González, L. M. (2018). La gestión de riesgos en Ecuador: una aproximación evolutiva desde el control interno. *Cofin Habana*, *12*(2), 306–318. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2073-60612018000200022

Constitución de la República del Ecuador. (2008). *Constitución vigente del Ecuador*. https://www.asambleanacional.gob.ec

Goberna, R. (2024). *La creciente amenaza de los ciberataques en Ecuador*. Grupo Goberna. https://grupogoberna.com

Instituto Tecnológico Superior Compu Sur. (2023). *Política de gestión de riesgos*. ITECSUR.

Instituto Tecnológico Superior Compu Sur. (2023). *Procedimiento de auditoría interna*. ITECSUR.

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

ISO/IEC. (2018). ***ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management*****. ISO.**

Lule-Uriarte, M. N., Serrano-Mesía, M. M., & Montenegro-Cruz, N. Y. (2023). La gestión educativa: factor clave en la calidad educacional. ***Revista Científica UISRAEL*****,** ***10*****(3), 57–71. https://doi.org/10.35290/rcui.v10n3.2023.893**

Moran Maldonado, D. M. (2023). ***La gestión de riesgos mediante aplicación de la norma ISO 31000 en la Unidad Educativa Antonio Ante*** **[Tesis de pregrado, Universidad Técnica del Norte]. https://repositorio.utn.edu.ec/handle/123456789/13421**

Oliveira, J., & Fernandes, C. (2021). Risk management in higher education institutions: Application of ISO 31000. ***Journal of Risk and Financial Management*****,** ***14*****(6), 251. https://doi.org/10.3390/jrfm14060251**

Ubicación de ITECSUR, Ecuador. Fuente: Google. (s.f.). ***[Itecsur matriz, Ecuador]*****. Google Maps. Recuperado el 16 de abril de 2025 de https://www.google.com/maps/place/Quito**

ANEXOS

ANEXO 1. Procedimiento de elaboración de un procedimiento normalizado de trabajo.

ITECSUR	**PROCEDIMIENTO GENERAL**	**PN/PGA/001/01** **Página 1 de 6** **Rev: 0** **Fecha de Edición:**
	PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO NORMALIZADO DE TRABAJO	
Procedimientos relacionados:		

INDICE

Redactado por:	Revisado por:	Aprobado por:

Procedimiento de elaboración de Procedimientos Normalizados de Trabajo (PNT)		Código: **PN/PGA/001/01**
		Página: 2 de 6
Procedimientos relacionados:		

1. Objetivo

Identificar los distintos tipos de procedimientos que se realizan en el día a día dentro del Instituto Superior Universitario Compu Sur-campus matriz y establecer los pasos a seguir para la elaboración, revisión y control de los Procedimientos Normalizados de Trabajo (PNT)

2. Responsabilidad de aplicación y alcance

La responsabilidad y alcance de este procedimiento recae sobre todo el personal técnico del Instituto Superior Universitario Compu Sur campus matriz que cree un PNT.

3. Definiciones

Procedimiento: Conjunto de acciones que deben realizarse de manera ordenada y sistemática para cumplir con un proceso y alcanzar resultados óptimos dentro de una empresa.

Procedimiento Normalizado de Trabajo: Documento que describe detalladamente como debe realizarse una tarea específica para asegurar uniformidad y eficiencia en el producto a alcanzar.

Responsable del proceso: Persona que ha sido encargada la elaboración de un PNT.

4. Descripción

Los procedimientos que se podrán crear dentro del Instituto Superior Universitario Compu Sur-campus matriz son:

Procedimiento de elaboración de Procedimientos Normalizados de Trabajo (PNT)	Código: **PN/PGA/001/01**
	Página: 3 de 6
Procedimientos relacionados:	

- **Procedimientos Generales o de Actividades (PGA):** Describen las acciones o actividades que se realizan diariamente dentro del Instituto y que suman para el alcance de la planificación estratégica del Instituto.
- **Procedimientos de Productos (PP):** Describen las acciones o actividades que realizan los funcionarios del Instituto para la creación de nuevos productos en beneficio de los estudiantes.
- **Procedimientos de Servicios (PS):** Describen las acciones o actividades que realizan los funcionarios del instituto para brindar los mejores servicios a cada uno de los estudiantes del Instituto.

Portada y encabezamiento: Los procedimientos deberán contener el nombre del Instituto, el grupo al que pertenece el procedimiento (Generales o de actividades, productos o servicios), título del PNT.

Número de Código: El código del procedimiento deberá estar compuesto de la siguiente manera:

PN (Procedimiento Normalizado)

PGA, PP, PS (De acuerdo al tipo de procedimiento)

001 (Número de identificación del procedimiento)

Procedimiento de elaboración de Procedimientos Normalizados de Trabajo (PNT)	Código: **PN/PGA/001/01**
	Página: 4 de 6
Procedimientos relacionados:	

01 (Número de versión del procedimiento)

Quedando finalmente el código del procedimiento de la siguiente manera: PN/PGA/001/01

Finalmente la portada y encabezamiento deberá contener:

Fecha de aprobación

La persona que lo ha redactado con la firma y fecha

La persona que revisado y aprobado con la firma y fecha.

Los pasos a seguir para la elaboración de nuevos procedimientos serán los siguientes:

- Detectar la necesidad de un nuevo PNT o revisión de uno existente.
- Asignar un responsable de la elaboración del PNT.
- Redactar el borrador del PNT tomando en cuenta todas las recomendaciones realizadas en este procedimiento.
- Revisión técnica del PNT.
- Ajustar borrador según las observaciones realizadas.
- Aprobar el PNT.
- Publicar el PNT en el medio oficial.

- Informar al personal involucrado.

Procedimiento de elaboración de Procedimientos Normalizados de Trabajo (PNT)	Código: **PN/PGA/001/01**
	Página: 5 de 6
Procedimientos relacionados:	

4.1. Apartados de los procedimientos normalizados de trabajo

En todos los PNT del Instituto deberán existir los siguientes apartados:

- Objetivo: Explicar de manera clara y concisa el objetivo del procedimiento.
- Responsabilidad de aplicación y alcance: Establecer quién es el responsable de la aplicación de este procedimiento.
- Definiciones: Colocar todas las definiciones que sean necesarias para que el procedimiento sea de fácil entendimiento.
- Descripción: Se deberá especificar todas las especificaciones necesarias que deberá contener el procedimiento.
- Registros: Se deberá explicar los registros que se genere el procedimiento, en caso de no existir se deberá colocar no aplica.
- Control de copias y registro de lectura del procedimiento: Se debe registrar la cantidad de copias entregadas y quien ha leído cada una de las copias.
- Anexos: Se incluirán todos los que sean necesarios dependiendo el procedimiento.

4.2. Redacción de los procedimientos

Procedimiento de elaboración de Procedimientos Normalizados de Trabajo (PNT)	Código: **PN/PGA/001/01** **Página: 6 de 6**
Procedimientos relacionados:	

Los procedimientos deberán ser redactados de manera clara y concisa, deberán ser de fácil comprensión para los funcionarios, en todos los casos se deberá evitar crear dudas en su redacción, en caso de que alguno de los apartados no sea necesario se deberá colocar no aplica.

4.3. Distribución

El procedimiento deberá ser distribuido a todo el personal que vaya a poner en práctica este procedimiento y se debe llevar un registro de las copias distribuidas y del personal que haya leído el procedimiento.

4.4. Revisión y control de cambios

Este procedimiento deberá ser revisado periódicamente y en caso de sufrir cambios deberán ser registrados y notificados a todo el personal que tenga competencia en este procedimiento. Se recomienda llevar un registro para el control de cambios

5 Registros

En caso de existir cambios se deberán registrar en la siguiente tabla:

Versión No.	Cambios realizados	Fecha

6 Control de copias y registro de lectura del procedimiento

Se debe llevar un registro de la cantidad de copias entregadas y quien ha leído cada una de estas copias:

Nombre	Firma	Fecha

ANEXO 2. Modelo de Auditoría Interna

1. Propósito

Definir el proceso para planificar, realizar y documentar auditorías internas del SGR, evaluando su conformidad con la ISO 31000:2018 y la eficacia de la gestión de riesgos en el instituto.

2. Alcance

Aplica a todas las actividades y procesos del instituto ITECSUR en su sede matriz.

3. Responsabilidades

Auditor Líder:

- Coordinar el programa de auditoria interna.
- Supervisar los resultados diarios de los hallazgos del equipo auditor.
- Presentar los resultados acordados a las autoridades.

Equipo Auditor:

- Realizar las auditorias siguiente el procedimiento establecido.
- Solicitar y recopilar las evidencias objetivas de la evaluación.
- Detallar los hallazgos en lenguajes entendibles para su contraparte.
- Elaborar el informe de auditoria con el registro de no conformidades.

Responsables de áreas auditadas:

- Asegurar la agenda requerida para la revisión de auditoria en relaciona al cronograma de trabajo.
- Proveer el acceso a la información de evidencias requerida por el equipo auditor.
- Implementar las acciones acordadas con la auditoria para la mejora continua.

4. Definiciones

Auditoría Interna: Proceso independiente y documentado para evaluar la conformidad del SGR con los requisitos establecidos.

No Conformidad: Incumplimiento de un requisito del sistema de gestión.

Oportunidades de mejora: Hace referencia a mejoras que puede tener el sistema que no están relacionados a incumplimientos de requisitos, sino que nacen de la experiencia de revisión.

Acción Correctiva: Medida para eliminar la causa de una no conformidad.

5. Procedimiento

5.1. Planificación de auditoría

1. Definir el alcance y objetivo:

- Se identifica el procesos, actividades y sede del instituto como parte de la evaluación.

- Se debe establecer los objetivos específicos de evaluación.

2. Elaborar el programa de auditoria:

- El programa de auditorias internas periódicas se debe desarrollar considerando una revisión documental y una visita en sitio.

3. Designar el equipo auditor:

- Se asegurará la independencia e imparcialidad del auditor interno. En caso de no poder contar con el auditor o sus capacidades, se debe contratar a un consultor independiente.
- Se debe asegurar las capacidades y conocimientos de los auditores internos y auditor líder a través de certificaciones verificadas.

5.2. Ejecución de auditoría

1. Reunión de apertura:

- Presentación del equipo auditor.
- Confirmación de alcance, reuniones y actores del día.
- Aclaración de roles y responsabilidades.

2. Revisión documental:

- Verificación de cumplimiento de la implementación de la norma a través de cuestionario de las cláusulas. Se solicitará la revisión de políticas, procesos, procedimientos y registros requeridos.

3. Recolección de evidencias:

- Se realizará entrevistas con los responsables para la validación del cumplimiento documental.
- Revisión de resultados de los controles e implementaciones realizadas.

4. Evaluación de conformidad:

- Se comparará las evidencias recopiladas en relación al cumplimiento de la norma.
- Se identificarán las fortalezas, no conformidades y oportunidades según aplique.

5. Reunión de cierre:

- Se presentará las fortalezas y hallazgos obtenidos de la revisión.

5.3. Informe de auditoría

1. Preparación del informe:

- El informe detallará los siguientes campos de sustentación:

1. Alcance y objetivo de la auditoría.
2. Evidencias obtenidas.
3. No conformidades y oportunidades de mejora detectadas.

2. Comunicación de resultados:

- Presentación del informe a las autoridades y dirección del instituto.
- Discusión de los hallazgos y acciones requeridas.
- Generación de informe final.

5.4. Seguimiento

1. Acciones correctivas:

- Se establecen las acciones correctivas a través de un plan de acción a los responsables correspondientes con el objetivo de atacar la causa raíz a través de la aplicación de la

metodología de los 5 porques.

- Se establecen plazos de planes de acción según la prioridad.

2. Verificación:

- Evaluación de eficacia de las acciones correctivas una vez se hayan implementado.
- Documentación del cierre de la no conformidad con las evidencias respectivas.

6. Registros

- Programa de auditoría.
- Plan de auditoría.
- Lista de verificación basada en la norma ISO 31000:2018.
- Norma ISO 31000:2018.
- Informe de auditoria interna.
- Registro de no conformidades.
- Registro de acciones correctivas y mejoras.

7. Referencias

- ISO/IEC 31000:2018.
- Procedimiento de auditoría interna.
- Política de Gestión de riesgos.

ANEXO 3. Modelo de Informe de No Conformidades

INFORME DE NO CONFORMIDAD

Empresa: [NOMBRE]

Centro/Sede: [ESPECIFICAR]

Tipo de auditoría: [DOCUMENTAL/EN SITIO]

Auditor: [NOMBRE]

Fecha: [FECHA]

Referencia normativa de no conformidad: [CLÁUSULA DE LA NORMA]

PROCESO	DESCRPICIÓN [DECRIPCIÓN DEL PROCESO]
CRITERIOS DE REFERENCIA:	[DESARROLLO DE LA MUESTRA OBTENIDA]
CRITERIOS DE LA NO CONFORMIDAD	[DESCRIPCIÓN DE LA NO CONFORMIDAD, SE DEBE DETALLAR EL INCUMPLIMIENTO EN RELACIÓN A LA NORMA Y LA MUESTRA OBTENIDA]
CAUSA	[EVALUACIÓN DE LOS 5 PORQUES E IDENTIFICACIÓN DE PROCESOS Y RESPONSABLES INVOLUCRADOS]
PROPUESTA DE ACCIÓN CORRECTIVA	[DESCRIPCIÓN DEL PLAN DE ACCIÓN CORRECTIVO]
	[DATOS DE REGISTRO DE ACCIÓN CORRECTIVA. ACCIÓN: RESPONSABLE: NOMBRE Y FIRMA: FECHA DE INICIO: FECHA DE CIERRE]
Firma del Auditado: [FIRMA]	Firma del Auditor [FIRMA]

FICHA DE VERIFICACIÓN

RESPONSABLE DE VERIFICACIÓN: [NOMBRE]	FECHA DE VERIFICACIÓN: [FECHA]
METODO DE VERIFICACIÓN:	[DESCRIPCIÓN DE INDICADOR DE AVANCE SOBRE PLAN DE ACCIÓN]
EVIDENCIAS Y REGISTROS CONSTATADOS	[DESCRIPCIÓN DE REVISIÓN DE EVIDENCIAS Y MUESTRAS]
OBSERVACIONES	[NOVEDADES DE CORRECIÓN QUE SE VISUALIZAN EN EL PLAN DE ACCIÓN]
Firma del Verificador: [FIRMA]	Firma del Auditor [FIRMA]