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

ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

2026

OFICINA ASESORA DE INFORMÁTICA

1. Introducción

El Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PITRSPI es el instrumento operativo mediante el cual la Alcaldía Distrital de Cartagena de Indias identifica, analiza, evalúa y define las acciones de tratamiento de los riesgos asociados a la seguridad de la información, la privacidad de los datos personales y la seguridad digital.

El PITRSPI 2026 se formula en cumplimiento del Plan Institucional de Seguridad y Privacidad de la Información – PISPI 2026, como parte del ciclo de mejora continua del Modelo de Seguridad y Privacidad de la Información – MSPI, y en coherencia con el Modelo Integrado de Planeación y Gestión – MIPG.

La presente versión incorpora ajustes incrementales derivados de la actualización del MSPI (2025), sin modificar los criterios institucionales de gestión del riesgo previamente definidos.

2. Contexto estratégico de la entidad

La Alcaldía Distrital de Cartagena desarrolla su gestión institucional en un entorno de transformación digital progresiva, con alta dependencia de la información, los sistemas de información, los servicios digitales y el tratamiento de datos personales para el cumplimiento de sus funciones misionales y administrativas.

En este contexto, la materialización de riesgos de seguridad y privacidad de la información puede afectar la continuidad de los servicios, el cumplimiento normativo, la confianza ciudadana y los objetivos estratégicos del Distrito, lo que exige un tratamiento sistemático, articulado y transversal de dichos riesgos.

3. Marco Normativo

El PITRSPI 2026 de la Alcaldía Distrital de Cartagena se fundamenta en el siguiente marco normativo:

3.1 Normativa Nacional.

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015. Por el cual se reglamentan parcialmente disposiciones de la Ley 1581 de 2012.
- Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 1078 de 2015. Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se deroga el Decreto 1008 de 2018.
- Política de Gobierno Digital, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- Política de Seguridad Digital – MinTIC.
- Resolución 500 de 2021 - Lineamientos y estándares de la estrategia de seguridad digital y adopción del Modelo de Seguridad y Privacidad de la Información – MSPI.

- Resolución 02277 de 2025 - Actualización del Anexo 1 de la Resolución 500 de 2021.
- Modelo Integrado de Planeación y Gestión – MIPG, liderado por el Departamento Administrativo de la Función Pública.

3.2 Normativa Internacional.

- ISO 31000: Gestión del Riesgo – Principios y directrices.
- ISO/IEC 27001: Sistemas de Gestión de Seguridad de la Información – Requisitos.
- ISO/IEC 27005: Gestión de riesgos relacionados con la seguridad de la información.
- ISO/IEC 27701: Sistemas de gestión de la información de privacidad – Extensión de ISO/IEC 27001 e ISO/IEC 27002.

3.3 Modelos y Guías.

- Modelo de Seguridad y Privacidad de la Información – MSPI, expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC (actualización 2025).
- Lineamientos de gestión del riesgo de seguridad y privacidad de la información definidos en el marco del MSPI.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, expedida por el Departamento Administrativo de la Función Pública.
- Política de Administración del riesgo de la Alcaldía de Cartagena

4. Objetivos del Plan

4.1Objetivo General.

Gestionar y tratar de manera sistemática los riesgos de seguridad y privacidad de la información y seguridad digital de la Alcaldía Distrital de Cartagena, en coherencia con el PISPI 2026 y el MSPI, contribuyendo al cumplimiento de los objetivos institucionales.

4.2 Objetivos Específicos.

- Identificar y priorizar los riesgos institucionales de seguridad y privacidad de la información.
- Definir y ejecutar acciones de tratamiento coherentes con el PISPI 2026.
- Reducir la probabilidad e impacto de incidentes de seguridad digital.
- Fortalecer el seguimiento, control y mejora continua de la gestión del riesgo.

5. Alcance

El PITRSPI 2026 aplica a:

- Todos los procesos, dependencias y servidores públicos del Distrito.
- Activos de información físicos, digitales y humanos.
- Sistemas de información, servicios tecnológicos y tratamiento de datos personales.
- Relación con terceros y proveedores tecnológicos.

6. Metodología para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

La metodología para PITRSPI 2026 define el enfoque y las etapas generales para la gestión de los riesgos asociados a la seguridad y privacidad de la información y a la seguridad digital en la Alcaldía Distrital de Cartagena.

Esta metodología se desarrolla en concordancia con los lineamientos institucionales, los modelos y políticas vigentes en materia de seguridad y privacidad de la información, así como con las buenas prácticas reconocidas para la gestión del riesgo.

El enfoque adoptado es sistemático, preventivo y basado en riesgos, y permite identificar, analizar, evaluar, tratar y monitorear los riesgos que puedan afectar la información, los datos personales y los servicios digitales de la Alcaldía Distrital de Cartagena.

6.1 Identificación y descripción de riesgos.
La identificación de riesgos se realiza a nivel institucional, a partir del análisis de los activos de información, los procesos críticos y el contexto interno y externo de la entidad, conforme a los lineamientos de MinTIC y a la metodología institucional de administración del riesgo definida por Función Pública.

Los riesgos se documentan de manera estructurada y el resultado de esta etapa se consolida en la matriz institucional de riesgos de seguridad y privacidad de la información.

6.2 Análisis y evaluación de riesgos.
Los riesgos identificados son analizados y evaluados conforme a los criterios definidos por la entidad, considerando:

- La probabilidad de ocurrencia.
- El impacto potencial en los ámbitos institucional, legal, operativo, financiero y reputacional.
- El nivel de riesgo resultante, de acuerdo con la matriz de evaluación institucional.

Con base en esta valoración, los riesgos son clasificados y priorizados para su tratamiento durante la vigencia 2026.

6.3 Tratamiento de riesgos.
Para los riesgos priorizados se definen las opciones de tratamiento:

- Mitigar: mediante la implementación o fortalecimiento de controles.
- Evitar: eliminando la fuente del riesgo.
- Transferir: a través de mecanismos contractuales, aseguramiento u otros instrumentos.
- Aceptar: previa justificación técnica y aprobación por la instancia competente.

Las acciones de tratamiento incorporan controles administrativos, técnicos y organizacionales, y se documentan en el Plan de Tratamiento de Riesgos, indicando responsables, plazos y recursos requeridos.

6.4 Aceptación, seguimiento y revisión de riesgos.
Los riesgos residuales serán aceptados conforme a los niveles de autoridad definidos por la Alcaldía. El PITRSPI contempla mecanismos de:

- Seguimiento periódico a la ejecución de las acciones de tratamiento.
- Revisión de los riesgos ante cambios relevantes en el contexto institucional, normativo, tecnológico u operativo.

- Actualización anual del plan, como parte del ciclo de mejora continua y del fortalecimiento del Sistema de Control Interno.

De manera transversal, la gestión de riesgos se apoya en acciones de comunicación, sensibilización y capacitación, orientadas a fortalecer la cultura institucional en seguridad y privacidad de la información, las cuales se desarrollan a través del Plan de Cambio, Cultura, Apropiación, Capacitación y Sensibilización, articulado con el Plan Institucional de Capacitación – PIC o formulado de manera específica para la vigencia 2026.

6.5 Indicadores y mecanismos de monitoreo.

El monitoreo del PITRSPI se apoya en indicadores que permiten evaluar el avance y la efectividad del tratamiento de riesgos, tales como:

- Porcentaje de riesgos críticos con acciones de tratamiento implementadas.
- Nivel de avance del PITRSPI.
- Número de incidentes de seguridad digital gestionados.
- Cumplimiento de las acciones dentro de los plazos definidos.

Estos mecanismos de monitoreo se integran a los procesos institucionales de seguimiento, evaluación y control, garantizando la trazabilidad con los instrumentos de gestión del riesgo institucional y los reportes asociados al MIPG.

7. Plan de acción

Nª	Actividad	Entregables	Responsables	Nombre del indicador
1	Actualizar la metodología institucional de gestión de riesgos de seguridad y privacidad de la información conforme al MSPI vigente y lineamientos nacionales	Metodología institucional actualizada	Oficina Asesora de Informática	Metodología actualizada
2	Actualizar la documentación institucional asociada a seguridad y privacidad de la información	Documentación institucional actualizada	OAI / Dependencias responsables	Documentación actualizada
3	Actualizar e identificar los activos de información y procesos críticos en las dependencias	Inventario institucional de activos	Dependencias / OAI	Activos identificados

4	Identificar los riesgos de seguridad y privacidad de la información a nivel institucional	Matriz institucional de riesgos SPI	Dependencias / OAI	Riesgos identificados
5	Sensibilizar a las dependencias sobre la metodología actualizada de gestión de riesgos SPI	Registros de sensibilización y materiales	OAI	Dependencias sensibilizadas
6	Formular y aprobar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	PITRSPI 2026 formulado	OAI	PITRSPI formulado
7	Establecer indicadores y mecanismos de seguimiento del PITRSPI	Indicadores definidos	OAI / Control Interno	Indicadores definidos
8	Realizar seguimiento y evaluación al avance del PITRSPI	Informes de seguimiento	OAI	Seguimiento realizado
9	Identificar y documentar los controles existentes de seguridad y privacidad de la información	Inventario de controles existentes	OAI / Dependencias	Controles identificados
10	Realizar evaluación preliminar de la efectividad y madurez de los controles existentes	Informe de evaluación preliminar de controles	OAI / Control Interno	Controles evaluados

8. Responsables del PITRSPI y líneas de defensa

- **Primera línea:** Dependencias responsables de los procesos.
- **Segunda línea:** Oficina Asesora de Informática (gestión del riesgo de seguridad y privacidad).
- **Tercera línea:** Oficina de Control Interno (evaluación independiente).

El Comité Institucional de Gestión y Desempeño ejercerá seguimiento estratégico.

9. Presupuesto

La ejecución del PISPI 2026 se articulará a la planeación y presupuesto institucional, considerando recursos asociados a:

- Talento humano y fortalecimiento de capacidades.
- Herramientas tecnológicas y controles de seguridad.
- Capacitación y sensibilización.

- Seguimiento, control y mejora continua.

La asignación específica se definirá conforme a la disponibilidad presupuestal y la priorización institucional.

11. Lineamientos de seguimiento, control y mejora continua

El seguimiento al PISPI se realizará a través de los mecanismos definidos en el MIPG, incluyendo:

- Seguimiento a la implementación del MSPI.
- Reportes de avance institucional.
- Insumos para Control Interno y FURAG.

Los resultados alimentarán el ciclo de mejora continua del plan, sin generar estructuras paralelas de control.

10. Anexos –

Se anexa plan en Excel.

11. Aprobación

Firma de los integrantes del comité institucional de gestión y desempeño de la Alcaldía distrital de Cartagena de indias.

Aprobado Mediante Acta del Comité Institucional de Gestión y Desempeño XXXX del xx de xxxxxxxx de xxxx