

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 2025

Tabla de Contenido

1.	INTRODUCCIÓN.....	3
2.	OBJETIVO.....	3
3.	ALCANCE.....	4
4.	DEFINICIONES.....	4
5.	MARCO NORMATIVO	4
6.	MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	6
7.	PLAN DE ACCION	8
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 2025

I. INTRODUCCIÓN

La Universidad Industrial de Santander, como entidad del sector público, acoge las directrices establecidas en el Decreto 612 de 2018 para integrar sus planes institucionales y estratégicos. En su misión de fortalecer la investigación, la extensión y la formación, la Universidad ha incorporado el uso intensivo de recursos tecnológicos e informáticos, lo que le permite avanzar en la excelencia académica y en el bienestar de toda su comunidad universitaria.

El uso de Tecnologías de la Información y las Comunicaciones (TIC) en los procesos misionales y de apoyo requiere la implementación de controles rigurosos y selectivos que aseguren la integridad de la información, la confidencialidad de los datos y la disponibilidad de los servicios prestados a través de los recursos tecnológicos de la Universidad. En este sentido, resulta imperativa la adopción de un Modelo de Seguridad y Privacidad de la Información alineado con la misión, visión y estructura organizacional de la Universidad.

A la fecha, la Universidad ha logrado importantes avances en la implementación de este modelo. Por ejemplo, ya cuenta con una Política de Seguridad y Privacidad de la Información, aprobada mediante la Resolución No. 1674 de 2023, lo que refleja su firme compromiso con la protección de los activos de información. No obstante, el Modelo de Seguridad y Privacidad de la Información aún se encuentra en fase de planeación en algunos de sus elementos. A través de este plan, se pretende avanzar en todas las etapas del modelo, fomentando una cultura de mejora continua en la gestión de la seguridad de la información.

El Plan de Seguridad y Privacidad de la Información incorpora acciones para cada una de las cinco etapas que componen el ciclo de funcionamiento del modelo: diagnóstico, planificación, implementación, evaluación del desempeño y mejora continua; de este modo, la Universidad se compromete a asegurar que la seguridad de la información evolucione en sintonía con las demandas tecnológicas y las regulaciones vigentes, promoviendo un entorno seguro y confiable para la gestión de la información en todos sus procesos.

2. OBJETIVO

Establecer el plan de acción a seguir durante la vigencia 2025 en lo que respecta a los lineamientos de seguridad y privacidad de la información, dentro del marco de la estrategia de Gobierno Digital y garantizar la integridad, confidencialidad y disponibilidad de la información en la Universidad, consolidando un enfoque estructurado que promueva la mejora continua y el cumplimiento de las regulaciones vigentes.

	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2025

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).

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 I 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.
- **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.

	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2025

- **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 coordina la adopción del modelo de seguridad y privacidad de la información, sin embargo, todas las UAA, funcionarios o líderes de procesos que tengan activos de información a cargo, serán corresponsables en la adopción de los lineamientos estipulados en el presente plan de seguridad y privacidad de la información institucional y en los entregables que se originen por la adopción del mismo, según corresponda.

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/>

6.2. Gobierno y Roles en Seguridad de la Información

La gestión de la seguridad de la información en la Universidad Industrial de Santander es responsabilidad del Comité Institucional de Gestión y Desempeño, el órgano encargado de coordinar y supervisar todas las acciones relacionadas con la seguridad de la información.

	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2025

El responsable de seguridad de la información es el líder de la implementación del modelo de seguridad y privacidad, y en el caso de la UIS, este rol lo desempeña el Jefe de la División de Tecnologías de la Información y la Comunicación. Los demás roles y responsabilidades relacionados con la seguridad de la información están definidos de forma clara en la Política de Seguridad y Privacidad de la Información.

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 próxima a publicarse y socializarse (se incluye en el plan de acción).

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, a través de sus unidades académico administrativas y líderes de proceso, lleva a cabo la gestión y clasificación de los activos de información institucionales. Esto incluye la identificación, clasificación, y protección de los activos de información tanto físicos como lógicos, con el fin de garantizar su disponibilidad, integridad y confidencialidad, siguiendo las mejores prácticas de seguridad.

6.5. Protección de Datos Personales

En cumplimiento de la Ley 1581 de 2012 sobre la protección de datos personales, la Universidad Industrial de Santander asegura el manejo adecuado de la información personal de los miembros de su comunidad universitaria y otras partes externas. Para ello, la Rectoría de la Universidad aprobó la Resolución No. 1227 de 2013, mediante la cual se establece 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 Guía de Gestión de Incidentes de Seguridad, elaborada por la División de Tecnologías de la Información y la Comunicación.

	PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	AÑO 2025

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 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 2025 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.



PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AÑO 2025

Área de intervención	Ítem	Descripción de la actividad	Responsable	Fecha de finalización	Producto o entregable
Políticas de seguridad y privacidad de la información	1	Divulgar y socializar la Política de Privacidad y Seguridad de la Información (Fase II)	DTIC	30-nov-25	Plan de socialización y divulgación ejecutado
Gestión de riesgos	2	Publicar y socializar la metodología de gestión de riesgos de seguridad de la información.	DTIC	30-jun-2025	Metodología publicada y socializada
	3	Actualizar el mapa de riesgos de seguridad de la información de acuerdo a la nueva metodología definida y la aplicabilidad de controles del MSPI.	DTIC	30-nov-2025	Mapa de riesgos actualizado
Activos de información	4	Actualizar el inventario de activos de información digital a cargo de DTIC.	DTIC	30-nov-25	Inventario DTIC actualizado
	5	Publicar y socializar la guía de identificación de activos de información.	DTIC	31-jul-25	Guía publicada y socializada
	6	Solicitar la actualización del inventario de activos de información digital a las diferentes UAA.	DTIC	30-sep-25	Solicitud enviada
	7	Consolidar y enviar el inventario actualizado al Comité Institucional de Gestión y Desempeño	DTIC	30-nov-25	Inventario actualizado y enviado al Comité
Gestión de incidentes	8	Publicar y socializar la guía de gestión de incidentes de	DTIC	31-may-25	Documento publicado en la Intranet



PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AÑO 2025

Área de intervención	Ítem	Descripción de la actividad	Responsable	Fecha de finalización	Producto o entregable
		seguridad de la información.			
Monitoreo	9	Definir los indicadores de gestión de seguridad de la información a seguir al interior de la Universidad	DTIC	30-Nov-25	Hoja de vida de los indicadores adoptados
Mejora continua	10	Documentar el subproceso de Seguridad de la Información en el Sistema de Gestión de Calidad, dentro del proceso Servicios Informáticos y de Telecomunicaciones (Fase II)	DTIC	30-Nov-25	Subproceso publicado, incluyendo procedimientos y/o guías.



PLANES INSTITUCIONALES Y ESTRATÉGICOS DEL DECRETO 612 DE 2018

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AÑO 2025

8. TABLA DE CONTROL DE CAMBIOS

Versión	Fecha de aprobación del cambio	Descripción de cambios realizados
1	19/01/2020	Creación del documento.
2	19/01/2021	Actualización del documento.
3	19/01/2022	Actualización del documento.
4	17/01/2023	Actualización del documento.
5	30/01/2024	Actualización del documento.
6	29/01/2025	Actualización general del documento siguiendo los lineamientos de estructura sugeridos.