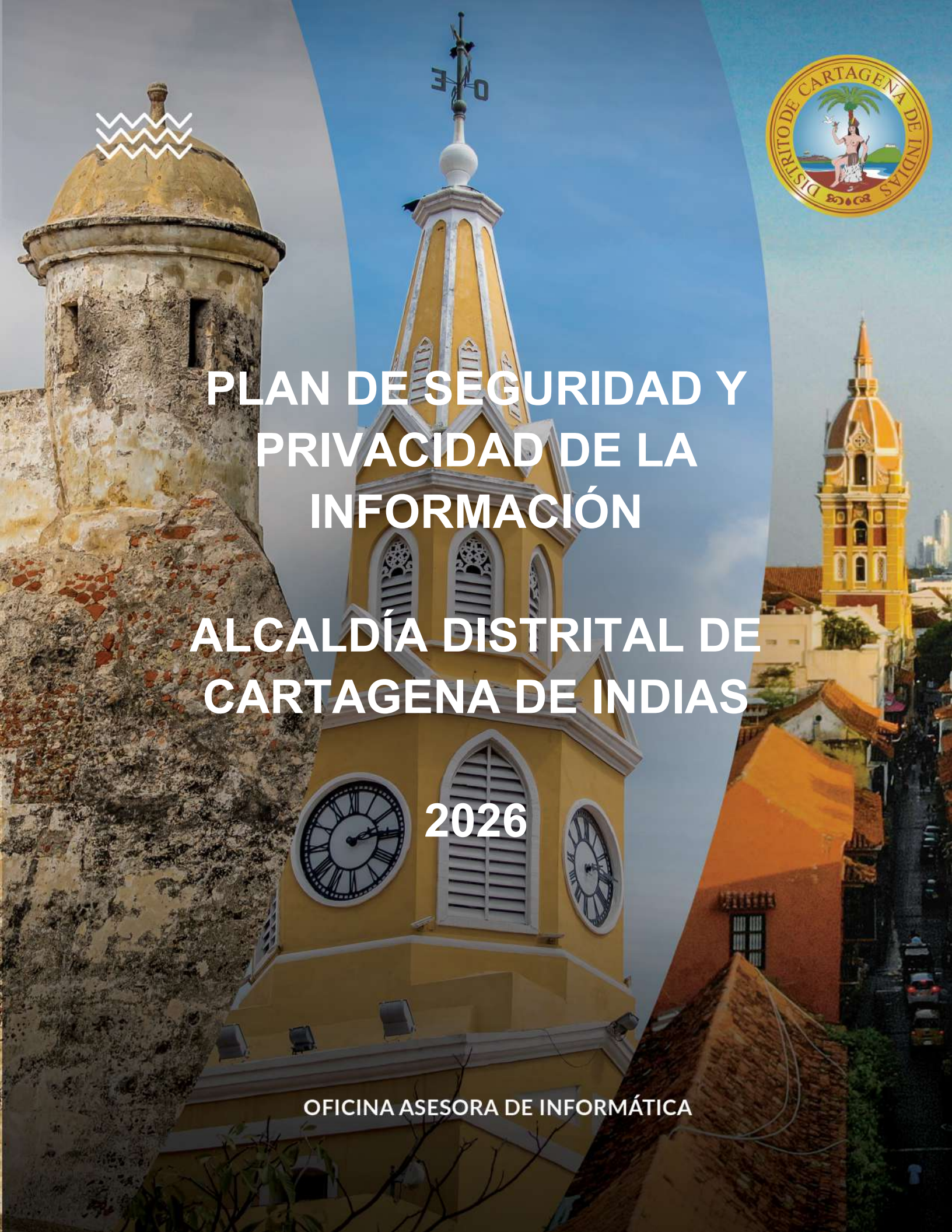

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

2026

OFICINA ASESORA DE INFORMÁTICA

1. Introducción

El Plan Institucional de Seguridad y Privacidad de la Información – PISPI 2026 corresponde a la actualización anual del plan formulado para el período 2024–2027, en cumplimiento del Decreto 612 de 2018 y del Decreto 767 de 2022, y se fundamenta en los resultados de ejecución, seguimiento y control obtenidos durante la vigencia 2025, así como en la actualización del Modelo de Seguridad y Privacidad de la Información – MSPI (2025).

Esta actualización no constituye una reformulación integral, sino un ajuste incremental orientado a garantizar la continuidad de las acciones estratégicas, la alineación normativa, la coherencia institucional y la mejora continua, considerando el nivel de madurez institucional y los riesgos identificados.

El PISPI se articula de manera directa con la Política de Gobierno Digital, la Política de Seguridad Digital y el Modelo Integrado de Planeación y Gestión – MIPG, y se consolida como un habilitador transversal para la prestación de servicios, la gestión institucional y la generación de confianza digital en la ciudadanía.

En este marco, el PISPI de la Alcaldía Distrital de Cartagena de Indias constituye el instrumento estratégico mediante el cual se definen los lineamientos, responsabilidades y acciones orientadas a la protección de los activos de información, el adecuado tratamiento de los datos personales y la implementación de la seguridad digital como condición habilitante de la gestión pública.

2. Marco Estratégico Institucional

El PISPI 2026 se desarrolla como actualización anual del plan institucional vigente para el período 2024–2027, y se mantiene enmarcado en la estrategia institucional de la Alcaldía Distrital de Cartagena de Indias, en coherencia con la misión institucional, los objetivos estratégicos del Distrito y los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

En este marco, la seguridad y la privacidad de la información se conservan como componentes transversales de la gestión pública, orientados a soportar la administración de la información, la gestión de los riesgos institucionales, la transformación digital del Distrito, la protección de los derechos fundamentales de la ciudadanía y el fortalecimiento de la confianza en la administración distrital, sin modificar el enfoque estratégico previamente definido.

La Alcaldía Distrital de Cartagena de Indias ejerce sus funciones misionales en un entorno altamente dependiente de la información, los sistemas de información y los servicios digitales, tanto para la planeación, ejecución y control de la gestión pública como para la prestación de servicios a la ciudadanía. En consecuencia, la seguridad y la privacidad de la información se

reconocen y mantienen como condiciones habilitantes para la operación institucional, la continuidad de los servicios, la transparencia y la protección de los derechos fundamentales.

Este enfoque permite que la seguridad y la privacidad de la información continúen aportando al cumplimiento de la misión institucional, al desempeño organizacional y a la generación de valor público, en articulación con el MIPG, y en alineación con los objetivos estratégicos del Distrito.

3. Marco Normativo y de Referencia

El presente plan se actualiza y ejecuta en cumplimiento de, como mínimo, el siguiente marco normativo y técnico:

3.1 Marco normativo nacional

- Ley 1581 de 2012 y normas reglamentarias sobre protección de datos personales.
- Ley 1712 de 2014 – Transparencia y acceso a la información pública.
- Decreto 1078 de 2015 - Decreto Único Reglamentario del sector TIC.
- Decreto 1083 de 2015 – Función Pública.
- Decreto 612 de 2018 - Integración de los planes institucionales y estratégicos al Plan de Acción Institucional.
- Decreto 767 de 2022 - Actualización de los lineamientos de la Política de Gobierno Digital.
- 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.
- Circulares externas, guías y lineamientos expedidos por la Superintendencia de Industria y Comercio.
- Decreto 1499 de 2017 - Adopción del Modelo Integrado de Planeación y Gestión.

3.2 Marco normativo y técnico internacional

- ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información.
- ISO/IEC 27002:2022 – Controles de seguridad de la información.
- ISO/IEC 27701:2019 – Sistema de Gestión de Información de Privacidad.
- ISO 31000:2018 – Gestión del riesgo.
- ISO/IEC 27005 – Gestión del riesgo de seguridad de la información.
- ISO/IEC 22301 – Gestión de la continuidad del negocio.
- Marco de Ciberseguridad del NIST (CSF).
- Directiva NIS y NIS2 de la Unión Europea, como referentes de buenas prácticas en ciberseguridad y resiliencia digital.

4. Objetivos del Plan

4.1 Objetivo general

Actualizar y ejecutar el Plan Institucional de Seguridad y Privacidad de la Información para la vigencia 2026, garantizando la protección de los activos de información del Distrito, el

cumplimiento del régimen de protección de datos personales y la implementación de la Política de Seguridad Digital, en coherencia con el MSPI, la Política de Gobierno Digital y el MIPG.

4.2 Objetivos específicos

- Fortalecer la implementación del Modelo de Seguridad y Privacidad de la Información en la Alcaldía Distrital de Cartagena.
- Garantizar el adecuado tratamiento y protección de los datos personales bajo responsabilidad de la entidad.
- Gestionar de manera sistemática los riesgos de seguridad y privacidad de la información.
- Consolidar capacidades institucionales y cultura organizacional en seguridad digital.
- Asegurar la articulación del PISPI con los demás instrumentos de planeación institucional.

5. Alcance

El PISPI 2026 aplica a todos los procesos, dependencias, sistemas de información, infraestructuras tecnológicas, servidores públicos, contratistas, terceros y proveedores que gestionen, accedan o traten información institucional de la Alcaldía Distrital de Cartagena de Indias, independientemente del medio o formato.

6. Diagnóstico

Con base en los ejercicios de seguimiento del PISPI 2025, los reportes institucionales y los referentes de control aplicables, se evidencian los siguientes aspectos:

- Avances en la adopción progresiva del MSPI y en la formalización del proceso de seguridad y privacidad de la información.
- Necesidad de fortalecer el liderazgo institucional y la apropiación transversal de la seguridad digital en todas las dependencias.
- Riesgos asociados al tratamiento de datos personales, la gestión de terceros, la continuidad de los servicios y la atención de incidentes de seguridad digital.
- Brechas en cultura organizacional, sensibilización y capacitación, que requieren acciones sostenidas y articuladas al PIC.

Este diagnóstico orienta la priorización de acciones del PISPI 2026, sin perjuicio del detalle operativo desarrollado en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PITRSPI.

7. Componentes del PISPI 2026

El PISPI 2026 se estructura a partir de componentes que permiten organizar, articular y dar continuidad a la gestión institucional de la seguridad y privacidad de la información y la seguridad digital, en coherencia con la Política de Gobierno Digital, la Política de Seguridad Digital, el Modelo Integrado de Planeación y Gestión – MIPG y el Modelo de Seguridad y Privacidad de la Información – MSPI actualizado.

Estos componentes establecen el marco institucional de referencia para la implementación, seguimiento y mejora continua de las acciones en materia de seguridad digital, cuya ejecución

operativa se desarrolla a través de los planes, programas e instrumentos específicos definidos por la entidad para la vigencia 2026.

7.1 Gobierno, liderazgo y responsabilidades en seguridad y privacidad de la información.

Este componente orienta el esquema de gobierno institucional de la seguridad y privacidad de la información, mediante:

- El ejercicio del rol del Comité Institucional de Gestión y Desempeño, como órgano de orientación, seguimiento y toma de decisiones en materia de seguridad y privacidad de la información.
- La coordinación del proceso de Seguridad y Privacidad de la Información bajo la responsabilidad de la Oficina Asesora de Informática, conforme a lo establecido en el MSPI y en la estructura organizacional de la entidad.
- La articulación del PISPI con el MIPG, la Política de Gobierno Digital, la Política de Seguridad Digital y las demás políticas institucionales aplicables.

7.2 Gestión de la seguridad de la información y la seguridad digital.

Este componente establece el marco institucional para la gestión de la seguridad de la información y la seguridad digital en la entidad, a través de:

- La continuidad en la implementación y mejora del Sistema de Gestión de Seguridad de la Información – SGSI, conforme a los lineamientos del MSPI.
- La aplicación, actualización y seguimiento de políticas, lineamientos, procedimientos y controles de seguridad de la información.
- La gestión de incidentes de seguridad digital, de acuerdo con los lineamientos institucionales y la normativa vigente.

7.3 Protección de datos personales.

Este componente articula la seguridad y privacidad de la información con el régimen de protección de datos personales, considerando la implementación progresiva del Programa Integral de Gestión de Datos Personales, mediante:

- La articulación del PISPI con el Programa Integral de Gestión de Datos Personales como instrumento específico para el cumplimiento del régimen de protección de datos personales.
- El cumplimiento de las obligaciones legales y reglamentarias en materia de protección de datos personales y de los lineamientos impartidos por la Superintendencia de Industria y Comercio.
- El fortalecimiento progresivo de la gestión de los derechos de los titulares y del control sobre los terceros que tratan datos personales por cuenta de la entidad.

7.4 Gestión de riesgos de seguridad y privacidad de la información.

Este componente orienta la gestión institucional de los riesgos de seguridad y privacidad de la información, en articulación con los instrumentos institucionales de gestión del riesgo, a través de:

- La articulación directa con el Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PITRSPI 2026.

- El tratamiento de los riesgos priorizados conforme al MSPI y a los lineamientos de la Política de Gobierno Digital.
- El seguimiento a la eficacia de los controles implementados.

7.5 Cultura, apropiación y desarrollo de capacidades en seguridad digital.

Este componente orienta el fortalecimiento de la cultura organizacional en seguridad y privacidad de la información, mediante:

- La articulación del PISPI con el Plan de cambio, cultura, apropiación, capacitación y sensibilización en Seguridad y Privacidad de la Información y Seguridad Digital, como instrumento específico.
- La coordinación con el Plan Institucional de Capacitación – PIC o, en su defecto, la ejecución de acciones específicas para la vigencia 2026.
- La integración progresiva del enfoque de seguridad digital en los procesos de talento humano y las estrategias de comunicación interna.

7.6 Continuidad y resiliencia digital

Este componente agrupa las acciones orientadas al fortalecimiento progresivo de la continuidad y resiliencia digital institucional, a través de:

- La articulación con los planes y procedimientos institucionales de continuidad del negocio y recuperación ante desastres.
- La alineación con los procesos críticos y los servicios digitales priorizados del Distrito.
- La integración con la gestión de incidentes de alto impacto.

8. Plan de acción

ACTIVIDADES	ENTREGABLES	NOMBRE DEL INDICADOR	FORMULA DEL INDICADOR	META	RESPONSABLES
Socializar el esquema de gobierno y responsabilidades del PISPI a las dependencias	Actas y material de socialización	Dependencias socializadas	(Dependencias socializadas / Total de dependencias) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Asignar, mediante acto administrativo, al comité institucional de gestión y desempeño las funciones relacionadas con la seguridad y privacidad de la información, asegurando la adopción, implementación y mejora continua del MSPI.	Acto administrativo con las funciones de seguridad y privacidad de la información.	Formalización de funciones de seguridad y privacidad de la información en el Comité Institucional de Gestión y Desempeño	(Acto administrativo expedido y vigente /Acto administrativo programado) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Articular roles y responsabilidades con las áreas de la entidad para la adopción del MSPI	Roles y responsabilidades en seguridad de la información de	Articulación de roles y responsabilidades en seguridad de la información	(Áreas que aplican los roles definidos/Árras con roles	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información -

	las diferentes áreas o procesos de la entidad.		asignados) x 100		Todas las dependencias del distrito
Realizar seguimiento a la aplicación de políticas, lineamientos y controles de seguridad de la información	Informes de seguimiento	Cumplimiento de políticas	(Procesos evaluados / Procesos definidos) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Ejecutar el Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PITRSPI 2026	Informes de avance del PITRSPI	Avance del PITRSPI	(Actividades ejecutadas / Actividades programadas) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Gestionar los Riesgos de Seguridad de la Información	Plan de tratamiento de riesgos de seguridad y privacidad de la infomración	Avance en la formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	(Riesgos con tratamiento definido/Total de riesgos identificados) x 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Gestionar los incidentes de seguridad digital conforme a los lineamientos institucionales	Registro y reportes de incidentes	Incidentes gestionados	(Incidentes gestionados / Incidentes reportados) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Articular el PISPI con la implementación progresiva del Programa Integral de Gestión de Datos Personales	Documento de articulación PISPI–PGDP	Articulación formalizada	(Instrumentos articulados / Instrumentos definidos) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información/Oficina Asesora Juridica - Todas las dependencias del distrito
Fortalecer la gestión de los derechos de los titulares de datos personales	Procedimientos y registros de atención	Solicitudes atendidas	(Solicitudes atendidas / Solicitudes recibidas) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Realizar seguimiento al tratamiento de datos personales por parte de terceros	Informes de verificación	Contratos verificados	(Contratos verificados / Contratos identificados) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Ejecutar el Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PITRSPI 2026	Informes de avance del PITRSPI	Avance del PITRSPI	(Actividades ejecutadas / Actividades programadas) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Implementar el Plan de cambio, cultura, apropiación, capacitación y sensibilización en	Material pedagógico y reportes de ejecución	Avance del plan de cultura	(Actividades ejecutadas / Actividades	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - -

Seguridad y Privacidad de la Información y Seguridad Digital			programadas) × 100		Talento Humano/Escuela de gobierno/Oficina de comunicaciónes y prensa -Todas las dependencias del distrito
Articular la seguridad digital con los planes institucionales de continuidad del negocio y recuperación ante desastres	Documento de articulación	Articulación lograda	(Planes articulados / Planes identificados) × 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Realizar auditorias internas del SGSI	Informe de auditoria con hallazgos y recomendaciones	Porcentaje de auditorías internas realizadas.	(Auditorías realizadas / Total de auditorías programadas) x 100	100%	Oficina Asesora de Informática/proceso seguridad y privacidad de la información/Oficina Asesora de Control interno

9. Roles y Responsabilidades

- **Comité Institucional de Gestión y Desempeño:** Direcciona y realiza seguimiento estratégico al PISPI.
- **Oficina Asesora de Informática:** Lidera la implementación del PISPI, MSPI y Seguridad Digital.
- **Secretaría General:** Articula la seguridad de la información con la gestión administrativa y contractual.
- **Oficina Jurídica:** Garantiza el cumplimiento del régimen de protección de datos personales y la gestión contractual asociada.
- **Oficina de Control Interno:**
- **Talento Humano**: Integra la seguridad digital en los procesos de capacitación y gestión del talento.
- **Todas las dependencias:** Implementan y cumplen los lineamientos del PISPI en sus procesos.
- **Responsables de proceso y líderes de dependencia:** Implementan y aseguran el cumplimiento de los lineamientos del PISPI en su ámbito de competencia.
- **Servidores públicos, contratistas y terceros:** Cumplen las políticas y reportan incidentes de seguridad y privacidad.

10. 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. Auditorías y Monitoreo

Se llevarán a cabo auditorías para verificar el cumplimiento del plan. Los resultados serán utilizados para mejorar las políticas y procedimientos existentes**.**

12. Revisión y Mejora Continua

El PISPI será revisado trimestralmente para garantizar su alineación con los objetivos institucionales, el marco normativo y las necesidades operativas. Se incorporarán los lineamientos más recientes del MinTIC en cada actualización. Los resultados serán comunicados a las partes interesadas, fomentando una cultura de seguridad y mejora continua.

13. Anexos –

Se anexa plan en formato Excel.

14. 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