Personería Distrital de Cartagena de Indias

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2025

GESTION TIC

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....2
2. OBJETIVOS.....2
3. ALCANCE DEL PLAN.....2
4. MARCO NORMATIVO 3
5. RESPONSABLES.....**¡Error! Marcador no definido.**
6. DEFINICIONES 3
7. CLASIFICACION Y TRATAMIENTO DE LA INFORMACIÓN**¡Error! Marcador no definido.**
8. ACTIVIDADES .....**¡Error! Marcador no definido.**

1. INTRODUCCIÓN

El presente documento forma parte del Sistema de Gestión de Seguridad de la Información (SGSI) de la Personería Distrital de Cartagena de Indias, y tiene como propósito establecer los controles, acciones y responsables requeridos para mitigar o tratar los riesgos que puedan comprometer la seguridad y la privacidad de la información institucional.

Este plan se elabora con base en los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), especialmente en lo dispuesto por la **"Guía para la gestión de seguridad y privacidad de la información"** y el **Modelo de Seguridad y Privacidad de la Información (MSPI)**, en armonía con el **Modelo Integrado de Planeación y Gestión (MIPG)**.

El plan de tratamiento de riesgos considera los resultados del análisis de riesgos previamente realizado, enfocado en la protección de la **confidencialidad**, **integridad**, **disponibilidad** y **privacidad** de los activos de información relacionados con los sistemas institucionales **SIAP**, **SIGPER** y **PERTH**, **SITIO WEB**, así como la infraestructura tecnológica que los soporta.

Este documento es de carácter dinámico y será actualizado conforme se presenten cambios tecnológicos, normativos o institucionales que puedan impactar la seguridad de la información.

2. OBJETIVOS

Establecer e implementar medidas de tratamiento para mitigar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información tratada por los sistemas institucionales y demás de que se generen en el ejercicio de las funciones de la personería distrital de Cartagena de Indias.

3. ALCANCE DEL PLAN

Este plan cubre los activos de información, infraestructuras tecnológicas y procesos relacionados con la operación de los sistemas de información institucionales, así como el manejo de datos personales y datos sensibles.

4. MARCO NORMATIVO

- Ley 1581 de 2012: Protección de datos personales.
- Ley 1273 de 2009: Protección de la información y los datos.
- Ley 1712 de 2014: Transparencia y acceso a la información pública.
- Decreto 1377 de 2013: Reglamentación de la Ley 1581.
- Decreto 1499 de 2017: Fortalecimiento del MIPG.

5. ESTRATEGIAS DE TRATAMIENTO

- **Mitigación**: Implementar controles técnicos y administrativos para reducir la probabilidad o el impacto del riesgo.
- **Transferencia**: Externalizar la gestión del riesgo mediante contratos o seguros.
- **Aceptación**: Cuando el nivel de riesgo sea bajo o el costo del tratamiento supere el beneficio.
- **Eliminación**: Cuando sea posible eliminar el activo o proceso que origina el riesgo.

6. RESPONSABLES

El tratamiento de los riesgos de la seguridad y privacidad de la información se encuentra bajo la responsabilidad del proceso de Gestión TIC. La Alta Dirección de la Personería de Cartagena de Indias, los lideres de procesos, jefes de oficina, Personeros delegados y demás, apoyarán la ejecución del presente plan mediante la participación y compromiso con las actividades que requieran de su apoyo y gestión, y fomentando en el personal a cargo la participación en las actividades que le correspondan.

7. DEFINICIONES

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Confidencialidad: Propiedad que determina que la información no está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Criterios de riesgos: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.

Declaración de aplicabilidad: Documento que enumera los controles de seguridad que hacen parte del ANEXO A de la NTC-ISO/IEC 27001:2022, y que serán aplicables en la entidad para el Sistema de Gestión de Seguridad de la Información – SGSI.

Evaluación del Riesgo: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.

Evento: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.

Nivel de riesgo: Valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Plan de Acción: Conjunto de acciones establecidas para mitigar el nivel de riesgo residual una vez realizada la evaluación de los riesgos de seguridad de la información.

Reducir/Mitigar: El riesgo se trata mediante la transferencia o la implementación de acciones que mitiguen su nivel. No necesariamente es un control adicional.

Vulnerabilidad: es una falencia o debilidad de un activo de información o de un control de seguridad que puede ser explotada por un atacante para afectar la seguridad de la información.

8. MATRIZ DE TRATAMIENTO DE RIESGOS

Riesgo Identificado	Nivel de Riesgo	Tratamiento Seleccionado	Controles o Acciones	Responsable
Acceso no autorizado a los sistemas de información	Alto	Mitigación	Implementación de bloque de ataques Robot Force	Proceso-Gestión TIC
Pérdida de información por Ataques al servidor web	Alto	Mitigación	Copias de seguridad diarias, servidor redundante, monitoreo proactivo	Proceso-Gestión TIC
Filtración de datos personales en correos o medios físicos	Medio	Mitigación	Sensibilización a funcionarios, cifrado de archivos, políticas de envío	Talento Humano y Proceso-Gestión TIC
Malware en equipos del usuario final	Alto	Mitigación	Antivirus actualizado, restricción de descargas, controles en navegación web	Proceso-Gestión TIC
Desactualización de los sistemas de información	Medio	Mitigación	Cronograma de actualizaciones, pruebas en entorno de ensayo	Coordinación TIC
Acceso remoto sin cifrado	Alto	Eliminación / Mitigación	Bloqueo de acceso no cifrado, uso de VPN institucional	Proceso-Gestión TIC

9. ACTIVIDADES DEL PLAN DE TRATAMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Actividad	Descripción	Responsable(s)	Recursos	Indicador
Implementar Manejo de Intentos de acceso no validos en los sistemas de información	Configurar autenticación multifactor para los usuarios de los sistemas SIAP, SIGPER y Perth	Proceso-Gestión TIC	Licencias de autenticador, personal técnico	Porcentaje de acceso validos a los sistemas
Realizar copias de seguridad diarias	Implementar y verificar copias de seguridad automáticas del servidor.	Proceso-Gestión TIC	Software de backup, almacenamiento externo	Frecuencia y éxito de copias de seguridad
Actualizar y mantener antivirus institucional	Mantener los sistemas de protección antivirus en todos los	Proceso-Gestión TIC	Licencias antivirus	Porcentaje de equipos protegidos

	dispositivos institucionales.			
Diseñar cronograma de actualizaciones a los sistemas de información	Planificar aplicación periódica de parches y nuevas versiones del sistema.	Proceso-Gestión TIC	Calendario de Desarrollos TI	Número de actualizaciones ejecutadas

	REVISADO POR:	APROBADO POR:
Personero Auxiliar	Líder de Proceso	Comité de Gestión y desempeño

CONTROL DE CAMBIOS

VERSION	FECHA	DESCRIPCION DEL CAMBIO
01	01-2025	Se formula la estructura documental de los planes institucionales
02	08-2025	Se agrega matriz de riesgo que contempla riesgos priorizados, con medidas de tratamiento alineadas con los controles definidos en estándares reconocidos (como ISO/IEC 27001 o el Modelo de Seguridad y Privacidad del MinTIC), se modifican las actividades.