PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 2.0

CORPORACIÓN AUTÓNOMA REGIONAL DEL RIO GRAN DE LA MAGDALENA
CORMAGDALENA

2025

Contenido

1. INTRODUCCIÓN

La Corporación Autónoma Regional del Río Grande de la Magdalena – CORMAGDALENA, en cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI versión 2025, la Resolución 500 de 2021, la Resolución

02277 de 2025, el Decreto 338 de 2022, la Ley 1581 de 2012, la Ley 1712 de 2014, y los lineamientos de la política de Gobierno Digital, adopta el presente Plan de Seguridad y Privacidad de la Información, como instrumento técnico y operativo para implementar el Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI, articulado al ciclo PHVA.

2. OBJETIVO

Definir las actividades, responsabilidades, controles, procesos, acciones de mitigación y mecanismos de mejora continua necesarios para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información administrada por CORMAGDALENA, conforme a los requerimientos del MSPI 2025 y la ISO/IEC 27001:2022.

2.1. OBEJTIVOS ESPECIFICOS.

✓ Implementar los 93 controles ISO/IEC 27001:2022, alineados al Anexo 1 del MSPI 2025.
✓ Ejecutar la estrategia institucional de seguridad digital conforme al Decreto 338/2022.
✓ Desarrollar la gestión integral del riesgo de seguridad y privacidad de la información.
✓ Fortalecer la protección de datos personales bajo Ley 1581 y responsabilidad demostrada.
✓ Establecer procedimientos de respuesta ante incidentes y reporte al CSIRT.
✓ Incorporar procesos de continuidad, recuperación y resiliencia tecnológica.
✓ Promover cultura de ciberseguridad, sensibilización y conciencia institucional.
✓ Mantener y mejorar el SGSPI mediante el ciclo PHVA.

3. ALCANCE

Este plan aplica a todos los procesos, dependencias, funcionarios, contratistas, proveedores y terceros que acceden, almacenan, procesan o transmiten

información de CORMAGDALENA, en cualquier formato, medio o plataforma física o digital.

4. DEFINICIONES

Aquí se mantiene la mayoría de definiciones existentes, pero se actualizan conceptos clave:

- **SGSPI:** Sistema de Gestión de Seguridad y Privacidad de la Información.
- **Incidente de Seguridad Digital:** Según Decreto 338/2022.
- **Infraestructura Crítica Cibernética (ICC):** Servicios esenciales protegidos por MinTIC.
- **Controles ISO/IEC 27001:2022:** 93 controles en 4 dominios.
- **Responsabilidad Demostrada:** Obligación de evidenciar cumplimiento (Ley 1581 / MSPI 2025).

(Opcional: puedo depurar la lista completa.)

5. MARCO NORMATIVO

• Ley 1581 de 2012, Decreto 1377 de 2013
• Ley 1712 de 2014
• Decreto 338 de 2022
• Resolución 500 de 2021
• Resolución 02277 de 2025
• MSPI 2025
• ISO/IEC 27001:2022

6. GOBERNANZA DEL SGSPI

El SGSPI se gestionará mediante el Comité Institucional, Responsable SPI, líderes de proceso, administradores tecnológicos y propietarios de activos.

7. ESTADO ACTUAL DEL SGSPI (Debe Actualizarse)

Con base en el Diagnóstico del Estado Actual del Área de Tecnologías de la Información realizado en 2024 por el contratista INFOTIC S.A., CORMAGDALENA presenta un nivel de madurez inicial en la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI, de acuerdo con los criterios establecidos en el Modelo de Seguridad y Privacidad de la Información – MSPI 2025 del MinTIC.

La evaluación evidencia que, si bien existen controles técnicos y administrativos implementados de manera parcial, estos no se encuentran articulados bajo un enfoque de sistema de gestión, ni alineados plenamente con la norma ISO/IEC 27001:2022, razón por la cual la entidad requiere fortalecer su marco de gobernanza, gestión de riesgos, documentación, monitoreo y mejora continua.

NIVEL DE MADUREZ MSPI 2025

De acuerdo con el diagnóstico, CORMAGDALENA se ubica en el Nivel 1 – Inicial, caracterizado por:

- Controles de seguridad implementados de forma reactiva y no sistemática.
- Ausencia de una gestión integral del riesgo de seguridad y privacidad.
- Falta de documentación formal del SGSPI.
- Baja articulación entre seguridad de la información, procesos misionales y toma de decisiones.
- Principales brechas identificadas (ISO/IEC 27001:2022)

DOMINIO A.5 – CONTROLES ORGANIZACIONALES

- Falta de formalización del SGSPI mediante actos administrativos.
- Roles y responsabilidades de seguridad no plenamente definidos.
- Ausencia de políticas y procedimientos operativos documentados.

DOMINIO A.6 – CONTROLES RELACIONADOS CON LAS PERSONAS

- Procesos de capacitación y sensibilización no estructurados.
- Bajo nivel de apropiación de responsabilidades en seguridad de la información.

DOMINIO A.7 – CONTROLES DE SEGURIDAD FÍSICA

- Controles físicos existentes sin documentación ni evaluación periódica.
- Ausencia de análisis de criticidad de sedes y activos físicos.

DOMINIO A.8 – CONTROLES TECNOLÓGICOS

- Implementación parcial de controles técnicos sin trazabilidad.
- Falta de monitoreo centralizado, gestión formal de vulnerabilidades y pruebas de continuidad.
- Enfoque de cierre de brechas

El presente Plan de Acción del SGSPI 2025–2027 se formula para cerrar progresivamente las brechas identificadas, permitiendo a CORMAGDALENA avanzar del Nivel 1 (Inicial) hacia niveles Intermedio y Avanzado del MSPI, mediante la implementación estructurada de controles, la gestión del riesgo, la adopción de la Declaración de Aplicabilidad (SoA), la mejora de capacidades institucionales y la consolidación de una cultura de seguridad y privacidad de la información.

ARTICULACIÓN CON EL DIAGNOSTICO DEL ESTADO ACTUAL

8. CONTROLES A IMPLEMENTAR

La entidad adopta los 93 controles ISO/IEC 27001:2022 en dominios A.5, A.6, A.7 y A.8, articulados al Anexo 1 del MSPI 2025. Su estado se documentará en el SoA.

9. PROCEDIMEINTOS OBLIGATORIOS A INCLUIR

- Gestión de Incidentes

(De acuerdo a ISO 27035 y Decreto 338)

- Gestión de Riesgos
(MSPI 2025 + ISO 27005)

- Continuidad – BCP + DRP
(ISO 22301 / ISO 27001 A.5 y A.8)

- Protección de Datos
(Ley 1581, principios y derechos)

- Vulnerabilidades y eventos
(Integración con CSIRT)

- Auditoría y mejora continua
(ISO 27001 A.5 + PHVA)

10. PLAN DE ACCIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (SGSPI)

10.1. OBJETIVO

Definir las actividades operativas, responsables, plazos, evidencias e indicadores necesarios para implementar, mantener y mejorar el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), dando cumplimiento a la Política General de Seguridad y Privacidad de la Información y cerrando las brechas identificadas en el Diagnóstico del Estado Actual TI 2024.

10.2. PLAN DE ACCION MSPI

10.2.1. GOBERNANZA Y LIDERAZGO DEL SGSPI

Actividad	Responsable	Plazo	Evidencia	Indicador
Formalizar el Responsable de Seguridad y Privacidad de la Información	Dirección General	Corto plazo (2025)	Acto administrativo de designación	Responsable SPI designado (Sí/No)
Formalizar el Comité de Seguridad de la Información dentro del Comité de Gestión y Desempeño	Secretaría General	Corto plazo (2025)	Acta de comité	% sesiones realizadas / programadas
Aprobar Política SPI versión 2.0	Dirección General	Corto plazo (2025)	Resolución de adopción	Política aprobada (Sí/No)

10.2.2. GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD

Actividad	Responsable	Plazo	Evidencia	Indicador
Definir metodología de gestión de riesgos MSPI	Responsable SPI	Corto plazo (2025)	Metodología aprobada	Metodología adoptada (Sí/No)
Identificar activos críticos de información	Responsables de proceso	Corto plazo (2025)	Inventario de activos	% activos identificados
Valorar riesgos de seguridad y privacidad	Responsable SPI	Mediano plazo (2025)	Matriz de riesgos	% riesgos valorados
Formular Plan de Tratamiento de Riesgos	Responsable SPI	Mediano plazo (2025)	PTR aprobado	% riesgos con tratamiento

10.2.3. INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Actividad	Responsable	Plazo	Evidencia	Indicador
Actualizar inventario de activos de información	Responsable SPI	Corto plazo (2025)	Inventario institucional	Inventario actualizado (Sí/No)
Clasificar activos según niveles de sensibilidad	Responsables de proceso	Mediano plazo (2025)	Matriz de clasificación	% activos clasificados
Identificar activos con datos personales	Responsable SPI	Mediano plazo (2025)	Registro de activos con datos	% activos con datos identificados

10.2.4. IMPLEMENTACIÓN DE CONTROLES ISO/IEC 27001:2022

Actividad	Responsable	Plazo	Evidencia	Indicador
Elaborar Declaración de Aplicabilidad (SoA)	Responsable SPI	Corto plazo (2025)	SoA aprobada	SoA elaborada (Sí/No)

Implementar controles dominio A.5 – Organización	Responsable SPI	Mediano plazo (2025–2026)	Procedimientos documentados	% controles A.5 implementados
Implementar controles dominio A.6 – Personas	Talento Humano / SPI	Mediano plazo (2025–2026)	Registros de capacitación	% personal capacitado
Implementar controles dominio A.7 – Seguridad física	Secretaría General	Mediano plazo (2026)	Registros de control físico	% controles A.7 implementados
Implementar controles dominio A.8 – Seguridad tecnológica	Área TI	Largo plazo (2026–2027)	Configuraciones técnicas	% controles A.8 implementados

10.2.5. GESTIÓN DE INCIDENTES DE SEGURIDAD

Actividad	Responsable	Plazo	Evidencia	Indicador
Diseñar procedimiento de gestión de incidentes	Responsable SPI	Corto plazo (2025)	Procedimiento aprobado	Procedimiento definido (Sí/No)
Articular gestión de incidentes con CSIRT	Responsable SPI	Mediano plazo (2025)	Protocolo de reporte	% incidentes reportados
Realizar simulacros de incidentes	Área TI / SPI	Largo plazo (2026–2027)	Informes de simulacro	Nº simulacros ejecutados

10.2.6. CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN

Actividad	Responsable	Plazo	Evidencia	Indicador
Elaborar BCP institucional	Responsable SPI	Mediano plazo (2025)	BCP aprobado	BCP elaborado (Sí/No)
Elaborar DRP tecnológico	Área TI	Mediano plazo (2025)	DRP aprobado	DRP elaborado (Sí/No)
Ejecutar pruebas de continuidad	Área TI / SPI	Largo plazo (2026–2027)	Informes de pruebas	Nº pruebas ejecutadas

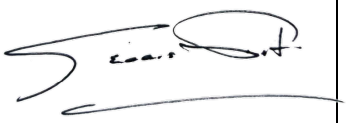
10.2.7. SEGUIMIENTO, AUDITORÍA Y MEJORA CONTINUA

Actividad	Responsable	Plazo	Evidencia	Indicador
Realizar auditorías internas SGSPI	Responsable SPI	Anual	Informes de auditoría	Nº auditorías realizadas

Revisar indicadores MSPI	Comité Institucional	Semestral	Actas de revisión	% indicadores cumplidos
Actualizar el Plan SPI	Responsable SPI	Anual o por cambio	Versión actualizada	Plan actualizado (Sí/No)

11. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
 Nombre: Alvin Ellis Nieto **Cargo:** Ingenieros TI Secretaria General	 Nombre: Cesar Rico Morales **Cargo: Profesional Universitario – Secretaria General**	 Nombre: Alvaro Redondo Castillo **Cargo: director ejecutivo** Fecha: 30-01-2026