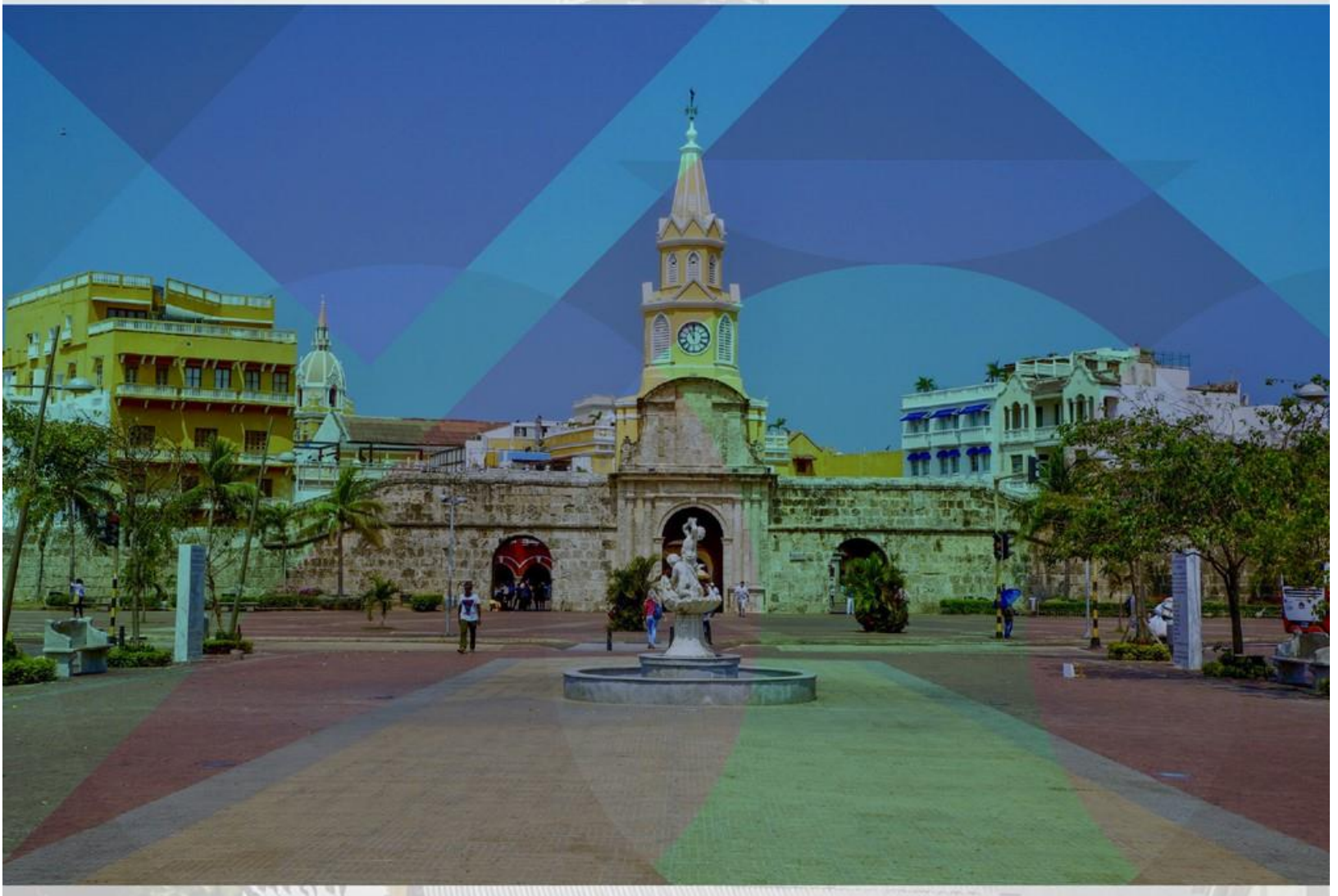
OFICINA ASESORA DE
INFORMÁTICA

Salvemos Juntos
a Cartagena

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

CONTROL DE CAMBIOS

VERSION	DESCRICPCION 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 documento en lenguaje claro

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan de Seguridad de la Información tiene como objetivo orientar a las dependencias del Distrito de Cartagena para dar cumplimiento al Decreto 612 de 2018 por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado y al Decreto 767 del 2022 que actualiza la Política de Gobierno Digital. Además, este último exige la elaboración, por parte de cada entidad pública, de un Plan de Seguridad y Privacidad de la Información.

En esa línea, el Distrito de Cartagena ha estructurado la Política de Gobierno Digital, la cual busca promover el uso y la apropiación de las tecnologías de la información y las comunicaciones (TIC) para instalar capacidades para que la Alcaldía y la ciudadanía sean más competitivas, proactivas e innovadoras. Esto con el fin de que generen valor público en un entorno de confianza digital.

Para ello, se definieron dos componentes: TIC para el Estado y TIC para la sociedad. Ambos tienen habilitadores por cuatro elementos transversales: Seguridad de la Información, Arquitectura, Cultura y apropiación y Servicios ciudadanos digitales.

Con el primer habilitador se pretende que las entidades públicas implementen los lineamientos de seguridad de la información en sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información. Esto tiene como fin 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).

El segundo habilitador pretende que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI. Este habilitador es el que soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora las mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar.

El tercer habilitador es el de Cultura y Apropiación, el cual busca desarrollar las capacidades de los sujetos obligados y los Grupos de Interés, requeridas para el acceso, uso y aprovechamiento de las TIC.

Por último, el habilitador de Servicios Ciudadanos Digitales, con el que se busca que todas las entidades públicas implementen lo dispuesto en el Decreto 1413 de 2017 (incorporado en el título 17, parte 2, libro 2 del Decreto 1078 de 2015), que establece los lineamientos para la prestación de los servicios ciudadanos digitales y para permitir el acceso a la administración pública a través de medios electrónicos.

Por otro lado, este documento también conversa con la Resolución 0500 de marzo 10 del 2021, expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, la cual tiene como objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información. Además, da pautas para la puesta en marcha de la Guía de Gestión de Riesgos de Seguridad de la Información y contiene los lineamientos y estándares para la estrategia de seguridad digital y el procedimiento para la gestión de los incidentes en esta materia.

Teniendo en cuenta lo anteriormente descritos en el siguiente documento acotará en los términos del Plan de Seguridad de Información de la Alcaldía de Cartagena, la Política de Gobierno Digital de acuerdo con lo definido por el Ministerio de las TIC con el objetivo de impulsar la Innovación Pública Digital desde la entidad.

2. GLOSARIO

- **Activo:** en este contexto se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización (MINTIC, 2016)
- **Análisis de Riesgo**: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (MINTIC, 2016)
- **Confidencialidad:** La información es disponible solo a personal autorizados. (NORMA INTERNACIONAL, 2018)
- **Contratistas:** 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. Además, es sinónimo de salvaguarda o contramedida. En suma, es una medida que modifica el riesgo. (MINTIC, 2016)
- **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. (ICONTEC INTERNACIONAL, 2013)
- **Guía:** documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información. (MINTIC, 2016)
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. (MINTIC, 2016)
- **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 o *stakeholder*** actores, organizaciones o grupos de interés que participan en tomas de decisiones o en actividades de procesos. (MINTIC, 2016)
- **Política:** orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad. (ICONTEC INTERNACIONAL, 2007)

- **Privacidad de datos**: aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que tiene una organización o un individuo para determinar qué datos, en un sistema informático, pueden ser compartidos con terceros.
- **Procedimiento**: descripción detallada de la manera en la que se implementa una política. (MINTIC, 2016)
- **Riesgo:** escenario en el que una amenaza concreta puede explotar una vulnerabilidad y causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (MINTIC, 2016)
- **Rol:** papel o función que alguien o algo desempeña. (MINTIC, 2016)
- **Seguridad de la información**: preservación de la confidencialidad, integridad y disponibilidad de la información. (MINTIC, 2016)
- **Sistema de Gestión de Seguridad de la Información (SGSI)**: conjunto de elementos interrelacionados que utiliza una organización para establecer políticas y objetivos de seguridad de la información. También contempla las acciones que se llevan a cabo para alcanzar los fines, con base en el enfoque de gestión y de mejora continua. (MINTIC, 2016)
- **Tecnologías de la Información y las Comunicaciones (TIC):** Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (LEY 1341, 2009)

a. SIGLAS

- **MSPI:** Modelo de seguridad y Privacidad de la información.
- **TI:** Tecnologías de la Información.
- **ISO:** Organización Internacional de Normalización (ISO es su sigla en inglés). organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de normalización propias de cada país.

b. NOMENCLATURA

- **ISO 27000:** Conjunto de normas internacionales, orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) o por su denominación en inglés Information Security Management System (ISMS). Estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos. (ICONTEC INTERNACIONAL, 2017)

3. CONTEXTO ESTRATEGICO 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

Al 2024 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

4.2 PROPÓSITO DEL PLAN INSTITUCIONAL

El Plan de Seguridad de la Información (PSI) busca trazar y planificar la manera en la que la Alcaldía Distrital de Cartagena de Indias implementará del Modelo de Seguridad y Privacidad de la Información (MSPI).

4.3 ÁMBITO DEL PLAN INSTITUCIONAL

El Plan de Seguridad 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 cumplido 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 INSTITICIONAL

4.4.1 IDENTIFICACION DE LA SITUACION ACTUAL

Política de Seguridad y Privacidad de la Información contiene 50 ítems de control que conforman el plan de acción. Desde el inicio de la implementación de estas acciones ha habido incremento en el cumplimiento de las mismas, como se aprecia en la siguiente tabla.

TRIMESTRE	PORCENTAJE DE AVANCE
I	18%
II	29%
III	32%
IV	63%

Tabla 1 Porcentaje de avances

No obstante, hay varios factores que hacen que no se llegue al 100% en los porcentajes de avance. Uno de ellos es que hay dependencias del Distrito que, pese a que deben ser parte activa en esto y las mesas de trabajo que se han realizado, no han enviado soportes que den constancia del cumplimiento de las responsabilidades en esta materia, otro es la ausencia de herramientas tecnológicas para el cumplimiento de los controles y otra es ausencia de personal para cubrir requerimientos específicos.

Por otro lado, en cuanto al desarrollo y la aplicación del Plan de Seguridad y Privacidad de la Información su porcentaje de avance fue de 61% para 2022. No se logró el 100% porque no se cumplieron cinco de las actividades.

De acuerdo con las controles y mediciones del Departamento Administrativo de la Función Pública (DAFP) y el desempeño evaluado en el FURAG (Formulario Único de Reporte de Avances de la Gestión), la Oficina Asesora de Informática ha logrado un 17% de avance entre septiembre y diciembre, obteniendo un total de 83% de cumplimiento.

4.4.2 IDENTIFICACIÓN DE ASPECTOS CRÍTICOS

Para el cumplimiento del plan se han identificado los siguientes aspectos críticos que se deben intervenir.

La Alcaldía Distrital de Cartagena debe:

- Formular un plan para el tratamiento de riesgos que reconozca la acción de gestión apropiada, los recursos, las responsabilidades y las prioridades que se deben tener en cuenta para manejar las amenazas a la seguridad de la información.
- Implementar el Plan de Tratamiento de Riesgos para lograr los objetivos de control establecidos, en los cuales se considera la financiación y la asignación de funciones y responsabilidades.
- Aplicar los controles seleccionados para cumplir los objetivos de este tipo.
- Definir cómo medir la eficacia de los controles o grupos seleccionados de estos y especificar cómo se van a usar los resultados. Esto con el fin de valorar la eficacia de los controles para producir hallazgos comparables y reproducibles.
- Implementar programas de formación y cultura para fomentar buenas prácticas en estos temas.
- Gestionar la operación y recursos del MSPI.
- Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
- Ejecutar procedimientos de seguimiento, revisión y otros controles para:
    - ✓ Detectar rápidamente errores en los resultados del procesamiento.
    - ✓ Identificar con prontitud los incidentes e intentos de violación a la seguridad.
    - ✓ Posibilitar que la dirección determine si las actividades de seguridad delegadas al personal o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
    - ✓ Ayudar a detectar eventos de seguridad para así manera impedir incidentes de seguridad mediante el uso de indicadores.
    - ✓ Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.
- Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la Política y objetivos del MSPI y la revisión de los controles de seguridad) en las que se consideren los resultados de las auditorías de seguridad, los incidentes, la medición de la eficacia sugerencias y la retroalimentación de todas las partes interesadas.
- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

- Revisar las valoraciones de los riesgos a intervalos planificados y revisar el nivel de riesgo residual y riesgo aceptable encontrado teniendo en cuenta los cambios en: la entidad, la tecnología, los objetivos y procesos de la entidad, las amenazas identificadas, la eficacia de los controles implementados y los eventos externos (tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales y en el clima social).
- Realizar auditorías internas del MSPI a intervalos planificados.
- Emprender una revisión del MSPI, realizada por la Dirección, de forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de MSPI.
- Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.
- Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del MSPI.
- Implementar las mejoras identificadas en el MSPI.
- Emprender las acciones correctivas y preventivas adecuadas en las que se apliquen las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y de la propia.
- Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel detalle apropiado de acuerdo con las circunstancias y, cuando sea pertinente, llegar a acuerdos sobre cómo proceder.
- Asegurar que las mejoras logren los objetivos previstos.

4.4.3 PRIORIZACION DE ASPECTOS CRITICOS

Al implementar estas acciones la Alcaldía Distrital de Cartagena, espera obtener los siguientes resultados:

METAS	INSTRUCTIVOS O HERRAMEINTAS A UTILIZAR	RESULTADOS ESPERADOS
Política de Seguridad y Privacidad de la Información	Guía 2 Política General MSPI	Documento con la Política de Seguridad de la Información aprobado por la Alta Dirección y socializada al interior de la entidad. Manual con las Políticas de Seguridad y Privacidad de la Información, aprobadas por la Alta Dirección y socializadas al interior de la entidad.
Procedimientos de seguridad de la información	Guía 3 Procedimientos de Seguridad y Privacidad de la Información	Procedimientos documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
Roles y responsabilidades de seguridad y privacidad de la información	Guía 4 Roles y responsabilidades de seguridad y privacidad de la información	Acto administrativo que cree o modifique las funciones del Comité de Gestión Institucional (o el que haga sus veces), en el que se incluyan los temas de seguridad de la información; revisado y aprobado por la Alta Dirección. Este

METAS	INSTRUCTIVOS O HERRAMEINTAS A UTILIZAR	RESULTADOS ESPERADOS
		deberá designar quien será el encargado de seguridad de la información.
Inventario de activos de información	Guía 5 Gestión De Activos	Documento con la metodología para identificación, clasificación y valoración de activos de información. Este será validado por el Comité de Seguridad de la Información o quien haga sus veces y revisado y aprobado por la Alta Dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales. Inventario de activos de IPv6
Integración del MSPI con el Sistema de Gestión documental	Guía 6 Gestión Documental	Integración del MSPI con el sistema de gestión documental de la entidad
Identificación, Valoración y tratamiento de riesgo	Guía 7 Gestión de Riesgos. Guía 8 Controles de Seguridad	- Documento con la metodología de gestión de riesgos. - Documento con el análisis y evaluación de riesgos. - Documento con el Plan de Tratamiento de Riesgos Documento con la declaración de aplicabilidad. - Documentos revisados y aprobados por la Alta Dirección
Plan de Comunicaciones	Guía 14 Plan de comunicación, sensibilización y capacitación	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.
Plan de diagnóstico de IPv4 a IPv6	Guía 20 Transición IPv4 a IPv6	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6
Planificación y Control Operacional	Documento con el Plan de Tratamiento de Riesgos Documento con la declaración de aplicabilidad	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la Alta Dirección.
Implementación del plan de tratamiento de riesgos.	Guía 7 Gestión Riesgos	Informe de la ejecución del plan de tratamiento de riesgos aprobados por el dueño de cada proceso.

METAS	INSTRUCTIVOS O HERRAMEINTAS A UTILIZAR	RESULTADOS ESPERADOS
Indicadores de gestión.	Guía 9 Indicadores Gestión Seguridad	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
Plan de mejora continua	Resultados de la ejecución del Plan de Revisión y Seguimiento a la implementación del MSPI Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI Guía 17 Mejora Continua	- Documento con el plan de mejoramiento - Documento con el plan de comunicación de resultados

4.5 FORMULACIÓN DEL PLAN

4.5.1 CORTO PLAZO

ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	ENTREGABLES	RESPONSABLES	NOMBRE DEL INDICADOR	FORMULA DEL INDICADOR	META
Identificar vulnerabilidades que sirvan como insumo para la fase de planificación del sistema de seguridad y privacidad de la información	2/1/2023	12/30/2023	Documento diagnóstico	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Diagnóstico	Número de documentos de diagnóstico presentados	1
Definir los diferentes grupos de interés e identificar las necesidades y expectativas en temas de tecnologías de la información de los actores que interactúan con la Alcaldía Distrital de Cartagena de Indias	2/1/2023	12/30/2023	Caracterización de los grupos de interés	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Política General	Número de política presentada	1
Identificar los Inventarios de activos de información (el cual incluye bases de datos de todas las dependencias	2/1/2023	12/30/2023	Documento con la metodología para identificación, clasificación y valoración de	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Inventario de activos	Número de inventarios actualizados	1

del Distrito y la infraestructura TI)			activos de información.					
Elaborar el plan de comunicación y sensibilización a los diferentes titulares de los derechos en el tratamiento de sus datos	2/1/2023	12/30/2023	Documento con el plan de comunicación, sensibilización	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Plan de capacitación seguridad y privacidad de la información	Número capacitaciones realizadas en el año/número de capacitaciones programadas	10	
	2/1/2023	12/30/2023	Listado de asistencia a capacitación para la entidad. Diapositivas, grabaciones			Número de personas capacitadas/número de personas programadas a capacitar	300	
Realizar la planificación y control operacional de acuerdo con lo establecido en la política de seguridad digital y alineados con la metodología para la identificación de riesgos de seguridad informática	2/1/2023	12/30/2023	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la Alta Dirección	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Planificación y control operacional.	Número de planes aprobados	1	
Implementar el Plan de Tratamiento de Riesgos que identifique la acción de gestión apropiada, los recursos, las responsabilidades	2/1/2023	12/30/2023	Informe de la ejecución del Plan de Tratamiento de Riesgos aprobado por el dueño de cada proceso	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Implementación del plan	Porcentaje de avance del cumplimiento del plan	100%	

y prioridades para manejar los riesgos de seguridad de la información de acuerdo con las políticas institucionales establecidas para las dependencias del Distrito								
Diseñar la batería de indicadores de gestión que permitan el control y avance de la implementación de la política de seguridad	2/1/2023	12/30/2023	Informe con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	indicadores de gestión	Número de informes de resultados de indicadores presentados	2	
elaboración del documento con el índice de la información clasificada, reservada, revisadas y los procedimientos asociados	2/1/2023	12/30/2023	Documento con el índice de la información clasificada, reservada, revidas y los procedimientos asociados	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Documento presentado y radicado	Número de documentos tramitados	1	
Implementar mecanismos para el cumplimiento de los derechos de los titulares de la información	2/1/2023	12/30/2023	Documentos con los derechos de los titulares de la información	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Documento presentado y radicado	Número de documentos tramitados	1	
Desarrollar el documento diagnóstico de los	2/1/2023	12/30/2023	Documento del diagnóstico de los componentes	Oficina Asesora de Informática/proceso	Diagnóstico componentes	Número de documentos	1	

componentes hardware y software de la entidad			Hardware y software de la entidad	seguridad y privacidad de la información	hardware y software			
Elaborar auditorías internas del MSPI a intervalos planificados	2/1/2023	12/30/2023	Informes de resultados de auditoria	Oficina Asesora de Informática/infraestructura	cumplimiento Plan de Auditorias	Número de auditorías realizadas	1	
Elaborar el Informe de la Infraestructura de red de comunicaciones	2/1/2023	12/30/2023	Informe de la Infraestructura de red de comunicaciones	Oficina Asesora de Informática/infraestructura	Infraestructura de red de comunicaciones	Número de documentos	1	

4.5.2 MEDIANO PLAZO

ACTIVIDADES	FECHA DE INICIO	FECHA FINAL	ENTREGABLES	RESPONSABLES
Plan de revisión y seguimiento para la implementación del MSPI.	01-02-24	31-12-24	Informes de revisión y seguimiento	Oficina Asesora de Informática
NOMBRES DE LOS INDICADORES		**INDICES**	**METAS**	
Seguimiento a la implementación MSPI		**%**	**100%**	
DESCRIPCION DEL RECURSO REQUERIDO		**TIPO**	**OBSERVACIONES**	
Humanos, tecnológicos			**NA**	

5. HERRAMIENTA DE SEGUIMIENTO DEL PLAN INSTITUCIONAL

ACTIVIDADES	NOMBRE DEL INDICADOR	FÓRMULA DEL INDICADOR	META	MEDICIÓN TRIMESTRAL			
				1	2	3	4
Identificar vulnerabilidades que sirvan como insumo para la fase de planificación del sistema de seguridad y privacidad de la información.	Diagnóstico	Total de número de documentos diagnóstico-presentados	1				
Definir los diferentes grupos de interés e identificar las necesidades y expectativas en temas de tecnologías de la información de los diversos actores que interactúan con la Alcaldía Distrital de Cartagena.	Política General	Número de política presentada	1				

ACTIVIDADES	NOMBRE DEL INDICADOR	FÓRMULA DEL INDICADOR	META	MEDICIÓN TRIMESTRAL			
				1	2	3	4
Identificar los inventarios de activos de información que incluya bases de datos de las dependencias del Distrito y la infraestructura TI.	Inventario de activos	Número de inventarios actualizados	1				
Elaborar el plan de capacitación y sensibilización a los diferentes titulares de los derechos en el tratamiento de sus datos.	Plan de capacitación, seguridad y privacidad de la información	Número capacitación realizados en el año/número de capacitación programadas	10				
		Número de personas capacitadas/número de personas programadas a capacitar	300				
Realizar la planificación y control operacional de acuerdo con lo establecido en la Política de Seguridad Digital y alineados con la metodología para la identificación de riesgos de seguridad informática.	Planificación y control operacional.	Número de planes aprobados	1				
Implementar el Plan de Tratamiento de Riesgos que identifique la acción de gestión apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de seguridad de la información de acuerdo con las políticas institucionales establecidas para las dependencias del Distrito.	Implementación del plan	Porcentaje de avance del cumplimiento del Plan.	100%				

ACTIVIDADES	NOMBRE DEL INDICADOR	FÓRMULA DEL INDICADOR	META	MEDICIÓN TRIMESTRAL				
				1	2	3	4	
Diseñar la batería de indicadores de gestión que permitan el control y avance de la implementación de la política de seguridad.	Indicadores de gestión	Número de informes de resultados de indicadores presentados	2					
Elaboración del documento con el índice de la información clasificada, reservada, revisadas y los procedimientos asociados.	Documento presentado y radicado	Número de documentos tramitados	1					
Implementar mecanismos para el cumplimiento de los derechos de los titulares de la información.	Documento presentado y radicado	Número de documentos tramitados	1					
Desarrollar el documento del diagnóstico de los componentes Hardware y software de la entidad.	Diagnóstico componentes hardware y software	Número de documentos	1					
Elaborar auditorías internas del MSPI a intervalos planificados.	Cumplimiento Plan de Auditorias	Número de auditorías realizadas	1					
Elaborar el Informe de la Infraestructura de red de comunicaciones.	Informe mensual Infraestructura de red de comunicaciones	Número de informes realizados	1					

6. ANEXOS

Se anexa Plan en Excel para los seguimientos correspondientes.

7. BIBLIOGRAFÍA

ICONTEC INTERNACIONAL. (16 de 11 de 2007). *Norma tecnica colombiana NTC/IEC-ISO 27002.* Obtenido de Tecnologia de la Informació. Tecnicas de seguridad.

ICONTEC INTERNACIONAL. (2013). *Norma tecnica 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 tecnica colombiana NTC-ISO 27000.* Obtenido de Tecnologia de la información. Tecnicas de seguridad. Sistema de gestión de seguridad de la información- Vision 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. (06 de 05 de 2016). *Guía de auditoria - Guía N° 15.* Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-5482_G15_Auditoria.pdf

MINTIC. (15 de 03 de 2016). *Guía para la gestión y clasificación de activos de información- Guía N° 5.* Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_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/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC. (25 de 04 de 2016). *Procedimientos de seguridad de la información- Guía N°3.* Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-5482_G3_Procedimiento_de_Seguridad.pdf

MINTIC. (25 de 04 de 2016). *Roles y responsabilidades- Guía N° 4.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

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

8. CONTROL DE CAMBIOS

VERSION	DESCRICPCION 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 documento en lenguaje claro

9. FIRMA DE LOS INTEGRANTES DEL COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO DE LA ALCALDIA DISTRITAL DE CARTAGENA DE INDIAS

SECRETARIO GENERAL

Aprobado mediante acta número 04 del 01 del mes septiembre del 2023 del comité Institucional de Gestión y Desempeño.