RESOLUCIÓN 018 DE 2026
(30 DE ENERO)

"Por la cual se adopta el Plan Estratégico de Seguridad y Privacidad de la Información de la Universidad Surcolombiana vigencia 2026-2027"

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 requiere 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 acuerdo con el Decreto Único Reglamentario del Sector de la Función Pública, el Decreto 1083 de 2015 y su modificación mediante el 1499 de 2017 y el Decreto 612 de 2018 del Departamento Administrativo de la Función Pública, los organismos y entidades de los órdenes nacional y territorial de la Rama Ejecutiva del Poder Público deben liderar la gestión estratégica con las TIC mediante la definición, implementación, ejecución, seguimiento y divulgación del Plan Estratégico de Seguridad y Privacidad de la Información, el cual debe estar alienado a la estrategia y al modelo integrado de la institución, teniendo un enfoque en la generación de valor público para habilitar las capacidades y servicios tecnológicos necesarios para impulsar las transformaciones, la eficiencia y la transparencia del Estado.

RESOLUCIÓN 018 DE 2026
(30 DE ENERO)

"Por la cual se adopta el Plan Estratégico de Seguridad y Privacidad de la Información de la Universidad Surcolombiana vigencia 2026-2027"

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: (…) 12. Plan de Seguridad y Privacidad de la Información (…)"*

Que, en cumplimiento de lo dispuesto en la Resolución 500 de 2021, la entidad 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, teniendo como premisa que dicha estrategia gira en torno a 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, se hace necesario elaborar y adoptar el Plan Estratégico de Seguridad y Privacidad de la Información – PESI – para la vigencia 2026–2027, de conformidad con 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 001 de la misma fecha, al analizar el proyecto de Resolución y el Plan de Seguridad y Privacidad de la Información vigencia 2026 de la Universidad Surcolombiana, decidió aprobarlo.

Que en merito de lo expuesto,

RESUELVE:

ARTÍCULO 1°. Aprobar y adoptar el Plan Estratégico de Seguridad y Privacidad de la Información – PESI – para la vigencia 2026–2027, el cual hace parte integral del presente acto administrativo.

ARTÍCULO 2°. El Plan Estratégico de Seguridad y Privacidad de la Información – PESI – para la vigencia 2026–2027 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.

ARTÍCULO 3°. El Plan Estratégico de Seguridad y Privacidad de la Información – PESI – para la vigencia 2026–2027, 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.

RESOLUCIÓN 018 DE 2026
(30 DE ENERO)

"Por la cual se adopta el Plan Estratégico de Seguridad y Privacidad de la Información de la Universidad Surcolombiana vigencia 2026-2027"

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: 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 ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Sistema de Gestión de Seguridad y Privacidad de la Información

Vigencia 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), desarrolló el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual constituye una herramienta fundamental para fortalecer la seguridad y la protección de la información en las organizaciones, integrando las mejores prácticas de la norma ISO/IEC 27001:2022 y cumpliendo con las disposiciones normativas vigentes en Colombia relacionadas con la seguridad y privacidad de la información.

Por lo anterior, y teniendo en cuenta que la Universidad Surcolombiana, dentro de su Plan de Desarrollo institucional 2025-2034 define la Misión 5.PY.5.6 Fortalecer los sistemas de Gestión, se diseña el Plan Estratégico de Seguridad y Privacidad de la Información, con el objetivo de definir principios, lineamientos y controles necesarios para proteger la confidencialidad, integridad, disponibilidad y privacidad de la información, priorizando la implementación de las NTC ISO-IEC 27001 Y 27701 y los controles requeridos, garantizando un enfoque sistemático basado en el ciclo de mejora continua PHVA (Planear, Hacer, Verificar y Actuar), reflejando el compromiso institucional con la implementación y certificación de su Sistema de Gestión de Seguridad y privacidad de la Información y un Programa Integral de Gestión de Datos Personales.

2. OBJETIVO

Establecer el marco de principios, lineamientos y controles necesarios para proteger la confidencialidad, integridad, disponibilidad y privacidad de la información de la Universidad Surcolombiana, garantizando su manejo seguro durante todo su ciclo de vida y cumpliendo con los requisitos legales, regulatorios y contractuales aplicables, definidos en el Sistema Gestión de Seguridad y Privacidad de la Información de la Universidad, alineados al Modelo de Seguridad y Privacidad de la Información (MSPI).

3. ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información al buscar la implementación y certificación del Sistema de Gestión de Seguridad y Privacidad de la Información, comparte el alcance definido dentro de la Política del Sistema de Gestión de Seguridad y Privacidad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la entidad.

4. MARCO NORMATIVO

- Artículos 15, 20, 23 y 74 del a Constitución Política de Colombia, referente al derecho al habeas data, al derecho a la intimidad, el derecho a la información, derecho de petición y derecho de acceso a la información pública.

- Ley 527 de 1999, "por medio de 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, "por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".

- Ley 1273 de 2009, "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- Ley 1581 de 2012, "por la cual se dictan disposiciones generales para la protección de datos personales".

- Ley 1712 de 2014, "por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

- Ley 1755 de 2015, "por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo".

- 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*", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

- 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*". MINTIC.

- Manual de Gobierno Digital – MINTIC.

- Modelo de Seguridad y Privacidad de la Información – MINTIC.

- 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 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.

5. RESPONSABLES

COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD: Aprobar los documentos de Alto Nivel y velar por la implementación del SGSPI

RECTOR(A) Y VICERRECTOR(A) ADMINISTRATIVO(A): Garantizar los recursos requeridos.

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN Y OFICIAL DE PROTECCIÓN DE DATOS PERSONALES: Coordinar las actividades de implementación del SGSI y seguimiento al cumplimiento de actividades del (PESI)

DIRECTOR CENTRO DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL: Garantizar análisis de vulnerabilidades de la plataforma tecnológica y la implementación de controles de seguridad de la información que minimicen la materialización de los riesgos y permitan la continuidad en la prestación del servicio.

LÍDERES DE PROCESOS: Cumplir con las políticas y lineamientos definidos por el Sistema de Gestión de Seguridad de la Información y controles definidos por el Centro de Información, Tecnologías y Control Documental.

6. DEFINICIONES

A continuación, se listan los términos que podrían usarse dentro del documento con su respectiva definición.

- **Activo de información:** Todo aquello que tiene valor para la entidad, por lo tanto, debe protegerse. De acuerdo con la norma ISO/IEC 27001, los activos de información se clasifican en: información, software, activos físicos, personas, servicios e intangibles como reputación, imagen de la entidad, etc.

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

- **Control**: Las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad y privacidad de la información por debajo del nivel de riesgo asumido. También utilizado como sinónimo de salvaguarda, como una medida que modifica el riesgo.

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

- **Gestión de incidentes de seguridad y privacidad de la información:** Proceso estructurado para detectar, analizar, contener, erradicar y recuperarse de eventos no deseados (incidentes) que amenazan la confidencialidad, integridad o disponibilidad de los datos y sistemas de una

organización, minimizando el impacto negativo y restaurando la normalidad operativa lo más rápido posible, protegiendo así la reputación y la confianza del cliente.

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

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

- **Plan de continuidad del negocio:** Es un documento estratégico y un conjunto de procedimientos que detalla cómo una organización mantendrá sus operaciones críticas, se recuperará y responderá ante interrupciones (desastres, ciberataques, fallos) para minimizar el impacto, proteger activos y asegurar la entrega de servicios esenciales**,** garantizando su supervivencia y reputación.

- **Vulnerabilidad**: La vulnerabilidad es una debilidad en un activo de información (hardware, software, proceso, personal, ubicación física) que una amenaza puede explotar para causar daño (pérdida de confidencialidad, integridad o disponibilidad). (ISO/IEC 27001)

7. DESARROLLO DEL PLAN

7.1. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

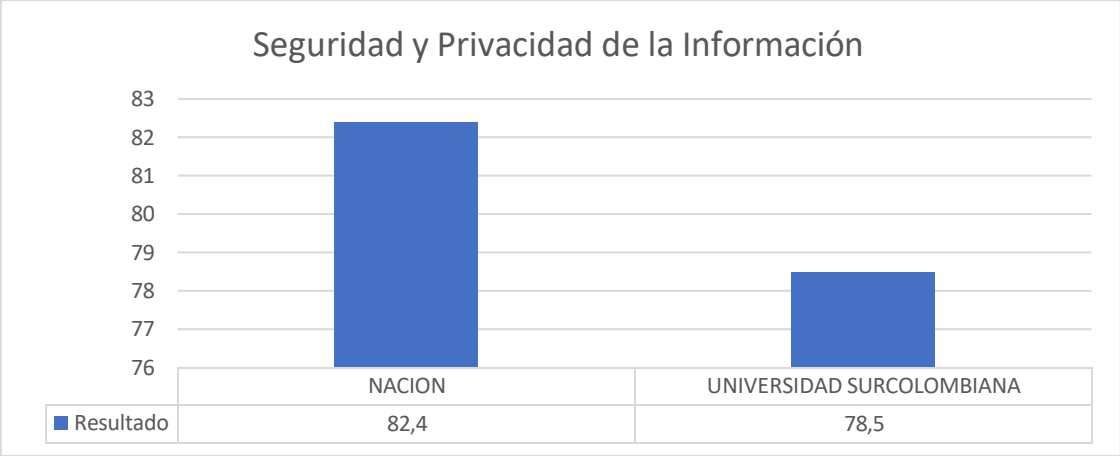
A continuación, se detalla el estado actual de avance de la implementación del Sistema de Gestión de Seguridad y privacidad de la Información de la Universidad Surcolombiana con base en el instrumento de evaluación modelo de seguridad y privacidad de la información de MINTIC y los resultados de desempeño MIPG 2024.

COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
Planificación	Contexto de la organización	14%	14%
	Liderazgo	10%	14%
	Planificación	12%	14%
	Soporte	10%	14%
Implementación	Operación	15%	16%
Evaluación de Desempeño	Evaluación del desempeño	10%	14%
Mejora Continua	Mejora	9%	14%
TOTAL		**80%**	**100%**

Tabla 1. Resumen NTC ISO-IEC 27001:2022

COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
Planificación	Contexto de la organización	14%	14%
	Liderazgo	10%	14%
	Planificación	12%	14%
	Soporte	10%	14%
Implementación	Operación	15%	16%
Evaluación de Desempeño	Evaluación del desempeño	10%	14%
Mejora Continua	Mejora	9%	14%
TOTAL		**80%**	**100%**

Tabla 2. Brecha Anexo A ISO 27001:2022

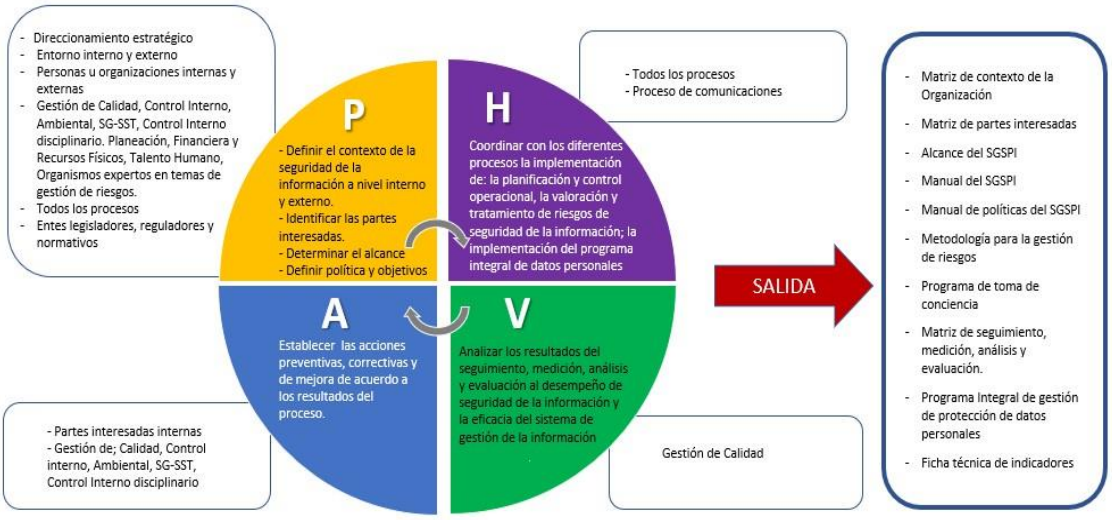


Gráfica 1. Resultados desempeño 2024 MIPG

7.2. Proceso gestión de seguridad y privacidad de la información

La Universidad Surcolombiana adopta el Proceso Gestión de Seguridad y Privacidad de a Información como un proceso de nivel estratégico con el objetivo de garantizar continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la Universidad, mediante la definición de políticas, procedimientos y lineamientos en seguridad y privacidad de la información.

Caracterización:



Gráfica 2 Caracterización

7.3 política y objetivos del sistema gestión de seguridad y privacidad de la información de la universidad surcolombiana

(Adoptados mediante resolución No 255 del 29 de noviembre de 2023, o aquella que los modifique, derogue o sustituya)

La Universidad Surcolombiana como institución de Educación Superior del orden nacional, establece que la información es un activo vital para el desarrollo de las actividades misionales, motivo por el cual, está comprometida a proteger los activos de información y la información de identificación personal en sus roles de controlador y procesador de la misma, orientando sus esfuerzos a la preservación de la confidencialidad, integridad y disponibilidad de la información.

Como pilares fundamentales del sistema de gestión de seguridad y privacidad de la información y lineamientos de ciberseguridad, las directivas de la Universidad promoverán la gestión por procesos y la gestión de riesgos, a través de la creación de cultura y toma de conciencia en funcionarios, administrativos, estudiantes, docentes, contratistas y/o terceros que hagan uso de los activos de información de la Universidad.

Esta política apoya y complementa el Plan de Desarrollo Institucional, Plan Estratégico de Tecnologías de la Información y las comunicaciones, la adopción de buenas prácticas del Modelo Integrado de Planeación y Gestión-MIPG y otros lineamientos de seguridad y privacidad de la información, al igual que el cumplimiento legal y normativo.

Las políticas de seguridad y privacidad de la información, brindan orientación y soporte, y son de obligatorio cumplimiento por parte de cada uno de los funcionarios administrativos, estudiantes, docentes, contratistas y/o terceros que tengan acceso a los activos de información de la Universidad.

Los controles establecidos en las políticas y en el sistema de gestión de seguridad y privacidad de la información, se fundamentan y tienen como propósito el cumplimiento de los requisitos legales, reglamentarios, institucionales y contractuales así como la mejora continua de nuestros procesos.

La Universidad Surcolombiana, plantea para el desarrollo de esta política, los siguientes objetivos del sistema de gestión de seguridad y privacidad de la información:

- Implementar y obtener la certificación del Sistema de Gestión de Seguridad de la información a través de las políticas, procedimientos y controles en materia de seguridad de la información, que permitan el cumplimiento de los objetivos institucionales.

- Implementar y obtener la certificación del Sistema de Gestión de privacidad de la información a través de las políticas, procedimientos y controles en materia de privacidad de la información, que permitan el cumplimiento de los objetivos institucionales.

- Propiciar la cultura de la seguridad y privacidad de la información a través de la toma de conciencia en funcionarios administrativos, estudiantes, docentes, contratistas y/o terceros que hagan uso de la información y otros activos asociados de la Institución.

- Optimizar la infraestructura tecnológica para asegurar la confidencialidad, integridad y disponibilidad de la información por medio de la identificación de mejoras, monitoreo y seguimiento de los activos, tipo instalaciones de procesamiento de información.

- Gestionar los riesgos de seguridad, privacidad y ciberseguridad de la información, pertinentes a las partes interesadas, a través de la implementación de las opciones de tratamiento y los controles aplicables.

- Gestionar las debilidades, eventos e incidentes de seguridad y las violaciones de la información de identificación personal que afecten la confidencialidad, integridad disponibilidad mediante el análisis de eventos, la recolección de la evidencia, implementación de las acciones necesarias y el aprendizaje de las lecciones para prevenir
- incidentes futuros.

- Mejorar el desempeño del sistema de gestión de seguridad y privacidad de la Información por medio del aumento de la eficacia de los controles de seguridad y privacidad de la información.

7.4 alcance del sistema gestión seguridad y privacidad de la información

El alcance para la certificación en las normas NTC ISO IEC 27001 y NTC ISO IEC 27701 es: “Gestión de seguridad y privacidad de la información para la prestación de servicios de diseño, formación, investigación y proyección social y proyectos especiales en educación superior a través de programas de pregrado y posgrado ofrecidos en las instalaciones de la Universidad Surcolombiana en la sede de Neiva”. Se excluyen de la certificación las sedes de Pitalito, Garzón y La Plata.

La inclusión y la exclusión de los controles del anexo A de la norma NTC ISO IEC 27001 y los controles de los anexos A y B de la norma NTC ISO IEC 27701 se encuentran documentados con sus

justificaciones en el documento ES-GSI-DA-06 DECLARACIÓN DE APLICABILIDAD del Sistema de Gestión de Seguridad y Privacidad de la Información.

8. MATRIZ OPERATIVA Y DE ALINEACIÓN ESTRATÉGICA

Se adjunta documento Excel

9. RECURSOS

Con base en los proyectos definidos para implementar las estrategias contempladas en la iniciativa de ***Fortalecimiento de las capacidades institucionales para la seguridad y privacidad de la información*** se presenta el presupuesto aproximado:

ACTIVIDADES	Vigencia 2026
Fortalecimiento del Sistema de gestión de seguridad y privacidad de la información.	$490.000.000
Fortalecimiento del plan de Continuidad de la operación de los servicios de la Universidad	$700.000.000
Implementación del Programa Integral de Gestión de Datos Personales	$0
Fortalecimiento estrategias cambio, cultura y apropiación del Sistema Gestión Seguridad y Privacidad de la Información	$130.000.000
Total	**$620.000.000**

Tabla 3. Recursos

10. SEGUIMIENTO Y MEDICIÓN DEL PLAN

El seguimiento del Plan estratégico de seguridad y privacidad de la información se realizará de acuerdo a los indicadores definidos por el SGSPI e indicadores de seguridad y privacidad de la información del proceso de Gestión de Información, Tecnologías y Control Documental

11. INDICADOR GENERAL

El indicador general será la certificación del Sistema de Gestión de Seguridad y Privacidad de la Información de la Universidad Surcolombiana bajo las NTC ISO/IEC 27001 Y 27701.

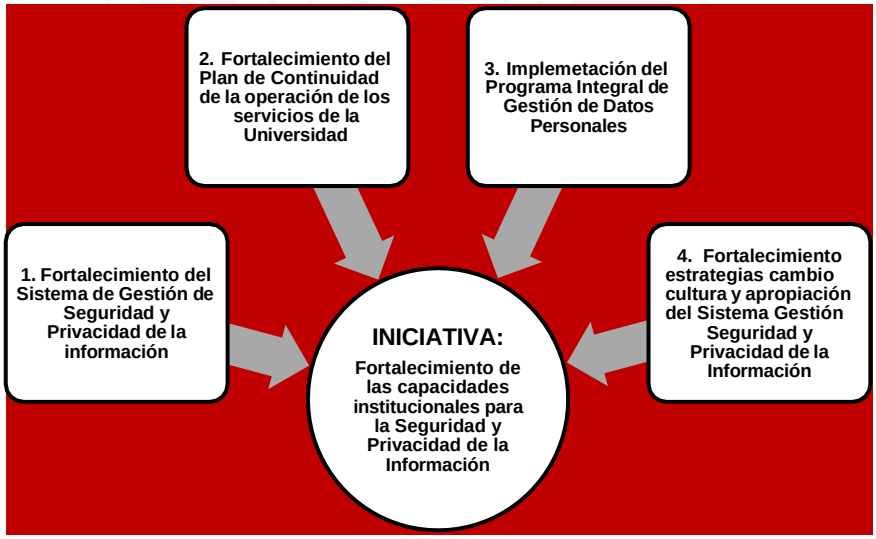
Nombre del Indicador: Índice de Conformidad Normativa Integral (ICNI)

ICNI= controles implementados (27001) + Requisitos de privacidad cumplidos/ Total de Controles Aplicables (ambas normas)

12. ESTRATEGIAS Y MODELO DE OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. INICIATIVA: FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES PARA LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Universidad establecerá una estrategia en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad y privacidad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Sistema de Gestión de seguridad y privacidad de la Información de la Universidad Surcolombiana, la gestión de riesgos y la gestión de incidentes de seguridad y privacidad de la información.

Por esta razón, la Universidad define las siguientes cuatro (4) estrategias específicas, que permitirán establecer en su conjunto el modelo de operación del Sistema de Gestión de Seguridad y Privacidad de la información.



Gráfica 3. Estrategias específicas de seguridad digital

12.1 portafolio de proyectos / actividades:

Para cada estrategia específica, la Universidad Surcolombiana define los siguientes proyectos y productos esperados, que tienen como objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI):

Iniciativa	Proyecto	Actividades	Indicador
Fortalecimiento de las capacidades institucionales para la seguridad y Privacidad de la Información	Fortalecimiento del Sistema de gestión de seguridad y privacidad de la información.	Elaborar toda la documentación del SGSPI e implementación de controles necesarios según requerimientos de las normas 27001 y 27701	Documentación aprobada y publicada Declaraciones de Aplicabilidad de las NTC ISO - IEC 27001 Y 27701 socializadas y aprobadas para el proceso de certificación
		Apoyar en la consolidación de activos de información, con relación a la responsabilidad de las funciones del Responsable de Seguridad de la información y Oficial de Protección de Datos personales.	Matriz de activos de información actualizada y publicada.
		Realizar el seguimiento al cumplimiento de los objetivos definidos para el plan de tratamiento de riesgos y a la ejecución de los controles definidos en los mapas de riesgos del SGSPI	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información.
		Realizar la reunión de análisis del reporte de eventos e incidentes de seguridad y privacidad de la información (en caso que se presenten) en coordinación con el Grupo de Respuesta a Incidentes de seguridad y privacidad de la información.	Porcentaje de eventos e incidentes de Seguridad y Privacidad de la Información monitoreados.
	Fortalecimiento del plan de Continuidad de la operación de los servicios de la Universidad	Realizar el diagnóstico de estado frente a los lineamientos y documentación del Plan de Continuidad de la Operación (BCP) en los Procesos de la universidad	Porcentaje de avance en la documentación y apropiación del Plan de Continuidad de la Operación (BCP) en los Procesos.
		Realizar reuniones de trabajo conjuntas con los procesos priorizados con el fin de orientar la aplicación y diseño del Plan Continuidad de la Operación (BCP).	
		Realizar reuniones de trabajo conjuntas con los procesos priorizados con el fin de orientar la	

		aplicación y diseño del Plan Continuidad de la Operación (BCP)	
		Realizar un simulacro de aplicabilidad del Plan de Continuidad de las Operación (BCP), atendiendo el alcance y programación realizada de acuerdo con los procesos priorizados	
	Implementación del Programa Integral de Gestión de Datos Personales	Realizar el reporte de las Bases de Datos de la Universidad Surcolombiana ante el Registro Nacional de Bases de Datos de la SIC	Número de constancias emitidas por el Registro Nacional de Bases de Datos
		Realizar seguimiento al Programa Integral al Protección de Datos Personales.	Programa Integral de Protección de Datos Personales implementado y con seguimiento
	Fortalecimiento estrategias cambio cultura y apropiación del Sistema Gestión Seguridad y Privacidad de la Información	Implementar el Programa de Toma de conciencia, cambio y Cultura de Seguridad y Privacidad de la Información.	Nivel de apropiación institucional en Seguridad y Privacidad de la Información
		Realizar el informe de análisis de los resultados obtenidos de evaluación del conocimiento de Cultura en Seguridad y Privacidad de la Información	

Tabla 4. Portafolio de proyectos/actividades

12.2 Plan de implementación del modelo de seguridad y privacidad de la información

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación	
					Tareas	
					Fecha Inicio	Fecha Final
Fortalecimiento del Modelo Gestión de Seguridad y Privacidad de la Información	Documentación Sistema Gestión de Seguridad y Privacidad de la Información	eElaborar, revisar, actualizar y aprobar por parte del Comité de Seguridad y Privacidad de la Información	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Contratistas del SGSPI–	Documentación aprobada y publicada	05/01/2026	30/07/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación	
					Tareas	
					Fecha Inicio	Fecha Final
		de la Universidad Surcolombiana a la política y objetivos del SGSI, y demás documentación requerida por el SGSPI	Líder SGSPI-Equipo del SGSPI -Líderes de Procesos			
	Activos de Información	Apoyar en la identificación, clasificación, valoración y rotulado de activos de los activos de información, de acuerdo con los lineamientos definidos por el SGSPI	Responsable de Seguridad de la información y Oficial de Protección de Datos personales - Contratistas del SGSPI – Líder SGSPI-Equipo del SGSPI -Líderes de Procesos	Matriz de inventario activos de información ES GSPI MR 05 MATRIZ DE INVENTARIO DE ACTIVOS DE LA INFORMACIÓN actualizada y enviada para validación a los procesos correspondientes	20/01/2026	30/05/2026
		Realizar e, seguimiento a la Publicación de la Matriz de inventario de Activos de Información actualizada		Matriz de inventario activos de información ES GSPI MR 05 MATRIZ DE INVENTARIO DE ACTIVOS DE LA INFORMACIÓN actualizada y validada por los procesos correspondientes	02/02/2026	30/05/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación Tareas Fecha Inicio	Fechas Programación Tareas Fecha Final
		Asesorar frente a las necesidades identificación, clasificación, valoración y rotulado de Activos de Información		Solicitudes de identificación, clasificación y valoración	02/02/2026	30/05/2026
	Riesgos de Seguridad y privacidad de la Información	Identificación de Riesgos de Seguridad y Privacidad de la Información,	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Contratistas del SGSPI - Líder SGSPI- Equipo del SGSPI -Líderes de Procesos	Correos electrónicos Mapas de riesgos	02/02/2026	30/05/2026
		Aceptación de Riesgos Identificados		Correo electrónico y/o acta de aprobación	02/03/2026	30/05/2026
		Publicación		Mapas de riesgos publicados	02/02/2026	30/05/2026
		Seguimiento Plan de Tratamiento		Seguimiento gestión de riesgos SGSPI ES GSPI MR 06 MATRIZ RIESGOS SGSPI	20/02/2026	20/12/2026
		Plan de Mejoramiento		Correos electrónicos y/o actas de reunión, Documentación actualizada	20/02/2026	20/12/2026
		Monitoreo y Revisión		Correos electrónicos ES GSPI MR 06 MATRIZ RIESGOS SGSPI	20/02/2026	20/12/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación Tareas Fecha Inicio	Fechas Programación Tareas Fecha Final
	Incidentes de Seguridad y Privacidad de la Información	Revisión y ajuste de ser necesario de la política, procedimiento y reporte de Gestión de incidentes de seguridad y privacidad de la información de la información	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder SGSPI- Equipo del SGSPI -Grupo de Respuesta a incidentes de Seguridad y privacidad de la información	correos electrónicos, listados de asistencia a reuniones de trabajo	20/01/2026	30/01/2026
		Publicar y Socializar el procedimiento actualizado de incidentes de seguridad y privacidad de la información de ser requerido		Documentación actualizada en el SGC	02/02/2026	27/02/2026
		Realizar informe gerencial de los ataques incidentes de Seguridad y Privacidad de la Información recibidos en la Universidad		Presentación y Acta Grupo de Respuesta a incidentes de Seguridad y Privacidad de la Información	05/01/2026	30/12/2026
		Socializar los boletines informativos de seguridad Digital reportados por el		Correos electrónicos o listas de asistencia	02/02/2026	18/12/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación Tareas Fecha Inicio	Fechas Programación Tareas Fecha Final
		ColCERT				
		Gestionar los incidentes y/o ataques de Seguridad de la Información identificados		ES-GSPI-PR-01 GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	05/01/2026	30/12/2026
		Realizar seguimiento a los informes de eventos asociados a SGSPI		Seguimiento reporte lecciones aprendidas ES-GSPI-FO-03 REPORTE DE EVENTOS Y/O INCIDENTES DE SEGURIDAD Y/O PRIVACIDAD DE LA INFORMACIÓN	05/01/2026	30/12/2026
	Seguimiento a vulnerabilidades	Apoyar la definición de los lineamientos, mecanismos y el alcance para la realización de pruebas de vulnerabilidades	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder del SGSPI-Director CITCD	Actas de Reuniones con el Director, grupo interno de seguridad de la información y protección de datos personales y funcionarios del Centro de Información, Tecnologías y Control Documental (CITCD)	02/02/2026	2702/2026
		Realizar seguimiento a los informes de vulnerabilidades asociados a SGSPI			02/02/2026	27/02/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación Tareas Fecha Inicio	Fechas Programación Tareas Fecha Final
		Apoyar la Definición de mecanismos para el Análisis de Vulnerabilidades y/o Pentest		Documentación contractual o mecanismos definidos	02/02/2026	27/02/2026
		Apoyar en la ejecución de las pruebas de vulnerabilidades y/o pentest		Informe Ejecución Pruebas	02/02/2026	30/06/2026
		Apoyar el seguimiento al plan de remediación de acuerdo con las vulnerabilidades identificadas		Seguimiento Remediación vulnerabilidades	02/02/2026	30/12/2026
	Documentación y registro	Revisión de la documentación asociada al Sistema de Gestión de Seguridad y Privacidad de la Información (Manual Políticas, Resolución, lineamientos, etc.) e identificación de necesidades de actualización	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder del SGSPI	Documentos actualizados en el SGC	05/01/2026	30/12/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación	
					Tareas	
					Fecha Inicio	Fecha Final
Fortalecimiento del plan de Continuidad de la operación de los servicios de la entidad		Revisar y alinear la documentación del SGSPI de la Universidad al MSPI, de acuerdo con la Normatividad vigente			05/01/2026	30/12/2026
		Matriz de Requisitos Legales de Seguridad de la Información			05/01/2026	30/12/2026
	Continuidad del Negocio	Asesorar la estructuración del Documento Plan de Continuidad del Negocio	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder del SGSPI- Director CITCD	Documento aprobado por el Comité de Seguridad y Privacidad de la Información	05/01/2026	20/01/2026
		Definición del plan de pruebas Plan de Continuidad		Plan de pruebas de las de continuidad diseñado	02/02/2026	30/03/2026
		Actualización del Manual de Análisis de Riesgos - RIA		Documento actualizado en SGC	02/02/2026	30/12/2026
		Documentación del Manual Plan de continuidad de la Operación - BCP			02/02/2026	30/12/2026
		Apoyar en la ejecución del		Actas de reuniones	02/02/2026	30/12/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación	
					Tareas	
					Fecha Inicio	Fecha Final
		Plan de Recuperación de Desastres		trabajo realizadas conjuntamente con el CITCD y demás procesos		
Implementación del Programa Integral de Gestión de Datos Personales	Datos Personales	Proceso de identificación y capacitación funcionarios y contratistas que manejan datos personales	Responsable de Seguridad de la información y Oficial de Protección de Datos personales	Memorando firmado y enviado por Responsable de Seguridad de la información y Oficial de Protección de Datos personales	20/01/2026	30/12/2026
		Revisión de bases de datos reportadas		Correos electrónicos	05/01/2026	30/03/2026
		Registro y actualización de las bases de datos en la plataforma RNBD		Certificado del registro de BD que expide la SIC	05/01/2026	30/03/2026
Fortalecimiento de las estrategias de Cambio, Cultura y Apropiación del Sistema de Gestión de Seguridad de la Información.	Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Programa de Toma de conciencia, cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder SGSPI	Documentación actualizada en SGC	05/01/2026	30/01/2026
		Ejecutar el Programa de		Correo electrónico,	20/01/202	30/12/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación Tareas Fecha Inicio	Fechas Programación Tareas Fecha Final
		Toma de conciencia, cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación (charlas, plegables, pendones, letreros en las dependencias ,)		Listados de asistencia, evaluaciones	6	
		Analizar resultados de la ejecución del Programa de Toma de conciencia, cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación		Indicadores del SGSPI	20/01/2026	30/12/2026
Planeación y seguimiento	Desarrollo Transversal	Seguimiento y reporte del estado de las Acciones Correctivas, correcciones y	Responsable de Seguridad de la información y Oficial de Protección de Datos	Correos electrónicos	20/01/2026	30/12/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación Tareas Fecha Inicio	Fechas Programación Tareas Fecha Final
		Oportunidades de Mejora	personales – Líder SGSPI			
		Provisión de información sobre el avance de cumplimiento de los indicadores de medición del SGSPI		Medición indicadores ESGSPI MR 08 MATRIZ DE SEGUIMIENTO MEDICIÓN ANÁLISIS Y EVALUACIÓN y EV CAL FO 04 FICHA TÉCNICA DE INDICADORES DE GESTIÓN	20/01/2026	30/12/2026
		Actualizar el documento de autodiagnóstico de la Universidad en la implementación de Seguridad y Privacidad de la Información		Documento de diagnóstico de MinTIC para Medición del MSPI	01/03/2026	30/06/2026
		Revisión de los controles de la norma ISO 27001 y 27701		Correos, citaciones de seguimiento, actas de reuniones con los procesos	01/06/2026	30/12/2026
		Formación auditores internos en Seguridad de la Información y Auditoría		Auditores formados Resultado de los ejercicios de auditorías realizados y Certificación	20/01/2026	30/12/2026

Líneas Estratégicas	Gestión	Actividades	Responsable	Evidencia	Fechas Programación	
					Tareas	
					Fecha Inicio	Fecha Final
		Interna y Externa				

Tabla 5. Plan de implementación del modelo de seguridad y privacidad de la información

13. 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 Coordinadora Sistema de 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

ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

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
Documentación Sistema Gestión de Seguridad y Privacidad de la Información	Contratación personal de prestación de servicios para elaborar, revisar, actualizar y aprobar por parte del Comité de Seguridad y Privacidad de la Información de la Universidad Surcolombiana a la política y objetivos del SGSI, y demás documentación requerida por el SGSPI	$ 260.000.000	Líder SGSPI-Equipo del SGSPI-Líderes de Procesos	Documentación aprobada y publicada	05/01/2026	30/07/2026	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
Activos de Información	Apoyar en la identificación, clasificación, valoración y rotulado de activos de los activos de información, de acuerdo con los lineamientos definidos por el SGSPI	$ -	Líder SGSPI-Equipo del SGSPI-Líderes de Procesos	Matriz de inventario activos de información ES GSPI MR 05 MATRIZ DE INVENTARIO DE ACTIVOS DE LA INFORMACIÓN actualizada y enviada para validación a los procesos correspondientes	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
	Realizar e, seguimiento a la Publicación de la Matriz de inventario de Activos de Información actualizada	$ -					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
	Asesorar frente a las necesidades identificación, clasificación, valoración y rotulado de Activos de Información	$ -		Solicitudes de identificación, clasificación y valoración	02/02/2026	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
Riesgos de Seguridad y privacidad de la Información	Identificación de Riesgos de Seguridad y Privacidad de la Información	$ -	Líder SGSPI-Equipo del SGSPI-Líderes de Procesos	Correos electrónicos-mapas de riesgo	02/02/2026	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
	Aceptación de Riesgos Identificados	$ -		Correos electrónicos y/o acta de aprobación	02/03/2026	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
	Publicación	$ -		Mapas de riesgos publicados	02/02/2026	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
	Seguimiento Plan de Tratamiento	$ -		Seguimiento gestión de riesgos SGSPI ES GSPI MR 06 MATRIZ RIESGOS SGSPI	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

UNIVERSIDAD SURCOLOMBIANA

ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

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
	Plan de Mejoramiento	$ -		Correos electrónicos y/o actas de reunión, Documentación actualizada	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
	Monitoreo y Revisión	$ -		Correos electrónicos ES GSPI MR 06 MATRIZ RIESGOS SGSPI	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
Incidentes de Seguridad y Privacidad de la Información	Revisión y ajuste de ser necesario de la política, procedimiento y reporte de Gestión de incidentes de seguridad y privacidad de la información de la información	$ -	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder SGSPI- Equipo del SGSPI -Grupo de Respuesta a incidentes de Seguridad y privacidad de la información	correos electrónicos, listados de asistencia a reuniones de trabajo	20/01/2026	30/01/2026	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
	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad y privacidad de la información de ser requerido	$ -		Documentación actualizada en el SGC	02/02/2026	27/02/2026	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
	Realizar informe gerencial de los ataques incidentes de Seguridad y Privacidad de la Información recibidos en la Universidad	$ -		Presentación y Acta Grupo de Respuesta a incidentes de Seguridad y Privacidad de la Información	05/01/2026	30/12/2026	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
	Socializar los boletines informativos de seguridad Digital reportados por el ColCERT	$ -		Correos electrónicos o listas de asistencia	02/02/2026	18/12/2026	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
	Gestionar los incidentes y/o ataques de Seguridad de la Información identificados	$ -		ES-GSPI-PR-01 GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	05/01/2026	30/12/2026	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
	Realizar seguimiento a los informes de eventos asociados a SGSPI	$ -		Seguimiento reporte lecciones aprendidas ES-GSPI-FO-03 REPORTE DE EVENTOS Y/O INCIDENTES DE SEGURIDAD Y/O PRIVACIDAD DE LA INFORMACIÓN	05/01/2026	30/12/2026	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

UNIVERSIDAD SURCOLOMBIANA

ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

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
Seguimiento a vulnerabilidades	Apoyar la definición de los lineamientos, mecanismos y el alcance para la realización de pruebas de vulnerabilidadesl	$ -	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder del SGSPI-Director CITCD	Actas de Reuniones con el Director, grupo interno de seguridad de la información y protección de datos personales y funcionarios del Centro de Información, Tecnologías y Control Documental (CITCD)	02/02/2026	27/02/2026	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
	Realizar seguimiento a los informes de vulnerabilidades asociados a SGSP	$ -			02/02/2026	27/02/2026	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
	Apoyar la Definición de mecanismos para el Análisis de Vulnerabilidades y/o Pentest	$ -		Documentación contractual o mecanismos definidos	02/02/2026	27/02/2026	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
	Apoyar en la ejecución de las pruebas de vulnerabilidades y/o pentest	$ -		Informe Ejecución Pruebas	02/02/2026	30/06/2026	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
	Apoyar el seguimiento al plan de remediación de acuerdo con las vulnerabilidades identificadas	$ -		Seguimiento Remediación vulnerabilidades	02/02/2026	30/12/2026	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
Documentación y registro	Revisión de la documentación asociada al Sistema de Gestión de Seguridad y Privacidad de la Información (Manual Políticas, Resolución, lineamientos, etc.) e identificación de necesidades de actualización	$ -	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder del SGSPI	Documentos actualizados en el SGC	05/01/2026	30/12/2026	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
	Revisar y alinear la documentación del SGSPI de la Universidad al MSPI, de acuerdo con la Normatividad vigente	$ -			05/01/2026	30/12/2026	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
	Matriz de Requisitos Legales de Seguridad de la Información	$ -			05/01/2026	30/12/2026	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

UNIVERSIDAD SURCOLOMBIANA

ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

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
Continuidad del negocio	Asesorar la estructuración del Documento Plan de Continuidad del Negocio	$ -	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder del SGSPI- Director CITCD- Grupo de repuesta a incidesntes de seguridad y privacidad de la información	Documento aprobado por el Comité de Seguridad y Privacidad de la Información	05/01/2026	20/01/2026	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
	Definición del plan de pruebas Plan de Continuidad	$ -		Plan de pruebas de las de continuidad diseñado	02/02/2026	30/03/2026	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
	Actualización del Manual de Análisis de Riesgos - RIA	$ -		Documento actualizado en SGC	02/02/2026	30/12/2026	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
	Documentación del Manual Plan de continuidad de la Operación - BCP	$ -			02/02/2026	30/12/2026	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
	Apoyar en la ejecución del Plan de Recuperación de Desastres	$700,000,000		Actas de reuniones trabajo realizadas conjuntamente con el CITCD y demás procesos	02/02/2026	30/12/2026	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
Datos personales	Proceso de identificación y capacitación funcionarios y contratistas que manejan datos personales	$ -	Responsable de Seguridad de la información y Oficial de Protección de Datos personales	Memorando firmado y enviado por Responsable de Seguridad de la información y Oficial de Protección de Datos personales	20/01/2026	30/12/2026	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
	Revisión de bases de datos reportadas	$ -		Correos electrónicos	05/01/2026	30/03/2026	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
	Registro y actualización de las bases de datos en la plataforma RNBD	$ -		Certificado del registro de BD que expide la SIC	05/01/2026	30/03/2026	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

UNIVERSIDAD SURCOLOMBIANA

ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

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
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Programa de Toma de conciencia, cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	$ -	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder SGSPI	Documentación actualizada en SGC	05/01/2026	30/01/2026	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
	Ejecutar el Programa de Toma de conciencia, cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación (charlas, plegables, pendones, letreros en las dependencias)	$ 130.000.000		Correo electrónico, Listados de asistencia, evaluaciones	20/01/2026	30/12/2026	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
	Analizar resultados de la ejecución del Programa de Toma de conciencia, cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	$ -		Indicadores del SGSPI	20/01/2026	30/12/2026	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
Desarrollo Transversal	Seguimiento y reporte del estado de las Acciones Correctivas, correcciones y Oportunidades de Mejora	$ -	Responsable de Seguridad de la información y Oficial de Protección de Datos personales – Líder SGSPI	Correos electrónicos	20/01/2026	30/12/2026	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
	Provisión de información sobre el avance de cumplimiento de los indicadores de medición del SGSPI	$ -		Medición indicadores ES GSPI MR 08 MATRIZ DE SEGUIMIENTO MEDICIÓN ANÁLISIS Y EVALUACIÓN y EV CAL FO 04 FICHA TÉCNICA DE INDICADORES DE GESTIÓN	20/01/2026	30/12/2026	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
	Actualizar el documento de autodiagnóstico de la Universidad en la implementación de Seguridad y Privacidad de la Información	$ -		Documento de diagnóstico de MinTIC para Medición del MSPI	01/03/2026	30/06/2026	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
	Revisión de los controles de la norma ISO 27001 y 27701	$ -		Correos, citaciones de seguimiento, actas de reuniones con los procesos	01/06/2026	30/12/2026	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
	Formación auditores internos en Seguridad de la Información y Auditoría Interna y Externa	$ 100.000.000		Auditores formados Resultado de los ejercicios de auditorías realizados y Certificación	20/01/2026	30/12/2026	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