PLAN DE SEGURIDAD DE LA INFORMACIÓN

ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

Selvemos Juntos a Cartagena

Alcaldía Distrital De Cartagena de Indias - Bolívar

Dirección: Centro diagonal 30 # 30 - 78 Plaza de la Aduana.
(57) + (5) 6411370 - Línea Gratuita: 018000 415 393
alcalde@cartagena.gov.co / atencionalciudadano@cartagena.gov.co

1. INTRODUCCION

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, se ha definido en dos componentes: TIC para el estado y TIC para la sociedad, que son habilitados por cuatro elementos transversales: Seguridad de la Información, Arquitectura, cultura y apropiación y Servicios Ciudadanos Digitales. En lo particular, indica que el habilitador de seguridad de la información tiene como propósito que las entidades públicas implementen los lineamientos de seguridad 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).

Pr otro lado, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, que tiene como objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, 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:** Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.
- **Control:** Las políticas, los procedimientos, las prácticas y las 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. En una definición más simple, 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**: Los procedimientos 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 ESTRATEGICO DE LA ENTIDAD

3.1. MISION

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. VISION

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. PROPÒSITO DEL PLAN INSTITUCIONAL

El Plan de Seguridad de la Información (PSI), que tiene por objetivo trazar y planificar la manera como la **Alcaldía Distrital de Cartagena de Indias** realizará o continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

4.3. ÀMBITO 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

En los 50 ítem 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 el cumplimiento; terminando año con el cumplimiento del 63%de las acciones planteadas en la política de seguridad; no obstante, existen varios factores que hacen que no se llegue a la total satisfacción dado que las diferentes dependencias deben ser parte activa del cumplimiento y que a pesar de haberse generado mesas de trabajo o enviado notificación, no se ha tenido el soporte

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

En cuanto al desarrollo y aplicación del plan de seguridad y privacidad de la información este cerro el 2022 con un porcentaje de avance de un 61, 26% debido a que no se cumplieron 5 de las actividades que se encontraban en el plan las cuales se realizarán en el 2023.

Frente a la evaluación de los resultados y acatar las recomendaciones efectuadas por el DAFP, en la medición de la Gestión y Desempeño Institucional a través del FURAG, vigencia 2022, Política de gobierno digital, se concluye que entre septiembre y diciembre hay un avance del 17%, terminando en diciembre con un cumplimiento de un 83%

IDENTIFICACION ASPECTOS CRITICOS

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

La **Alcaldía Distrital de Cartagena de** debe;

- Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.
- Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades.
- Implementar los controles seleccionados, para cumplir los objetivos de control.
- Definir cómo medir la eficacia de los controles o grupos de controles seleccionados y especificar cómo se van a usar estas mediciones con el fin de

valorar la eficacia de los controles para producir resultados comparables y reproducibles.

- Implementar programas de formación y de toma de conciencia.
- 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, tanto los que tuvieron éxito como los que fracasaron.
    - Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
    - Ayudar a detectar eventos de seguridad, y de esta 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) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y 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 identificado, 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
    - 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, en 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, aplicando las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización.
- Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel detalle apropiado a las circunstancias y en donde sea pertinente, llegar a acuerdos sobre cómo proceder.
- Asegurar que las mejoras logran los objetivos previstos.

4.4.2. PRIORIZACION DE ASPECTOS CRITICOS

Al implementar estas acciones la Alcaldía distrital de Cartagena de indias deberá 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, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad Manual con las políticas de seguridad y privacidad de la información, debidamente 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, debidamente 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 a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad
Inventario de activos de información	Guía 5 Gestión De Activos	Documento con la metodología para identificación, clasificación y valoración de activos de información, 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
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	Documento con el plan de mejoramiento Documento con el plan

	MSPI Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI Guía 17 Mejora Continua	de comunicación de resultados

4.5. FORMULACION 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 del diagnóstico	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Diagnostico	Numero de documentos de diagnóstico presentados	1
Definir los diferentes grupos de interés identificando las necesidades y expectativas en temas de tecnologías de la información de los diversos 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	Numero de política presentada	1
Identificar los Inventarios de activos de información (el cual incluye bases de datos	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	numero de inventarios actualizados	1

de todas las dependencias 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	numero 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.	numero de planes aprobados	1

Implementar el plan de tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información de acuerdo con las políticas institucionales establecidas para todas las dependencias del distrito	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%%
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	numero de informes de resultados de indicadores presentados	2
elaboración del documento con el índice de la información clasificada,	2/1/2023	12/30/2023	Documento con el índice de la información clasificada, reservada,	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Documento presentado y radicado	Numero de documentos tramitados	1

reservada, revisadas y los procedimientos asociados			revidas y los procedimientos asociados				
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	Numero de documentos tramitados	1
Desarrollar el documento del diagnóstico de los componentes Hardware y software de la entidad	2/1/2023	12/30/2023	Documento del diagnóstico de los componentes Hardware y software de la entidad	Oficina Asesora de Informática/proceso seguridad y privacidad de la información	Diagnostico componentes hardware y software	numero de documentos	1
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	numero 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	numero de documentos	1

4.5.2. MEDIANO PLAZO

ACTIVIDADES	FECHA DE 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		**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	FORMULA 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	Diagnostico	Numero de documentos de diagnóstico presentados	1				

Definir los diferentes grupos de interés identificando las necesidades y expectativas en temas de tecnologías de la información de los diversos actores que interactúan con la Alcaldía Distrital de Cartagena de Indias	Política General	Numero de política presentada	1				
Identificar los Inventarios de activos de información (el cual incluye bases de datos de todas las dependencias del distrito y la infraestructura TI)	inventario de activos	numero de inventarios actualizados	1				
Elaborar el plan de comunicación y sensibilización a los diferentes titulares de los derechos en el tratamiento de sus datos	plan de capacitación seguridad y privacidad de la información	numero capacitaciones realizadas en el año/número de capacitaciones 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.	numero de planes aprobados	1				
Implementar el plan de tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y	implementación del plan	porcentaje de avance del cumplimiento del plan	100%%				

prioridades para manejar los riesgos de seguridad de la información de acuerdo con las políticas institucionales establecidas para todas 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	indicadores de gestión	numero 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	Numero de documentos tramitados	1					
Implementar mecanismos para el cumplimiento de los derechos de los titulares de la información	Documento presentado y radicado	Numero de documentos tramitados	1					
Desarrollar el documento del diagnóstico de los componentes Hardware y software de la entidad	Diagnostico componentes hardware y software	numero de documentos	1					
Elaborar auditorías internas del MSPI a intervalos planificados	cumplimiento plan de auditorias	numero de auditorías realizadas	1					
Elaborar el Informe de la Infraestructura de red de comunicaciones	Infraestructura de red de comunicaciones	numero de documentos	1					

6. ANEXOS –

Se anexa plan en Excel para los seguimientos correspondientes

7. FIRMA DE LOS INTEGRANTES DEL COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO DE LA ALCALDIA 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.

9. 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