Gobernación del Archipiélago
de San Andrés, Providencia y Santa Catalina

PLAN DE TRATAMIENTO DE RIESGOS

VERSIÓN 1.2

Principales modificaciones por versión de este documento

Historial de Versiones

Versión	Autor	Fecha	Descripción de la Modificación
00	Ing. Viviana López B. Ing. Enrique Santiago	22 Octubre del 2018	Elaboración de Estructura y Contenido
1.0	Ing. Shary Llanos Antonio	30 de Enero de 2021	Seguimiento y actualización
1.1	Ing. Jonathan Marín M.	19 de julio de 2022	Seguimiento y actualización
1.2	Ing. Jonathan Marín M.	18 de enero de 2023	Seguimiento y actualización

Este documento ha sido revisado por:

Versión	Revisor	Firma
00	Grupo TIC	
1.0	Secretaría General – Grupo TIC	
1.1	Secretaría TIC	
1.2	Secretaría TIC	

Este documento ha sido aprobado por:

Versión	Revisor	Firma
00	Secretaría General	
1.0	Secretaría General	
1.1	Secretaría TIC	
1.2	Secretaría TIC	

CONTENIDO

1. INTRODUCCIÓN

Este documento hace parte integral del programa de seguridad de la información, enfocados a brindar un acercamiento al Modelo de Seguridad y privacidad de la información – MSPI propuesto por el gobierno nacional.

El Sistema de Gestión de Seguridad de la Información- SGSI que propone el ministerio de las TIC – MSPI, brinda un modelo que posee un conjunto de lineamientos, políticas, normas y procesos que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación de un sistema de seguridad de la información.

Mediante el establecimiento del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y/o Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos de la Entidad.

La GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA comprometida con la gestión de la seguridad de la información de sus procesos misionales, adopta la gestión de la seguridad de sus activos de información definiendo el presente plan de tratamiento de riesgos resultante del análisis de riesgos realizado en la Entidad.

Así da cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

2. DEFINICIONES

Activo: Elemento que por la importancia que tiene para los procesos de la organización, es considerado como un bien que tienen un valor para lo organización. Los activos pueden incluir, personas, edificios, sistemas computacionales, redes, registros en papel, faxes, etc.

Activo de Información: colección de datos en formato físico o digital generado o transformado por la organización y que se considera parte de la materia prima de los procesos de la organización.

Nivel de Clasificación de los Activos de Información: Valor ponderado del activo de información asignado por el propietario de este de acuerdo con las propiedades de seguridad de la información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Administración de riesgos: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos

Análisis del riesgo: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

Asumir el riesgo: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

Causa: medios, circunstancias y/o agentes que generan riesgos.

Calificación del riesgo: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Compartir o transferir el riesgo: opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.

Consecuencia: efectos que se pueden presentar cuando un riesgo se materializa.

Control: acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

Control preventivo: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

Control correctivo: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

Debilidad: situación interna que la entidad puede controlar y que puede afectar su operación.

Evaluación del riesgo: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

Evitar el riesgo: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

Frecuencia: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

Identificación del riesgo: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

Impacto: medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

Mapa de riesgos: documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

Materialización del riesgo: ocurrencia del riesgo identificado

Opciones de manejo: posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).

Plan de contingencia: conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio

Probabilidad: medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

Procedimiento: conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cum

Confidencialidad: propiedad de los activos de información referente a que este solo sea accesible a los usuarios a los que la entidad previamente les ha otorgado la autorización.

Integridad: propiedad de los activos de información referente a que solo los usuarios autorizados por la organización puedan realizar cambios sobre los activos en el marco de un proceso legítimo de la compañía.

Disponibilidad: propiedad de los activos de información referente a que estos, siempre estén al alcance los usuarios de la organización en el momento en el que sean requeridos dentro de un proceso legítimo de la compañía.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información: Proceso continuo a través del cual la organización garantiza la preservación de las propiedades de la seguridad de la información, conocidas como: Confidencialidad, Integridad y Disponibilidad como también a otras propiedades como la autenticidad, no repudio y trazabilidad.

3. OBJETIVO

- Definir los lineamientos para tratar de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que la Gobernación pueda estar expuesto, y de esta manera lograr preservar la integridad, confidencialidad, disponibilidad y autenticidad de la información.

- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

4. ALCANCE

El plan de tratamiento de riesgos incluye a todos los activos identificados y valorados en los procesos como parte de la clasificación de activos y en el análisis de riesgos realizado en la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA.

A continuación, se relacionan los activos cubiertos en el alcance:

4.1 Procesos incluidos:

Se consideran parte del alcance todos los procesos incluidos el mapa de procesos de la organización, tales como:

- Proceso de Gestión Administrativa y tecnológica
- Proceso de Gestión Documental
- Proceso de Gestión de Talento Humano

- Proceso de Servicio al Ciudadano
- Procesos de Gestión Financiera
- Proceso de Gestión Jurídica

4.2 Plataformas Tecnológicas:

Se consideran parte del alcance todas las plataformas de hardware y software que soportan a los procesos incluidos en el alcance, tales como:

- Plataforma de red cableada
- Plataforma de red Inalámbrica
- Servidores
- Estaciones de trabajo
- Impresoras
- Sitio web
- Sistemas de Información
- Sistemas de seguridad lógica

4.3 Activos de Información:

Se consideran parte del alcance todos los documentos lógicos relacionados con los procesos incluidos en el alcance que han sido identificados y clasificados, tales como:

- Documentos electrónicos.
- Documentos físicos.

4.4 Exclusiones del alcance

Todos los activos de información que no han sido relacionados en los apartados anteriores de este documento.

5. PARTES INTERESADAS

La alta dirección comprometida con la seguridad de la información a través del Grupo TIC asesora a las áreas en el proceso de implementación de controles de seguridad para la protección de la información, y realiza el proceso de sensibilización en Seguridad y privacidad de la información, con el fin de crear un cultura en seguridad que permita minimizar los riesgos a los que está expuesta la información, así mismo los líderes de las áreas cumplen con los procedimientos establecidos para la clasificación y protección de los activos de información que hacen parte de los procesos de cada una de las áreas.

El comité de MIPG quien hace las veces de comité de seguridad hará seguimiento a la implementación del plan, con el fin, de evidenciar en el siguiente ciclo el avance de la madurez del modelo de Seguridad y privacidad de la información.

6. PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

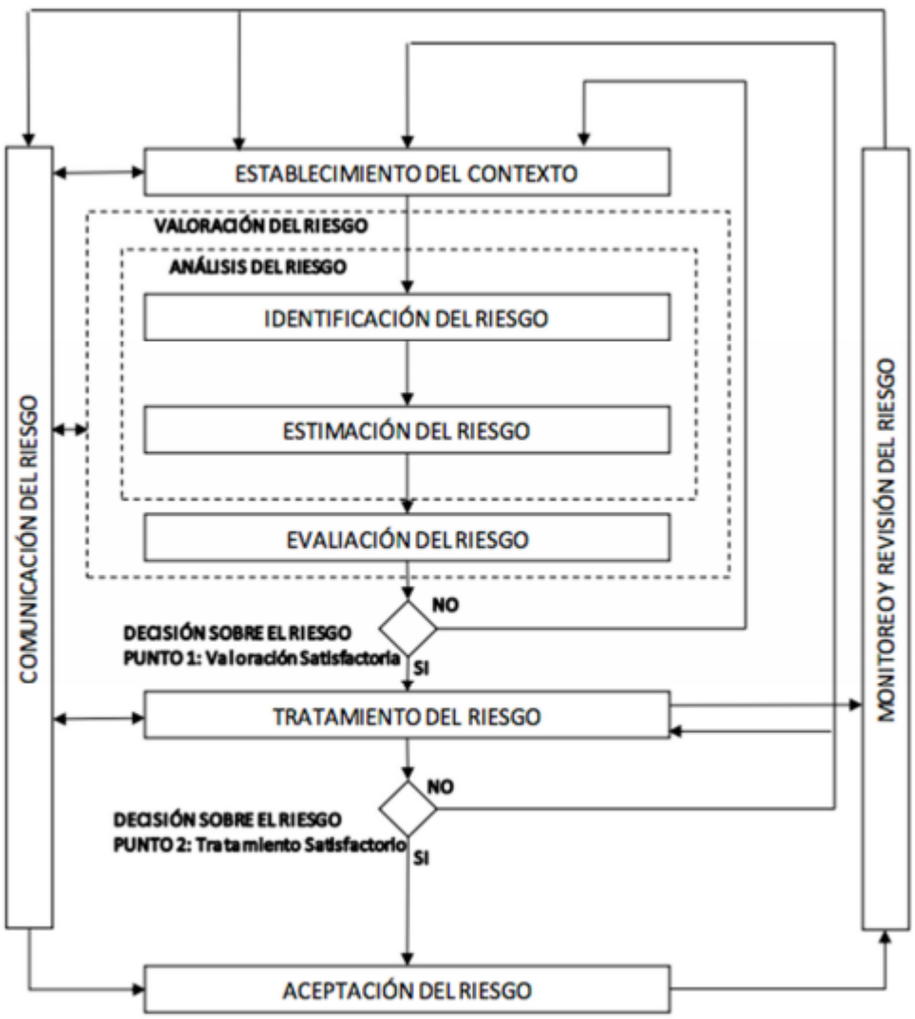

Ilustración 1. Proceso para la administración de riesgos de seguridad y privacidad de la información

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Para la evaluación de riesgos de seguridad y privacidad de la información se tomará como insumo la matriz de Activos de Información, sobre la cual se implementará el presente Plan sobre los Activos de Información que tengan un nivel alto de clasificación al evaluar los criterios de confidencialidad, integridad y disponibilidad, según los siguientes criterios.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración 1. Criterios de Clasificación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Ilustración 2. Niveles de Clasificación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

7. CONTEXTO ESTRATÉGICO

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta primera etapa, se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad; es la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las CAUSAS del riesgo.

La Gobernación busca desarrollar una cultura de seguridad de la información donde los funcionarios y contratistas logren reconocer los riesgos a los que están expuestos en su

entorno. Para cumplir tal objetivo la gobernación debe tener una adecuada administración de los riesgos institucionales y los de corrupción.

La administración adecuando de los riesgos de la seguridad de la información en la entidad tiene como propósito dar soporte al modelo de seguridad de la información al interior de la Gobernación, conformidad legal y evidencia de la debida diligencia.

8. PLAN DE TRATAMIENTO

Una vez identificados los activos, valorados y evaluado el nivel de riesgos al que se encuentran expuestos, se procede a determinar el tratamiento que habrá de darse a cada uno de ellos, que acciones deberán realizarse, quienes serán los responsables de esta implementación y que procedimientos se ejecutarán para monitorizar y hacer seguimiento de la ejecución de las acciones.

Por motivos de confidencialidad de los controles y las medidas específicas para tratar los riesgos de seguridad de la información, el plan de tratamiento de riesgos se describirá de forma general, indicando las macro actividades encaminadas para cada riesgo o requisito de seguridad de la información.

A continuación, se relaciona el plan de tratamiento de riesgo propuesto:

GESTION	ACTIVIDAD	TAREA	RESPONSABLE	FECHA
Gestion de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Grupo TIC	jun-dic
	Sensibilización	Socialización guía de gestión de riesgos de seguridad y privacidad de la información.	Grupo TIC	abr-may
	Identificación de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Identificación, análisis y evaluación de riesgos de seguridad y privacidad de la información	Grupo TIC	abr-sep
		Realimentación, revisión y verificación de los riesgos identificados		abr-sep
	Aceptación de riesgos identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Grupo TIC	jun-nov
	Publicación	Publicación de matriz de riesgos	Grupo TIC	jun-nov
	Seguimiento fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y velicación de evidencias	Grupo TIC	jun-dic
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Grupo TIC	jun-dic
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Grupo TIC	jun-dic
		Actualización guía gestión de riesgos seguridad de la información de acuerdo a los cambios solicitados.		jun-dic
	Monitoreo y revisión	Generación, presentación y reporte de indicadores.	Grupo TIC	jun-dic

9. RECURSOS

La Entidad en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, dispone de los siguientes recursos:

RECURSOS	VARIABLE
Humanos	La Secretaría TIC es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - Octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI).
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías.

El propietario de este documento es el Oficial de Seguridad de la Información o quien haga sus veces en la Entidad, quien debe encargarse de actualizarlo por lo menos una vez al año.

10. ANEXOS

Adjunto a este documento se anexa: Plan detallado de tratamiento de Riesgos: Versión 1.0 construida por la Gobernación de San Andrés y providencia.

REFERENCIAS BIBLIOGRÁFICAS

1. Norma ISO/IEC 27001: Elemento de la norma 4.3
2. Guía de Gestión de Riesgos de MINTIC: publicada en el portal de MINTIC como: articles-5482_G7_Gestion_Riesgos.pdf
3. Decreto 1078 de 2015: “Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea”
4. 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.

5. Política de Gobierno Digital (en donde se encuentra como habilitador el Modelo de Seguridad de la Información)
6. Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la Protección de Datos Personales Decreto 2693 de 2012“
7. Documento de Políticas de Seguridad de la Información: Versión 1.0 construida por la Gobernación de San Andrés y providencia.
8. Política Pública: CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad Digital.