



PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Oficina de Gestión Informática –
Sistemas y Soporte Técnico

23Enero2026

Vigilancia y Mejora Continua



SG-CFR136975



Universidad Tecnológica del Chocó Diego Luis Córdoba
Nit. 891680089-4

Carrera 22 #18B-10 B. Nicolás Medrano – Ciudadela Universitaria
Tel: (+57) 6046726565. Línea gratuita: 018000338324

contactenos@utchedu.co, notificacionesjudiciales@utchedu.co

utchedu.co

Quibdó, Chocó (Colombia)



INTRODUCCIÓN

En cumplimiento del Decreto 612 de 2018 y conforme a los requisitos del *Sistema de Gestión de Seguridad de la Información (SGSI)* basado en *ISO/IEC 27001:2022*, la **Universidad Tecnológica del Chocó** establece el presente siguiente **Plan de Tratamiento de Riesgos de Seguridad de la Información**, con el propósito de gestionar de forma sistemática los riesgos asociados al uso, procesamiento, almacenamiento y transmisión de información institucional, para la vigencia 2026.

La Universidad Tecnológica del Chocó, en cumplimiento de la normativa vigente y alineada con *ISO/IEC 27001*, establece el Plan de Tratamiento de Riesgos para gestionar las amenazas que afectan la confidencialidad, integridad y disponibilidad de la información institucional.

El plan define, para cada riesgo identificado: el activo afectado, la valoración, la opción de tratamiento (evitar, reducir, transferir o aceptar), los controles aplicables según *ISO/IEC 27001*, los responsables, los plazos y los indicadores de seguimiento.

Este instrumento permite disminuir el riesgo residual a niveles aceptables, soporta la toma de decisiones de la Alta Dirección y contribuye al cumplimiento de los objetivos estratégicos institucionales. Su ejecución se articula con los líderes de proceso y se supervisa mediante indicadores, auditorías, incidentes y revisión por la dirección, garantizando mejora continua del SGSI.

OBJETIVOS

Objetivo General

Establecer e implementar un Plan de Tratamiento de Riesgos que reduzca el riesgo residual de los activos de información a niveles aceptables, preservando la confidencialidad, integridad y disponibilidad de la información institucional en cumplimiento de los lineamientos del SGSI.

Objetivos Específicos

- **Identificar y analizar** los riesgos asociados a los activos de información dentro del alcance del SGSI.



Código: 530

- **Dar cumplimiento a los lineamientos** del Gobierno Nacional y a lo expedido por el Ministerio de las TIC así como el cumplimiento de los requisitos legales y regulatorios pertinentes, relacionados con la seguridad de la información y la privacidad y protección de datos personales.
- **Seleccionar y aplicar** las opciones de tratamiento más adecuadas (evitar, reducir, transferir o aceptar) según la evaluación de riesgos.
- **Asignar controles, responsables y plazos** para la implementación del tratamiento de riesgos conforme al Anexo A de ISO 27001.
- **Monitorear y medir** la eficacia de los controles implementados mediante indicadores y seguimiento periódico.
- **Mantener y mejorar** continuamente el proceso de tratamiento de riesgos en coherencia con el ciclo PDCA del SGSI.
- **Promover la mejora continua**, mediante el proceso de gestión de riesgos de Seguridad de la Información y la evaluación de la eficacia de los planes de tratamiento

ALCANCE

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la Universidad Tecnológica del Chocó comprende la gestión, protección y tratamiento de la información institucional en sus dimensiones de confidencialidad, integridad, disponibilidad y privacidad. Este alcance aplica a los procesos, recursos tecnológicos, servicios digitales, infraestructura, personal interno y proveedores que participan en el ciclo de vida de la información, desde su creación hasta su disposición final.

El alcance se define en cumplimiento del **Decreto 612 de 2018**, la **Política de Gobierno Digital** y la **Política de Seguridad Digital**, las cuales establecen lineamientos para la gestión segura de la información y la continuidad digital de las entidades públicas. Adicionalmente, se alinea con los requisitos establecidos en la **Norma ISO/IEC 27001**, considerando el contexto institucional, las partes interesadas, los requisitos legales, los riesgos asociados a los activos de información y los servicios que soportan la operación académica, administrativa e investigativa de la Universidad.

Este alcance incluye los sistemas de información, plataformas digitales, servicios en la nube, redes institucionales, infraestructura física asociada, proveedores tecnológicos y el talento humano involucrado en la operación, administración, soporte y custodia de la información institucional, independientemente de su medio de almacenamiento o transmisión.



MARCO NORMATIVO

- **Constitución Política de Colombia (1991)**
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125>
Establece derechos fundamentales relacionados con la protección de datos personales, intimidad, habeas data e información pública.
- **Ley 1581 de 2012 — Protección de Datos Personales**
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49972>
Regula la protección de datos personales y establece principios y procedimientos para su tratamiento.
- **Decreto 1377 de 2013 — Reglamenta parcialmente la Ley 1581**
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=54113>
Define medidas de implementación para el tratamiento de datos personales y mecanismos de autorización.
- **Ley 1712 de 2014 — Transparencia y Acceso a la Información Pública**
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56652>
Garantiza el derecho de acceso a la información pública y establece obligaciones de publicación y protección.
- **Ley 527 de 1999 — Comercio Electrónico y Mensajes de Datos**
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=286>
Regula la validez jurídica de mensajes de datos, firmas digitales y comercio electrónico.
- **Ley 1341 de 2009 — TIC y Sociedad de la Información**
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36608>
Define principios del sector TIC, incluyendo acceso, seguridad y promoción de la información digital.
- **Decreto 612 de 2018 — Modelo de Seguridad y Privacidad de la Información (MSPI)**
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87356>
Establece lineamientos para la implementación del MSPI en entidades públicas y su integración con Gobierno Digital.
- **Decreto 1008 de 2018 — Política de Gobierno Digital**
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=87915>
Regula la adopción de Gobierno Digital, servicios ciudadanos digitales y gestión de información.



- **Decreto 333 de 2021 — Política de Seguridad Digital**

<https://www.suin-juriscal.gov.co/viewDocument.asp?id=30042820>

Actualiza lineamientos sobre seguridad digital, gestión del riesgo y capacidades institucionales.

2. Políticas y Lineamientos Mintic

- **Política de Gobierno Digital**

<https://www.mintic.gov.co/portal/inicio/Gobierno-Digital/>

Define lineamientos de transformación digital, seguridad, servicios ciudadanos y gestión de datos.

- **Política de Seguridad Digital**

<https://www.mintic.gov.co/portal/inicio/Politica-Seguridad-Digital/>

Establece estrategias y capacidades para proteger el entorno digital del Estado.

- **Modelo de Seguridad y Privacidad de la Información (MSPI)**

<https://www.mintic.gov.co/portal/inicio/Politica-Seguridad-Digital/Modelo-de-Seguridad-y-Privacidad-de-la-Informacion/>

Proporciona un marco de gestión del riesgo y controles para proteger la información estatal.

- **Modelo Integrado de Planeación y Gestión (MIPG)**

<https://www.funcionpublica.gov.co/web/mipg>

Integra dimensiones de gestión pública, incluyendo seguridad de la información y riesgo.

- **Manual de Gestión de Seguridad de la Información para el Estado**

https://www.mintic.gov.co/portal/604/articles-16378_manual_seguridad_informacion.pdf

Documento técnico que guía la implementación del MSPI en entidades públicas.

3. Protección de Datos — Autoridad Competente (SIC)

- **Superintendencia de Industria y Comercio (SIC) – Protección de Datos**

<https://www.sic.gov.co/proteccion-de-datos-personales>

Autoridad nacional que vigila y regula el cumplimiento de protección de datos personales.

- **Registro Nacional de Bases de Datos (RNBD)**

<https://www.sic.gov.co/registro-nacional-de-bases-de-datos>

Obligación para responsables del tratamiento de registrar bases de datos con información personal.



- **Normativa y Guías de Tratamiento de Datos**

<https://www.sic.gov.co/normatividad-proteccion-de-datos-personales>

Recopilación oficial de circulares, resoluciones y guías de cumplimiento.

4. Archivo y Gestión Documental

- **Archivo General de la Nación (AGN) – Normatividad**

<https://www.archivogeneral.gov.co/normatividad>

Regula el ciclo de vida de la información documental pública, incluyendo conservación, seguridad y acceso.

5. Normas Técnicas y Estándares Internacionales

(Las ISO se consultan mediante ficha oficial e implementación certificada.)

- **ISO/IEC 27001 — Sistemas de Gestión de Seguridad de la Información**

<https://www.iso.org/standard/82875.html>

Norma internacional que define requisitos para implementar, mantener y mejorar un SGSI.

- **ISO/IEC 27002 — Controles de Seguridad**

<https://www.iso.org/standard/75652.html>

Ofrece controles, prácticas y guías para proteger la información.

- **ISO/IEC 27005 — Gestión del Riesgo de Seguridad de la Información**

<https://www.iso.org/standard/80585.html>

Define metodologías para identificar, analizar y tratar riesgos de información.

- **ISO/IEC 22301 — Gestión de Continuidad del Negocio**

<https://www.iso.org/standard/75106.html>

Establece requisitos para asegurar continuidad operativa ante interrupciones.

- **ISO/IEC 27035 — Gestión de Incidentes de Seguridad**

<https://www.iso.org/standard/60803.html>

Guía para gestionar eventos e incidentes relacionados con seguridad de información.

- **NIST Cybersecurity Framework (CSF)**

<https://www.nist.gov/cyberframework>

Marco complementario de referencia mundial para ciberseguridad basado en identificación, protección, detección, respuesta y recuperación.



DEFINICIONES

- **SGSI:** Sistema para gestionar la seguridad de la información en la organización.
- **Activo de información:** Recurso con valor (datos, sistemas, infraestructura, personas).
- **Riesgo:** Posibilidad de daño a la información por amenazas y vulnerabilidades.
- **Control:** Medida para reducir un riesgo.
- **Confidencialidad:** Solo acceden quienes están autorizados.
- **Integridad:** Información correcta y sin alteraciones no autorizadas.
- **Disponibilidad:** Información accesible cuando se necesita.
- **Amenaza:** Evento o actor que puede causar daño (malware, atacantes, errores).
- **Vulnerabilidad:** Debilidad que puede ser explotada.
- **Incidente:** Evento que afecta la seguridad (caída, fuga, ataque).
- **Brecha de datos:** Exposición o acceso no autorizado a información.
- **Hardening:** Reducción de puntos débiles en sistemas.
- **Continuidad:** Capacidad de seguir operando tras incidentes.
- **Gobierno Digital:** Uso de TIC para servicios públicos eficientes y seguros.
- **Seguridad Digital:** Protección del entorno digital del Estado.
- **MSPI:** Marco para gestionar seguridad y privacidad en entidades públicas.
- **MIPG:** Modelo de gestión pública que incluye seguridad de la información.
- **Interoperabilidad:** Sistemas que intercambian datos de forma segura.

MARCO DE REFERENCIA PARA LA EJECUCIÓN DE LOS PROCESOS

La Universidad tiene publicada en la página principal un documento llamado *Plan de Seguridad y Privacidad de la Información del año 2024 en su versión 1* a lo cual se le efectuaron varias modificaciones integrales para una Política de Administración de Riesgos conjunta en todos los procesos:

- Tipo de Riesgos a tratar
- Normatividad aplicable de acuerdo al tipo de riesgo
- Metodologías a implementar para la administración de los riesgos
- Opciones para el tratamiento
- Responsabilidades de acuerdo a las líneas de defensa
- Técnicas para identificación de oportunidades
- Periodicidad de los monitoreos y revisiones
- Formas de información, comunicación y reporte
- Formas de documentación del proceso



El proceso de gestión de riesgos de seguridad de la información contiene las siguientes fases:

- Comprensión del contexto.
- Identificación del riesgo de seguridad de la información.
- Análisis del riesgo de seguridad de la información.
- Evaluación del riesgo de seguridad de la información.
- Tratamiento del riesgo de seguridad de la información.
- Comunicación del riesgo de seguridad de la información.
- Monitoreo y revisión del riesgo de seguridad de la información.

En dicho documento se especifica cada una de las fases y se muestra el mapa de calor, escalas de medición y la forma de analizar y evaluar los riesgos; de acuerdo a la "Guía para la administración del riesgo y el diseño de controles en entidades públicas v5", de fecha diciembre de 2020 del Departamento Administrativo de la Función Pública – DAFP.

DESCRIPCIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS

El Plan de Tratamiento de Riesgos de la Universidad Tecnológica del Chocó establece las actividades necesarias para mitigar los riesgos identificados sobre los activos de información institucionales. Estas actividades se definen con el propósito de reducir el impacto y/o la probabilidad de materialización de los riesgos, fortaleciendo la confidencialidad, integridad y disponibilidad de la información.

La estructuración del plan se realiza siguiendo las recomendaciones establecidas en la *Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del MinTIC (2016)*, contemplando para cada riesgo los controles, responsables, recursos, cronogramas y mecanismos de seguimiento que permitan una gestión adecuada y verificable.



Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización
Actualizar de directrices y/o documentos relacionados con la gestión de riesgos	Apoyar cuando se requiera la actualización de la política, Guía metodológica y demás lineamientos de la gestión de riesgos	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	2 ene-26	2 dic-26
Sensibilizar y/o comunicar	Socializar las directrices y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información.	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	2 abr-26	30-abr-26
Realizar proceso de identificación, evaluación y análisis de riesgos de seguridad y privacidad de la información	Analizar el contexto, Identificar, Analizar y Evaluar los Riesgos - Seguridad y Privacidad de la Información de acuerdo a la metodología.	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	2 abr-26	30-abr-26
	Realimentar a las partes interesadas, realizar revisión y verificación de los riesgos identificados y valorados (Ajustes)	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	2-abr-26	30-abr-26
Definir y aceptar los Planes de Tratamiento de Riesgos	Definir los planes de tratamiento de los riesgos que se encuentren por encima del nivel aceptable de los riesgos, de acuerdo a la metodología.	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	2 abr-26	30-abr-26
	Aceptar y aprobar los riesgos identificados y sus respectivos planes de tratamiento.	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	2-abr-26	30-abr-26
Realizar publicación y/o Comunicación	Publicar los riesgos de seguridad y privacidad de la información de los procesos de acuerdo a las directrices definidas por la universidad	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	2-abr-26	30-abr-26
Realizar seguimiento a los Riesgos y Planes de Tratamiento	Realizar seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	1 may-26	2 dic-26
Mejoramiento	Identificar las oportunidades de mejora De acuerdo al resultado del seguimiento de la implementación de los controles de seguridad y privacidad de la información y de los planes de tratamiento	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	1-may-26	2 dic-26
	Revisión y/o actualización de los Riesgos de Seguridad y privacidad de la información; así como sus respectivos planes de tratamiento de acuerdo con los resultados obtenidos en los seguimientos, los incidentes de seguridad de la información presentados y/o la materialización de los riesgos; o según las observaciones presentadas por la Dirección de Planeación Institucional.	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	1 may-26	2-dic-26
Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Oficial de Seguridad y Privacidad de la Información. Jefe de la Oficina de Gestión Informática - Sistemas y Soporte Técnico. Profesional de la Dirección de Planeación Institucional	1 may-26	2-dic-26

Tabla 1. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información UTCH



TENER PRESENTE

Los controles seleccionados para el tratamiento de los riesgos de Seguridad y Privacidad de la Información estarán asociados tanto a las medidas definidas en el Anexo A de la norma ISO/IEC 27001 como a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. Esta articulación permitirá definir las acciones específicas para el tratamiento de riesgos, identificar vulnerabilidades y establecer capacidades institucionales orientadas al fortalecimiento de la seguridad y privacidad de la información en la Universidad Tecnológica del Chocó, en concordancia con el Decreto 612 de 2018 y la Política de Gobierno Digital.

MATERIALIZACIÓN DE RIESGOS

Si durante la vigencia se materializar un riesgo, este debe ser reportado a la Oficina de Gestión Informática – Sistemas y Soporte Técnico. Así mismo se deberá realizar el proceso de identificación, análisis y valoración del riesgo, para determinar si los niveles de probabilidad e impacto fueron modificados, o si los controles implementados no fueron suficientes o efectivos para el tratamiento de estos, después de la materialización. Se registran los cambios en las matrices de riesgo de cada proceso.

En caso de materialización de un riesgo que no esté identificado, éste se deberá documentar y realizar todo el proceso de administración, de acuerdo con la metodología definida para tal fin.

RECURSOS PARA LA GESTION DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los recursos con los que cuenta la Institución para la administración de los riesgos de Seguridad y Privacidad de la Información son:

Recurso	Descripción (Actividades Asociadas según ISO/IEC 27001)
Recursos Humanos Competentes	Personal con roles asignados (ej. Oficial de Seguridad, analistas TIC) dedicado a identificar, analizar, evaluar y tratar riesgos; gestionar incidentes; implementar controles del Anexo A; definir responsabilidades; y participar en la mejora continua del SGSI.



Infraestructura Tecnológica	Equipamiento y componentes tecnológicos utilizados para soportar el SGSI, tales como servidores, redes, sistemas de almacenamiento, respaldos, sistemas de alta disponibilidad y mecanismos de autenticación, orientados a preservar la CIA (Confidencialidad, Integridad y Disponibilidad).
Herramientas de Software de Seguridad	Soluciones orientadas al monitoreo, análisis de vulnerabilidades, gestión de incidentes, gestión de accesos, inventario de activos y correlación de eventos, que permiten implementar y verificar controles del Anexo A y soportar la evaluación y <u>tratamiento del riesgo</u> .
Políticas, Procedimientos y Documentación	Conjunto de documentos que soportan el SGSI: políticas de seguridad, procedimientos operativos, registros, guías técnicas, instructivos, alcances, criterios de riesgo y controles. Permiten cumplir con requisitos documentales y operativos del estándar.
Modelos y Referenciales Normativos	Normas, guías y buenas prácticas utilizadas como referencia para la gestión del riesgo (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005), que permiten estandarizar metodologías, controles y procesos de evaluación y tratamiento del riesgo.
Programas de Concientización y Capacitación	Actividades de formación para personal interno, orientadas a fortalecer la cultura de seguridad, disminuir riesgos asociados al factor humano y cumplir con las actividades del control A.6.3 "Concientización, educación y formación en seguridad de la información".
Estructura Organizacional y Roles Definidos	Comité de Seguridad, Alta Dirección y funciones definidas que permiten tomar decisiones sobre niveles de riesgo aceptables, aprobación de tratamientos, asignación de recursos y evaluación del <u>desempeño del SGSI</u> .
Recursos Financieros (Presupuesto)	Fondos destinados a adquirir herramientas, contratar servicios, mantener la infraestructura, capacitar personal e implementar actividades del Plan de Tratamiento de Riesgos para cumplir con la mejora continua del SGSI.
Mecanismos de Medición, Auditoría y Seguimiento	Indicadores de desempeño, métricas, auditorías internas, revisiones de la dirección y seguimiento del plan de tratamiento, necesarios para cumplir con la fase "Verificar" del ciclo PDCA y con los requisitos de evaluación del desempeño del estándar.

Tabla 2. Recursos para la Gestión de los Riesgos de Seguridad y Privacidad de la Información



SC CER130675



Universidad Tecnológica del Chocó Diego Luis Córdoba
NIT: 891680089-4

Carrera 22 #18B-10 B. Nicolás Medrano – Ciudadela Universitaria

Tel: (+57) 6046726565. Línea gratuita: 018000938824

✉ contactenos@utchedu.co, notificacionesjudiciales@utchedu.co

🌐 utchedu.co

📍 Quibdó, Chocó (Colombia)



PRESUPUESTO PARA LA IMPLEMENTACIÓN DE PLANES DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La estimación, asignación y administración del presupuesto necesario para la implementación de los Planes de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Universidad Tecnológica del Chocó se realizará de acuerdo con los requisitos establecidos en la ISO/IEC 27001, específicamente en la cláusula 7.1 — Recursos, la cual exige que la organización determine y proporcione los recursos necesarios para establecer, implementar, operar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

En este sentido, los dueños del riesgo (líderes de proceso) serán responsables de identificar los recursos financieros requeridos para la implementación de los controles y actividades de tratamiento en sus áreas, así como de presentar la justificación técnica y económica correspondiente. La Alta Dirección, mediante las instancias institucionales definidas, será la responsable de evaluar, aprobar y garantizar la disponibilidad de los recursos necesarios para dar cumplimiento al tratamiento de los riesgos priorizados.

Este enfoque asegura que la UTCH cuente con los recursos necesarios para ejecutar de manera adecuada las acciones de mitigación definidas, mantener la eficacia del SGSI y cumplir con los objetivos de seguridad establecidos.

MEDICIÓN, SEGUIMIENTO Y MONITOREO DE LOS RIESGOS Y SUS PLANES DE TRATAMIENTO

La medición, el seguimiento y el monitoreo de los riesgos de Seguridad y Privacidad de la Información, así como de los controles y planes de tratamiento asociados, se realizará conforme a los requisitos establecidos en la ISO/IEC 27001, específicamente en los apartados relacionados con la evaluación del desempeño del Sistema de Gestión de Seguridad de la Información (SGSI), la medición de la eficacia de los controles y los procesos de mejora continua.

En la Universidad Tecnológica del Chocó, los líderes de proceso (como dueños del riesgo) serán responsables de realizar el seguimiento periódico al estado de los riesgos identificados, a la implementación de los controles y al avance de los planes de tratamiento



definidos para sus áreas. Dichos resultados serán validados en conjunto con el Oficial de Seguridad de la Información y deberán contar con los soportes requeridos.

Posteriormente, y con base en la evidencia presentada, la Dirección de Planeación Institucional consolidará la información y realizará el respectivo monitoreo institucional, teniendo en cuenta la periodicidad y fechas de cumplimiento definidas en la metodología institucional para la gestión del riesgo, así como los criterios establecidos para la aceptación del riesgo.

El seguimiento y monitoreo se realizarán mediante el indicador "Tratamiento de Riesgos de Seguridad de la Información", definido en el marco de la implementación del SGSI en la UTCH, cuyo propósito es:

Determinar la proporción de riesgos que cuentan con planes de tratamiento definidos, con el fin de establecer el nivel de gestión de riesgos de seguridad de la información en la Universidad, de acuerdo con los niveles de aceptación establecidos en la metodología de análisis y evaluación de riesgos.

Medir el nivel de implementación de los controles asociados a los riesgos identificados, con el propósito de determinar el grado de avance en la ejecución de los planes de tratamiento y en la aplicación de los controles establecidos para mitigar los riesgos de Seguridad y Privacidad de la Información.

Este proceso de medición, seguimiento y monitoreo permitirá evaluar la eficacia de los controles, verificar el cumplimiento de los objetivos de seguridad establecidos y promover la mejora continua del SGSI, en coherencia con el enfoque de desempeño y mejora definido por la ISO/IEC 27001.

Atentamente,

RAFAEL SANDOVAL MORALES

Jefe Gestión Informática – Sistemas y Soporte Técnico

a-rafael.sandoval@utch.edu.co

<p>Realizó: Rafael Sandoval Morales Cargo: Jefe Oficina Gestión Informática – Sistemas y soporte técnico (e) Fecha: 23 de enero de 2026</p>	<p>Revisó: Ingrid Zamanta Mosquera Cargo: Técnico Administrativa – Oficina Gestión Informática – Sistemas y soporte técnico Fecha: 23 de enero de 2026</p>	<p>Aprobó: Rafael Sandoval Morales Cargo: Jefe Oficina Gestión Informática – Sistemas y soporte técnico (e) Fecha: 23 de enero de 2026</p>
--	---	---