# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIVERSIDAD INDUSTRIAL DE SANTANDER

División de Servicios de Información
Universidad Industrial de Santander
Bucaramanga, Enero de 2024

Control de versiones del documento

| Versión | Fecha | Responsable | Descripción |
|---|---|---|---|
| 1 | 19/01/2020 | División de Servicios de Información | Versión 1 |
| 2 | 19/01/2021 | División de Servicios de Información | Versión 2 |
| 3 | 19/01/2022 | División de Servicios de Información | Versión 3 |
| 4 | 17/01/2023 | División de Servicios de Información | Versión 4 |
| 5 | 30/01/2024 | División de Servicios de Información | Versión 5 |

Tabla de Contenido

Control de versiones del documento....2
1. INTRODUCCIÓN....4
2. DEFINICIONES....5
3. MARCO NORMATIVO....5
4. OBJETIVO....7
5. GENERALIDADES....7
6. ALCANCE....7
7. PLAN DE ACCION....8

# 1. INTRODUCCIÓN

La Universidad Industrial de Santander como entidad del sector público acoge las directrices del decreto 612 de 2018, dadas para la integración de sus planes institucionales y estratégicos, y teniendo presente que en el quehacer de sus pilares: Investigación, Extensión y Formación, incorpora, utiliza y fomenta la utilización de recursos tecnológicos e informáticos en pro de fortalecer la naturaleza pública de sus servicios y de escalar hacia una excelencia académica para el bienestar de la comunidad universitaria.

La incorporación de determinadas Tecnologías de Información y Comunicación en los procesos educativos y administrativos requieren la aplicación de controles selectivos con el fin de garantizar la integralidad de la información, la confidencialidad de los datos y la disponibilidad de los servicios que se ofrecen por medio de los recursos tecnológicos o informáticos incorporados por las entidades; en concordancia con lo expuesto, la Universidad Industrial de Santander requiere implementar un Sistema de Gestión de Seguridad y Privacidad de la Información alineado con su misión, visión, procesos, procedimientos y estructura organizacional con el fin de garantizar la Integridad, disponibilidad, confidencialidad y no repudio, de la información tanto física como digital.

Tomando como referente el decreto 1008 de 2018 sobre la política de gobierno digital[1] - en particular al habilitador "Seguridad de la Información" – y el manual de gobierno digital[2], la Universidad Industrial de Santander seleccionó la guía del Modelo de Seguridad y Privacidad de la Información (MSPI) aprobada por el MinTIC[3], para iniciar el proceso de implementación del Plan de Seguridad y Privacidad de la Información, el cual sugiere cinco etapas para llevar acabo el ciclo de funcionamiento del modelo de operación: Etapa diagnóstica, etapa de planificación, de implementación, de evaluación de desempeño y de mejora continua.

*Figura 1: Fuente MinTIC – Etapas MSPI*

[1] Decreto 1008 de 2018 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902

[2] Versión 6 del manual de gobierno en digital https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/Manual-de-Gobierno-Digital/

[3] Versión 3.0.2 MSPI - MinTIC https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

## 2. 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.
- **DSI**: División de Servicios de Información.
- **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.
- **UAA**: Unidad(es) Académico Administrativa(s).

## 3. 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. Titulo 9 Políticas y Lineamientos de TI, Capitulo 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.
- **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

## 4. OBJETIVO

Establecer el plan de acción a seguir en la vigencia 2024, relacionado con los lineamientos de seguridad y privacidad de la información en el marco de la estrategia de Gobierno Digital, teniendo la Política de Seguridad y Privacidad de la Información de la Universidad, aprobada mediante Resolución No. 1674 de 2023 y el Modelo de Seguridad y Privacidad de la Información emanado por el MinTIC.

## 5. GENERALIDADES

La División de Servicios de Información 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.

Los procedimientos sugeridos por el MSPI e identificados por la DSI, pueden afectar de manera transversal a diferentes procesos institucionales, por ende y en vista de las particularidades del funcionamiento institucional, se les recomienda a los líderes de procesos ajustar o crear los procedimientos de su competencia, según las implicaciones del presente plan de seguridad y de las políticas de seguridad y privacidad de la información.

La División de Gestión de Talento Humano coordinará las acciones de formación relacionadas con la sensibilización y socialización a la comunidad universitaria, en corresponsabilidad con la División de Servicios de Información y la Dirección de Certificación y Gestión Documental, en el marco de la seguridad y privacidad de la información requeridas por el desarrollo del presente plan.

La División de Servicios de Información orientará a la UAA que presente dudas relacionadas con los lineamientos técnicos de seguridad de la información por la gestión de sus activos de información de carácter digital.

La Dirección de Certificación y Gestión Documental orientará a la UAA que presente dudas relacionadas con los lineamientos técnicos de seguridad de la información por la gestión de sus activos de información de carácter documental.

## 6. ALCANCE

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

## 7. PLAN DE ACCION

El plan de acción a seguir en términos de seguridad y privacidad de la información comprende el siguiente cronograma:

| Área de intervención | Actividad | Responsable | Fecha de inicio | Fecha de finalización | Entregable |
|---|---|---|---|---|---|
| Políticas de seguridad y privacidad de la información | Divulgar y socializar la Política de Privacidad y Seguridad de la Información con las UAA que tienen procesos involucrados | División de Servicios de Información | 1-feb-24 | 30-nov-24 | Registros de asistencia INFOTIPS |
| | Actualizar el Manual de Implementación de las Políticas de Seguridad y Privacidad de la Información, de acuerdo a los ajustes solicitados por las diferentes UAA involucradas. | UAA, División de Servicios de Información | 1-abr-24 | 30-sep-24 | Manual de Implementación actualizado |
| | Definir los indicadores de gestión de seguridad de la información a seguir al interior de la Universidad | División de Servicios de Información | 15-ene-2024 | 30-Nov-24 | Hoja de vida de los indicadores adoptados |
| | Documentar el subproceso de Seguridad de la Información en el Sistema de Gestión de Calidad, dentro del proceso Servicios Informáticos y de Telecomunicaciones | División de Servicios de Información | 15-ene-2024 | 30-Nov-24 | Subproceso publicado |

| | | | | | |
|---|---|---|---|---|---|
| Activos de información | Actualizar el inventario de activos de información digital de la División de Servicios de Información | División de Servicios de Información | 1-feb-24 | 30-nov-24 | Inventario actualizado |
| | Capacitar a los funcionarios de las diferentes UAA encargados de la actualización del inventario de activos de información digital. | División de Servicios de Información | 1-feb-24 | 31-jul-24 | Registros de asistencia |
| | Solicitar la actualización del inventario de activos de información digital a las diferentes UAA. | División de Servicios de Información | 1-ago-24 | 30-sep-24 | Solicitud enviada |
| | Consolidar y enviar el inventario actualizado al Comité Institucional de Gestión y Desempeño | División de Servicios de Información | 1-oct-24 | 30-nov-24 | Inventario actualizado y enviado al Comité |
| Gestión de riesgos | Actualizar la metodología de gestión de riesgos de seguridad digital y enviar al equipo de MIPG. | División de Servicios de Información | 1-feb-24 | 31-ago-24 | Metodología enviada a equipo MIPG |
| | Revisar el documento de aplicabilidad de controles del MSPI para definir posibles nuevas acciones y controles a ejecutar por parte de la DSI, relacionados con la seguridad digital. | División de Servicios de Información | 1-feb-24 | 30-nov-24 | Declaración de aplicabilidad de controles actualizada |

| | | | | | |
|---|---|---|---|---|---|
| Gestión de riesgos | Actualizar el mapa de riesgos de seguridad digital | División de Servicios de Información | 1-feb-24 | 30-nov-24 | Mapa de riesgos actualizado |
| | Definir el plan de acción a seguir producto del análisis de vulnerabilidades realizado con RENATA. | División de Servicios de Información | 1-feb-24 | 30-jun-24 | Plan de acción |
| Gestión de incidentes | Publicar la guía de gestión de incidentes de seguridad de la información, dentro de los documentos del proceso Servicios Informáticos y de Telecomunicaciones | División de Servicios de Información | 1-feb-24 | 31-may-24 | Documento publicado en la Intranet |