PLAN DE GESTIÓN Y TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

1. Introducción

La gestión de riesgos de seguridad digital (en adelante GRSD) es el conjunto de elementos, medidas y herramientas encaminadas a la intervención de las amenazas y las vulnerabilidades con el fin de disminuir o mitigar los riesgos existentes.

La GRSD permite identificar, comprender, evaluar y mitigar los riesgos, sus vulnerabilidades y el impacto en los activos de información de la Entidad; permite la toma de decisiones basada en información confiable y veraz, ajustado a esto, es importante definir un esquema que permita visualizar y medir todas las acciones necesarias para llevar a cabo una adecuada GRSD.

2. Objetivo

Definir la planificación de las actividades orientadas a fortalecer la gestión y el tratamiento de los riesgos asociados a la seguridad digital, de la información que es generada, tratada y custodiada por la Gobernación de Santander; con el fin preservar la confidencialidad, integridad y disponibilidad, de sus activos de información en la Entidad.

3. Objetivos específicos

- Fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información de la Gobernación de Santander, a través de la implementación y mejora de los controles de seguridad alineados con el Modelo de seguridad y privacidad de la información y la norma ISO 27001:2013.
- Gestionar los riesgos de seguridad digital de la información de la Gobernación de Santander alineado con los requerimientos metodológicos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.
- Apoyar la evaluación y revisión de los controles definidos en el plan de tratamiento de los riesgos de seguridad de la información.
- Brindar una herramienta para realizar seguimiento en el cumplimiento de cada una de las actividades de GRSD

4. Actividades de gestión y tratamiento de riesgos de seguridad digital

El Plan GRSD define las actividades a ejecutar para la adecuada mitigación de los riesgos y su afectación sobre los activos de información de la Gobernación de Santander, estas actividades son estructuradas de la siguiente manera, alineado a lo planteado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP[1]

[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas - Tomado de https://www.funcionpublica.gov.co/documents/28587410/34298398/2020-12-16_Guia_administracion_riesgos_diseño_controles_final.pdf/fa179c5e-45bb-dffd-027c-043d4733c834?t=1609857497641

Actividad	Responsable	Periodo Implementación 2021				Periodo Implementación 2022				Resultado
		T1	T2	T3	T4	T1	T2	T3	T4	
Actualización de metodología de GRSD.	Despacho Secretaria de las TIC.									Documento con la metodología de GRSD alineado a la política de administración de riesgos institucional.
Elaboración del formato de identificación y valoración de activos de información.	Despacho Secretaria de las TIC.									Formato de identificación y valoración de activos de información.
Sensibilización en GRSD en toda la Entidad.	Despacho Secretaria de las TIC / SIG.									Actas y grabaciones de participación en sensibilización.
Actualización del formato de registro y evaluación de riesgos de seguridad digital.	Despacho Secretaria de las TIC / SIG.									Actualización del formato de registro y evaluación de riesgos incluyendo seguridad digital.
Identificación y valoración de los activos de información.	Primera Línea de defensa.									Matrices de activos de información diligenciadas por la primera línea.
Identificación y evaluación de riesgos inherentes de seguridad digital.	Primera Línea de defensa.									Matrices de riesgos de SD, incluyendo su valoración.
Identificación de controles existentes.	Primera Línea de defensa.									Matriz con el listado de controles existentes identificados.
Elaboración del plan de tratamiento de riesgos de seguridad digital.	Primera Línea de defensa.									Plan de trabajo con las actividades para el tratamiento del riesgo y sus fechas de implementación.
Publicación de la matriz de riesgos página web institucional.	Despacho Secretaria de las TIC / SIG.									Listado de riesgos de seguridad digital publicados en la página web.
Monitoreo.	Primera Línea de defensa/ Despacho Secretaria de las TIC / SIG.									Matriz de riesgos con el resultado del monitoreo realizado.