OFICINA ASESORA DE
INFORMÁTICA

Salvemos Juntos
a Cartagena

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

TABLA DE CONTENIDO

1. INTRODUCCION

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Alcaldía Distrital de Cartagena de Indias es un documento que se enfoca en el marco estratégico de controles preventivos y en acciones que buscan reducir la exposición a vulnerabilidades que representan riesgos para la entidad. Este, además, se construyó con el propósito de proteger la integridad de la información del Distrito, de la ciudadanía y de terceros.

Asimismo, este tiene como fin dar pautas para salvaguardar los datos públicos y privados para cumplir con los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital, las cuales son directrices del Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC).

Del mismo modo, este documento se alinea con lo establecido en el CONPES 3995 de 2020, el cual describe la política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital. El Modelo de Seguridad y Privacidad de MINTIC, lineamientos para las entidades públicas que conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información.

El Decreto 1008 de 14 de junio 2018, que establece los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones y la Resolución 500 de 2021 (por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital).

Adicionalmente, el Plan conversa con la Norma Internacional para la Gestión del Riesgo ISO 31000:2018 y la Guía para la Administración y el Diseño de Controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión. Por último, incluye el método sistemático MAGERIT implementado para analizar los peligros derivados del uso de tecnologías de la información y comunicaciones.

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, 2017)
- **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. (ICONTEC INTERNACIONAL, 2017)
- **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 *skateholder***: actores, organizaciones o grupos de interés que participan en tomas de decisiones o en actividades de procesos. (MINTIC, 2016)
- **Política del Sistema de Gestión y Seguridad de la Información:** manifestación de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.
- **Política:** orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad. (MINTIC, 2016)
- **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. (ICONTEC INTERNACIONAL, 2017)
- **Ingeniería social:** conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.
- **Ataque DDoS:** Ataque distribuido de denegación de servicio, es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente. (Gonzalez, 2022)
- **MAGERIT:** método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- **Front Office:** actividades que un negocio lleva a cabo para atender a sus clientes

SIGLAS

- **SGSI**: Sistema de Gestión de la Seguridad de la Información.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información (MSPI, 2021)

3. CONTEXTO ESTRATEGICO DE LA ENTIDAD

a. 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.

b. 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

c. 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

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 para establecer un plan de trabajo que permita identificar y gestionar los riesgos de la información durante el periodo actual de conformidad a la Norma ISO 31000 y la metodología MAGERIT.

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 funcionarios, contratistas, a la ciudadanía y a las personas que, por cumplimiento de los compromisos contractuales o en ejercicio de sus funciones, realicen tratamiento de datos de la cual la Alcaldía es responsable. Del mismo modo, comprende los diferentes activos de información.

Para alcanzar lo anterior se debe habilitar, inicialmente, las funciones de liderazgo para asesorar y apoyar el proceso de diseño, implementación y mantenimiento del plan mencionado. Posterior a eso, se dictará una capacitación con el fin de fomentar espacios para la generación de una cultura de gestión integral del riesgo.

4.4 DESARROLLO DEL PLAN INSTITICIONAL

4.4.1 IDENTIFICACION DE LA SITUACION ACTUAL

La Alcaldía de Cartagena cuenta con un mapa de riesgos de seguridad de la información, el cual debe acompañarse de campañas para el levantamiento de los activos de información y fortalecer los controles

4.4.2 IDENTIFICACION ASPECTOS CRITICOS

Para el cumplimiento del plan se han identificado aspectos críticos que se deben intervenir. Por lo tanto, la Alcaldía 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.
- Efectuar los controles designados para cumplir los objetivos de control.
- 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 mismos para producir hallazgos 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.
    - ✓ 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 CRÍTICOS

Al implementar estas acciones la Alcaldía distrital de Cartagena se espera obtener los siguientes resultados:

Metas	Instructivos o herramientas a utilizar	Resultados esperados
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
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.

Metas	Instructivos o herramientas a utilizar	Resultados esperados
		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.
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 los secretarios y Jefes de Oficinas.
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.
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

Actividades:

La Alcaldía Distrital de Cartagena de Indias da cumplimiento a las políticas de seguridad de la información, y para mejorar y conservar los niveles de confidencialidad, integridad y disponibilidad de la información institucional; se apoya en normas, estándares, políticas y directrices establecidas por los entes competentes para el adecuado manejo de la información. Esto mediante la identificación y gestión de los riesgos de seguridad de la información.

A continuación, se relaciona el plan de actividades que se deben desarrollar:

CICLO PHVA	META	ACTIVIDAD
Planear	Definir estado actual y estado deseado. Valoración del riesgo	Planificación del tratamiento del riesgo.
Hacer	Mitigar y controlar riesgos en seguridad de la información.	Implementación del Plan de Tratamiento de Riesgo
Verificar	Examinar si el Plan es efectivo.	Monitoreo y revisión continua de los riesgos.
Actuar	Identificar vulnerabilidades.	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información.

Lineamientos riesgos de seguridad de la información:

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI)3, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales y cultura y apropiación.

Planificación de la GRSD

La fase de planificación comprende los aspectos expuestos en la política de riesgos del Distrito de Cartagena, sin embargo, se realizan algunas precisiones con relación a los siguientes criterios:

- ✓ Definición del contexto interno, externo y de los procesos de la entidad pública.
- ✓ Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- ✓ Identificación de activos.

- ✓ Identificación de riesgos.
- ✓ Valoración de riesgos.
- ✓ Definición del tratamiento de los riesgos.

Respecto a estas actividades, el presente documento busca profundizar en lo concerniente a riesgos de seguridad digital, en cada una de ellas, siendo el documento político de riesgos el documento metodológico par el Distrito.

Definición del contexto interno, externo y de los procesos de la entidad pública

En el marco del Distrito, se entiende por contexto externo:

- ✓ Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.
- ✓ Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública. Por ejemplo, la Ley 1581 de 2012 o la Ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el Decreto 1078 de 2015 o el Decreto 1499 de 2017.
- ✓ Dependencias económicas y financieras de empresas.
- ✓ Entorno cultural.
- ✓ Cualquier otro factor externo de tipo internacional, nacional (Gobierno), regional o local.
- ✓ Ciudadanos a los cuales la entidad pública brinda servicios por medios digitales, como trámites por páginas web.
- ✓ Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas con la entidad pública.

Por su parte, el contexto interno comprende factores que impactan directamente a:

- ✓ Al Distrito de Cartagena y sus dependencias, en general, su organización, sistemas de información o servicios, reglamentación interna, número de sedes y empleados, entre otros aspectos.
- ✓ Cada uno de los procesos sobre los cuales están soportadas las operaciones.

Los siguientes son factores claves para el Distrito y los procesos:

Para el Distrito en	Para los procesos
✓ Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros ✓ Flujos de información y los procesos de toma de decisiones	✓ Identificación de los procesos y su respectiva caracterización ✓ Detalle de las actividades que se llevan a cabo en el proceso ✓ Flujos de información

Para el Distrito en	Para los procesos
✓ Empleados, contratistas ✓ Objetivos estratégicos y la forma de alcanzarlos ✓ La misión, visión, valores y cultura de la organización ✓ Sus políticas, procesos y procedimientos Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros) ✓ Toda la estructura organizacional ✓ Roles y responsabilidades ✓ Sistemas de información o servicios	✓ Identificación y actualización de los activos en la cadena de valor de la entidad pública ✓ Recursos ✓ Alcance del proceso ✓ Relaciones con otros procesos de la entidad pública ✓ Cantidad de ciudadanos afectados por el proceso ✓ Procesos de gestión de riesgos que se tienen actualmente implementados ✓ Personal involucrado en la toma de decisiones

Cabe indicar que el alcance de la administración del riesgo de seguridad digital debe ser extensible y aplicable a todos los procesos de la Alcaldía de Cartagena que consideren los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información.

5. RESPONSABLE DE SEGURIDAD DIGITAL

El Distrito de Cartagena debe designar a una persona como responsable de seguridad digital y seguridad de la información. Esta debe pertenecer a un equipo que haga parte de secretarios y Jefes de Oficinas y sus responsabilidades, que deben estar orientadas a la gestión del riesgo de en el entorno digital, se presentan a continuación:

- ✓ Definir el procedimiento para la identificación y valoración de activos.
- ✓ Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (identificación, análisis, evaluación y tratamiento).
- ✓ Asesorar y acompañar la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigarlos.
- ✓ Apoyar el seguimiento a los planes de tratamiento de riesgo definidos.
- ✓ Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital

Nota: como complemento de esta actividad, el Distrito debe tomar como referencia lo definido en el apartado de roles y responsabilidades del Modelo de Seguridad y Privacidad de la Información.

5.1 IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN:

Un activo es cualquier elemento que tenga valor para la organización. Sin embargo, en el contexto de seguridad digital estos hacen referencia a elementos como aplicaciones y servicios web, redes, información física o digital, tecnologías de información (TI), tecnologías de operación (TO) y que utiliza la organización para funcionar en el entorno digital.

Posterior a esa claridad, como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar y valorar los activos de información. Esto lo debe hacer la Primera Línea de Defensa y los líderes, cada vez que apliquen la gestión del riesgo. Cabe mencionar que se contará con la orientación del responsable de seguridad digital.

En ese sentido, la identificación de los activos permite determinar qué es lo más importante que cada proceso del Distrito en materia de bases de datos, archivos, servidores web o aplicaciones necesarias para que la entidad pueda prestar sus servicios. Así, pues, la Alcaldía podrá saber qué es lo que debe proteger para garantizar, tanto su funcionamiento interno como el externo, lo que aumenta la confianza en el uso de las herramientas digitales.

Ahora bien, como modelo a seguir se relaciona el siguiente formato que las dependencias deberán diligenciar para la identificación de los activos (esto se debe realizar por proceso):

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712/2014	Ley 1581 del 2012	Criticidad respecto a su confidencialidad	Criticidad con respecto a completitud e integridad	Nivel de criticidad
Gestión del talento humano	Base de datos nomina	Base de datos con información de nómina de las entidades	Director talento humano	información	Información reservada	Contine datos personales	ALTA	ALTA	ALTA
Gestión del talento humano	Aplicativo de nomina	Servidor web que contiene el front office de la entidad	Jefe de la oficina asesora de informatica	software	NA	NA	ALTA	MEDIA	ALTA

5.2 IDENTIFICACIÓN DEL RIESGO INHERENTES DE SEGURIDAD DIGITAL

Mediante las actividades de identificación se reconocerán tres riesgos inherentes de seguridad de la información:

- ✓ Pérdida de la confidencialidad
- ✓ Pérdida de la integridad
- ✓ Pérdida de la disponibilidad

Para cada riesgo se debe asociar el grupo de activos, o activos específicos del proceso, y analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

5.3 IDENTIFICACIÓN DE AMENAZAS

A continuación, se presentan amenazas deliberadas (D), fortuitas (F) y ambientales (A) que representan situaciones o fuentes que pueden hacer daño a los activos de información y materializar los riesgos:

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Pérdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	F
Perturbación debida a la radiación	Radiación electromagnética	F
	Radiación térmica	F
	Impulsos electromagnéticos	F
Compromiso de la información	Interceptación de señales de interferencia comprometida	F

TIPO	AMENAZA	ORIGEN
	Espionaje remoto	D, F
	Escucha encubierta	F, D
	Hurto de medios o documentos	D, F
	Hurto de equipo	D, F
	Recuperación de medios reciclados o desechados	D, F
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D, F
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	D, F
	Saturación del sistema de información	D, F
	Saturación del sistema de información	D, F
	Incumplimiento en el mantenimiento del sistema de información.	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
	Uso de software falso o copiado	D, F
	Corrupción de los datos	D, F
	Procesamiento ilegal de datos	D, F
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D, F
	Falsificación de derechos	D, F
	Negación de acciones	D, F
	Incumplimiento en la disponibilidad del personal	D, F

Para esos casos se recomienda prestar atención a las fuentes de amenazas humanas:

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	Piratería Ingeniería social Intrusión, accesos forzados al sistema Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador Acto fraudulento Soborno de la información Suplantación de identidad Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/Terrorismo Guerra de la información Ataques contra el sistema DDoS Penetración en el sistema Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Ventaja política Explotación económica Hurto de información Intrusión en privacidad personal Ingeniería social Penetración en el sistema Acceso no autorizado al sistema

FUENTE DE AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.

5.4 IDENTIFICACIÓN DE VULNERABILIDADES

Vulnerabilidades comunes

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos
	Copia no controlada	Hurtos medios o documentos.
RED	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaces	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	
	Ubicación en área susceptible de inundación	
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
ORGANIZACIÓN	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos

TIPO DE ACTIVO	EJEMPLO DE VULNERABILIDADES	EJEMPLO DE AMENAZAS
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

5.5 VALORACIÓN DEL RIESGO

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la política de gestión del riesgo del Distrito de Cartagena

	Frecuencia de la actividad	probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	**20%**
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	**40%**
media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	**60%**
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	**80%**
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	**100%**

La determinación del impacto del riesgo se debe medir de acuerdo con lo establecido en la Política de Administración de Riesgos del Distrito de Cartagena, puesto que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización de la amenaza.

La siguiente tabla referencia cómo se debe calcular el impacto.

	Afectación económica	reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor – 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivo
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Basado en la probabilidad y el impacto definido, se obtiene el nivel de riesgo inherente o el análisis preliminar.

Esto se hará mediante la aplicación de esta matriz de calor que es resultado de cruzar la probabilidad vs impacto y para definir el nivel de severidad para el riesgo de seguridad de la información identificado.

Ver la siguiente matriz para su aplicación.

probabilidad	Muy alta 100%					
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy baja 20%					
		Leve 20%	Menor 40%	Moderado 60%	Menor 80%	Catastrófico 100%
	Impacto					

Extremo	
Alto	
Moderado	
bajo	

5.6 IDENTIFICACIÓN Y EVOLUCIÓN DE CONTROLES EXISTENTES

El Distrito de Cartagena podrá mitigar y tratar los riesgos de seguridad de la información con la implementación de los controles sugeridos en la ISO/IEC 27001:2013. Así, acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen (la lista completa se encuentra en el documento maestro del Modelo de Seguridad y Privacidad de la Información - MSPI):

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se documentarán y pondrán a disposición de los usuarios que los necesiten.
Gestión de cambios	Control: se controlarán los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema, se hará seguimiento al uso de los recursos y llevarán a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberán separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se implementarán controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la pérdida de datos
Respaldo de información	Control: se harán copias de respaldo de la información, del *software* y de las imágenes de los sistemas y se pondrán a prueba regularmente de acuerdo con una política de copias de respaldo.

CORTO PLAZO

ACTIVIDADES	FECHA DE NICIO	FECHA FINAL	ENTREGABLES	RESPONSABLES	NOMBRE DEL INDICADOR	FORMULA DEL INDICADOR	META
1. Determinar los activos relevantes para la Alcandía Distrital de Cartagena de Indias, su interrelación y su valor, en el sentido de qué perjuicio (costo) supondría su degradación.	2/1/2023	1/12/2023	Caracterización de los activos de la Alcaldía Distrital de Cartagena de Indias	Oficina Asesora de Informática / proceso Seguridad y privacidad de la información	Caracterización de los activos	Número de caracterizaciones de los activos realizadas	10
2. Realizar las mesas de trabajo con las dependencias el Distrito para la determinación de las amenazas a las que están expuestos activos de información.	2/1/2023	1/12/2023	Caracterización de las amenazas de la Alcaldía Distrital de Cartagena de Indias	Oficina Asesora de Informática / proceso Seguridad y privacidad de la información	Caracterización de las amenazas	Número de caracterizaciones de las amenazas realizadas	10
3. Realizar el levantamiento del mapa de riesgos tecnológicos de las dependencias del Distrito, estableciendo una metodología para su seguimiento y control.	2/1/2023	1/12/2023	Mapa de riesgos tecnológicos	Oficina Asesora de Informática / proceso Seguridad y privacidad de la información	Mapa de riesgos tecnológicos	Número de mapas de riesgo de seguridad levantados en el Distrito	5
4. Realizar seguimiento y monitoreo a los riegos de seguridad levantados en el Distrito.	7/1/2023	1/12/2023	informa de seguimiento a los riesgos	Oficina Asesora de Informática / proceso Seguridad y privacidad de la información	informe de seguimiento	Número de informes de seguimiento presentados	4
5.Generar acciones y recomendaciones para el control y seguimiento a los riesgos-	7/1/2023	1/12/2023	plan de mejoramiento	Oficina Asesora de Informática / proceso Seguridad y privacidad de la información	plan de mejora	Valor numérico de los planes de mejoramiento presentados derivado del informe de seguimiento	4

MEDIANO PLAZO

ACTIVIDADES	FECHA DE 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		**INDICES**	**METAS**	
Seguimiento a la implementación de los controles		**%**	**100%**	
DESCRIPCIÓN DEL RECURSO REQUERIDO		**TIPO**	**OBSERVACIONES**	
Humanos, tecnológicos			**N/A**	

6. HERRAMIENTA DE SEGUIMIENTO DEL PLAN INSTITUCIONAL

ACTIVIDADES	NOMBRE DEL INDICADOR	FORMULA DEL INDICADOR	META	MEDICIÓN TRIMESTRAL			
				1	2	3	4
1. Determinar los activos relevantes para la Alcaldía Distrital de Cartagena de Indias, su interrelación y su valor, en el sentido de qué perjuicio (costo) supondría su degradación	Caracterización de los activos	Número de caracterizaciones de los activos realizadas	10				
2. Realizar las mesas de trabajo con las dependencias el Distrito para la determinación de las amenazas a las que están expuestos activos de información	Caracterización de las amenazas	Número de caracterizaciones de las amenazas realizadas	10				

ACTIVIDADES	NOMBRE DEL INDICADOR	FORMULA DEL INDICADOR	META	MEDICIÓN TRIMESTRAL			
				1	2	3	4
3. Realizar el levantamiento del mapa de riesgos tecnológicos de las dependencias del Distrito, estableciendo una metodología para su seguimiento y control	Mapa de riesgos tecnológicos	Número de mapas de riesgo de seguridad levantados en el Distrito	5				
4. Realizar seguimiento y monitoreo a los riegos de seguridad levantados en el Distrito	informe de seguimiento	Número de informes de seguimiento presentados	4				
5.Generar acciones y recomendaciones para el control y seguimiento a los riesgos	plan de mejora	valor numérico de los planes de mejoramiento presentados derivado del informe de seguimiento	4				

7. ANEXOS

Se anexa plan en Excel para los seguimientos correspondientes.

8. FIRMA DE LOS INTEGRANTES DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO DE LA ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

9. BIBLIOGRAFÍA

Gonzalez, A. (2022). *Ataques DDOS.* Obtenido de http://profesores.elo.utfsm.cl/~agv/elo322/1s19/projects/reports/Ataques%20DDOS.pdf

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

MINTIC. (11 de 05 de 2016). *Elaboración de la política general de seguridad y privacidad de la información- Guía N°2.* Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-5482_G2_Politica_General.pdf

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. (29 de 07 de 2016). *Modelo de seguridad y privacidad de la información -Modelo.* Obtenido de https://gobiernodigital.mintic.gov.co/692/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

MSPI. (15 de febrero de 2021). Obtenido de MINTIC: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

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

A. 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

_____

SECRETARIO GENERAL

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