Gobernación del Archipiélago
de San Andrés, Providencia y Santa Catalina

# PLAN DE TRATAMIENTO DE RIESGOS

VERSIÓN 1.0

## DESCRIPCIÓN BREVE

Este plan se define de acuerdo con los lineamientos de MINTIC, con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medidas de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.


## ACTUALIZÓ: ING. SHARY LLANOS ANTONIO

Enero de 2021

Principales modificaciones por versión de este documento

**Historial de Versiones**

| Versión | Autor | Fecha | Descripción de la Modificación |
|---|---|---|---|
| 00 | Ing. Viviana López B.<br>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 |

**Este documento ha sido revisado por:**

| Versión | Revisor | Firma |
|---|---|---|
| 00 | Grupo TIC | |
| 1.0 | Secretaría General – Grupo TIC | |

**Este documento ha sido aprobado por:**

| Versión | Revisor | Firma |
|---|---|---|
| 00 | Secretaría General | |
| 1.0 | Secretaría General | |

# 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 ANDRES, 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

El objetivo del presente documento es definir el plan de tratamiento de los riesgos identificados en los procesos evaluados como parte del programa de seguridad de la información en la GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRES, PROVIDENCIA Y SANTA CATALINA.

# 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 ANDRES, 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 Servicio al Ciudadano
- Procesos de Gestión Financiera
- Proceso de Gestión Jurídica
- Proceso de Gestión de Talento Humano

## 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. 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.

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

| ID | Dominio de la Norma | Tratamiento | Acción | Monitorización y Seguimiento | Responsables | % Avance |
|---|---|---|---|---|---|---|
| A.5 | POLITICA DE SEGURIDAD DE LA INFORMACION | SI | Reducir | Documento revisión de políticas de seguridad | OSI y Comité | 90% |
| A.6 | ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION | SI | Reducir | Documento de Nombramiento de OSI y Comité | OSI y Comité | 50% |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | SI | Reducir | Registro de capacitación en seguridad | OSI y Comité | 80% |
| A.8 | GESTION DE ACTIVOS | SI | Reducir | Documento de Clasificación de Activos | OSI y Comité | 90% |
| A.9 | CONTROL DE ACCESO | SI | Reducir | Bitácora de revisión de derechos de usuarios | OSI y Comité | 80% |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.10 | CRIPTOGRAFIA | SI | Reducir | Relación de Sistemas que usan cifrado | OSI y Comité | 0% |
| A.11 | SEGURIDAD FISICA Y AMBIENTAL | SI | Reducir | Bitácora de registros de acceso físico | OSI y Comité | 60% |
| A.12 | SEGURIDAD EN LAS OPERACIONES | SI | Reducir | Bitácora de registro de backups | OSI y Comité | 60% |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | SI | Reducir | Registro de acuerdos de confidencialidad con terceros | OSI y Comité | 90% |
| A.14 | ADQUISICION DESARROLLO Y MANTENIMIENTO DE SISTEMAS | SI | Reducir | Separación de Entorno de Producción y desarrollo | OSI y Comité | 90% |
| A.15 | RELACIONES CON LOS PROVEEDORES | SI | Reducir | Documento de entendimiento de las políticas de seguridad por parte de los proveedores | OSI y Comité | 80% |

***Tabla 1. Plan de tratamiento de riesgo propuesto***

A continuación, se relaciona el cronograma propuesto para el tratamiento del riesgo identificado:

| ID | Dominio de la Norma | Planificación | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Feb. | Mar. | Abril | Mayo | Jun. | Julio | Agos. | Sept. | Oct. | Nov. | Dic. |
| A.5 | POLITICA DE SEGURIDAD DE LA INFORMACION | | | | | | | | | | | |
| A.6 | ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION | | | | | | | | | | | |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | | | | | | | | | | | |
| A.8 | GESTION DE ACTIVOS | | | | | | | | | | | |
| A.9 | CONTROL DE ACCESO | | | | | | | | | | | |
| A.10 | CRIPTOGRAFIA | | | | | | | | | | | |
| A.11 | SEGURIDAD FISICA Y AMBIENTAL | | | | | | | | | | | |
| A.12 | SEGURIDAD EN LAS OPERACIONES | | | | | | | | | | | |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | | | | | | | | | | | |
| A.14 | ADQUISICION DESARROLLO Y MANTENIMIENTO DE SISTEMAS | | | | | | | | | | | |
| A.15 | RELACIONES CON LOS PROVEEDORES | | | | | | | | | | | |
| A.16 | GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION | | | | | | | | | | | |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO | | | | | | | | | | | |
| A.18 | CUMPLIMIENTO | | | | | | | | | | | |

***Tabla 2. Cronograma propuesto para la ejecución del plan de tratamiento de riesgo***

# 6. 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 General a través del Grupo 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 de la Entidad, quien debe encargarse de actualizarlo por lo menos una vez al año.

# 7. 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 BIBLIOGRAFICAS

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.