PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

JUVENAL DÍAZ MATEUS
Gobernador de Santander

SHIRLEY PAOLA CASTELLANOS MARTÍNEZ
Secretaria TIC

Bucaramanga, diciembre de 2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO 4
3. OBJETIVOS ESPECÍFICOS 5
4. ALCANCE 6
5. MARCO LEGAL 7
6. DEFINICIONES 9
7. INDICADORES DE MEDICIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 10
8. ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA VIGENCIA 2025 12

1. INTRODUCCIÓN

El Departamento de Santander valora su información institucional como un recurso esencial para alcanzar sus objetivos, misión y visión. Sin embargo, esta información puede verse comprometida por incidentes de seguridad, como el robo o fuga de información sensible o el acceso no autorizado, lo que podría poner en riesgo su integridad, confidencialidad y disponibilidad.

El Gobierno Nacional, mediante el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), establece directrices para la seguridad de la información que las entidades públicas deben seguir. Según estas directrices, el Departamento de Santander diseñó una estrategia integral de seguridad digital. La estrategia se fundamenta en la gestión de riesgos, seguridad y privacidad de la información y en la gestión de incidentes, para adoptar e implementar eficazmente los lineamientos establecidos por el Modelo de Seguridad y Privacidad de la Información (MSPI).

La Secretaría de Tecnologías de la Información y las Comunicaciones (SETIC) presenta el Plan de Seguridad y Privacidad de la Información correspondiente al año 2025. El propósito de este plan es garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información institucional, así como de sus activos de información asociados. Igualmente, busca potenciar las capacidades de seguridad de la información tanto de los funcionarios como la de los usuarios, fortaleciendo sus habilidades para resguardar de manera efectiva la información institucional. Este plan representa el compromiso integral con la salvaguarda de la información sensible y la mejora continua de las prácticas de seguridad.

La ejecución de este plan resulta fundamental para asegurar que el Departamento de Santander cumpla con sus obligaciones legales y éticas, preservando así la confianza de la comunidad en su capacidad para gestionar la información de manera segura y responsable. El Departamento de Santander se compromete a revisar y actualizar periódicamente este plan, validando su eficacia en la protección de la información.

2. OBJETIVO

Definir las actividades destinadas a salvaguardar la confidencialidad, integridad y disponibilidad de la información perteneciente al Departamento de Santander. A través de la aplicación de medidas de seguridad que sirvan para prevenir, detectar y responder a incidentes de seguridad, la gestión de riesgos y la protección de la infraestructura y sistemas de información. Con el fin de proteger los activos de información del Departamento de Santander, cumplir con regulaciones legales y normativas aplicables, y asegurar la continuidad del negocio en caso de incidentes de seguridad.

3. OBJETIVOS ESPECÍFICOS

- Definir medidas de seguridad para proteger los activos de información y garantizar la continuidad del negocio en caso de incidentes de seguridad, tales como planes de contingencia y recuperación de desastres.

- Fortalecer las capacidades del recurso humano de en temas relacionados con seguridad y privacidad de la información mediante la implementación de estrategias de sensibilización y capacitación.

- Cumplir con regulaciones legales y normativas aplicables en materia de seguridad de la información.

4. ALCANCE

Este plan de seguridad de la información abarca todos los activos de información vinculados a los procesos institucionales del Departamento de Santander. Se extiende a funcionarios, contratistas, proveedores y demás partes interesadas que, en el ejercicio de sus funciones, requieran acceso a dichos activos y a la información institucional.

5. MARCO LEGAL

Para garantizar que se cumplan las normativas sobre seguridad y privacidad de la información, el Departamento de Santander acata un marco legal de referencia. El marco pretende orientar la interpretación, aplicación y seguimiento de las normas vigentes, para salvaguardar eficazmente los activos de información de la Entidad. A continuación, se presenta el marco legal establecido:

NORMATIVIDAD	DESCRIPCIÓN
Resolución 00500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta elmodelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Documento Maestro del Modelo de Seguridad y Privacidad de la Información	Conjunto de políticas, procedimientos y controles que son necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información, así como para cumplir con las regulaciones y estándares de seguridad y privacidad aplicables
Ley 1581 de 2012	Ley que tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el Artículo 20 de la misma.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
CONPES 3975 de 2019	Política Nacional para la Transformación Digital e Inteligencia Artificial
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública
Decreto 1008 del 14 de junio	Lineamientos generales de la política de Gobierno Digital

NORMATIVIDAD	DESCRIPCIÓN
Ley 1266 de 2008	Regula el manejo de la información contenida en bases de datos personales
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Guía del Riesgo DAFP	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de laInformación y las Comunicaciones
Guía del Riesgo DAFP	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5
Guía No 7 Gestión del Riesgo	Gestión de Riesgos emitida por el MinTIC
Norma ISO/IEC 27005	Metodología de gestión de riesgos de seguridad de la información
Norma ISO/IEC 27001	Norma ISO para la implementación de un sistema de gestión de seguridad de la información.

6. DEFINICIONES

Activos de Información: Son todos los recursos, tanto físicos como digitales, que contienen información valiosa para la Entidad, por ejemplo, documentos impresos, bases de datos, servidores, dispositivos móviles, y redes.

Amenaza: Una posible fuente de daño a los activos de información, como virus informáticos, ataques cibernéticos, o robo físico de dispositivos.

Base de datos personales: La Ley 1581 de 2012 en Colombia establece las normas para la protección de datos personales y su libre circulación. Según esta ley, una base de datos personales es un conjunto organizado de datos personales que sea objeto de tratamiento. Esto incluye información como nombres, apellidos, direcciones, números de identificación, entre otros.

Confidencialidad: Propiedad de que la información sólo esté disponible para aquellos con autorización para verla.

Disponibilidad: Propiedad de que la información sólo esté siempre accesible para aquellos con autorización para verla.

Integridad: Propiedad de que la información no ha sido alterada de manera no autorizada.

Indicadores: Métricas utilizadas para evaluar el nivel de seguridad de una organización.

Riesgo de Seguridad Digital: El potencial de pérdida o daño a los activos de información debido a amenazas o vulnerabilidades.

Sensibilización: La educación y concientización de los empleados de una organización acerca de los riesgos y medidas de seguridad de la información.

Vulnerabilidad: Debilidad en los sistemas o procesos que podría ser aprovechada por una amenaza para causar daño a los activos de información.

7. INDICADORES DE MEDICIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los indicadores de medición son una herramienta valiosa para evaluar el estado de la seguridad de la Entidad y dar información que permita la toma de decisiones informadas para mejorarla. A continuación, los indicadores planteados para la vigencia 2024:

INDICADOR No 1. PROGRESO EN LA IDENTIFICACIÓN DE ACTIVOS DE INFORMACION					
DEFINICIÓN					
El indicador permite determinar y hacer seguimiento al número de activos de información que han sido identificados en la Entidad.					
DESCRIPCIÓN DE VARIABLES			**FÓRMULA**		
Dep1: Número de dependencias que han identificado activos de información.			$\frac{Dep\ 1}{Dep\ 2} * 100$		
Dep2: Número total de dependencias en la Entidad.					
METAS					
Bajo	< =50%	**Medio**	51% - 89%	**Alto**	90% - 100%

INDICADOR No 2. PORCENTAJE DE PERSONAL CAPACITADO EN SEGURIDAD DE LA INFORMACIÓN					
DEFINICIÓN					
Este indicador mide la cantidad de personal que ha recibido capacitación en seguridad de la Información.					
DESCRIPCIÓN DE VARIABLES			**FÓRMULA**		
Emp1: Número de empleados de planta capacitados en seguridad de la información			$\frac{Emp\ 1}{Emp\ 2} * 100$		
Emp2: Número total de empleados					
METAS					
Bajo	< =25%	**Medio**	25% - 60%	**Alto**	>=60%
INDICADOR No 3. ADOPCIÓN DEL MSPI EN EL DEPARTAMENTO DE					

SANTANDER					
DEFINICIÓN					
Este indicador mide el avance de implementación de MSPI en el Departamento de Santander.					
DESCRIPCIÓN DE VARIABLES			**FÓRMULA**		
MSPI1: Cantidad de requisitos del MSPI implementados			$\frac{MSPI\ 1}{MSPI\ 2} * 100$		
MSPI2: Cantidad total de requisitos del MSPI					
METAS					
Bajo	< =25%	**Medio**	25% - 90%	**Alto**	>=90%

INDICADOR No 4. IDENTIFICACIÓN DE BASES DE DATOS PERSONALES					
DEFINICIÓN					
El indicador permite determinar y hacer seguimiento al número de las bases de datos que contienen información personal en la Entidad.					
DESCRIPCIÓN DE VARIABLES			**FÓRMULA**		
DP1: Número total de dependencias donde se ha verificado la presencia de bases de datos con información personal y han sido identificadas.			$\frac{DP\ 1}{DP\ 2} * 100$		
DP2: Número total de dependencias en la Entidad.					
METAS					
Bajo	< =75%	**Medio**	80% - 90%	**Alto**	95% - 100%

8. ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA VIGENCIA 2025

A continuación, se detallan las actividades clave para la vigencia 2025 del plan de seguridad y privacidad de la información:

INICIATIVA	ACTIVIDAD	RESPONSABLE	FECHA
Activos de Información, riesgos de seguridad digital y datospersonales	Consolidación de la matriz de activos de información	Dirección de Gobierno Digital	IV Trimestre 2025
	Realizar la consolidación de los riesgos de seguridad digital a corte de 2025	1era línea de defensa con apoyo de la Dirección de Gobierno Digital	III y IV trimestre de 2025
	Consolidación de las bases de datos personales.	Dirección de Gobierno Digital	IV Trimestre 2025
	Reporte a SIC de las bases de datos personales	Dirección de Gobierno Digital	I Trimestre 2026
Cultura y Sensibilizaciónen seguridad de la información	Diseñar e implementar sesiones de capacitación y sensibilización en seguridad de la información para funcionarios y contratistas	Dirección de Gobierno Digital	III Trimestre 2025
	Envío de boletines, correos electrónicos sobre las últimas amenazas y las medidas de seguridades recomendadas	Dirección de Gobierno Digital	IV Trimestre 2025
Indicadores de seguridad de la información	Dar cumplimiento y realizar seguimiento a los indicadores de Seguridad de la Información	Dirección de Gobierno Digital	IV Trimestre 2025

INICIATIVA	ACTIVIDAD	RESPONSABLE	FECHA
Cumplimiento normativo	Asegurar la implementación y el desarrollo de las políticas de seguridad digital y privacidad dela información.	Comité institucional de gestión y desempeño - Dirección de gobierno digital	II y IV Trimestre 2025