RESOLUCIÓN 017 DE 2026
(30 DE ENERO)

"Por la cual se adopta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Universidad Surcolombiana vigencia 2025

EL RECTOR DE LA UNIVERSIDAD SURCOLOMBIANA
en uso de sus atribuciones legales y reglamentarias, y;

CONSIDERANDO:

Que de conformidad con lo preceptuado en el numeral 2 y 15 del Artículo 31 del Acuerdo Superior 075 de 1994 - Estatuto General de la Universidad Surcolombiana-, le corresponde al Rector: *"Cumplir y hacer cumplir las normas legales, estatutarias y reglamentarias vigentes"* igualmente, *"Suscribir los actos necesarios para el cumplimiento de los objetivos de la Universidad, ateniéndose a las disposiciones legales vigentes".*

Que, en cumplimiento de su misión institucional, la Universidad Surcolombiana debe impulsar y materializar los cambios que demandan los tiempos modernos, con el fin de mantener su posicionamiento y liderazgo en la formación de talento humano al servicio de la región surcolombiana y del país, para lo cual se hace necesario fortalecer elementos, herramientas y sistemas que consoliden su espíritu corporativo y su proyección institucional.

Que la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC – ha identificado la necesidad de diseñar e implementar herramientas, técnicas, modelos y metodologías que apoyen a las entidades públicas en la formulación de los Planes Estratégicos de Tecnologías de la Información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan Estratégico de Seguridad y Privacidad de la Información, como referentes del proceso de Transformación Digital del Estado.

Que, conforme a los principios de "Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones" y de "Masificación del Gobierno en Línea", hoy Gobierno Digital, consagrados en los numerales 1 y 8 del artículo 2 de la Ley 1341 de 2009, el Estado y los agentes del sector de las Tecnologías de la Información y las Comunicaciones deberán colaborar, dentro del marco de sus competencias, para priorizar el acceso y uso de las TIC en la producción de bienes y servicios, así como adoptar las medidas necesarias para garantizar su máximo aprovechamiento en el desarrollo de las funciones públicas.

Que, de conformidad con lo dispuesto en el Decreto Único Reglamentario del Sector de la Función Pública – Decreto 1083 de 2015 –, modificado por el Decreto 1499 de 2017 y complementado por el Decreto 612 de 2018, las entidades de los órdenes nacional y territorial de la Rama Ejecutiva del Poder Público deben liderar la gestión estratégica de las Tecnologías de la Información y las Comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación del Plan Estratégico de Seguridad y Privacidad de la Información, el cual debe encontrarse alineado con la estrategia institucional y el Modelo Integrado de Planeación y Gestión – MIPG –, con un enfoque orientado a la generación de valor público, la eficiencia, la transparencia y la transformación digital del Estado.

Que el Anexo 4 "Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas", en su Capítulo 3 relativo a la interacción del Modelo de Seguridad y Privacidad de la

RESOLUCIÓN 017 DE 2026
(30 DE ENERO)

Información – MSPI – con el Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MGRSD –, señala que, en desarrollo de la estrategia de Gobierno Digital prevista en el Decreto 1078 de 2015, las entidades públicas deben implementar el Modelo de Seguridad y Privacidad de la Información – MSPI –, con el propósito de conformar un Sistema de Gestión de Seguridad de la Información al interior de cada entidad.

Que el Modelo de Seguridad y Privacidad de la Información – MSPI – integra, en cada una de sus fases, actividades asociadas a la gestión de riesgos de seguridad digital, constituyéndose esta práctica en su eje fundamental, razón por la cual la guía de gestión del riesgo del Departamento Administrativo de la Función Pública, junto con los lineamientos del referido Anexo, permiten dar cumplimiento a las tareas requeridas para la adecuada gestión del riesgo de seguridad digital.

Que de conformidad al Artículo 2.2.22.3.14 del Decreto 1083 de 2015, *"Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (…)11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (…)"*

Que, en cumplimiento de lo dispuesto en la Resolución 500 de 2021, la Universidad establece una estrategia de seguridad digital que integra principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, fundamentada en la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI – definido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Que en atención a lo anterior la Universidad Surcolombiana debe elaborar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2026 para la Entidad, de acuerdo a las directrices impartidas por el Gobierno Nacional a través del Departamento Administrativo de la Función Pública y el Ministerio de Tecnologías de la Información y las comunicaciones.

Que el Comité Administrativo de esta Casa de Estudios, en sesión ordinaria del 29 de enero de 2026, según Acta No. 01 de la misma fecha, analizó y aprobó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026.

RESUELVE:

ARTÍCULO 1°. Aprobar y adoptar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026, el cual hace parte integral del presente acto administrativo.

ARTÍCULO 2°. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026 podrá ser objeto de modificaciones durante su ejecución, de conformidad con las circunstancias de tiempo, modo y lugar, la disponibilidad de recursos presupuestales y las necesidades institucionales.

RESOLUCIÓN 017 DE 2026
(30 DE ENERO)

ARTÍCULO 3°. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026, adoptado mediante el presente acto administrativo, será socializado al interior de la institución con los diferentes grupos de interés y partes interesadas de la Universidad Surcolombiana.

ARTÍCULO 4°. La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE Y CÚMPLASE

Dada en Neiva, a los treinta (30) días del mes de enero del año 2026

RUBEN DARIO VALBUENA VILLARREAL
Rector

ALBERTO POLANIA PUENTES
Secretario General

Proyectó: Proyectó: Martha Liliana Hermosa Trujillo
Profesional Especializado (E)
Responsable de seguridad de la Información y Oficial de Protección de Datos Personales
Líder Sistema Gestión de Seguridad y Privacidad de la información

UNIVERSIDAD
SURCOLOMBIANA

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

Sistema de Gestión de Seguridad y Privacidad de la Información

Vigencia 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el actual entorno digital, donde la información se ha convertido en uno de los activos más valiosos, es fundamental para la Universidad Surcolombiana garantizar la seguridad y privacidad de los datos que maneja de sus estudiantes, docentes, administrativos, egresados, proveedores, terceros y ciudadanos. La protección de esta información constituye un elemento esencial para garantizar la continuidad de los servicios universitarios, mantener la confianza de la comunidad y cumplir con las obligaciones legales y regulatorias aplicables en materia de seguridad y privacidad de la información

Este documento tiene como objetivo identificar, evaluar y mitigar los posibles riesgos a los que se enfrenta la Institución, con el fin de fortalecer sus sistemas y procesos para ofrecer un entorno seguro y confiable para toda la comunidad universitaria.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la Universidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos institucionales.

Por lo anterior, la Universidad siguiendo los lineamientos del Documento CONPES 3995 de 2020, Decreto 1078 de 2015 que señala el habilitador de Seguridad y Privacidad de la Información, reglamentado por la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad de la información adoptando las buenas prácticas y los lineamientos de los estándares NTC ISO IEC 27001, NTC ISO 31000 entre otros.

Los principios de protección de la información se enmarcan en:

- **Confidencialidad**: propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad**: propiedad que la información se mantenga exacta y completa.
- **Disponibilidad**: propiedad que la información sea accesible y utilizable en el momento que se requiera.

Por lo anterior y en cumplimiento del Decreto 612 de 2018, se actualiza el presente documento.

2. OBJETIVO

Brindar a la Universidad Surcolombiana una herramienta con enfoque sistemático que le permita definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, a que pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad y disponibilidad de la información.

2.1. OBJETIVOS ESPECÍFICOS DE LA GUÍA METODOLÓGICA DE RIESGOS

- Brindar lineamientos y principios que propendan por la unificación de criterios para la administración de los riesgos de seguridad y privacidad de la información.
- Fortalecer el sistema de gestión de riesgos de la Universidad Surcolombiana incorporando controles y medidas de seguridad y privacidad de la información que estén acordes al entorno operativo de la Institución.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas
- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad y privacidad de la información, y su mitigación.
- Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital de acuerdo con los contextos establecidos en los procesos institucionales
- Cumplir con los requisitos legales, reglamentarios y de las normas técnicas colombianas

3. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información de manera que permita integrar en los procesos de la Universidad, buenas prácticas que contribuyan a la toma de decisiones y prevengan incidentes que puedan afectar el logro de los objetivos institucionales, mediante la implementación de lineamientos que permitan identificar, analizar, tratar, evaluar y monitorear riesgos en la Universidad Surcolombiana

Para el Plan de Tratamiento de Riesgos se tendrán en cuenta los riesgos que se encuentren en niveles alto y extremo, los criterios para la evaluación y aceptación de riesgos acorde con los lineamientos definidos por la Universidad. Los riesgos que se encuentren en niveles inferiores serán aceptados por la Universidad y su plan de acción para mantenerlos en niveles bajos será la implementación de controles definidos en los diferentes mapas de riesgos de los procesos a los cuales se les realizará seguimiento.

4. MARCO NORMATIVO Y REFERENCIA

Los siguientes documentos de referencia, normativos, vinculantes hacen parte integral del presente documento, sus consideraciones, alcance y construcción:

- **Constitución Política de Colombia** 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. Artículo 20. Libertad de Información.
- **Ley 527 de 1999**, "por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones".
- **Ley 594 de 2000** - Ley General de Archivos
- **Ley Estatutaria 1266 de 2008**, "por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales".
- **Ley 1273 de 2009**, "Delitos Informáticos" protección de la información y los datos.
- **Ley 1341 de 2009**, "Tecnologías de la Información y aplicación de seguridad".
- **Decreto 2952 de 2010,** "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"
- **CONPES 3701 de 2011**. Lineamientos de Política para Ciberseguridad y Ciberdefensa
- **Ley 1581 de 2012,** "Protección de Datos personales".
- **Decreto 2609 de 2012**, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
- **Decreto 1377 de 2013**, por la cual se reglamenta la ley 1581 de 2012
- **Ley 1712 de 2014**, "De transparencia y del derecho de acceso a la información pública nacional"
- **Decreto 1083 de 2015**, "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- **CONPES 3995 de 2020**. Política nacional de confianza y seguridad digital
- **Decreto 612 de 2018**, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado".
- **Decreto 1008 de 2018**, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital".
- **Ley 1915 de 2018**, "Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de Propiedad Intelectual - Derechos de Autor".
- **Resolución P4042 de 2019**, Por medio de la cual se crea, organiza y conforma un grupo interno de trabajo de seguridad de la Información y Protección de Datos personales y se asignan funciones de coordinador a un empleado público de la Universidad Surcolombiana
- **Resolución 086 de 2021**, Programa integral de gestión de datos personales
- **Resolución 087 de 2021**, Política de privacidad de datos personales
- **Resolución 500 de 2021**, Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
- **Decreto 767 de 2022**, Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- **Resolución 120 de 2023**, por la cual se crea el Grupo de Respuesta a Incidentes de Seguridad y Privacidad de la Información de la Universidad Surcolombiana
- **Resolución 209 de 2023**, por la cual se crea el Comité de Seguridad y Privacidad de la Información de la Universidad Surcolombiana

- **Resolución 255 de 2023**, Política y Objetivos del sistema de Gestión de Seguridad y Privacidad de la Información

4.1. Requisitos Técnicos

- NTC ISO IEC 27001 Sistemas de gestión de la seguridad de la información
- GTC ISO IEC 27002 Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para Controles de Seguridad de la Información
- NTC ISO IEC 27005 Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
- NTC ISO 19011 Directrices para la Auditoria de los Sistemas de Gestión.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Guía de Administración de riesgos y el diseño de controles en entidades públicas

5. RESPONSABLES

En concordancia con la Política de Seguridad y Privacidad de la Información de la Universidad Surcolombiana y con los lineamientos del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), la Institución establece de manera general los roles, responsabilidades y autoridades asociados a la seguridad de la información, con el propósito de asegurar una adecuada gobernanza, control y rendición de cuentas en la protección de los activos de información y activos asociados. La definición detallada, específica y operativa de estos roles, responsabilidades y autoridades se encuentra documentada en el Documento institucional AP-THU-DA-03 Roles, Responsabilidades y Autoridades de la institución, el cual complementa el presente apartado y constituye el marco de referencia obligatorio para la asignación, ejercicio y seguimiento de funciones en materia de seguridad y privacidad de la información en la Universidad.

5.1 Líderes de proceso

a. Aplicar las directrices para la gestión de riesgos y oportunidades al interior de su proceso.

a. Identificar y comunicar riesgos y oportunidades, de carácter operacional, y solicitar la aprobación de los planes de tratamiento para su gestión.

b. Realizar control de las matrices organizacionales para su actualización y consulta.

c. Realizar seguimiento a la gestión de riesgos y oportunidades y a las actividades derivadas.

d. Reportar los resultados y la información relacionada con la gestión de riesgos y oportunidades a las partes interesadas y a la dirección en los ejercicios de revisión.

e. Motivar la cultura de riesgo al interior de su proceso o servicio.

f. Participar en la definición de proyectos y planes para la gestión de riesgos y oportunidades estratégicas.

5.2. Comité de seguridad y privacidad de la información

a. Analizar, validar y aprobar el perfil de riesgos de seguridad y privacidad de la información de la Universidad, a partir de los resultados del proceso institucional de gestión de riesgos, con el fin de asegurar su alineación con el contexto organizacional, los objetivos estratégicos, los requerimientos legales y normativos aplicables, y los lineamientos del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

a. Analizar y determinar aquellas situaciones cuando se presenten violaciones a los códigos de seguridad y privacidad de la información y existan riesgos en la administración de la información de los Titulares e informar a la autoridad de protección de datos.

b. El Comité de Seguridad y Privacidad de la Información de la Universidad es responsable de analizar, validar y orientar la evaluación de los riesgos estratégicos asociados a la seguridad, privacidad y ciberseguridad de la información, asegurando que dichos riesgos sean identificados y evaluados en coherencia con los objetivos estratégicos institucionales, el contexto interno y externo, y las obligaciones legales y regulatorias aplicables. En ejercicio de su autoridad, el Comité podrá definir lineamientos, criterios y prioridades para la gestión de estos riesgos, solicitar ajustes a las evaluaciones realizadas por los responsables de proceso, y emitir conceptos técnicos sobre la criticidad, aceptabilidad y necesidad de tratamiento de los riesgos estratégicos identificados. Asimismo, el Comité tendrá la facultad de escalar a las instancias de alta dirección aquellos riesgos estratégicos cuyo nivel exceda los criterios institucionales de aceptación o que puedan comprometer la continuidad institucional, la reputación, el cumplimiento normativo o los derechos de los titulares de la información.

c. Revisar y aprobar el Plan de tratamiento de los riesgos estratégicos

d. Aprobar los niveles de aceptación del riesgo para la gestión de los riesgos de seguridad, privacidad y ciberseguridad de la información del nivel estratégico de la Universidad y revisarlos de manera periódica por lo menos una vez al año.

5.3. Proceso de gestión de seguridad y privacidad de la información

a. Definir los lineamientos e instrumentos que permiten la gestión de riesgos y oportunidades de la Universidad Surcolombiana.

b. Administrar, mantener y actualizar de manera sistemática el inventario de activos de información y de otros activos asociados, garantizando la identificación, clasificación, valoración y asignación de responsables de los activos de información, tecnológicos, físicos y humanos que soportan los procesos misionales, estratégicos y de apoyo de la Universidad,

en coherencia con los lineamientos del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y los requerimientos legales y normativos aplicables.

c. Acompañar a los procesos en la identificación, análisis, evaluación y gestión de los riesgos y oportunidades, así como en la actualización, validación y registro oportuno de las matrices definidas, garantizando su coherencia con los lineamientos institucionales y el Sistema de Gestión de Seguridad y Privacidad de la Información.

d. Realizar seguimiento a la gestión de riesgos y oportunidades y a las actividades derivadas, e informa cualquier desviación a los líderes de procesos.

e. Reportar los resultados de la gestión de riesgo incluidos la eficacia de los controles a la alta dirección y demás partes interesadas.

f. Desarrollar programas de capacitación orientados a la gestión de riesgos y oportunidades, promoviendo y fortaleciendo la cultura de riesgo al interior de los procesos y servicios institucionales, e impulsando la definición e implementación de estrategias que faciliten su adopción y consolidación en toda la Universidad.

g. Identificar, consolidar, analizar y reportar los riesgos de seguridad y privacidad de la información derivados del cumplimiento de requerimientos legales, regulatorios y normativos aplicables a la Universidad, incluyendo aquellos relacionados con protección de datos personales, seguridad digital, transparencia, archivo, continuidad del servicio, uso de tecnologías de la información y control institucional. Esta actividad garantiza que los riesgos asociados al incumplimiento legal sean gestionados de manera sistemática, trazable y articulada con el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y con el Sistema Institucional de Administración de Riesgos.

5.4. Proceso gestión de calidad

a. Revisar las directrices para la Gestión de Riesgos y Oportunidades para la Seguridad y Privacidad de la Información, los criterios definidos para la identificación, análisis y valoración de los riesgos, garantizando su alineación y coherencia con la Política de Administración de Riesgos de la Universidad, el Sistema de Gestión de Seguridad y Privacidad de la Información y los lineamientos institucionales vigentes.

5.5. Funcionarios administrativos, docentes, estudiantes y contratistas

a. Aplicar las directrices definidas en el presente documento

b. Participar en las etapas del proceso de gestión del riesgo.

c. Promover el desarrollo y la cultura de riesgos y oportunidades de Seguridad y Privacidad de la Información al interior de la Universidad y sus partes interesadas.

d. Reportar de manera oportuna, veraz y completa cualquier evento o incidente real o potencial que pueda afectar la confidencialidad, integridad, disponibilidad o privacidad de la información de la Universidad, de conformidad con las políticas, procedimientos y lineamientos institucionales vigentes en materia de seguridad, privacidad y ciberseguridad de la información.

6. DEFINICIONES

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad y privacidad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad y privacidad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad y privacidad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad y privacidad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Transferencia del riesgo. Compartir con otra de las partes la pérdida o la ganancia de un riesgo.

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSPI: Sistema de Gestión de Seguridad y Privacidad de la Información.

7. DESARROLLO DEL PLAN

7.1. Política de administración de riesgos

El Comité de Seguridad y Privacidad de la Información de la Universidad Surcolombiana, a través del sistema de gestión de seguridad y privacidad de la información, se compromete a mantener la cultura de la gestión de riesgos asociados, con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos de TI, gestionando los riesgos de los procesos y proyectos, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de amenazas asociadas a la información y otros activos de información asociados, que comprometan la disponibilidad, confidencialidad e integridad, fortaleciendo las medidas de control de manera continua y oportuna

La política define los lineamientos para la gestión de los riesgos y establece pautas de acción necesarias para todos los funcionarios administrativos, docentes, contratistas y/o terceros que requieran acceso a los sistemas de información o aplicaciones de la Universidad Surcolombiana.

Las opciones para el tratamiento del riesgo se deben seleccionar con base en el resultado de la valoración del riesgo, el costo esperado de implementar estas opciones y los beneficios esperados como resultado de tales opciones.

Las siguientes son las alternativas planteadas para el tratamiento del riesgo:

- **Reducir o Mitigar el riesgo.** Acciones que se toman para disminuir la probabilidad de las consecuencias negativas, o ambas, asociadas con un riesgo, mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable.

- **Retener o Aceptar el riesgo.** Aceptación de la pérdida o ganancia proveniente de un riesgo particular. La decisión sobre la retención sin acción posterior se debe tomar dependiendo de la evaluación del riesgo.

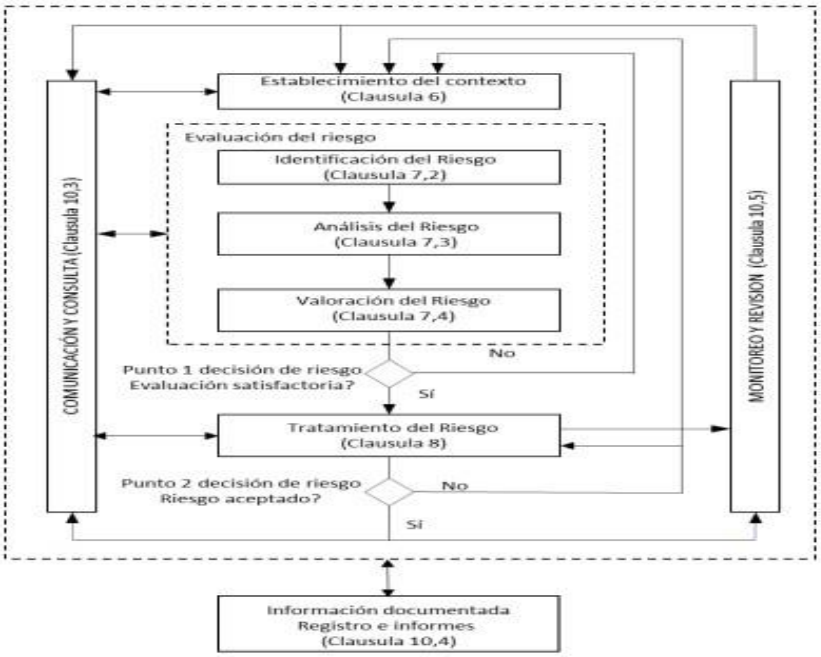
- **Evitar el riesgo.** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación, se debe evitar la actividad o acción que da origen al riesgo en particular.

- **Transferir o Compartir el riesgo.** Compartir con otra de las partes la pérdida o la ganancia de un riesgo. El riesgo se debe transferir a otra persona que pueda gestionar de manera más eficaz el riesgo en particular dependiendo la evaluación del riesgo.

7.2. Visión general del proceso de gestión de riesgo en la seguridad y privacidad de la información

El modelo de gestión de riesgos de seguridad y privacidad de la información diseñada basada en la norma NTC ISO IEC 27005 para la adecuada administración de riesgos en la seguridad de la información; lo componen los siguientes elementos:

La gestión de riesgos de seguridad y privacidad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.



Gráfica 1 Proceso de gestión de riesgo en la seguridad y privacidad de la información. Tomado de la norma NTC ISO IEC 27005

7.2.1. Establecimiento del contexto de riesgos de seguridad y privacidad de la información

El contexto de gestión de riesgos de seguridad y privacidad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la Universidad Surcolombiana y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en sus procesos, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Universidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

Criterios de evaluación del riesgo de seguridad y privacidad de la información:

La evaluación de los riesgos de seguridad y privacidad de la información se enfocará en:

- El valor estratégico del proceso de información en la Universidad Surcolombiana.
- La criticidad de la información y otros activos de información asociados involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la Universidad Surcolombiana.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Universidad Surcolombiana.

Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Universidad Surcolombiana, causados por un evento de seguridad y privacidad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad y privacidad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

Criterios de Aceptación

Los criterios de aceptación dependerán de las políticas, metas, objetivos de la Universidad Surcolombiana y de las partes interesadas.

7.2.2. Valoración de los riesgos de seguridad y privacidad de la información

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Universidad Surcolombiana, esta fase consta de las siguientes etapas:
La valoración del Riesgo de seguridad y privacidad de la información consta de las siguientes actividades:

7.2.2.1. Identificación de riesgos y oportunidades

Existen dos enfoques comúnmente utilizados para realizar la identificación de riesgos.

a) Enfoque basado en eventos: identificar los escenarios estratégicos a través de una consideración de las fuentes de riesgo, y cómo utilizan o impactan a las partes interesadas para alcanzar el objetivo deseado de esos riesgos.

b) Enfoque basado en activos: identificar escenarios operativos, que se detallan en términos de activos, amenazas y vulnerabilidades.

En un enfoque basado en eventos, el concepto subyacente es que los riesgos pueden identificarse y evaluarse a través de una evaluación de eventos y consecuencias. Los eventos y las consecuencias pueden determinarse a menudo mediante un descubrimiento de las preocupaciones de la alta dirección, los propietarios de los riesgos y los requisitos identificados al determinar el contexto de la organización (ISO/IEC 27001:2022, cláusula 4). Las entrevistas con la alta dirección y las personas de la organización que tienen una responsabilidad en un proceso de negocio pueden ayudar a identificar no sólo los eventos y consecuencias relevantes, sino también los propietarios de los riesgos.

Un enfoque basado en eventos puede establecer escenarios de alto nivel o estratégicos sin dedicar una cantidad de tiempo considerable a la identificación de activos a nivel detallado.

Esto permite a la organización centrar sus esfuerzos de tratamiento de riesgos en los riesgos críticos.

La evaluación de los eventos mediante este enfoque puede aprovechar los datos históricos en los que los riesgos permanecen invariables durante largos periodos, y permite a las partes interesadas implicadas alcanzar sus objetivos.

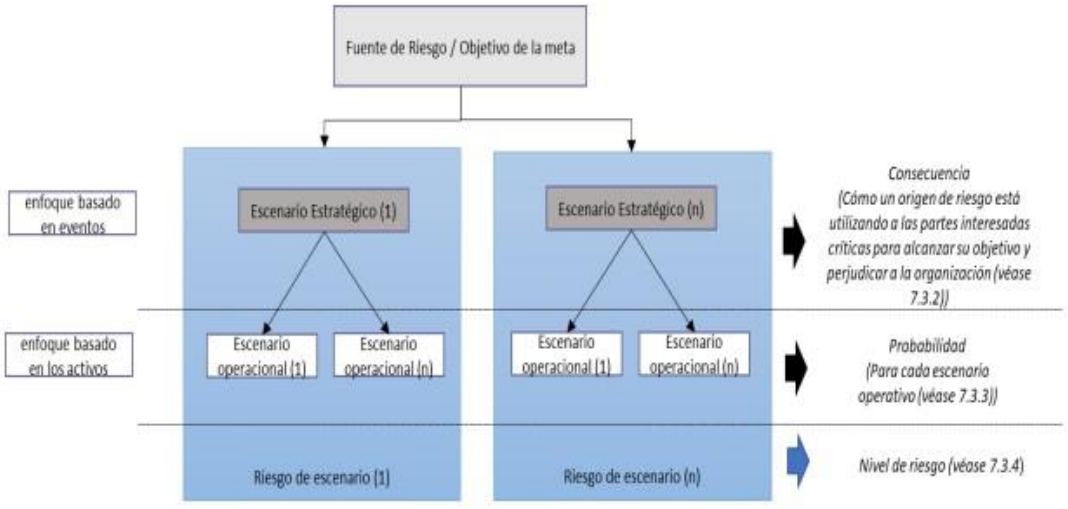
Sin embargo, en el caso de los riesgos para los que no se dispone de datos históricos o no son fiables, el asesoramiento basado en el conocimiento y la experiencia de los expertos o la investigación de las fuentes de riesgo puede ayudar a la evaluación.

Con un enfoque basado en los activos, el concepto subyacente es que los riesgos pueden identificarse y evaluarse mediante una inspección de los activos, las amenazas y las vulnerabilidades. Un activo es cualquier cosa que tenga valor para la organización y que, por tanto, requiera protección. Los activos deben ser identificados, teniendo en cuenta que un sistema de información se compone de actividades, procesos e información que debe ser protegida. Los activos pueden identificarse como primarios y de apoyo según su tipo y prioridad, destacando sus dependencias, así como sus interacciones con sus fuentes de riesgo y las partes interesadas de la organización. Una amenaza explota una vulnerabilidad de un activo para comprometer la confidencialidad, integridad y/o disponibilidad de la información correspondiente.

Si todas las combinaciones válidas de activos, amenazas y vulnerabilidades pueden enumerarse en el ámbito del SGSPI, entonces, en teoría, se identificarían todos los riesgos. Para los siguientes pasos de la evaluación de riesgos, debe elaborarse una lista de activos asociados a la información y a las instalaciones de procesamiento de la información.

El enfoque basado en los activos puede identificar las amenazas y vulnerabilidades específicas de los activos y permite a la organización determinar el tratamiento específico de los riesgos a un nivel detallado.

Gráfica 2 Evaluación del riesgo basada escenarios de riesgo.



7.2.2.2 Identificación de amenazas, controles y vulnerabilidades

Después de haber identificado los activos de información y de tener el resultado de la priorización del impacto sobre el sistema de gestión de la seguridad y privacidad de la información, se deben identificar las amenazas que pueden causar daños en los activos de información primarios y/o de soporte de mayor impacto. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y los controles y medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la Universidad Surcolombiana. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de la información y otros activos de información asociados.

7.2.2.3. Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad/posibilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Posibilidad**: la posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse y que tan posible es que la amenaza explote la vulnerabilidad sobre el activo de información.
- **Impacto**: hace referencia a las consecuencias que puede ocasionar a la Universidad Surcolombiana la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la posibilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio,

disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre la información o los activos de información asociados o la operación del negocio.

Para realizar el análisis de riesgo de un proceso, se deberá calificar el impacto y la posibilidad de cada uno de los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos los cuales pueden ser valorados de manera cualitativa y/o cuantitativa.

Para la estimación de la posibilidad se van a utilizar la metodología de valoración cualitativa:

Estimación del Riesgo: POSIBILIDAD			
Posibilidad	**Valor**	**Descripción**	**Frecuencia**
Casi Seguro	A	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.
Probable	B	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en El último año.
Posible	C	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Improbable	D	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Raro	E	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años

Tabla 1 Valoración Posibilidad

Para la estimación de la consecuencia/impacto se va a utilizar la metodología de valoración cuantitativa:

Estimación del Riesgo: CONSECUENCIA - IMPACTO		
Posibilidad	**Valor**	**Descripción**
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	2	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la Universidad Surcolombiana. Tiene un impacto bajo en los procesos de otras áreas de la Universidad Surcolombiana.
Moderado	3	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la Universidad Surcolombiana. Puede además causar un deterioro en el

Estimación del Riesgo: CONSECUENCIA - IMPACTO		
Posibilidad	**Valor**	**Descripción**
		desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	4	La materialización del riesgo **retrasa el cumplimiento de los objetivos de la Universidad Surcolombiana** y tiene un **impacto significativo en la imagen su pública**. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	5	La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la** Universidad Surcolombiana, tiene un **impacto catastrófico en su imagen pública**. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.

Tabla 2 Valoración Impacto

7.2.2.4. Determinación del riesgo inherente y residual

El análisis del riesgo determinado por su posibilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la Universidad Surcolombiana. La exposición al riesgo
es la ponderación de la posibilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

Tabla 1 Esquema general de Matriz de Riesgo Institucional y Zona de Riesgo

EVALUACION DEL RIESGO - CONSECUENCIA NEGATIVA					
POSIBILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastròfico (5)
Casi seguro (A)	A	A	E	E	E
Probable (B)	M	A	A	E	E
Posible (C)	B	M	A	E	E
Improbable (D)	B	B	M	A	E
Raro (E)	B	B	M	A	A

Las zonas de riesgo se diferencian por colores y por número de la zona de la siguiente manera:

Tabla 3 Convención Zonas de Riesgo

B: Zona de riesgo baja: Asumir el riesgo
M: Zona de riesgo moderado: Asumir el riesgo, reducir el riesgo
A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir
E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir

El análisis del riesgo permite además identificar oportunidades de mejora, cuando la consecuencia es positiva:

EVALUACION DEL RIESGO – CONSECUENCIA POSITIVA					
POSIBILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastròfico (5)
Casi seguro (A)	A	A	E	E	E
Probable (B)	M	A	A	E	E
Posible (C)	B	M	A	E	E
Improbable (D)	B	B	M	A	E
Raro (E)	B	B	M	A	A

Gráfica 3 Esquema general de Matriz de Oportunidades y Zonas de Oportunidades

Las zonas de oportunidad se diferencian por colores y por número de la zona de la siguiente manera:

B: Zona de oportunidad baja: Asumir la oportunidad
M: Zona de oportunidad moderada: Asumir la oportunidad.
A: Zona de oportunidad Alta: Aumentar la posibilidad de ocurrencia, compartir o transferir
E: Zona de oportunidad extrema: Aumentar la posibilidad de ocurrencia y/o el impacto de la oportunidad, asumir, compartir o transferir.

Tabla 4 Convención Zonas de Oportunidad

7.2.2.5. Evaluación de los riesgos

Una vez se valoran los impactos, la posibilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo y oportunidades, para los cuales

se deberán comparar frente a los criterios de evaluación definidos en el contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto Alto o aprovechar la oportunidad.

7.3. Tratamiento de los riesgos de seguridad y privacidad de la información

En esta etapa la Universidad Surcolombiana define los planes de tratamiento de riesgos y riesgos residuales sujeto a las decisiones de aceptación del Comité de Seguridad y Privacidad de la Información.

Las opciones de tratamiento definidas en la Universidad Surcolombiana son:

- **Evitar el riesgo**: decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Retener o Aceptar el riesgo**: aceptación de la pérdida o ganancia proveniente de un riesgo particular.
- **Reducir o Mitigar el riesgo**: acciones que se toman para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas a un riesgo.
- **Transferir o Compartir el riesgo**: compartir con otras partes la pérdida o la ganancia de un riesgo.

Para el tratamiento del riesgo es importante tener en cuenta la relación costo beneficio:

- El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios.
- El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo
- El costo y el tiempo del tratamiento es adecuado a los beneficios
- La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.

i. Estrategias Orientadas al Conocimiento

Mediante actividades de inducción, sensibilización y capacitación periódica se busca que todos los funcionarios administrativos, docentes, contratistas, estudiantes y/o terceros que tengan relación con la Universidad Surcolombiana, apropien conocimientos en materia de:

- Ley de protección de datos personales
- Ley de transparencia y acceso a la información
- Políticas institucionales de seguridad digital
- Modalidades y control de ataques informáticos

ii. Estrategias Orientadas al Control de Acceso

Con el fin de prevenir y controlar el acceso no autorizado a los activos de información clasificados y reservados de la Universidad Surcolombiana, se realizará:

- Actualización de la clasificación de los activos de la información.
- Revisión y ajuste de los controles de acceso a los activos de información con roles y privilegios
- Robustecer el cumplimiento de los acuerdos de intercambio (transferencia / transmisión) seguro de información, confidencialidad, privacidad y protección de datos personales

iii. Estrategias de Fortalecimiento de Controles Técnicos

Con el objetivo de minimizar las amenazas informáticas y de ciberseguridad se implementará las siguientes estrategias:

- Verificación y control de copias de respaldo
- Control de cambios en plataformas tecnológicas
- Actualización, configuración y aplicación de parches de seguridad a los equipos de la plataforma crítica.

7.4. Comunicación y consulta

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información está dirigido a partes interesadas internas y externas, las actividades del plan se establecen con el propósito de socializar su contenido y su impacto en la Universidad, generando interés, motivación y compromiso en cada uno de los actores. Este plan se debe alinear con el proceso de comunicaciones (ES-CMU) de la Universidad el cual establece la estrategia de comunicación encaminadas a facilitar el acceso a la información a las partes interesadas.

Una vez sea aprobado el presente documento, será publicado en el Portal Institucional en el link: https://www.usco.edu.co/es/transparencia/

7.5. Vigilancia y revisión de los riesgos de seguridad y privacidad de la información

Esta actividad busca la alineación continua de la gestión de riesgos con los objetivos de la Universidad Surcolombiana, con los criterios de aceptación de riesgos y la pertinencia continua del proceso de gestión de riesgos para la seguridad de la información. Para ello se ha definido que la frecuencia de vigilancia y revisión sea semestral.

7.6 Plan de tratamiento de riesgos de seguridad y privacidad de la información

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos y aprovechar las oportunidades, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información:

Gestión	Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
Gestión de Riesgos Seguridad y Privacidad de la información	Sensibilización	Socialización lineamientos Metodología de Gestión de Riesgos de Seguridad y privacidad de la Información	Proceso Gestión de Seguridad y Privacidad de la Información	20/01/2026	30/05/2026
	Identificación de Riesgos y oportunidades de Seguridad y Privacidad de la Información	Actualización del contexto, inventario de activos de información, Identificación, Análisis y Evaluación de Riesgos	Proceso Gestión de Seguridad y Privacidad de la Información	02/02/2026	30/05/2026
		Retroalimentación, revisión y verificación de los riesgos identificados (ajustes)	Proceso Gestión de Seguridad y Privacidad de la Información y Lideres de Procesos	02/03/2026	30/05/2026
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos y Oportunidades identificados y planes de tratamiento	Líderes de proceso	02/032026	30/05/2026
	Seguimiento Planes de Tratamiento de riesgos	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	Proceso Gestión Seguridad y Privacidad de la Información	20/02/2026	20/12/2026
	Mejoramiento	Identificación de oportunidades de mejoras acorde a los resultados obtenidos durante la evaluación de riesgos residuales.	Proceso Gestión de Seguridad y Privacidad de la Información	01/03/2026	20/12/2026

Tabla 5 Plan de tratamiento de los riesgos de seguridad y privacidad de la información

7.6. Información documentada

7.7.1 Generalidades

Esta cláusula está relacionada con la norma ISO/IEC 27001:2022 numeral 7.5 que especifica los requisitos para que las organizaciones conserven información documentada sobre el proceso de evaluación de riesgos.

7.7.2. Información documentada sobre los procesos

Entrada: Conocimiento sobre los procesos de evaluación y tratamiento de los riesgos de la seguridad y privacidad de la información de acuerdo con las cláusulas 7 y 8, definidos por la organización.

Acción: La información sobre los procesos de evaluación y tratamiento de los riesgos para la seguridad y privacidad de la información debe documentarse y conservarse.

Activación: La norma ISO/IEC 27001 requiere información documentada sobre los procesos de evaluación y tratamiento de los riesgos para la seguridad y privacidad de la información.

Resultado: Información documentada requerida por las partes interesadas (por ejemplo, el organismo de certificación) o determinada por la organización como necesaria para la eficacia del proceso de evaluación de riesgos de seguridad y privacidad de la información o del proceso de tratamiento de riesgos de seguridad y privacidad de la información.

Orientación para la aplicación:

La información documentada sobre el proceso de evaluación de riesgos para la seguridad y privacidad de la información debe contener:

a) Una definición de los criterios de riesgo (incluidos los criterios de aceptación del riesgo y los criterios para realizar las evaluaciones de los riesgos para la seguridad y privacidad de la información);

b) Un razonamiento sobre la coherencia, la validez y la comparación de los resultados

c) Una descripción del método de identificación del riesgo (incluida la identificación de los propietarios del riesgo)

d) Una descripción del método de análisis de los riesgos para la seguridad y privacidad de la información (incluida la evaluación de las consecuencias potenciales, la probabilidad realista y el nivel de riesgo resultante)

e) una descripción del método para comparar los resultados con los criterios de riesgo y la priorización de los riesgos para su tratamiento.

La información documentada sobre el proceso de tratamiento de los riesgos para la seguridad y privacidad de la información debe contener descripciones de:

a) el método para seleccionar las opciones adecuadas de tratamiento de los riesgos para la seguridad y privacidad de la información;

b) el método para determinar los controles necesarios;

c) cómo se utiliza la norma ISO/IEC 27001:2022, Anexo A, para determinar que no se han pasado por alto inadvertidamente los controles necesarios;

d) cómo se elaboran los planes de tratamiento de riesgos;

e) cómo se obtiene la aprobación de los propietarios del riesgo.

7.3.3. Información documentada sobre los resultados

Entrada: Los resultados de la evaluación y el tratamiento de los riesgos para la seguridad y privacidad de la información.

Acción: La información sobre la evaluación de riesgos de seguridad y privacidad de la información y los resultados del tratamiento deben ser documentados y conservados.

Activación: La norma ISO/IEC 27001 requiere información documentada sobre la evaluación de riesgos de seguridad y privacidad de la información y los resultados del tratamiento.

Resultado: Información documentada sobre la evaluación de los riesgos para la seguridad y privacidad de la información y los resultados del tratamiento.
Guía de implementación:

Dado que las organizaciones están obligadas a realizar evaluaciones de riesgos a intervalos planificados o cuando se proponen o se producen cambios significativos, debería haber al menos evidencia de un calendario, y de que las evaluaciones de riesgos se realizan de acuerdo con ese calendario. Si se propone un cambio, o se ha producido, debe haber pruebas de la realización de una evaluación de riesgos asociada. De lo contrario, la organización debe explicar por qué el cambio es significativo o no.

La información documentada sobre los resultados de la evaluación de riesgos para la seguridad y privacidad de la información debe contener:

a) los riesgos identificados, su consecuencia y probabilidad;

b) la identidad del propietario o propietarios del riesgo;

c) los resultados de la aplicación de los criterios de aceptación del riesgo

d) la prioridad del tratamiento del riesgo.

También se recomienda registrar la justificación de las decisiones sobre riesgos, tanto para aprender de los errores en casos individuales como para facilitar la mejora continua.

La información documentada sobre los resultados del tratamiento de los riesgos para la seguridad y privacidad de la información debe contener

a) la identificación de los controles necesarios;

b) cuando sea apropiado y esté disponible, pruebas de que estos controles necesarios actúan para modificar los riesgos, de manera que se cumplan los criterios de aceptación de riesgos de la organización.

8. MATRIZ OPERATIVA Y DE ALINEACIÓN ESTRATÉGICA

Se adjunta documento Excel

9. RECURSOS

RECURSOS	VARIABLES
Humanos	Equipo del Sistema Gestión Seguridad y Privacidad de la información Líderes de Proceso Grupo de respuesta a incidentes de seguridad y privacidad de la información
Técnicos	NTC ISO IEC 27005 Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.

Tabla 8. Recursos

10. SEGUIMIENTO Y MEDICIÓN DEL PLAN

El monitoreo y seguimiento de los riesgos de seguridad y privacidad de la información aprobados por los procesos, así como sus controles y planes de tratamiento se realiza por parte del equipo del sistema de gestión de seguridad y privacidad de la información teniendo en cuenta las fechas establecidas validando los resultados de los seguimientos y evidencias de la implementación de los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de sus planes de tratamiento y controles, los profesionales del Sistema de Gestión de Seguridad y Privacidad de la información realizan la revisión de la información, con el propósito de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el grado de avance en la implementación de los controles de los riesgos de Seguridad y Privacidad de la Información establecidos en el plan de

tratamiento de riesgos de la Universidad, en el marco del Sistema de Gestión de Seguridad y Privacidad de la Información. Los resultados de este seguimiento y monitoreo ayudan a fortalecer la gestión de riesgos y son insumo importante para la mejora continua de todas las gestiones que componen el Plan Estratégico de Seguridad y Privacidad de la Información de la Universidad que determinan finalmente el desempeño del Sistema de Gestión de Seguridad y Privacidad de la Información.

11. INDICADOR GENERAL

Porcentaje de ejecución del Plan de tratamiento de Riesgos

No de actividades finalizadas/ No de acciones programadas X100

12. APROBACIÓN

El presente documento fue sustentado ante el Comité Administrativo de la Universidad con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
Nombre: MARTHA LILIANA HERMOSA TRUJILLO Cargo: Profesional Especializado. Responsable Seguridad de la Información y Oficial de Protección de Datos Personales Líder Sistema Gestión de Seguridad y Privacidad de la Información Nombre: NANCY CATHERINE MOLINA SÁNCHEZ Cargo: Profesional Especializado. Profesional de apoyo al Sistema de Gestión de Seguridad y Privacidad de la Información Nombre: ISABEL CRISTINA CLEVES RODRIGUEZ Cargo: Contratista. Profesional de apoyo Sistema de Gestión de Seguridad y Privacidad de la Información	Nombre: MARTHA LILIANA HERMOSA TRUJILLO Cargo: Profesional Especializado. Responsable Seguridad de la Información y Oficial de Protección de Datos Personales Coordinadora Sistema de Gestión de Seguridad y Privacidad de la Información	Comité Administrativo Universidad Surcolombiana

UNIVERSIDAD SURCOLOMBIANA

PLAN: TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
RESPONSABLE: MARTHA LILIANA HERMOSA TRUJILLO
VIGENCIA: 2026

MATRIZ OPERATIVA							ALINEACIÓN ESTRATÉGICA				
ACTIVIDAD PLAN	ETAPAS	PRESUPUESTO ESTIMADO	RESPONSABLE (S)	RESULTADO ESPERADO	FECHA DE INICIO	FECHA DE FINALIZACIÓN	¿LA ACTIVIDAD SE ASOCIA DIRECTAMENTE AL PDI 2025--2034?	MISIÓN	PROYECTO	ACCIÓN	UNIDAD DE MEDIDA
Sensibilización	Socialización lineamientos Metodología de Gestión de Riesgos de Seguridad y privacidad de la Información	0	Proceso Gestión Seguridad y Privacidad de la Información	21 Líderes de Proceso sensibilizados	20/01/2026	30/05/2026	SI	M5 Modernización Tecnológica, Transformación Digital E Infraestructura Física	M5.PY.5: Modernización, automatización e Integración de los sistemas de información y gestión universitaria	M5.PY.5.6: Fortalecer los sistemas de gestión	Implementación del Sistema de Gestión Documental
Identificación de Riesgos y oportunidades de Seguridad y Privacidad de la Información	Actualización del contexto, inventario de activos de información, Identificación, Análisis y Evaluación de Riesgos	0	Proceso Gestión Seguridad y Privacidad de la Información	Contexto e inventario de activos de información actualizado en los 21 procesos	2/02/2026	30/05/2026	SI	M5 Modernización Tecnológica, Transformación Digital E Infraestructura Física	M5.PY.5: Modernización, automatización e Integración de los sistemas de información y gestión universitaria	M5.PY.5.6: Fortalecer los sistemas de gestión	Implementación del Sistema de Gestión Documental
	Retroalimentación, revisión y verificación de los riesgos identificados (ajustes)	0	Proceso Gestión Seguridad y Privacidad de la Información	verificación de riesgos actualizada en los 21 de procesos	2/03/2026	30/05/2026	SI	M5 Modernización Tecnológica, Transformación Digital E Infraestructura Física	M5.PY.5: Modernización, automatización e Integración de los sistemas de información y gestión universitaria	M5.PY.5.6: Fortalecer los sistemas de gestión	Implementación del Sistema de Gestión Documental
Aceptación de Riesgos Aceptación, aprobación Riesgos y Oportunidades identificados y planes de tratamiento	Aceptación, aprobación Riesgos y Oportunidades identificados y planes de tratamiento	0	Líderes de proceso	Riesgos aceptados por los líderes de proceso	2/03/2026	30/05/2026	SI	M5 Modernización Tecnológica, Transformación Digital E Infraestructura Física	M5.PY.5: Modernización, automatización e Integración de los sistemas de información y gestión universitaria	M5.PY.5.6: Fortalecer los sistemas de gestión	Implementación del Sistema de Gestión Documental
Seguimiento Planes de Tratamiento de riesgos	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	0	Proceso Gestión Seguridad y Privacidad de la Información		20/02/2026	20/12/2026	SI	M5 Modernización Tecnológica, Transformación Digital E Infraestructura Física	M5.PY.5: Modernización, automatización e Integración de los sistemas de información y gestión universitaria	M5.PY.5.6: Fortalecer los sistemas de gestión	Implementación del Sistema de Gestión Documental
Mejoramiento	Identificación de oportunidades de mejoras acorde a los resultados obtenidos durante la evaluación de riesgos residuales.	0	Proceso Gestión Seguridad y Privacidad de la Información		1/03/2026	20/12/2026	SI	M5 Modernización Tecnológica, Transformación Digital E Infraestructura Física	M5.PY.5: Modernización, automatización e Integración de los sistemas de información y gestión universitaria	M5.PY.5.6: Fortalecer los sistemas de gestión	Implementación del Sistema de Gestión Documental