Contenido

1. INTRODUCCIÓN

El presente Plan de Tratamiento de Riesgos establece la hoja de ruta para gestionar las incertidumbres que amenazan la confidencialidad, integridad y disponibilidad de los activos de información del **Aeropuerto Internacional Matecaña.**

Este documento marca una evolución en la madurez de gobierno de TI del Aeropuerto, pasando de una gestión documental a una Ciberseguridad Basada en Riesgos (Risk-Based Security). El objetivo principal es reducir la exposición a amenazas críticas como el fraude financiero digital, el secuestro de información (Ransomware) y la indisponibilidad de servicios tecnológicos, alineándose con el MSPI (Modelo de Seguridad y Privacidad de la Información) del MinTIC y la norma ISO/IEC 27001:2022.

2. DEFINICIONES

Los siguientes términos son utilizados en el contexto de la gestión de la seguridad de la información y aplican para todas sus fases y momentos, incluyendo la de riesgos.

• Administración del riesgo: gestión Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
• Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
• Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado. Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
• Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.
• Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
• Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
• Consecuencia: Resultado de un evento que afecta los objetivos.
• Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

• Control: Medida que modifica el riesgo. 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.
• Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controle s del anexo A de ISO 27001.
• Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
• Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
• Evento: intervalo Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
• Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
• Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

3. OBJETIVO

Establecer la hoja de ruta para la mitigación, transferencia, evitación o aceptación de los riesgos de seguridad digital identificados en el Aeropuerto Internacional Matecaña. Este plan busca garantizar la Confidencialidad, Integridad y Disponibilidad (CIA) de los activos críticos (SIIF Nación, Gestión Contractual, Infraestructura Tecnológica) reduciendo el riesgo residual a niveles tolerables por la Alta Dirección.

4. OBJETIVOS ESPECIFICOS

- Revisión y actualización del marco de gestión de riesgos de seguridad y privacidad de la información a través del cual se mitiguen las vulnerabilidades y amenazas asociadas a los activos de información con lo que cuenta el Aeropuerto Internacional Matecaña.
- Mantener niveles de aceptación razonables de los riesgos en relación con los atributos de disponibilidad, integridad y confidencialidad de la información del Aeropuerto Matecaña.
- Realizar un seguimiento de los riesgos de seguridad y privacidad de la información.
- Dar seguimiento a los controles establecidos que atiendan la gestión de riesgos y que facilite la toma de decisiones.

5. ALCANCE

La gestión de riesgos de seguridad de la información, incluido su tratamiento será aplicado sobre todos los activos de información de la AIM identificados por cada uno de los procesos y que hacen parte del Registro de Activos de Información de la AIM (RAI); con base en las normas vigentes, la metodología definida por la entidad para la gestión del riesgo definida, las pautas y recomendaciones previstas en la ISO 27001 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

6. POLÍTICA DE ADMINISTRACION DE RIESGOS

El AIM, a través de su Modelo Integrado de Gestión, se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC que contribuyen al desarrollo social y económico del país, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida.

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, corrupción, Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los servicios del AIM procurando que no se materialicen, atendiendo los lineamientos establecidos en Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

• Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.
• Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de

funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.
• Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.
• Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de Seguridad y privacidad de la Información, seguridad le permite al AIM realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de seguridad y privacidad de la información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Dirección.

7. METODOLOGÍA DE TRATAMIENTO

El presente plan responde a los hallazgos de los Mapas de Riesgo de Gestión Tecnológica (DGGT01) y Seguridad Digital (DGGT06). Las acciones se categorizan en:

- Controles Preventivos: Para reducir la probabilidad de ocurrencia (ej. Mantenimiento, Capacitación).
- Controles Detectivos/Correctivos: Para reducir el impacto en caso de materialización (ej. Backups, Enlaces redundantes).

8. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016).

Tabla1. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

GESTIÓN	ACTIVIDADES	RESPONSABLE	FECHA ESTIMADA
Gestión de Riesgos	Actualización de La matriz DGGT06 (Riesgos de Gestión Tecnológica) con el formato institucional FOGT01 para la gestión de riesgos de Seguridad Digital.	Oficina Administrativa Financiera y Gestión Tecnológica.	Feb-26
	Revisión y actualización de los Mapa/Matriz de riegos de SD y GT	Oficina Administrativa Financiera y Gestión Tecnológica	Abr-26
	Seguimiento de la ejecución de los controles correspondientes al Mapa de riegos de SD y Matriz de Riesgos GT (Indicadores de Controles y Actividades)	Oficina Administrativa Financiera y Gestión Tecnológica	Jun-26
SGC	Identificación de oportunidades de mejora acorde a los resultados de la actualización y revisión de la documentación del proceso.	Oficina Administrativa Financiera y Gestión Tecnológica	Ago-26
	Identificación de oportunidades de mejora acorde a los resultados de la evaluación obtenida y la revisión de las políticas.	Oficina Administrativa Financiera y Gestión Tecnológica	Oct-26

9. SEGUIMIENTO Y MEDICIÓN (KPIs)

Para garantizar que este documento no sea letra muerta, se medirán los siguientes indicadores trimestralmente ante el Comité Institucional de Gestión y Desempeño:

- % de Ejecución del Plan de Tratamiento: Actividades Ejecutadas / Actividades Planeadas (Meta: >90% a noviembre de 2026).
- % de Ejecución del Mapa/Matriz GT/SD: Controles Implementados / Controles Planificados. (Meta: >90% a diciembre de 2026).
- Eficacia de los Controles (Reducción de Riesgo): Número de incidentes de seguridad materializados vs. Intentos bloqueados.

FUNCIONARIO	**NOMBRE**	**CARGO VINCULACION**	**FIRMA**
Elaborado por	Francisco Escobar Romero	Contratista TI	
Revisado por	Diana Agudelo	Contratista SGC	
Aprobado por	Comité Institucional de Gesti Desempeño		
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.			