

Universidad Industrial de Santander

Plan de Seguridad y Privacidad de la Información

Planes Institucionales y Estratégicos del Decreto 612 de 2018

División de Tecnologías de la Información y la Comunicación
Enero de 2026

Tabla de Contenido

1.	INTRODUCCIÓN.....	3
2.	OBJETIVO.....	4
3.	ALCANCE.....	4
4.	DEFINICIONES.....	4
5.	MARCO NORMATIVO	5
6.	MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	6
7.	PLAN DE ACCION	9
8.	TABLA DE CONTROL DE CAMBIOS	11

	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2026

I. INTRODUCCIÓN

La Universidad Industrial de Santander, como entidad del sector público, desarrolla sus planes institucionales en coherencia con lo dispuesto en el Decreto 612 de 2018 y demás lineamientos de planeación estratégica del Estado. En cumplimiento de su misión de formación, investigación y extensión, la Universidad avanza de manera decidida en procesos de transformación digital que fortalecen sus capacidades académicas, administrativas y de servicio a la comunidad universitaria.

Este proceso de digitalización y uso intensivo de tecnologías, plataformas y servicios de información exige una gestión integral de la seguridad y privacidad de la información, orientada a preservar la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información institucionales, así como la protección de los datos personales tratados en el desarrollo de sus funciones misionales y de apoyo. En este contexto, la seguridad de la información se concibe no solo como un componente tecnológico, sino como un habilitador estratégico para la continuidad operativa, la confianza institucional y el cumplimiento normativo.

La Universidad ha consolidado avances significativos en la adopción del Modelo de Seguridad y Privacidad de la Información, entre ellos la formulación y aprobación de la Política de Seguridad y Privacidad de la Información mediante Resolución No. 1674 de 2023, lo cual evidencia su compromiso con una gestión responsable del riesgo digital y la protección de sus activos de información. No obstante, algunos componentes del modelo se encuentran en proceso de fortalecimiento y maduración, lo que hace necesario continuar su despliegue progresivo bajo un enfoque de mejora continua.

En este marco, el Plan de Seguridad y Privacidad de la Información para la vigencia 2026 define un conjunto de acciones orientadas a fortalecer las capacidades institucionales en gestión de seguridad de la información, desarrolladas a lo largo de las cinco etapas del ciclo del modelo: diagnóstico, planeación, implementación, evaluación del desempeño y mejora continua. De este modo, la Universidad busca asegurar que su entorno digital evolucione de manera controlada y alineada con los desafíos tecnológicos actuales y las disposiciones normativas vigentes, promoviendo un ecosistema institucional confiable para la gestión de la información.

	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2026

2. OBJETIVO

Definir las acciones a desarrollar durante la vigencia 2026 para la implementación y fortalecimiento de los lineamientos de seguridad y privacidad de la información en la Universidad, en articulación con la estrategia de Gobierno Digital, con el fin de gestionar los riesgos sobre los activos de información, asegurar la confidencialidad, integridad y disponibilidad de la información institucional, y promover la mejora continua y el cumplimiento de la normativa vigente.

3. ALCANCE

El plan de seguridad y privacidad de la información de la Universidad Industrial de Santander es aplicable a todos los procesos, y actividades que gestionan, procesan o almacenan información o activos de información institucional.

4. DEFINICIONES

- **ACTIVO:** Cualquier cosa que tenga valor para la organización. Existen diversos tipos de activos en una organización como: información, software, programas de computador, físicos como los computadores, servicios, la gente y sus aptitudes, habilidades, y experiencia, e intangibles como Reputación o Imagen.
- **ACTIVO DE INFORMACIÓN:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **ACTIVOS DE INFORMACIÓN DIGITAL:** Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital. Ejemplo: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.
- **DTIC:** División de Tecnologías de la Información y la Comunicación.
- **MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:** Conjunto de lineamientos definido por el MinTIC para la adopción e implementación de controles relacionados con la seguridad y privacidad de la información digital y documental.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **SPI:** Seguridad y privacidad de la Información.
- **PSPI:** Política de Seguridad y Privacidad de la Información.
- **UAA:** Unidad(es) Académico Administrativa(s).

 	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2026

5. MARCO NORMATIVO

- **Decreto 612 de 2018.** Decreta lineamientos y planes de acción que las entidades del estado deben implementar para gestionar sus acciones institucionales.
- **Decreto 1008 de 2018.** 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 2710 de 2017.** Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Título 9 Políticas y Lineamientos de TI, Capítulo 1 Política de Gobierno Digital, Sección 2, Componentes, Instrumentos y Responsables de SPI. Manual Estrategia de Gobierno en Línea
- **Decreto 103 de 2015.** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **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.
- **Decreto 1377 de 2013** Por la cual se reglamenta parcialmente la Ley 1581 de 2012 para la protección de datos personales.
- **Ley 1581 de 2012** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2609 de 2012** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 2693 de 2012** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. Manual para la implementación de la estrategia de gobierno en línea 2012-2015
- **Ley 1437 de 2011:** Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y aplicación de criterios de seguridad.
- **Ley 1341 de 2009,** Marco General del Sector de TIC. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones-TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **Ley 1266 de 2008** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

 	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2026

- **Decreto 1151 de 2008** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones: Manual para la implementación de la estrategia de gobierno en línea.
- **Acuerdo 060 de 2001** Por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas.
- **Ley 599 DE 2000:** Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.
- **Decreto 1360 de 1989** Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
- **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.
- **Norma ISO/IEC 27001**, capítulos A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4

6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La División de Tecnologías de la Información y la Comunicación lidera y coordina la adopción del Modelo de Seguridad y Privacidad de la Información; no obstante, todas las Unidades Académico-Administrativas, así como los funcionarios y líderes de proceso que tengan activos de información bajo su responsabilidad, son corresponsables de la implementación de los lineamientos definidos en el presente Plan de Seguridad y Privacidad de la Información y de los productos que se deriven de su aplicación, de acuerdo con su ámbito de competencia.

6.1. Política de Seguridad y Privacidad de la Información

La Universidad Industrial de Santander cuenta con una Política de Seguridad y Privacidad de la Información Institucional, aprobada mediante la Resolución No. 1674 de 2023, la cual establece las normas, lineamientos y procedimientos necesarios para gestionar de manera adecuada la seguridad y privacidad de la información que recibe, maneja, transporta, genera o almacena en función de sus actividades misionales. La política cubre aspectos relacionados con la integridad, confidencialidad y disponibilidad de la información en todos los niveles de la institución. <https://uis.edu.co/pspi/>

	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2026

6.2. Gobierno y Roles en Seguridad de la Información

La gestión de la seguridad de la información en la Universidad Industrial de Santander se enmarca en su estructura de gobierno institucional y es orientada estratégicamente por el Comité Institucional de Gestión y Desempeño, instancia responsable de coordinar, articular y hacer seguimiento a las acciones relacionadas con la seguridad y privacidad de la información.

El responsable de la seguridad de la información lidera la implementación y operación del Modelo de Seguridad y Privacidad de la Información. En el caso de la Universidad Industrial de Santander, este rol es ejercido por el jefe de la División de Tecnologías de la Información y la Comunicación. Los demás roles, funciones y responsabilidades asociados a la seguridad y privacidad de la información se encuentran definidos en la Política de Seguridad y Privacidad de la Información vigente.

6.3. Gestión de Riesgos de Seguridad de la Información

En el MSE.01 Manual para la administración del riesgo, se establecen los lineamientos para la administración de riesgos de seguridad digital, entre otros. La metodología específica a implementar por parte de todos los procesos y unidades, está definida en la GSI.04 Guía para la gestión del riesgo de seguridad de la información.

Esta metodología está alineada con el Modelo Integrado de Planeación y Gestión (MIPG) e incluye la implementación de controles alineados con el Anexo A de la norma ISO 27001.

6.4. Clasificación y Control de Activos de Información

La Universidad, por medio de sus Unidades Académico Administrativas y de los líderes de proceso, realiza la gestión integral de los activos de información institucionales, lo que comprende su identificación, valoración, clasificación y protección, tanto en soportes físicos como digitales, con el propósito de preservar su confidencialidad, integridad y disponibilidad, de conformidad con las buenas prácticas en seguridad de la información. Estos lineamientos se encuentran en la GSI.03 Guía para la identificación de activos de información.

6.5. Protección de Datos Personales

En cumplimiento de lo dispuesto en la Ley 1581 de 2012 y demás normas que regulan la protección de datos personales, la Universidad Industrial de Santander garantiza el tratamiento adecuado de la información personal de los integrantes de su comunidad universitaria y de los terceros con los que se relaciona en el desarrollo de sus funciones.

	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2026

En este marco, mediante la Resolución No. 1227 de 2013, la Rectoría aprobó el Manual de Procedimientos Administrativos para el Tratamiento de Datos Personales.

6.6. Plan de Gestión de Incidentes de Seguridad

La Universidad gestiona los incidentes de seguridad de la información de manera ágil y eficiente. Cada UAA responsable de los activos de información críticos establece los mecanismos de protección y mitigación ante incidentes de seguridad, incluida la comunicación sobre estos eventos. Los lineamientos relacionados con la gestión de incidentes se encuentran definidos en la GSI.05 Guía para la gestión de eventos e incidentes de seguridad digital, del proceso Servicios Informáticos y de Telecomunicaciones.

6.7. Plan de Continuidad del Negocio y Recuperación ante Desastres

Los lineamientos para garantizar la disponibilidad de las instalaciones de procesamiento de información y los mecanismos de respaldo ante situaciones de emergencia o desastres están establecidos dentro de la Política de Seguridad y Privacidad de la Información.

6.8. Formación y Concienciación en Seguridad de la Información

La DTIC es responsable de ejecutar el plan de socialización y divulgación de la PSPI. Además, coordina con el subproceso de Formación de Personal para llevar a cabo actividades de formación y capacitación periódicas, enfocadas en sensibilizar a la comunidad universitaria sobre la importancia de la seguridad de la información.


6.9. Monitoreo, Auditoría y Evaluación Continua

La Dirección de Control Interno y Evaluación de Gestión es la unidad encargada de realizar auditorías internas sobre la seguridad de la información, asegurando que los procesos y controles implementados estén alineados con las normativas y estándares establecidos.

La División de Tecnologías de la Información y la Comunicación es la unidad encargada de definir y monitorear los indicadores de gestión para evaluar la efectividad del MSPI.

6.10. Ciclo de Mejora Continua

La Universidad adopta el ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar) sugerido por el MinTIC y otros modelos internacionales, como la ISO 27001. Este ciclo se aplica para realizar revisiones periódicas y actualizaciones del MSPI, basadas en auditorías internas, gestión de incidentes y cambios normativos, con el fin de asegurar

	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2026

que la seguridad de la información evolucione de acuerdo con las demandas tecnológicas y los estándares internacionales.

7. PLAN DE ACCION

El Plan de Acción 2026 establece las acciones a seguir relacionadas con el Modelo de Seguridad y Privacidad de la Información para el año en curso, asegurando que la Universidad cumpla con los lineamientos establecidos por las normativas vigentes y continúe avanzando en la implementación y mejora del MSPI.

Área de intervención	Ítem	Descripción de la actividad	Responsable	Fecha de finalización	Producto o entregable
Políticas de seguridad y privacidad de la información	1	Continuar con la divulgación y socialización de la Política de Privacidad y Seguridad de la Información	DTIC	30-nov-26	Actividades de divulgación y socialización ejecutadas
Gestión de riesgos	2	Socializar con las diferentes UAA la GSI.04 Guía para la gestión del riesgo de seguridad de la información.	DTIC	30-jun-2026	Taller o capacitación realizada
	3	Actualizar el mapa de riesgos de seguridad de la información.	DTIC	30-nov-2026	Mapa de riesgos actualizado
Gestión de incidentes	4	Socializar periódicamente los incidentes de seguridad de la información al Comité Institucional de Gestión y Desempeño	DTIC	30-nov-2026	Informes de incidentes de seguridad presentados
Activos de información	5	Solicitar la actualización del inventario de activos de información digital a las diferentes UAA.	DTIC	30-sep-26	Solicitud enviada
	6	Consolidar y enviar el inventario actualizado al Comité Institucional de Gestión y Desempeño	DTIC	30-nov-26	Inventario actualizado y enviado al Comité

Área de intervención	Ítem	Descripción de la actividad	Responsable	Fecha de finalización	Producto o entregable
Monitoreo	7	Presentar los indicadores del Modelo de seguridad y privacidad de la información al CIGD para aprobación.	DTIC	30-Jun-26	Hoja de vida de los indicadores presentados al CIGD.
Mejora continua / Proceso	8	Publicar y socializar el procedimiento de control de acceso físico a las instalaciones de procesamiento de información crítica.	DTIC	30-Jun-26	Procedimiento publicado y socializado.

 	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2026

8. TABLA DE CONTROL DE CAMBIOS

Versión	Fecha de aprobación	Descripción de cambios realizados
I	28/01/2026	Creación del documento.