1. OBJETIVO

Establecer las condiciones y/o actividades pertinentes para el tratamiento de amenazas de seguridad y privacidad de la información de la Universidad Surcolombiana con el fin de tomar las medidas de mitigación adecuadas.

2. ALCANCE

Brindar las medidas necesarias para el normal funcionamiento de la Universidad Surcolombiana facilitando acciones para evitar que las amenazas causen daños a la institución.

3. DEFINICIONES

Amenaza: causa potencial de un incidente no deseado, que puede provocar daños en un sistema o organización.

Seguridad de la información: es el conjunto de medidas y técnicas utilizadas para asegurar la confidencialidad, integridad y disponibilidad de la información.

Incidente seguridad: la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad.

Plan de remediación: conjunto de acciones que se desarrollan como respuesta a un incidente.

Grupo de interés: son grupos que no forman parte de la empresa, pero están relacionados por la actividad de la misma.

Responsable de Seguridad de la Información y Oficial de Protección de Datos Personales: profesional responsable de alinear las iniciativas de seguridad con los objetivos misionales, garantizando que los activos de la información de la institución cumplen con las tres características fundamentales que debe tener la información en una organización.

Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas.

4. MARCO DE REFERENCIA

La gestión de riesgos y oportunidades en la Universidad Surcolombiana considera para su labor, los lineamientos definidos en las directrices y políticas institucionales, además de las consideraciones definidas en:

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.

- La norma ISO 31000:2018– Gestión del riesgo. Principios y directrices.
- La norma ISO IEC 27005:2022 – Gestión de riesgos para la seguridad de la información.
- Los lineamientos definidos en los documentos del Sistema de Gestión de Seguridad y Privacidad de la Información.
- Los requisitos aplicables a la gestión del riesgo, detallados en el estándar ISO IEC 27001:2022 y la ISO IEC 27701:2025
- Código de Práctica para Controles de Seguridad de la Información - GTC ISO IEC 27002:2022 Tecnología de la Información. Técnicas de Seguridad.
- 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
- CONPES de Seguridad Digital (CONPES 3854 de 2016 y actualizaciones)
- Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)
- Política de Gobierno Digital (Decreto 1078 de 2015 y actualizaciones)
- Modelo Integrado de Planeación y Gestión – MIPG (DAFP)
- FURAG (Formulario Único de Reporte de Avance de la Gestión)
- Ley 1581 de 2012 y Decreto 1377 de 2013
- Lineamientos y guías de la Superintendencia de Industria y Comercio.

5. DESARROLLO

La inteligencia de amenazas es un proceso iterativo y continuo mediante el cual la Universidad **recopila y analiza** información, que le permite prevenir posibles incidencias de seguridad y privacidad, facilitar la toma de decisiones e identificar acciones preventivas que reduzcan la posibilidad de materialización de amenazas.

Para adelantar esta labor, la Universidad debe:

a) Identificar las posibles amenazas asociadas a los activos de información y otros activos asociados, para evitar la posible materialización de riesgos de seguridad y privacidad de la información, registrándolas en el formato ES-GSPI-FO-05 REGISTRO DE INTELIGENCIA DE AMENAZAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

b) Determinar y seleccionar fuentes de información internas y externas para el contacto con los organismos y entidades de nivel nacional que provean información y servicios de seguridad y privacidad de la información que sean de interés para la seguridad y privacidad de la información de la Institución. Ver ES-GSPI-DA-03 GUIA FUENTES DE INFORMACIÓN DE AMENAZAS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

c) Listado de contacto con autoridades y grupos de interés, para los activos tecnológicos. Ver ES-GSPI-DA-02 GUÍA DE CONTACTO CON LAS AUTORIDADES Y GRUPOS DE INTERÉS ESPECIAL. Adicionalmente, la Universidad deberá estar al tanto de:

- Información de interés, publicada por organismos a nivel mundial en temas de seguridad y privacidad de la información.
- Noticias o publicaciones que se realicen con respecto a posibles amenazas recientes o emergentes.

d) El Responsable de Seguridad de la Información y Oficial de Protección de Datos Personales compartirá información a través de los canales institucionales, que permita socializar posibles amenazas a todos los usuarios, prevenir la materialización de riesgos y cuando se considere necesario socializar aspectos puntuales con grupos de interés a través de los canales establecidos con cada uno.

e) Generar un resultado del análisis interno y deberá quedar registrado en el formato ES-GSPI-FO-05 REGISTRO DE INTELIGENCIA DE AMENAZAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, considerando en el informe los siguientes tipos de inteligencia:

- Inteligencia de amenazas estratégicas: intercambio de información de alto nivel sobre el cambiante panorama de amenazas (por ejemplo, tipos de atacantes o tipos de ataques)
- Inteligencia de amenazas tácticas: información sobre metodologías, herramientas y tecnologías de atacantes implicadas.
- Inteligencia operativa sobre amenazas: detalles sobre ataques específicos, incluidos indicadores técnicos.

Del análisis de estas amenazas se pueden identificar posibles riesgos de seguridad y privacidad de la información y continuar con el debido tratamiento cuando aplique. Ver ES-GSPI-MR-06 RIESGOS Y OPORTUNIDADES ENFOQUE BASADO EN ACTIVOS.

6. CONTROL DE CAMBIOS

VERSIÓN	DOCUMENTO Y FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS
01	EV-CAL-FO 17 – septiembre 01 de 2026	Creación documento

ELABORÓ	REVISÓ	APROBÓ
MARTHA LILIANA HERMOSA TRUJILLO Gestión Seguridad y Privacidad de la Información	LAURA LORENA PÉREZ CALDERÓN Profesional SGC	MAYRA ALEJANDRA BERMEO BALAGUERA Coordinador SGC