1. OBJETIVOS

Definir las directrices para:

a) Asegurar una respuesta rápida, eficaz, coherente y ordenada a los incidentes de seguridad y privacidad de la información, incluida la comunicación sobre los eventos de seguridad de la información.

b) Asegurar la categorización y priorización efectiva de los eventos de seguridad y privacidad de la información.

c) Asegurar una respuesta eficaz a los incidentes de seguridad y privacidad de la información.

d) Reducir la probabilidad o las consecuencias de futuros incidentes.

e) Asegurar una gestión coherente y eficaz de las pruebas relacionadas con los incidentes de seguridad y privacidad de la información para los fines de las acciones disciplinarias y legales.

f) Apoyar la notificación oportuna, coherente y eficaz de los eventos de seguridad y privacidad de la información que pueden ser identificados por los funcionarios administrativos, docentes, estudiantes, contratistas y/o terceros

2. ALCANCE

Las presentes directrices aplican a todos los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros de la Universidad Surcolombiana

3. DEFINICIONES

Activo: todo aquello que tiene valor para la Universidad Surcolombiana.

Amenaza: causa potencial de un incidente de seguridad y/o privacidad de la información que puede provocar daños en un sistema o en una organización.

Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la evaluación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos.

Confidencialidad: propiedad que determina que la información solo esté disponible y sea revelada a personas, entidades o procesos autorizados.

Consecuencia: Impacto generado por un evento o situación (favorable o adverso) que afecta los objetivos. Las consecuencias pueden expresarse cualitativa o cuantitativamente.

Continuidad de la Seguridad y privacidad de la Información: procesos y procedimientos para garantizar la continuidad de las operaciones de seguridad y privacidad de la información.

Control: medida tomada para mitigar o gestionar el riesgo.

Criterio de Riesgo: Términos de referencia con los que se evalúa la importancia de un riesgo, se basan en los objetivos de la organización y en el contexto externo e interno.

Disponibilidad: propiedad de que la información sea accesible y utilizable a solicitud de una persona, entidades o proceso autorizado, cuando ésta así lo requiera.

Escenario de Riesgo: Secuencia o combinación de eventos que llevan de la causa inicial a la consecuencia no deseada

Evaluación de riesgos: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Evento: ocurrencia o cambio de un conjunto particular de circunstancias. Un acontecimiento puede tener uno o varios sucesos y puede tener varias causas y varias consecuencias. Un evento también puede ser algo que se espera que no ocurra, o algo que no se espera que ocurra.

Evento de Seguridad de la Información: ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

Factor de riesgo: fuente que sola o en combinación tiene potencial originador de riesgos.

Fuente del Riesgo: Elemento que por sí solo o en combinación tiene el potencial de dar lugar a un riesgo. Una fuente de riesgo puede ser uno de estos tres tipos: humana, ambiental, técnica.

Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: evaluación del efecto y la consecuencia producida al materializarse un riesgo.

Identificación de Riesgo: Proceso de búsqueda, reconocimiento y descripción de riesgos. La identificación del riesgo implica la identificación de las fuentes de riesgo, los eventos sus causas y sus posibles consecuencias, igualmente, puede incluir datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de los interesados.

Incidente de seguridad de la información: evento único o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la empresa y amenazar la seguridad de la información

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Nivel de Riesgo: Importancia de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad. Nivel de riesgo = probabilidad (de un evento de interrupción) x pérdida (relacionada con la ocurrencia del evento)

Oportunidad: circunstancia en la cual existe la posibilidad de lograr algún tipo de mejora o de obtener algún beneficio.

Perfil de riesgo: descripción de cualquier conjunto de riesgos y su estado. El conjunto de riesgos puede contener aquellos que se relacionan con la Institución en su totalidad, con parte de la Institución, con los procesos o servicios o según necesidad.

Probabilidad: variable que mide la posibilidad de que un riesgo se materialice.

Proceso de gestión de riesgos para la seguridad y privacidad de la información: aplicación sistemática de las políticas, directrices, procedimientos y las prácticas de gestión a las actividades de establecimiento del contexto, evaluación de los riesgos (identificación, análisis, valoración), tratamiento, aceptación, comunicación y consulta, vigilancia y examen de los riesgos para la seguridad y privacidad de la información.

Propietario del Riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Riesgo: Los riesgos de seguridad de la información pueden asociarse con la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por tanto, causen daños a una organización.

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

Riesgo residual: riesgo que queda después del tratamiento del riesgo nivel resultante del riesgo después de aplicar los controles. Es el riesgo que queda, una vez se han aplicado los controles establecidos para su tratamiento, por lo cual requiere un permanente monitoreo de su evolución.

Riesgos de nivel Directivo: hace referencia a los riesgos que tienen un impacto directo sobre el cumplimiento de la planeación estratégica, con sus objetivos y planes estratégicos, así como los asuntos relativos al desempeño general de la Universidad Surcolombiana y que son relevantes para el Consejo Superior Universitario.

Riesgos de nivel operativo: Hace referencia a los riesgos que tengan un impacto directo sobre el cumplimiento de los objetivos de los procesos y servicios.

Sistema de gestión de seguridad y privacidad de la información-SGSPI: políticas, procedimientos, directrices, recursos y actividades, asociados, administrados colectivamente por la Universidad Surcolombiana, en la búsqueda de proteger sus activos de información. El SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad y privacidad de la información para lograr sus objetivos.

Tratamiento del riesgo: Proceso para modificar el riesgo, el tratamiento del riesgo puede consistir en evitar el riesgo decidiendo no iniciar o continuar con la actividad que lo origina, asumir o aumentar el riesgo para perseguir una oportunidad, eliminar la fuente de riesgo, cambiar la probabilidad, cambiar las consecuencias, compartir el riesgo con otra u otras partes (incluidos los contratos y la financiación del riesgo) y conservar el riesgo mediante una decisión informada.

Valoración del riesgo: Proceso de comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su importancia son aceptables o tolerables. La evaluación del riesgo ayuda a decidir el tratamiento del riesgo

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 políticas institucionales, además de las consideraciones definidas en:

- 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. GENERALIDADES

Estas directrices son la declaración general que establece la Universidad para gestionar eventos y/o incidentes de seguridad y privacidad de la información y otros activos de la información, con base en los siguientes controles de acuerdo a las normas:

ISO/IEC 27001:2022

A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
A.5.25 Evaluación y decisión sobre eventos de seguridad de la información

A.5.26 Respuesta a los incidentes de seguridad de la información
A.5.27 Aprendizaje de los incidentes de seguridad de la información
A.5.28 Recopilación de evidencias
A.6.8 Informes de eventos de seguridad de la información

ISO/IEC 27701:2025

A.3.11 Planificación y preparación para la gestión de incidentes
A.3.12 Respuesta a incidentes de seguridad de la información

6. DIRECTRICES

6.1 PLANIFICACIÓN Y PREPARACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1.1 Roles y responsabilidades

Los roles y responsabilidades para llevar a cabo los procedimientos de gestión de eventos y/o incidentes deben determinarse y comunicarse eficazmente a las partes interesadas internas y externas pertinentes. Ver AP-THU-DA-03 ROLES, RESPONSABILIDADES Y AUTORIDADES DE LA INSTITUCIÓN.

Se debe considerar lo siguiente:

a) establecer un método común para informar sobre eventos y/o incidentes de seguridad y/o privacidad de la información, ver ES-GSPI-PR-01 GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN;

b) establecer un proceso de gestión de eventos y/o incidentes para proporcionar a la Universidad la capacidad de gestionar los eventos y/o incidentes de seguridad y/o privacidad de la información, que incluye la administración, documentación, detección, clasificación, priorización, análisis, comunicación y coordinación de las partes interesadas;

c) establecer un proceso de respuesta a eventos y/o incidentes para proporcionar a la Universidad la capacidad de evaluar, responder y aprender de los incidentes de seguridad y/o privacidad de la información;

d) permitir que solo el personal competente se encargue de los problemas relacionados con los eventos y/o incidentes de seguridad y/o privacidad de la información dentro de la Universidad, quienes deben recibir capacitación periódica;

e) establecer un proceso para identificar la formación, la certificación y el desarrollo profesional continuo necesarios para el grupo de respuesta a incidentes de seguridad y/o privacidad de la información.

6.1.2 Procedimiento de Gestión de Incidentes

Los objetivos de la gestión de incidentes de seguridad y/o privacidad de la información deben acordarse con la alta dirección y asegurarse de que los responsables de la gestión de incidentes de seguridad y/o privacidad de la información comprendan las prioridades de la Universidad para manejarlos, teniendo en cuenta el marco temporal de resolución basado en las potenciales consecuencias y gravedad. Se debe implementar un procedimiento de gestión de eventos y/o incidentes (ver ES-GSPI-PR-01 GESTIÓN EVENTOS E INCIDENTES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN) para cumplir con estos objetivos y prioridades.

La Universidad debe crear un plan de acción de eventos y/o incidentes de seguridad y/o privacidad de la información (ver ES-GSPI-FO-03 REPORTE DE EVENTOS Y/O INCIDENTES DE SEGURIDAD Y/O PRIVACIDAD DE LA INFORMACIÓN) tomando en consideración los diferentes escenarios y procedimientos que se desarrollan e implementan para las siguientes actividades:

a) evaluación de los eventos y/o incidentes de seguridad y/o privacidad de la información

b) monitoreo, detección, clasificación, análisis e informes de los eventos y/o incidentes de seguridad y/o privacidad de la información (por medios humanos o automáticos);

c) gestión de los eventos y/o incidentes de seguridad y/o privacidad de la información hasta su conclusión, incluida la respuesta y la escalada según el tipo y la categoría del incidente, posible activación de la gestión de crisis y activación de planes de continuidad, recuperación controlada de un incidente y comunicación con partes interesadas internas y externas;

d) coordinación con partes interesadas internas y externas, tales como autoridades, grupos y foros de interés externos, proveedores y clientes, (ver ES-GSPI-DA-02 GUÍA DE CONTACTO CON LAS AUTORIDADES Y GRUPOS DE INTERÉS ESPECIAL);

e) registro de actividades de gestión de eventos y/o incidentes;

f) gestión de evidencia

g) análisis de la causa raíz y procedimientos posteriores al evento y/o incidente

h) identificación de las lecciones aprendidas y cualquier mejora en el procedimiento de gestión de eventos y/o incidentes o en los controles de seguridad y/o privacidad de la información en general que sean necesarios.

6.1.3 Procedimiento de presentación de informes

El procedimiento de presentación de informes debe incluir:

a) acciones a tomar en caso de un evento y/o incidente de seguridad y/o privacidad de la información;

b) uso de formularios de eventos y/o incidentes;

c) procesos de retroalimentación (lecciones aprendidas);

d) creación de informes de incidentes.

Cualquier requisito externo sobre la notificación de incidentes a las partes interesadas pertinentes dentro del plazo definido, debe ser considerado al implementar el procedimiento de gestión de incidentes.

En los incidentes de seguridad y/o privacidad de la información, es conveniente coordinar la respuesta y compartir información con organizaciones externas según corresponda, ya que los incidentes de seguridad y/o privacidad pueden trascender las fronteras institucionales y nacionales. (ver ES-GSPI-DA-02 GUÍA DE CONTACTO CON LAS AUTORIDADES Y GRUPOS DE INTERÉS ESPECIAL)

6.2 EVALUACIÓN Y DECISIÓN SOBRE EVENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Universidad debe crear un esquema de categorización, criterios y priorización de los eventos y/o incidentes de seguridad y/o privacidad de la información para la identificación de las consecuencias y la prioridad de los mismos.

El grupo de respuesta a incidentes de seguridad y privacidad de la información es responsable de coordinar y responder a los eventos y/o incidentes de seguridad y/o privacidad de la información, además, debe realizar la evaluación y tomar una decisión sobre los mismos.

Los resultados de la evaluación y la decisión deben ser documentados de manera detallada.

6.3 RESPUESTA A LOS INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Universidad debe establecer y comunicar el procedimiento de respuesta a los eventos y/o incidentes de seguridad y/o privacidad de la información a todas las partes interesadas pertinentes.

La respuesta al incidente debe incluir lo siguiente:

a) las consecuencias del incidente y los sistemas afectados;

b) recopilación de evidencia lo antes posible, después de la ocurrencia;

c) escalamiento, según sea necesario, que incluya actividades de gestión de crisis y posiblemente invocando planes de continuidad de negocio;

d) asegurar que todas las actividades de respuesta implicadas se registran correctamente para su posterior análisis;

e) comunicar la existencia del incidente de seguridad y/o privacidad de la información o de cualquier detalle pertinente a todas las partes interesadas internas y externas según el principio de necesidad de saber;

f) coordinar con las partes internas y externas como autoridades, grupos de interés, proveedores y clientes para mejorar la eficacia de la respuesta y ayudar a minimizar las consecuencias para otras organizaciones;

g) una vez que el incidente ha sido abordado con éxito, cerrarlo formalmente y registrarlo;

h) realizar análisis post-incidente para identificar la causa raíz. Asegurarse de que se documente y comunique de acuerdo con los procedimientos definidos;

i) identificar y gestionar las vulnerabilidades y debilidades de seguridad de la información, lo que incluye las relacionadas con los controles que han causado, contribuido o no han podido prevenir el incidente.

6.4 APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La información obtenida de la evaluación de incidentes de seguridad y/o privacidad de la información debe utilizarse para:

a) mejorar el plan de gestión de incidentes, incluidos los escenarios y el procedimiento de evento y/o incidentes;

b) identificar incidentes recurrentes o graves y sus causas para actualizar la evaluación de riesgos de seguridad y/o privacidad de la información de la Universidad y determinar e implementar los controles adicionales necesarios para reducir la probabilidad o consecuencias de futuros incidentes similares;

c) definir mecanismos que permitan recopilar, cuantificar y supervisar información sobre tipos de incidentes;

d) mejorar el conocimiento y la formación de los usuarios, respecto a lo que puede suceder, cómo responder a dichos incidentes y cómo evitarlos en el futuro.

6.5 RECOPILACIÓN DE EVIDENCIAS

La Universidad debe desarrollar y seguir procedimientos internos cuando se trate de las evidencias relacionadas con eventos de seguridad y/o privacidad de la información para los propósitos de acciones disciplinarias y legales. Estos procedimientos para la gestión de las evidencias deben proporcionar instrucciones para la identificación, recopilación, adquisición y preservación de las pruebas de conformidad y que sean admisibles para dichas acciones. Debe ser posible demostrar que:

a) los registros están completos y no han sido manipulados;

b) las copias de las pruebas electrónicas son probablemente idénticas a las originales;

c) cualquier sistema de información del que se hayan recopilado pruebas funcionaba correctamente en el momento en que se registraron dichas pruebas.

Cuando se disponga de evidencias, se debe buscar la certificación u otros medios pertinentes de calificación del personal y de los instrumentos, a fin de fortalecer el valor de las pruebas conservadas.

La evidencia digital puede trascender los límites organizativos o jurisdiccionales. En tales casos, debería asegurarse que la Universidad tenga derecho a recopilar la información requerida como prueba digital.

Todos los eventos y/o incidentes de seguridad y/o privacidad de la información deben ser evidenciados.

6.6 INFORMES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

El desarrollo de este control se encuentra en la AP-THU-DR-01 DIRECTRICES PARA EL CONTROL DE PERSONAS

7. RESPONSABILIDADES Y AUTORIDADES

Los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros deben cumplir con la política y directrices de seguridad y privacidad de la información definidas por la Universidad Surcolombiana; así mismo, deben reportar a los propietarios de la información y otros activos asociados las violaciones a la política, directrices y/o cualquier inconsistencia o irregularidad que pueda ser generada por los usuarios.

Los líderes de procesos y propietarios de la información y otros activos de la información deben revisar periódicamente los riesgos que se identifiquen sobre el uso inadecuado de los activos.

8. DOCUMENTOS RELACIONADOS Y REGISTROS

- ES-GSPI-PR-01 GESTIÓN DE EVENTOS E INCIDENTES SEGURIDAD Y

PRIVACIDAD DE LA INFORMACIÓN

- ES-GSPI-FO-03 REPORTE DE EVENTOS Y/O INCIDENTES DE SEGURIDAD Y/O PRIVACIDAD DE LA INFORMACIÓN
- ES-GSPI-DA-02 GUÍA DE CONTACTO CON LAS AUTORIDADES Y GRUPOS DE INTERÉS ESPECIAL
- AP-THU-DR-01 DIRECTRICES PARA EL CONTROL DE PERSONAS
- AP-THU-DA-03 ROLES, RESPONSABILIDADES Y AUTORIDADES DE LA INSTITUCIÓN
- EV-CDI-PR-03 PROCEDIMIENTO ORDINARIO – LEY 1952 DE 2019
- EV-CDI-PR-04 PROCEDIMIENTO ESPECIAL VERBAL – LEY 1952 DE 2019

9. CONTROL DE CAMBIO

VERSIÓN	DOCUMENTO Y FECHA DE APROBACIÓN	DESCRIPCION DE CAMBIOS
01	EV-CAL-FO 17 – agosto 28 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