Alcaldía Mayor de
Cartagena de Indias

Plan de seguridad y privacidad de la información

Alcaldía Distrital de Cartagena de Indias

2025

1. Introducción

El Plan Institucional de Seguridad y Privacidad de la Información (PISPI) de la Alcaldía Distrital de Cartagena establece las directrices, controles y medidas para proteger los activos de información, garantizando su confidencialidad, integridad, disponibilidad y privacidad, en cumplimiento de la normativa vigente, incluyendo la Ley 1581 de 2012, el Decreto 1377 de 2013, y demás regulaciones aplicables.

Este plan promueve el cumplimiento del Decreto 612 de 2018 y del Decreto 767 de 2022, que actualiza la política de Gobierno Digital. Alineado con el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, adopta estándares internacionales como la norma ISO/IEC 27001 para la gestión segura de la información y la mitigación de ciberamenazas.

La política de Gobierno Digital del Distrito fomenta el uso estratégico de tecnologías de la información para consolidar un Estado y una ciudadanía competitivos e innovadores, generando valor público en un entorno de confianza digital. Dentro de sus componentes, el habilitador de seguridad y privacidad de la información es fundamental para asegurar la implementación de lineamientos que protejan todos los procesos, servicios, sistemas y activos de información de la entidad, sirviendo de base para el desarrollo del MSPI.

La Resolución 0500 de 2021, expedida por el MinTIC, establece lineamientos para la implementación del MSPI, la gestión de riesgos de seguridad de la información, y el manejo de incidentes de seguridad digital. Esta normativa exige que las entidades adopten medidas técnicas, administrativas y de talento humano para integrar la seguridad digital en sus planes, mitigando riesgos y garantizando la protección de datos personales.

El artículo 5 de la resolución destaca la necesidad de una estrategia de seguridad digital que unifique políticas, procedimientos, guías y estándares para la gestión de la información, vinculándola al Plan de Acción institucional conforme al Decreto 1083 de 2015.

En este contexto, el presente Plan de Seguridad y Privacidad de la Información se enfoca en proteger los activos tecnológicos de la Alcaldía frente a ciberamenazas, fortaleciendo la confianza ciudadana y la eficiencia en la gestión pública.

2. Glosario

- **Activo:** En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Política del SGSI:** Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.
- **Política:** Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.
- **Privacidad de datos:** La privacidad de datos, también llamada protección de datos es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros
- **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).
- **Rol:** Papel, función que alguien o algo desempeña.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

3. Contexto estratégico de la entidad

3.1. Misión

Cartagena de Indias es un Distrito que impulsa el desarrollo social y económico, la preservación y promoción del patrimonio histórico, turístico y cultural, el comercio, la industria portuaria y marítima, la competitividad, la equidad social, la sostenibilidad ambiental y fiscal, mediante el ordenamiento del territorio y su relación con el agua, orientado a la adaptación al cambio climático, y apoyados en un modelo de gestión eficiente, transparente, y participativo; para garantizar el bienestar y la calidad de vida de la ciudadanía en general, con especial énfasis en sus pueblos y comunidades étnicas y los grupos de especial protección.

3.2. Visión

En el año 2027, el Distrito de Cartagena se destacará como un modelo global de ciudad productiva, inclusiva y sostenible. Será reconocida por la mejora continua de la calidad de vida para todos sus habitantes, especialmente en los territorios y entre los grupos poblacionales más vulnerables. Cartagena será una ciudad donde la protección de la vida, el disfrute efectivo de los derechos, y el desarrollo económico equitativo, que cierra brechas y genera empleo digno, serán

prioridades. La administración distrital fortalecerá las instituciones, impulsará procesos participativos, mejorará infraestructuras claves, protegerá el medio ambiente, y ordenará el desarrollo urbano alrededor del agua, garantizando el derecho a la ciudad para las generaciones presentes y futuras. Cartagena brillará como una Ciudad de Derechos.

3.3. Objetivos estratégicos institucionales

Los objetivos estratégicos están orientados a dar cumplimiento de la visión en concordancia con la misión del Distrito de Cartagena de Indias, los cuales se detallan a continuación:

1. Garantizar la seguridad humana en sus diferentes aspectos en el Distrito de Cartagena de Indias, mediante la disminución de las tasas de homicidios, mortalidad materna e infantil, violencia de género, pobreza extrema e inseguridad alimentaria a través de la implementación de estrategias focalizadas y programas de apoyo integral para proteger la vida de todos los ciudadanos, durante el período de gobierno 2024-2027.
2. Dignificar la vida de los habitantes del Distrito de Cartagena de Indias, reducir la pobreza multidimensional, el déficit habitacional, y ampliar la cobertura del saneamiento básico, a través de la implementación de estrategias integrales focalizadas en el fortalecimiento de la infraestructura educativa, en el fomento de las condiciones habitacionales adecuada y en el acceso de calidad de los servicios públicos, garantizando una vida digna para toda la población, durante el período de gobierno 2024-2027.
3. Promover el desarrollo económico equitativo y sostenible en el Distrito de Cartagena de Indias, para lograr al reducción de la brecha laboral de género, la disminución de las tasas de desempleo juvenil, al reducción de la informalidad laboral, mediante la formulación y ejecución de políticas y estrategias, el fomento al emprendimiento, el fortalecimiento de la economía popular, la diversificación económica y la creación de empleos de calidad en la ciudad, mejorando las condiciones económicas de la población, durante el período de gobierno 2024- 2027.
4. Consolidar la conectividad y sostenibilidad del Distrito de Cartagena de Indias a través de la protección de los cuerpos de agua, el aumento del número de áreas protegidas, el incremento de la tasa de espacio público efectivo per cápita y la mejora de la infraestructura vial para apoyar el desarrollo urbano sostenible y promover una mayor conectividad, accesibilidad y proximidad entre los ciudadanos, durante el período 2024-2027.
5. Fortalecer la relación del Estado con la ciudadanía cartagenera, incrementando los niveles de recaudo tributario y mejorando el índice de desempeño institucional, mediante la innovación pública, optimización y simplificación de procesos, la modernización administrativa y la eficiente participación ciudadana, garantizando una gobernanza eficiente, transparente y orientada al servicio de la ciudadanía, durante el período de gobierno 2024-2027.

3.4. Valores institucionales

La Administración Distrital en su acción promoverá el fomento de todos los valores, en especial los de: Honestidad, Respeto, Compromiso, Diligencia, Justicia y Solidaridad.

- Honestidad: Se compromete a hablar con la verdad y actuar con rectitud y transparencia en el cumplimiento de sus deberes, cumpliendo siempre con los preceptos de la ley.

- Respeto: Aceptar, valorar, reconocer y atender al otro de forma digna, promoviendo una interacción social armoniosa.
- Compromiso: Adoptar como propios los objetivos estratégicos y la misión de la entidad. Se compromete con el cumplimiento de los objetivos misionales, dedicando todas las energías y capacidades como servidores públicos para contribuir al mejoramiento del bienestar de la comunidad.
- Diligencia: Realizar las obligaciones y responsabilidades con interés, entusiasmo, prontitud y esfuerzo constante, asegurando al eficiencia y eficacia en el trabajo.
- Justicia: Actuar con total imparcialidad, sin juicios de valor anticipados, prejuicios o desconfianza, garantizando siempre igualdad, rectitud, equidad y unidad.
- Solidaridad: Apoyarse y coordinar con otros actores sociales, públicos y privados, en la implementación de acciones, planes y programas que contribuyan a satisfacer las necesidades fundamentales de la población más vulnerable.

4. Marco Normativo

Este plan se desarrolla conforme a las siguientes normativas y estándares aplicables:

- Ley 1273 de 2009: Delitos Informáticos.
- Ley 1581 de 2012: Protección de Datos Personales.
- Decreto 1377 de 2013: Reglamentación parcial de la Ley 1581 de 2012.
- Ley 1712 de 2014: Transparencia y Acceso a la Información Pública.
- Decreto 1078 de 2015: Decreto Único Reglamentario del Sector TIC.
- Decreto 1074 de 2015: Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
- Decreto 1083 de 2015 Sector de Función Pública
- Decreto 612 de 2018 Integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- ISO 22301:2019: Gestión de Continuidad del Negocio.
- ISO/IEC 27001:2022: Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27701: Extensión para la gestión de privacidad de la información.
- Resolución número 00500 de marzo 10 de 2021 lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
- Decreto 767 de 2022 Lineamientos generales de la Política de Gobierno Digital
- Modelo Integrado de Planeación y Gestión (MIPG).
- Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.
- Lineamientos y políticas del Gobierno Nacional para entidades públicas.

5. Objetivos del Plan

- Proteger los activos de información de la Alcaldía, garantizando su confidencialidad, integridad, disponibilidad y privacidad frente a amenazas internas y externas.

- Cumplir con la normativa de seguridad de la información y protección de datos personales, asegurando el adecuado tratamiento de los datos y la protección de los derechos de sus titulares.
- Fomentar una cultura organizacional de seguridad y privacidad, promoviendo su integración en la gestión pública y fortaleciendo la confianza ciudadana.
- Prevenir, detectar y responder a incidentes de seguridad, implementando controles efectivos para gestionar riesgos asociados a la información, las tecnologías y la ciberseguridad.
- Garantizar la continuidad de los servicios y procesos críticos, asegurando una operación segura y eficiente.

6. Alcance

El Plan de Seguridad y Privacidad de la Información de la Alcaldía Distrital de Cartagena aplica a todos los procesos, sistemas, recursos tecnológicos, empleados, contratistas, terceros y aliados estratégicos que acceden, manejan o gestionan información relacionada con la entidad.

7. Diagnóstico Actual

7.1 Seguridad de la Información (SGSI):

- Nivel de madurez: 45% (Efectivo).
- Requiere fortalecimiento en monitoreo, medición y formalización de controles.

7.2 Continuidad del Negocio (SCN):

- Nivel de madurez: 37% (Repetible).
- Falta estandarización y actualización de la documentación clave (BIA, RIA, BCP)

7.3 Protección de Datos Personales (PIGDP):

- Nivel de madurez: 50% (Efectivo).
- Requiere mejora en monitoreo, formación y gestión de terceros

8. Políticas de Seguridad y Privacidad de la Información

Las siguientes políticas buscan unificar y fortalecer los estándares de seguridad y privacidad de la información, asegurando el cumplimiento de las normativas vigentes y promoviendo la confianza ciudadana.

- **Uso Aceptable de Activos de Información:** Los usuarios deben utilizar los recursos de información de manera responsable, alineados con los objetivos institucionales y la normativa vigente.
- **Confidencialidad:** El acceso a la información será limitado al personal autorizado según roles definidos, empleando mecanismos robustos de autenticación.
- **Integridad de la Información:** Se aplicarán controles para prevenir alteraciones no autorizadas y garantizar la precisión de los datos.
- **Disponibilidad:** Se implementarán medidas para asegurar el acceso continuo a la información crítica, incluso durante interrupciones.

- **Gestión de Datos Personales:** El tratamiento de datos personales cumplirá con la Ley 1581 de 2012 y regulaciones complementarias, garantizando los principios de legalidad, seguridad, confidencialidad y finalidad.
- **Cultura de Seguridad y Privacidad:** Se fomentará una cultura organizacional orientada a la protección de la información, integrándola en los procesos de gestión.
- **Respuesta a Incidentes de Seguridad:** Se establecerán procedimientos para la detección, gestión, notificación y mitigación de incidentes, designando un equipo especializado.
- **Continuidad del Negocio:** Se desarrollarán planes para asegurar la operación de servicios críticos mediante estrategias de recuperación basadas en análisis de riesgos e impacto.
- **Seguridad Física y Lógica:** Los activos físicos y tecnológicos serán protegidos mediante controles de acceso, monitoreo y copias de seguridad.
- **Protección de Derechos de los Titulares:** Se respetarán los derechos de los titulares de datos personales, garantizando su consentimiento informado y el manejo seguro de su información.

9. Objetivos Estratégicos PISPI

Estos objetivos estratégicos alinean la seguridad de la información con las normativas vigentes, la protección de datos personales y las mejores prácticas internacionales, promoviendo una gestión eficiente, resiliente y centrada en la confianza ciudadana.

9.1 Fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI)

- Implementar y monitorear controles de seguridad según el MSPI (NTC-ISO/IEC 27001)
- Mejorar el nivel de madurez del SGSI.

9.2 Garantizar la Continuidad del Negocio

- Actualizar y validar periódicamente el Plan de Continuidad del Negocio (BCP) mediante simulacros y pruebas controladas.
- Desarrollar y validar un Plan de Recuperación ante Desastres (DRP) para asegurar la reanudación de servicios críticos tras interrupciones.
- Elevar el nivel de madurez del plan a "Efectivo" (60%) en un plazo de dos años.

9.3 Optimizar la Protección de Datos Personales

- Crear y mantener un inventario de las bases de datos personales gestionadas por la entidad.
- Diseñar e implementar programas de formación y sensibilización sobre la protección de datos, dirigidos a todos los niveles de la entidad.
- Aplicar estrategias alineadas con los lineamientos de la Superintendencia de Industria y Comercio (SIC) y del -Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

9.4 Fomentar una Cultura Organizacional de Seguridad y Privacidad de la información

- Implementar programas de capacitación continua para reforzar la conciencia sobre la seguridad de la información y la protección de datos personales.
- Realizar campañas de comunicación interna y simulaciones de incidentes para fomentar buenas prácticas de gestión de riesgos.

9.5 Gestionar Riesgos de Seguridad de la Información

- Identificar, evaluar y clasificar los riesgos mediante matrices de vulnerabilidades y análisis de impacto.
- Diseñar, implementar y monitorear controles de mitigación adecuados.
- Revisar periódicamente los controles para mantener su efectividad frente a cambios tecnológicos y nuevas amenazas.

9.6 Fortalecer la Gestión de Incidentes de Seguridad

- Establecer un protocolo de atención para la detección, contención, análisis, resolución y registro de incidentes.
- Incorporar las lecciones aprendidas en procesos de mejora continua para minimizar la recurrencia de incidentes.

10. Estrategias y Acciones Prioritarias

10.1 Fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI)

Estrategia: Desarrollar y mantener un sistema de gestión eficiente y alineado con la NTC-ISO/IEC 27001:2022.

Acciones Prioritarias:

- Definir, divulgar y actualizar políticas de seguridad de la información.
- Gestionar riesgos mediante el uso de herramientas modernas y matrices actualizadas de evaluación de riesgos.
- Monitorear y reportar indicadores clave de cumplimiento para asegurar la mejora continua.

10.2 Protección de Datos Personales

Estrategia: Garantizar el adecuado tratamiento de datos personales conforme a la Ley 1581 de 2012 y lineamientos de la SIC y el MinTIC.

Acciones Prioritarias:

- Implementar mecanismos de recolección y gestión de consentimientos informados.
- Realizar análisis de impacto en privacidad (DPIA) para identificar riesgos asociados al tratamiento de datos personales.
- Formalizar acuerdos de confidencialidad con terceros que manejen información sensible.
- Diseñar e implementar programas de sensibilización y capacitación continua para empleados y contratistas.

10.3 Garantizar la Continuidad del Negocio y la Recuperación ante Desastres

Estrategia: Asegurar la resiliencia operativa ante interrupciones mediante la preparación y pruebas regulares.

Acciones Prioritarias:

- Actualizar el análisis de impacto al negocio (BIA) para identificar procesos críticos.
- Diseñar estrategias de recuperación alineadas con los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO).
- Ejecutar simulacros periódicos y revisiones del Plan de Continuidad del Negocio (BCP) y Plan de Recuperación ante Desastres (DRP).

10.4 Gestión Integral de Riesgos de Seguridad de la Información

Estrategia: Identificar, evaluar y mitigar riesgos para proteger los activos de información de la entidad (Plan de tratamiento de riesgos de seguridad y privacidad de la información).

Acciones Prioritarias:

- Utilizar matrices de riesgo para la identificación y evaluación de vulnerabilidades.
- Determinar la probabilidad e impacto de los riesgos y diseñar controles de mitigación adecuados.
- Implementar un proceso de revisión periódica para actualizar controles conforme a nuevas amenazas.

10.5 Programas de Sensibilización y Capacitación

Estrategia: Crear una cultura organizacional de seguridad y protección de datos.

Acciones Prioritarias:

- Promover la conciencia sobre seguridad de la información mediante campañas internas de comunicación.
- Realizar capacitaciones sobre seguridad y privacidad de la infomración.
- Incluir programas específicos de buenas prácticas en gestión de riesgos y manejo de datos personales.

10.6 Gestión de Incidentes de Seguridad de la Información

Estrategia: Responder eficazmente a incidentes para minimizar su impacto y prevenir su recurrencia.

Acciones Prioritarias:

- Establecer un protocolo de gestión de incidentes que incluya detección, registro, contención, análisis y resolución.
- Asignar un equipo de respuesta y documentar las lecciones aprendidas para mejorar los procesos de seguridad.

11. Plan de acción

ACTIVIDADES	FECHA INICIO	FECHA FINAL	ENTREGABLES	RESPONSABLES
Diseñar e implementar el sistema de gestión de seguridad y privacidad de la información (SGSI) - Fase Diagnostico y Planeación - Revisión y actualización de la documentación	1/03/2025	31/12/2025	Documentación revisada y actualizada del sistema de gestión de seguridad y privacidad de la información. Registro de implementación del SGSI	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Diseñar e implementar el programa integral de protección de datos personales	1/03/2025	31/12/2025	políticas de tratamiento de datos personales Registros de consentimientos informados Acuerdos de confidencialidad Informe de cumplimiento de la normativa vigente Reporte de capacitaciones	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Diseñar e Implementar el Sistema de Continuidad del Negocio	1/03/2025	31/12/2025	Plan de Continuidad del Negocio (BCP). Plan de Recuperación de Desastres (DRP) Reportes de simulacros y pruebas.	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Gestionar los Riesgos de Seguridad de la Información	1/03/2025	31/12/2025	Plan de tratamiento de riesgos de seguridad y privacidad de la información	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Diseñar e Implementar Programa de Sensibilización y	1/03/2025	31/12/2025	Materiales de capacitación y sensibilización	Oficina Asesora de Informática/proceso seguridad y

Capacitación en Seguridad y Privacidad de la Información			Reporte de capacitaciones realizadas	privacidad de la información - Talento Humano/Escuela de gobierno/Oficina de comunicaciones y prensa
Gestionar Incidentes de Seguridad de la Información	1/03/2025	31/12/2025	Protocolo de gestión de incidentes. Registro de incidentes Informe de lecciones aprendidas.	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
Realizar auditorías internas del SGSI	1/03/2025	21/12/2025	Informe de auditoría con hallazgos y recomendaciones	Oficina Asesora de Informática/proceso seguridad y privacidad de la información – Oficina Asesora de Control Interno

Actividades	**Fecha inicio**	**Fecha final**	**Entregables**	**Responsables**
Plan de revisión y seguimiento, a la implementación del MSPI.	01-03-25	31-12-25	Informes de revisión y seguimiento	Oficina Asesora de informática
Nombres de los indicadores		**Índices**	**Metas**	
Seguimiento a la implementación MSPI		%	100%	
Descripción del recurso requerido		**Tipo**	**Observaciones**	
Humanos, tecnológicos, financieros			**El desarrollo de las actividades estará sujeto a la disponibilidad de los recursos (humanos, técnicos, tecnológicos, financieros) que faciliten su cumplimiento.**	

12. Roles y Responsabilidades

- **Responsable del Tratamiento de Datos:** Garantiza el cumplimiento de las leyes de protección de datos y de los lineamientos propios de la Alcaldía Distrital de Cartagena.
- **Oficial de Seguridad de la Información:** Supervisa la implementación del plan de seguridad en la institución.
- **Usuarios:** Cumplen con las políticas establecidas y reportan cualquier incidente de seguridad.

13. Presupuesto

Para el cumplimiento del Plan Institucional de Seguridad y Privacidad de la Información (PISPI) de la Alcaldía de Cartagena, se deben considerar los siguientes componentes presupuestales. Este presupuesto puede ajustarse según la priorización de actividades y la disponibilidad de recursos.

13.1 Recursos Humanos

- **Responsable del Tratamiento de Datos:** Salarios, formación especializada y certificaciones (ej., ISO 27001).
- **Oficial de Seguridad de la Información:** Salarios, formación especializada y certificaciones (ej., ISO 27001).
- **Equipo de respuesta a incidentes:** Asignación y formación.
- **Capacitaciones y sensibilizaciones:** Cursos para personal administrativo, técnicos, y contratistas.

13.2 Tecnología

- **Software:** Licencias de sistemas de gestión de seguridad (SGSI), monitoreo de riesgos, análisis de vulnerabilidades, Gestión de Identidades de usuarios IAM, Gestión de Gestión de servicios de tecnologías de la información (ITSM), la Gestión de operaciones de TI (ITOM), Gestión Seguridad EndPoint, Gestión de eventos de seguridad de la Información (SIEM) y para monitoreo de marca, dark y deep web.
- **Infraestructura:** Adquisición o actualización de servidores, redes seguras y almacenamiento de datos.
- **Herramientas de continuidad del negocio:** Soluciones para respaldo y recuperación (Backup y DRP).

13.3 Consultoría

- Servicios externos para diagnósticos, auditorías de SGSI, y creación de estrategias personalizadas para MSPI.

13.4 Auditorías y Certificaciones

- **Auditorías internas y externas:** Seguimiento y cumplimiento**.**
- **Certificaciones ISO:** Proceso de preparación y validación**.**

13.5 Comunicación y Cultura

- Diseño y difusión de campañas de sensibilización.
- Creación de manuales y guías para usuarios internos.

13.6 Planes de acción específicos

- **Protección de datos personales:** Desarrollo e implementación de políticas de tratamiento.
- **Gestión de incidentes:** Protocolos y simulacros regulares**.**

A continuación, se presenta una tabla presupuestaria estimada para el Plan Institucional de Seguridad y Privacidad de la Información (PISPI) de la Alcaldía de Cartagena.

Componente	Subcomponente	Cantidad Estimada	Costo Unitario	Costo Total
Recursos Humanos	Responsable del Tratamiento de Datos	1	$70,000.000	$70,000.000
	Oficial de Seguridad de la Información	1	$84,000.000	$84,000.000
	Equipo de respuesta a incidentes	1	$100,000.000	$100,000.000
	Capacitaciones internas	1	$32,000.000	$32,000.000
Tecnología	Infraestructura tecnológica	1	$350,000.000	$350,000.000
	Herramientas de continuidad del negocio	1	$200,000.000	$200,000.000
	Licencia plataforma Gestión de Identidades IAM	1	$250,000.000	$250,000.000
	Licenciamiento software para la Gestión de ITSM	1	$200,000.000	$200,000.000
	Licenciamiento para la Gestión de ITOM	1	$280,000.000	$280,000.000
	Licenciamiento para la Gestión Seguridad EndPoint.	1	$300,000.000	$300,000.000
	Licenciamiento para la Gestión de eventos de seguridad de la Información (SIEM)	1	$600,000.000	$600,000.000
	Licenciamiento para monitoreo de marca, dark y deep web.	1	$84,000.000	$84,000.000
Consultoría	Auditorías y diagnósticos externos	1	$90,000.000	$90,000.000
Auditorías y Certificaciones	Certificación ISO 27001	1	$30,000.000	$30,000.000
	Auditorías internas	1	$16,000.000	$16,000.000
Comunicación y Cultura	Campañas de sensibilización	1	$18,000.000	$18,000.000
	Diseño de manuales	1	$10,000.000	$10,000.000
Planes de Acción Específicos	Gestión de incidentes	1	$54,000.000	$54,000.000
	Protección de datos personales	1	$60,000.000	$60,000.000
	Simulacros y pruebas de continuidad	1	$72,000.000	$72,000.000
TOTAL ESTIMADO				$2.900.000.000

14. 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**.**

15. 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.

16. Anexos –

Se anexa plan en Excel

17. Aprobación

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

_____

Secretario General

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