PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024

JUVENAL DÍAZ MATEUS
Gobernador de Santander

SHIRLEY PAOLA CASTELLANOS MARTÍNEZ
Secretaria TIC

Bucaramanga, enero de 2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En un entorno digital e interconectado, la seguridad de la información se ha vuelto prioritaria para organizaciones de todos los tamaños y sectores. En este contexto, el Departamento de Santander presenta un plan para el tratamiento de riesgos de seguridad y privacidad de la información cuyo propósito principal es identificar, evaluar y mitigar los riesgos de este tipo que la Entidad enfrenta.

La gestión de riesgos de seguridad de la información se considera esencial para proteger los activos de información y asegurar la continuidad de las operaciones normales que respaldan los procesos misionales del Departamento de Santander. El plan se basa en el desarrollo de actividades orientadas a la detección y prevención de los riesgos de seguridad de la información, evitando posibles incidentes que puedan afectar la continuidad de su operación.

Igualmente, está enfocado en la toma de decisiones respaldada por información precisa y actualizada. A través de este plan, la Entidad se compromete a garantizar la seguridad de la información y la confidencialidad de los datos, mediante la implementación de controles necesarios para mitigar riesgos y asegurar un nivel adecuado de seguridad de la información en la Entidad.

2. OBJETIVO

Fortalecer la gestión de los riesgos vinculados a la seguridad de la información en el Departamento de Santander para el año 2024, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de sus activos de información. A través de la planificación de actividades específicas, buscando garantizar la protección de la información generada, procesada y resguardada por el Departamento de Santander, mediante la identificación, evaluación y mitigación de las amenazas y vulnerabilidades.

3. OBJETIVOS ESPECÍFICOS

- Fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información del Departamento de Santander mediante la implementación y actualización de actividades encaminadas a la definición de controles que cumplan con los lineamientos del Modelo de seguridad y privacidad de la información MSPI del MINTIC.
- Gestionar los riesgos de Seguridad de la Información en el Departamento de Santander de acuerdo con los procedimientos recomendados por la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.
- Evaluar y revisar regularmente los controles establecidos en el plan de tratamiento de los riesgos de Seguridad de la Información.
- Proporcionar una herramienta para monitorear el cumplimiento de las actividades relacionadas con la gestión de riesgos de seguridad de la información (GRSD).

4. ALCANCE

El alcance del presente plan de tratamiento de riesgos de seguridad y privacidad de la información incluye:

- La protección de la información generada, tratada y custodiada por el Departamento de Santander mediante la identificación, evaluación y mitigación de las amenazas y vulnerabilidades existentes en el entorno digital.
- El fortalecimiento del sistema de gestión de seguridad y privacidad de la información en el Departamento de Santander, implementando y actualizando los controles de seguridad que cumplan con el modelo de seguridad y privacidad de la información MSPI y la norma ISO 27001:2013.
- La gestión de los riesgos de seguridad de la información de acuerdo con los procedimientos recomendados por la guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.
- La evaluación y revisión periódica de controles establecidos en el plan de tratamiento de los riesgos de seguridad de la información.

5. MARCO LEGAL

El marco legal del plan de tratamiento de riesgos de seguridad y privacidad de la información se basa en las siguientes normativas:

- **Ley 1581 de 2012 sobre Protección de Datos Personales:** Esta ley establece las bases para la protección de datos personales en Colombia, incluyendo las obligaciones de las entidades en cuanto a la recolección, almacenamiento y tratamiento de datos personales.

- **Decreto 1377 de 2013:** Este decreto desarrolla la Ley 1581 de 2012 y establece las reglas para la protección de datos personales en el sector público, incluyendo las obligaciones de las entidades en cuanto a la Seguridad Digital.

- **Norma ISO 27001:2013:** Esta norma internacional establece los requisitos para la implementación de un sistema de gestión de seguridad de la información (SGSI), incluyendo la identificación, evaluación y tratamiento de riesgos de Seguridad Digital.

- **Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP:** Este documento establece las recomendaciones para la gestión de riesgos de Seguridad Digital en el sector público.

6. DEFINICIONES

- **Activos de información:** Refiere a los recursos valiosos de una organización, como datos, sistemas y redes, que requieren protección para garantizar la continuidad de las operaciones.

- **Confidencialidad:** Uno de los tres pilares fundamentales de la Seguridad de la Información, junto con la integridad y la disponibilidad, que se refiere a la protección de la información contra accesos no autorizados.

- **Continuidad de las operaciones:** La capacidad de una organización de mantener el funcionamiento de sus procesos críticos en caso de un incidente o desastre.

- **Control:** Medida o procedimiento implementado para mitigar un riesgo específico.

- **Entidad:** Refiere a la administración del Departamento de Santander, la organización para la cual se está desarrollando el presente plan de tratamiento de riesgos.

- **Evaluación:** Proceso de medir el nivel de riesgo asociado a un activo de información.

- **Gestión de riesgos de seguridad de la información:** Proceso de identificar, evaluar y mitigar los riesgos a los activos de información, incluyendo la información física en papel.

- **Integridad:** Uno de los tres pilares fundamentales de la Seguridad de la información, junto con la confidencialidad y la disponibilidad, que se refiere a la protección de la información contra cambios no autorizados.

- **Mitigación:** Proceso de reducir el nivel de riesgo asociado a un activo de información mediante la implementación de controles.

- **Plan de tratamiento de riesgos de seguridad y privacidad de la información:** Documento estratégico que tiene como objetivo identificar, evaluar y mitigar los riesgos a los que se enfrenta una organización en el ámbito digital.

- **Riesgo:** Posible amenaza o vulnerabilidad que podría causar daño a los activos de información de una organización.

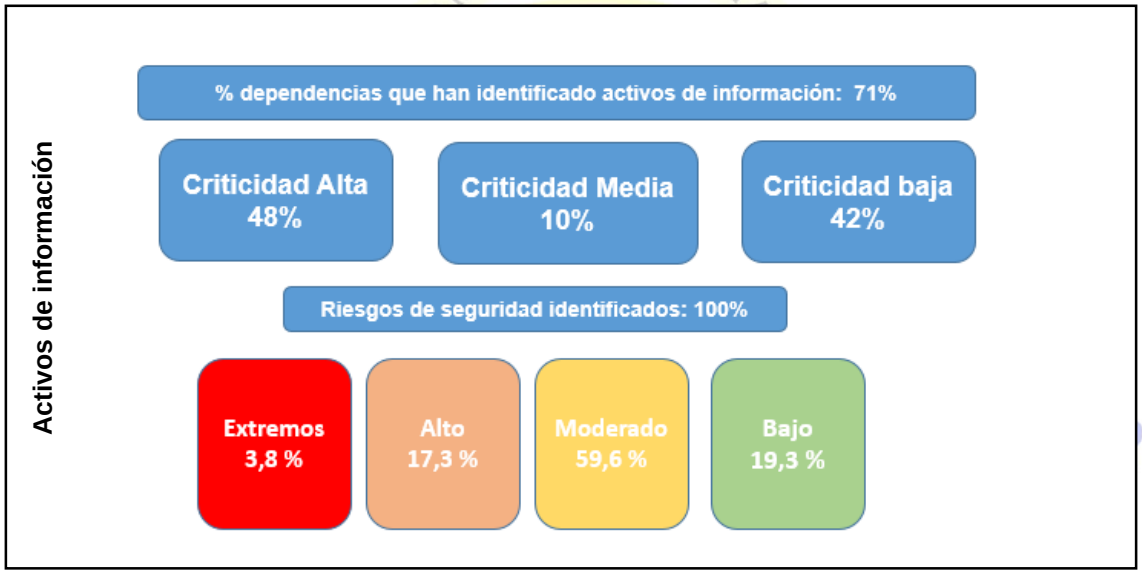
- **Seguridad de la información:** Proceso de proteger los activos de información de una organización contra amenazas y vulnerabilidades.

- **Tratamiento:** Proceso de mitigar el riesgo asociado a un activo de información mediante la implementación de controles.

7. DIAGNOSTICO

Se cuenta con una metodología desarrollada y aplicada desde el año 2021 para la gestión de riesgos de seguridad digital, la misma ha permitido realizar el levantamiento e identificación de activos de información de la gran mayoría de dependencias del Departamento de Santander como insumo para la identificación y posterior gestión de sus riesgos.

Actualmente, se está llevando a cabo el monitoreo y revisión en cada una de las dependencias para asegurar el correcto levantamiento y valoración de sus activos de información y la identificación de sus riesgos de seguridad de la información, a continuación, se presenta el avance a corte de 31 de diciembre de 2023:



8. ACTIVIDADES DE GESTIÓN Y TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El plan de gestión de riesgos de seguridad y privacidad de la información establece las acciones a llevar a cabo para lograr una mitigación efectiva de los riesgos y minimizar su impacto en los activos de información del Departamento de Santander.

Estas actividades están organizadas de acuerdo con las directrices establecidas en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP (Departamento Administrativo de la Función Pública):

Actividad	Responsable	Periodo implementación				Resultado
		T1	T2	T3	T4	
Matrices de activos de información actualizada 2024	1era línea de defensa / Gobierno digital		X			Matrices actualizadas con los activos de Seguridad Digital identificados
Actualización del plan de tratamiento de riesgos de seguridad digital	Gobierno digital	X				Plan de tratamiento de riesgos de seguridad digital actualizado a 2024
Revisión de la guía metodológica de GRSD	Gobierno digital		X			Acta de revisión de la guía metodológica de GRSD, guía actualizada en la intranet
Actualización del formato de identificación y valoración de activos de información	Gobierno digital		X			Formato en Excel de identificación y Valoración de activos de información actualizado a 2024

Actividad	**Responsable**	**Periodo implementación**				**Resultado**
		T1	**T2**	**T3**	**T4**	
Revisión del formato de registro y evaluación de riesgos de seguridad digital realizado por SIG	Gobierno digital		X			Comunicado a SIG con los comentarios de la revisión del formato de registro y evaluación de riesgos de seguridad digital
Revisión y monitoreo de riesgos de seguridad digital existentes	1era línea de defensa / Gobierno digital			X	X	Matrices de riesgos de seguridad digital actualizada a 2024