Contenido

1. INTRODUCCIÓN

El presente documento describe el Plan de Seguridad y Privacidad del Aeropuerto Internacional Matecaña (AIM), alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional de la entidad.
La Política de Gobierno Digital han definido ocho (8) componentes y tres (5) habilitadores transversales, donde el habilitador de Seguridad y Ciberseguridad busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, 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, para lo cual se hace indispensable diseñar el Plan de Seguridad y Privacidad de la Información que a continuación se detalla.

2. OBJETIVO GENERAL

Fortalecer la postura de ciberseguridad y resiliencia operacional del Aeropuerto Internacional Matecaña mediante la consolidación del Modelo de Seguridad y Privacidad de la Información (MSPI) y su alineación con el estándar ISO/IEC 27001:2022. Esto se logrará a través de una gestión de riesgos dinámica, el aseguramiento técnico de la infraestructura y la implementación de capacidades de recuperación ante desastres, garantizando la Confidencialidad, Integridad y Disponibilidad de los activos de información críticos para la gestión administrativa y financiera de la entidad, en cumplimiento del Decreto 1078 de 2015 y la Ley 1581 de 2012.

3. OBJETIVOS ESPECIFICOS

- Diagnosticar y Planificar (Gobernanza): Establecer una línea base real del estado de ciberseguridad mediante un Análisis de Brechas (Gap Analysis) técnico y normativo frente a las guías del MinTIC y los controles de la ISO 27001, unificando la gestión de ambos marcos.
- Blindar la Infraestructura (Protección): Ejecutar un programa de "Ciberhigiene Ofensiva" que incluya análisis de vulnerabilidades trimestrales (On-Premise y Nube) y la remediación efectiva de hallazgos mediante procesos de Retest obligatorios.
- Asegurar la Continuidad (Resiliencia): Diseñar, documentar y probar el Plan de Continuidad Tecnológica (PCT) y Recuperación de Desastres (DRP), asegurando que los servicios críticos (Financieros, Contractuales) puedan restablecerse en tiempos tolerables tras un incidente mayor.
- Cultura y Competencia (Factor Humano): Ejecutar el plan de toma de conciencia enfocado en las amenazas modernas (Phishing, Ingeniería

Social) para reducir el riesgo de error humano en las áreas administrativas.

- Mejora Continua (Evaluación): Evaluar el desempeño del sistema mediante auditorías internas y revisiones por la dirección que midan la eficacia real de los controles, activando planes de mejoramiento que cierren las brechas detectadas.

4. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información comprende la gestión estratégica, táctica y operativa de la seguridad para todos los procesos administrativos y de apoyo del Aeropuerto Internacional Matecaña (AIM). En articulación con la ejecución de la fase IV del Modelo de Seguridad y Privacidad de la Información (MSPI), las recomendaciones del FURAG 2025 y las actualizaciones del Sistema de Gestión de Calidad (SGC) asociadas al proceso de Gestión Tecnológica para la vigencia 2026, el plan se orienta a fortalecer la implementación de acciones y controles conforme a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

En consecuencia, su enfoque principal será robustecer la seguridad informática de la plataforma tecnológica del AIM, considerando las capacidades y recursos disponibles, con el fin de incrementar la confianza de los ciudadanos, usuarios, socios y demás partes interesadas, y garantizar la adecuada protección de la información institucional.

5. PROCEDIMIENTOS

El AIM ejecuta en su modelo de procesos, el procedimiento de Seguridad y Privacidad de la Información en el nivel estratégico que permitirá garantizar continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la entidad, por medio de la definición de políticas, programas, lineamientos, estrategias y actividades.

6. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFROMACIÓN

El AIM adopta la política y se convierten en una herramienta para el uso adecuado de los recursos informáticos del AIM, donde se desarrollan funciones y procedimientos de seguridad para concientizar a cada uno de los colaboradores de la organización en el uso adecuado de los recursos informáticos, permitiendo de esta manera obtener un mejor rendimiento y protección de los diversos sistemas de información y sus recursos.

7. PLAN DE IMPLEMENTACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de implementación para la dimensión de Seguridad y Privacidad de la información comprende el siguiente cronograma y se le hará seguimiento mes a mes.

Tabla1. Plan de Implementación

GESTIÓN	ACTIVIDADES	RESPONSABLE	FECHA ESTIMADA
MSPI	Inicio de ejecución de la Fase 4 del MSPI Mejora Continua o Evaluación del Desempeño para mantener la seguridad y privacidad de la información de manera progresiva y adaptada a nuevas amenazas.	Oficina Administrativa y Financiera Gestión Tecnológica	Feb-26
	Análisis de brechas de las políticas y tecnologías de acuerdo a la Guía MSPI del MinTic y Realizar diagnóstico de los resultados para identificar fortalezas y debilidades. (efectividad de los controles implementados)	Oficina Administrativa y Financiera Gestión Tecnológica	Mar-26
	Diseñar plan de mejoramiento donde se definan acciones específicas (actualización de políticas, capacitación, nuevas tecnologías) para corregir desviaciones y abordar vulnerabilidades.	Oficina Administrativa y Financiera Gestión Tecnológica	Abr-26
	Inicio de ejecución de las acciones específicas definidas en el plan de mejoramiento aplicando acciones correctivas y preventivas	Oficina Administrativa y Financiera Gestión Tecnológica	May-26
	Informe de retroalimentación de la Fase 4 del MSPI alineado con estándares internacionales como la ISO/IEC 27001.	Oficina Administrativa y Financiera Gestión Tecnológica	Dic-26
FURAG	Realizar análisis de vulnerabilidades de seguridad a los activos de información en su infraestructura On Premise.	Oficina Administrativa y Financiera Gestión Tecnológica	Ago-26
	Realizar análisis de vulnerabilidades de seguridad a los activos de información de su infraestructura en Nube Pública/Privada.	Oficina Administrativa y Financiera Gestión Tecnológica	Sep-26
	Realizar retest para verificar la mitigación de vulnerabilidades y la aplicación de actualizaciones y parches de seguridad en sus sistemas de información.	Oficina Administrativa y Financiera Gestión Tecnológica	Oct-26

SGC	Diseño, creación y ejecución de una Plan de Continuidad Tecnológica, documento obligatorio para asegurar la recuperación y continuidad de los servicios ante incidentes mayores.	Oficina Administrativa y Financiera Gestión Tecnológica	Nov-26

8. 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 Seguridad y Privacidad: Actividades Ejecutadas / Actividades Planeadas (Meta: >90% a noviembre de 2026).

FUNCIONARIO	**NOMBRE**	**CARGO VINCULACION**	**FIRMA**
Elaborado por	Francisco Escobar Romero	Contratista TI	
Revisado por	Diana Agudelo	Contratista SGC	
Aprobado por	Comité Institucional de Gestión 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.			