Alcaldía Mayor de
Cartagena de Indias

Plan de seguridad y privacidad de la información

Alcaldía Distrital de Cartagena de Indias
2024

1. Introducción

Este documento se elabora con el objetivo de orientar a las dependencias del distrito de Cartagena para dar cumplimiento con lo solicitado en el Decreto 612 de 2018 y todas las consideraciones expuestas, dentro de las cuáles se encuentra el decreto 767 del 2022 mediante el cual se actualiza la política de gobierno digital, y se exige la elaboración por parte de cada entidad, de un Plan de Seguridad y Privacidad de la Información

De igual forma el distrito de Cartagena ha estructurado la política de Gobierno Digital la cual tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital. Según esta, de acuerdo a los elementos que la componen: gobernanza, innovación pública digital, habilitadores, líneas de acción e iniciativas dinamizadoras. En lo particular, indica que el habilitador de seguridad y privacidad de la información tiene como propósito que las entidades públicas implementen los lineamientos de seguridad y privacidad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos, por lo tanto es el soporte principal para la construcción del Modelo de seguridad y Privacidad de la información (MSPI).

Por otro lado, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y las Comunicaciones, que tiene como "*objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital*". La resolución en mención precisa la necesidad de que "*los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital*". Es precisamente a través del artículo 5 de la resolución 0500 que se precisa la necesidad de "*adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el plan de seguridad y privacidad de la información que se integra al Plan de Acción en los términos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro 2 del decreto 1083 de 2015*". En atención a lo anterior, se presenta el plan de seguridad y privacidad de la información enfocado en la seguridad informática frente a ciber amenazas de activos de tecnologías de información de la entidad.

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.
- **Contratistas:** Aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.
- **Control:** Políticas, procedimientos, prácticas y 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. Es una medida que modifica el riesgo.
- **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.
- **Guía:** Documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Norma:** Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **Parte interesada:** (Stakeholder) persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **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
- **Procedimiento:** Constituyen la descripción detallada de la manera como se implanta una política.
- **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).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

3. Contexto estratégico de la entidad

3.1. Misión

Construida colectivamente con igualdad para todos y todas, incluidos niñas, niños, adolescentes y jóvenes. La Cartagena que se propone es una ciudad para soñar, que potencie su riqueza geográfica, ecológica, cultural, histórica, turística y portuaria, y la proyecte hacia el futuro con un desarrollo urbanístico incluyente, que privilegia infraestructuras urbanas para fortalecer la vocación natural de la ciudad, que faciliten la movilidad con base en transporte colectivo multimodal y medios ambientalmente sostenibles como las ciclorrutas, las alamedas y las vías peatonales. Una ciudad con dotación de parques y espacios públicos reservados para el encuentro, el disfrute y la apropiación colectiva. Una ciudad en la que los ciudadanos conviven pacíficamente, están tranquilas y tranquilos, respetan las normas, protegen su medio ambiente, reconocen y respetan la diversidad, cumplen los acuerdos y autorregulan sus comportamientos para garantizar el pleno ejercicio de las libertades y los derechos de todas y todos.

3.2. Visión

Cartagena de Indias será reconocida, como una ciudad inteligente, competitiva e incluyente desde una perspectiva urbana, socioeconómica, ambiental, fiscal y gobierno; una ciudad bien comunicada, con infraestructura de calidad, una ciudad internacional, y con oportunidades para la gente, atractiva para visitantes e inversionistas, confiable segura y tranquila, en la cual se disfrute de una mejor calidad de vida. Donde las personas independientemente de sus características reciban las mismas oportunidades y puedan competir en las mismas condiciones

3.3. Valores institucionales

La Administración Distrital en su acción promoverá el fomento de todos los valores, en especial los de: Honradez, Respeto por la vida, Equidad e inclusión social, los cuales se sustentarán en tres pilares fundamentales a saber: la Transparencia, la Seguridad y la Convivencia Ciudadana.

Honradez. La buena fe edifica y construye confianza, necesaria para el empoderamiento ciudadano y la autodeterminación de desarrollo. La Administración Distrital promoverá la honradez como base del desarrollo integral, constituyéndose en un requerimiento para edificar el modelo de desarrollo según las necesidades y aspiraciones de los habitantes de la ciudad de Cartagena.

Respeto por la Vida. El requisito básico de la construcción de toda sociedad prospera y progresista es el respeto por la vida. El diseño de políticas públicas distritales estará orientado a promover el respeto por la vida, como elemento constructor de ciudadanía, Estado y Nación.

Equidad e Inclusión Social. La administración Distrital propiciará condiciones para lograr un modelo de desarrollo integral, estableciendo como objetivo fundamental del presente plan de desarrollo, promover la equidad en oportunidades para todos los grupos poblacionales, especialmente a los grupos más vulnerables.

4. Estructura general del plan institucional

4.1. Nombre del plan institucional

Plan de seguridad y privacidad de la información (PSPI)

4.2. Propósito del plan institucional

El plan de seguridad y privacidad de la Información (PSPI), que tiene por objetivo trazar y planificar la manera como la Alcaldía Distrital de Cartagena de Indias continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

4.3. Ámbito del plan institucional

El plan de seguridad y privacidad de la Información que se generará para lograr el 100% de la implementación del MSPI al interior de todos los procesos de la Alcaldía Distrital de Cartagena de Indias, los cuales deben ser divulgados, conocidos y cumplidos por todos los colaboradores de la entidad, contratistas y terceros que tengan acceso a información de la Alcaldía Distrital de Cartagena de Indias.

4.4. Desarrollo del plan institucional

4.4.1. Identificación de la situación actual

En los ítems de control de la política de seguridad y privacidad de la información establecido como plan de acción, se puede apreciar que se fue generando un incremento en su implementación; terminando el año con un cumplimiento del 91% de las acciones planteadas en la política de seguridad.

Trimestre	% Cumplimiento
I	13
II	23
III	55
IV	91

En cuanto al desarrollo y aplicación del plan de seguridad y privacidad de la información este cerro el 2023 con un porcentaje de avance de un 94% debido a que no se obtuvo el 100% en 4 de las actividades las cuales se finalizarán en el 2024.

De acuerdo con la medición del FURAG que contiene la gestión desarrollada desde el año 2018, le resultado de la política de seguridad digital 2022 fue de 75.2

Con respecto al habilitador de seguridad y privacidad de la información se ha buscado desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en los procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información.

El Distrito cuenta con la política de seguridad digital la cual ha sido socializada con el personal de planta y contratistas a través de un ciclo de capacitaciones tendientes a fomentar la cultura de la seguridad informática y a conocer los lineamientos de la política.

Entre los productos con los que cuenta la política de gobierno digital de la Alcaldía de Cartagena se tienen:

Política de Seguridad y Privacidad de la Información
Manual con las políticas de seguridad y privacidad de la información
Plan de seguridad y privacidad de la información
Reporte de autodiagnóstico de seguridad y privacidad de la información (actividad periódica que debe realizarse cada año)
Se ha adoptado e implementado el modelo de Seguridad y Privacidad de la Información insumo para la elaboración del Plan de Seguridad y Privacidad de la Información,
Se avanza en la obtención del inventario de activos de información
Se avanza en el Plan de tratamiento de riesgos de seguridad informática
Plan de comunicación, sensibilización y capacitación para la entidad en seguridad digital
Protocolo estandarizado para la anonimización y protección de datos personales
Se avanza en la implementación de controles de seguridad y privacidad de la información

En cumplimiento a lo estipulado en el Modelo Integrado de Planeación y Gestión MIPG, como marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, incorpora la política de seguridad digital en el marco de la tercera dimensión: gestión con valores para resultados. El Comité de Gestión y Desempeño Institucional, con el objeto de articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política de Gobierno Digital designó como responsable de la Seguridad Digital y de la Seguridad de la Información en la entidad, a la Oficina Asesora de Informática. La implementación de la política por parte del Distrito de Cartagena se hará a través de la adopción e implementación del Modelo de Seguridad y Privacidad de la información - MSPI.

La Oficina Asesora de Informática ha establecido el formato para la programación de planes institucionales con código PTDDE02-F001, en el cual se proponen realizar 5 actividades enmarcadas en el modelo de seguridad y privacidad de la información para la implementación de la estrategia de seguridad digital en la Alcaldía de Cartagena.
al interior de las entidades

4.4.2. Priorización de aspectos críticos

Al implementar estas acciones la Alcaldía distrital de Cartagena de indias deberá obtener los siguientes resultados

Actividad	Instructivos o herramientas a utilizar	Resultados esperados
Hacer el autodiagnóstico haciendo uso del "instrumento de evaluación MSPI" para identificar el estado de la seguridad y privacidad de la información en la Alcaldía de Cartagena	Instrumento de evaluación MSPI	Documento de autodiagnóstico, identificando el nivel de madurez de implementación del MSPI en la Alcaldía de Cartagena, y sus acciones de mejora
Definir el alcance del MSPI, determinar los procesos y recursos tecnológicos en los que se realizará la implementación en la Alcaldía de Cartagena	Modelo de seguridad y privacidad de la información - MSPI	Documento de alcance del MSPI
Definir y aplicar un proceso para la identificación y clasificación de la información para identificar, clasificar y actualizar el inventario de los activos de información de la Alcaldía de Cartagena de acuerdo con el alcance definido.	Guía 5 Gestión De Activos	Documento metodológico para la identificación, clasificación y valoración de los activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por el comité de gestión y desempeño institucional. Matriz con la identificación, valoración y clasificación de activos de información.
Definir y aplicar un proceso para la valoración de los riesgos de la seguridad y privacidad de la información en la Alaciada de Cartagena	Guía 7 Gestión de Riesgos. Guía 8 Controles de Seguridad	Documento metodológico para la gestión de riesgos. Documento con el análisis y evaluación de los riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por el comité de gestión y desempeño institucional
Elaborar el plan de comunicación, capacitación, sensibilización y concientización con respecto a la seguridad y privacidad de la información a los funcionarios y contratistas de la Alcaldía de Cartagena	Guía 14 Plan de comunicación, sensibilización y capacitación	Documento con el plan de comunicación, capacitación, sensibilización y concientización para la Alcaldía de Cartagena
Hacer el autodiagnóstico haciendo uso del "instrumento	Instrumento de evaluación MSPI	Documento de autodiagnóstico, identificando el nivel de madurez

de evaluación MSPI" para identificar el estado de la seguridad y privacidad de la información en la Alcaldía de Cartagena a noviembre de 2024		de implementación del MSPI en la Alcaldía de Cartagena, y sus acciones de mejora

5. Formulación del plan

5.1. Corto plazo

Actividades	Fecha inicio	Fecha final	Entregables	Responsables
1. Hacer el autodiagnóstico haciendo uso del "instrumento de evaluación MSPI" para identificar el estado de la seguridad y privacidad de la información en la Alcaldía de Cartagena	1/02/2024	1/04/2024	Documento del diagnóstico	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
2. Definir el alcance del MSPI, determinar los procesos y recursos tecnológicos en los que se realizará la implementación en la Alcaldía de Cartagena	1/04/2024	30/04/2024	Documento de Alcance	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
3. Definir y aplicar un proceso para la identificación y clasificación de la información para identificar, clasificar y actualizar el inventario de los activos de información de la Alcaldía de Cartagena de acuerdo al alcance definido.	1/05/2024	30/08/2024	Procedimiento del inventario y clasificación de la información Documento metodológico del inventario y clasificación de la información	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
4. Definir y aplicar un proceso para la valoración de los riesgos de la seguridad y privacidad de la información en la Alaciada de Cartagena	1/07/2024	31/10/2024	Procedimiento y metodología para la gestión del riesgo institucional	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
5. Elaborar el plan de comunicación, capacitación, sensibilización y concientización con respecto a la seguridad y privacidad de la información a los funcionarios y contratistas de la Alcaldía de Cartagena	1/02/2024	30/11/2024	Documento con el plan de comunicación, capacitación, sensibilización y concientización	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Talento Humano/Escuela de gobierno/Oficina de comunicaciones y prensa

	1/02/2024	30/11/2024	Listado de asistencia a capacitación para la entidad. Diapositivas, grabaciones	
6. Hacer el autodiagnóstico haciendo uso del "instrumento de evaluación MSPI" para identificar el estado de la seguridad y privacidad de la información en la Alcaldía de Cartagena a noviembre de 2024	1/12/2024	31/12/2024	Documento del diagnóstico	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito

5.2. Mediano plazo

Actividades	**Fecha inicio**	**Fecha final**	**Entregables**	**Responsables**
Plan de revisión y seguimiento, a la implementación del MSPI.	01-02-24	31-12-24	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			El desarrollo de las actividades estará sujeto a la disponibilidad de los recursos (humanos, técnicos, tecnológicos, financieros) que faciliten su cumplimiento.	

6. Anexos –

Se anexa plan en Excel para los seguimientos correspondientes

7. 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

8. Documentos de referencia:

NTC / ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.

NTC/ISO 27002:2013 Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

Modelo de Seguridad y Privacidad de la Información Documento Maestro V 4.0. Dirección de Gobierno Digital

ICONTEC INTERNACIONAL. (16 de 11 de 2007). Norma técnica colombiana NTC/IEC-ISO 27002. Obtenido de tecnología de la Información. técnicas de seguridad.

ICONTEC INTERNACIONAL. (2013). Norma técnica colombiana NTC - IEC- ISO 27001. Obtenido de Tecnología de la información. Técnica de seguridad, sistema de gestión de la seguridad de la información.

ICONTEC INTERNACIONAL. (22 de 03 de 2017). Norma técnica colombiana NTC-ISO 27000. Obtenido de tecnología de la información. técnicas de seguridad. Sistema de gestión de seguridad de la información - visión general: https://www.academia.edu/37895745/NORMA_T%C3%89CNICA_NTC_ISO_IEC_COLOMBIANA_27000_TECNOLOG%C3%8DA_DE_LA_INFORMACI%C3%93N_T%C3%89CNICAS_DE_SEGURIDAD_SISTEMAS_DE_GESTI%C3%93N_DE_SEGURIDAD_DE_LA_INFORMACI%C3%93N_SGSI_VISI%C3%93N_GENERAL_Y_VOCABULARIO

LEY 1341. (30 de 07 de 2009). principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones.
Obtenido de ARTÍCULO 6. Definición de TIC.: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913#:~:text=6.,especial%20beneficiando%20a%20poblaciones%20vulnerables.

MINTIC. (15 de 03 de 2016). Guía para la gestión y clasificación de activos de informaciónGuía N° 5. Obtenido de
https://mintic.gov.co/gestionti/615/articles5482_G5_Gestion_Clasificacion.pdf

MINTIC. (29 de 07 de 2016). Modelo de seguridad y privacidad de la información. Obtenido de https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC. (25 de 04 de 2016). Procedimientos de seguridad de la información- Guía N°3. Obtenido de ttps://gobiernodigital.mintic.gov.co/692/articles5482_G3_Procedimiento_de_Seguridad.pdf

NORMA INTERNACIONAL. (2018). Directrices para la auditoría de los sistemas de gestión ISO 19011

9. Control de cambios

Versión	Descripción de cambios
1.0	* “Elaboración de Documento”.
2.0	Actualización del formato, cambio en las actividades a desarrollar y el periodo de tiempo
3.0	Actualización del formato, cambio en las actividades a desarrollar y el periodo de tiempo