Alcaldía Mayor de
Cartagena de Indias

Plan de tratamiento de riesgos de seguridad y privacidad de la información

Alcaldía Distrital de Cartagena de Indias
2024

1. Introducción

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Alcaldía Distrital de Cartagena de Indias se encuentra enfocado en vigilar de una manera eficaz la gestión integral de todo tipo de riesgo de la información. Esta es una entidad de carácter público y de asistencia al ciudadano donde se encuentra en constante intercambio de información con entes públicos y privados, así mismo como con la ciudadanía en general. Toda esta información que se recibe es la materia prima para el buen desarrollo de sus funciones y con base en ella se toman decisiones y se ejecutan acciones que pueden generar comunicados, resoluciones, oficios, etc. Esta información puede ser de carácter público para conocimiento de la ciudadanía en general o puede tratarse de investigaciones de mayor confidencialidad dentro del desarrollo de los procesos. Dado lo anterior, es de suma importancia tener en cuenta claramente el tipo de información que se está procesando para determinar los riesgos a los que está expuesta con el fin de protegerla debidamente.

Para la toma de decisiones con base en la información de altos estándares de calidad, en materia de políticas y gestión de seguridad de la información que permita tomar una disposición y prestar servicios a las personas y funcionarios(as) de la Alcaldía, es necesario que la información sea real, oportuna y de acceso a las personas que lo requieren.

Internacionalmente la norma ISO 31000 ayuda a establecer un sistema de Gestión de Riesgos de cualquier tipo, incluyendo riesgos asociados a la información, esto permite reducir las falencias propias de la información a través de un tratamiento continuo y apropiado de los controles que mitiguen las posibles afectaciones a la Entidad.

La metodología MAGERIT ayuda a realizar un análisis y gestión de riesgos y así mismo se puede implementar medidas de control adecuadas que permitan tener los riesgos mitigados.

Basado en la norma ISO 31000 y la metodología MAGERIT, la Alcaldía Distrital de Cartagena de Indias establece el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para identificar, valorar y gestionar los riesgos de seguridad de la información.

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 tratamiento de riesgos de seguridad y privacidad de la información (PTRSPI)

4.2. Propósito del plan institucional

Diseñar, consolidar e implementar el plan de tratamiento de riesgos de seguridad y privacidad de la información para cada uno de los procesos de la Alcaldía Distrital de Cartagena y establecer un plan de trabajo para identificar y gestionar los riesgos de la información durante el periodo actual cumpliendo la norma ISO 31000 y la metodología MAGERI

4.3. Ámbito del plan institucional

La gestión de riesgos de seguridad y privacidad de la información junto con su tratamiento se aplicará a todas las dependencias de la Alcaldía Distrital de Cartagena de Indias, lo que incluye a todos sus funcionarios, contratistas, a toda la ciudadanía en general y a aquellas personas que por cumplimiento de los compromisos contractuales o en ejercicio de sus funciones realicen tratamiento de la información de la cual la alcaldía es responsable; así como a los diferentes activos de información que hacen parte del sistema de información.

Para lograr alcanzarlo es importante habilitar inicialmente las funciones de liderazgo para asesorar y apoyar el proceso de diseño, implementación y mantenimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información, seguido de una capacitación y generación de una cultura en la entidad para la gestión integral del riego.

4.4. Desarrollo del plan institucional

4.4.1. Identificación de la situación actual

La Alcaldía de Cartagena cuenta con un mapa de riesgos de seguridad de la información, sin embargo, se hace necesario fortalecer las campañas para el levantamiento de los activos de información y fortalecer los controles.

En cuanto al desarrollo y aplicación del plan de tratamiento de riesgo de seguridad y privacidad de la información este cerro el 2023 con un porcentaje de avance de un 46% debido a que no se pudo avanzar en 2 de las actividades programadas 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 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).

4.4.2. Identificación 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 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.

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 8 actividades enmarcadas en el modelo nacional de gestión de riesgo de seguridad y privacidad de la información en entidades públicas.

4.4.3. 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
Definir el contexto interno, externo y de los procesos relacionados con la seguridad	"Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la	Documento de caracterización de las partes interesadas externas e internas y de los

de la información en el entorno digital de la Alcaldía de Cartagena	información. Diseño de Controles en Entidades Públicas"	procesos que tengan relación con la Alcaldía de Cartagena
Definir el alcance para aplicar la gestión de los riesgos de seguridad de la información donde se determinen los criterios diferenciales del MSPI de la Alcaldía de Cartagena	Modelo de seguridad y privacidad de la información - MSPI	Documento de alcance del MSPI
Establecer la política de gestión del riesgo de seguridad de la información de la Alcaldía de Cartagena	Guía de administración del riesgo de gestión del DAFP	Documento con la política de gestión del riesgo de seguridad de la información, debidamente aprobado por el comte de gestión y desempeño institucional, socializada al interior de la Entidad
Identificar de los activos de información de la Alcaldía de Cartagena	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. Inventario de activos de información actualizados
Identificar los riesgos inherentes de seguridad de información para asociarlos a los activos de información de la Alcaldía de Cartagena, identificar amenazas y vulnerabilidades	Guía 7 Gestión de Riesgos.	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
Identificar el nivel de confianza para la autenticación digital, identificar tramites y servicios ciudadanos digitales que deben contar con autenticación digital en la Alcaldía de Cartagena	Servicio de autenticación digital Guía para la administración del riesgo y el diseño de controles en entidades públicas.	Documento con el proceso de vinculación al servicio de autenticación digital Tramites y servicios digitales con autenticación digital

Identificar, implementar y evaluar los controles de seguridad de la información para los riesgos de seguridad de la información identificados sobre los activos de información en la Alcaldía de Cartagena	Guía 8 Controles de Seguridad	Documento con la metodología para identificación, implementación y evaluación de los controles de seguridad y privacidad de la información

5. Formulación del plan

5.1. Corto plazo

Actividades	Fecha inicio	Fecha final	Entregables	Responsables
1. Definir el contexto interno, externo y de los procesos relacionados con la seguridad de la información en el entorno digital de la Alcaldía de Cartagena	1/02/2024	1/04/2024	Documento de caracterización de las partes interesadas externas e internas y de los procesos que tengan relación con la Alcaldía de Cartagena	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
2. Definir el alcance para aplicar la gestión de los riesgos de seguridad de la información donde se determinen los criterios diferenciales del MSPI de la Alcaldía de Cartagena	1/04/2024	31/05/2024	Documento de Alcance	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
3. Establecer la política de gestión del riesgo de seguridad de la información de la Alcaldía de Cartagena	1/05/2024	30/06/2024	Documento de política de gestión del riesgo de seguridad de la información de la Alcaldía de Cartagena	Oficina Asesora de informática/proceso Seguridad y privacidad de la información - Comité de gestión y desempeño institucional
4. Definir los recursos para la gestión de los riesgos de seguridad de la información de la Alcaldía de Cartagena	1/05/2024	30/06/2024	Documento con los recursos para el desarrollo de la gestión de riesgos de seguridad de la información	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito

5. Identificar de los activos de información de la Alcaldía de Cartagena	1/07/2024	31/10/2024	Documento con la metodología para identificación, clasificación y valoración de activos de información.	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
6. Identificar los riesgos inherentes de seguridad de información para asociarlos a los activos de información de la Alcaldía de Cartagena, identificar amenazas y vulnerabilidades	1/08/2024	30/11/2024	Documento con la metodología para la gestión de los riesgos de seguridad de la información	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
7. Identificar el nivel de confianza para la autenticación digital, identificar tramites y servicios ciudadanos digitales que deben contar con autenticación digital en la Alcaldía de Cartagena	1/08/2024	30/11/2024	Documento con el proceso de vinculación al servicio de autenticación digital	Oficina Asesora de Informática/proceso seguridad y privacidad de la información - Todas las dependencias del distrito
8. Identificar, implementar y evaluar los controles de seguridad de la información para los riesgos de seguridad de la información identificados sobre los activos de información en la Alcaldía de Cartagena	1/09/2024	30/11/2024	Documento con la metodología para identificación, implementación y evaluación de los controles de seguridad y privacidad de la información	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 Plan de seguimiento a los riesgos	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

Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Anexo Técnico V 4. Dirección de Gobierno Digital

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