Modelo de Seguridad y Privacidad de la Información – MSPI
Corporación Autónoma Regional del Atlántico – C.R.A.
Versión Institucional 2025**

1. Introducción

La Corporación Autónoma Regional del Atlántico – C.R.A., como autoridad ambiental en jurisdicción del Departamento del Atlántico, administra, controla y protege el ambiente, los recursos naturales renovables y el desarrollo sostenible en su territorio. En desarrollo de su misión, la entidad gestiona información ambiental estratégica, datos técnicos, estudios, expedientes electrónicos, bases de datos de control y vigilancia, información sensible de usuarios, empresas y proyectos sometidos a licenciamiento, así como sistemas de información de monitoreo ambiental.

Dada la criticidad de estos activos de información, y considerando la creciente exposición a incidentes digitales que pueden afectar la operación institucional, la C.R.A. adopta el Modelo de Seguridad y Privacidad de la Información – MSPI, establecido por el Ministerio TIC, con el objetivo de:

- Preservar la confidencialidad, integridad y disponibilidad de la información ambiental y administrativa.
- Garantizar continuidad de los servicios ambientales esenciales.
- Proteger activos de información misionales como el Sistema de Información Ambiental del Atlántico, expedientes electrónicos, permisos, licencias y reportes ambientales.
- Fortalecer la gestión institucional en el marco del Sistema Integrado de Gestión – SIG y del Modelo Integrado de Planeación y Gestión – MIPG.

Este documento constituye la adaptación oficial del MSPI a la estructura organizacional, procesos misionales, necesidades y lineamientos de la C.R.A.

2. Alcance institucional del MSPI en la C.R.A.

El MSPI aplica a:

- Todos los procesos del Modelo de Operación por Procesos de la C.R.A.
- Todas las dependencias de la entidad, incluyendo Dirección General, Subdirecciones, Oficinas Asesoras y Grupos Internos de Trabajo.

- Todos los sistemas de información institucionales, bases de datos, infraestructura tecnológica, servicios en la nube, plataformas web, aplicativos misionales y soportes documentales.
- Sedes administrativas y puntos de operación internos o externos.
- Funcionarios, contratistas, prestadores de servicios tecnológicos, encargados de tratamiento de datos personales y terceros que accedan a información institucional.

El alcance se prioriza inicialmente en los procesos misionales:

1. Gestión Ambiental
2. Evaluación y Seguimiento Ambiental
3. Control y Vigilancia
4. Ordenamiento Ambiental Territorial
5. Gestión del Recurso Hídrico
6. Planificación y Monitoreo Ambiental
7. Atención al Usuario y Trámites Ambientales

Posteriormente se extenderá a los procesos estratégicos y de apoyo, integrando gradualmente a toda la organización.

3. Contexto institucional

3.1 Contexto interno

- Misión: Administrar y proteger el ambiente y los recursos naturales renovables del Atlántico.
- Modelo de gobernanza: Direccionamiento estratégico desde la Dirección General, soporte en Subdirecciones técnicas y operación transversal desde Oficinas asesoras.
- Recursos tecnológicos: Centro de datos institucional, servicios virtualizados, plataforma SIGA, laboratorio ambiental, aplicativos de trámites, herramientas de monitoreo.
- Cultura organizacional: En proceso de fortalecimiento hacia la gestión basada en riesgos, gobierno digital y seguridad de la información.
- Procesos críticos: Licenciamiento ambiental, seguimiento ambiental, monitoreo, laboratorio, control y vigilancia.

3.2 Contexto externo

- Normatividad ambiental y digital aplicable a las autoridades ambientales regionales.
- Relación permanente con MinAmbiente, MinTIC, SINA, entes de control, usuarios y operadores ambientales.
- Aumento de ciberamenazas contra el sector público, especialmente entidades con infraestructura crítica ambiental.

4. Marco jurídico aplicable a la C.R.A.

Incluye normas TIC del MSPI y las ambientales propias de la autoridad ambiental:

- Ley 99 de 1993
- Ley 1712 de 2014 (Transparencia)
- Ley 1581 de 2012 (Protección de datos personales)
- Decreto 1076 de 2015 (Sector Ambiente y Desarrollo Sostenible)
- Decreto 338 de 2022 (Política de Seguridad Digital)
- Resolución 500 de 2021 MinTIC
- Resolución 1447 de 2018 (Sistemas de Información Ambiental)
- ISO/IEC 27001:2022
- CONPES 3995 de 2020 y CONPES 4144 de 2025
- Decreto 767 de 2022 (Gobierno Digital)

Se incorporan además lineamientos de MinAmbiente aplicables a gestión de información ambiental.

5. Roles y responsabilidades en la C.R.A.

5.1 Alta Dirección

Garantiza recursos, lidera la adopción del MSPI y preside comités institucionales.

5.2 Comité Institucional de Gestión y Desempeño

Recibe informes, aprueba políticas, analiza riesgos y toma decisiones estratégicas.

5.3 Responsable de Seguridad de la Información

Asignado por acto administrativo. Funciones:

- Coordinar implementación del MSPI.
- Supervisar riesgos de seguridad digital.
- Gestionar incidentes.
- Administrar controles y reportes al Comité.

Debe pertenecer a un área distinta a TI.

5.4 Oficina TIC

- Implementa controles tecnológicos del MSPI.
- Gestiona plataformas, actualizaciones, respaldo y continuidad del negocio.

5.5 Responsables de proceso

- Identifican activos de información y riesgos.
- Reportan incidentes.
- Custodian información bajo su proceso.

5.6 Usuarios, contratistas y terceros

Obligación de cumplir políticas, reportar incidentes y proteger información.

6. Identificación y clasificación de activos de información

La C.R.A. gestionará:

- Activos misionales:
    - Expedientes electrónicos ambientales
    - Estudios técnicos
    - Monitoreos
    - Laboratorio ambiental
    - SIGA
    - Trámites ambientales
- Activos administrativos:
    - Gestión humana: Humano,
    - Subdirección financiera: PCT
    - Secretaria General: Gestión documental - ORFEO

Cada activo se clasificará según confidencialidad, integridad y disponibilidad, siguiendo matriz institucional.

Se adopta el **Inventario de Activos de Información – C.R.A. 2025**.

7. Valoración y tratamiento de riesgos

La C.R.A. adopta:

- Metodología institucional de riesgos
- Criterios de probabilidad, impacto y apetito al riesgo
- Identificación de amenazas específicas:
    - Manipulación de expedientes ambientales
    - Explotación de vulnerabilidades en sistemas web
    - Ataques a infraestructura del SIGA y bases de datos
    - Pérdida o alteración de datos de monitoreo
    - Brechas de datos personales de usuarios ambientales

Se elabora matriz de valoración y plan de tratamiento anual.

8. Declaración de Aplicabilidad (SoA)

La C.R.A. adopta los controles aplicables de la ISO/IEC 27001:2022 y del MSPI. Cada control tendrá:

- Responsable
- Evidencias
- Frecuencia
- Nivel de implementación
- Observaciones

9. Plan de Seguridad y Privacidad de la Información – C.R.A.

Incluye:

1. Objetivos institucionales de seguridad

2. Acciones por cada fase del MSPI
3. Recursos requeridos
4. Cronograma anual
5. Medidas de cultura y apropiación digital
6. Plan de continuidad y recuperación
7. Indicadores estratégicos

10. Fase de Operación

La C.R.A. implementará:

- Controles físicos, lógicos y administrativos
- Gestión de incidentes
- Seguridad en servicios en la nube
- Gestión de proveedores
- Seguridad en el ciclo de vida del software
- Copias de seguridad
- Protección de infraestructura crítica de monitoreo ambiental
- Protección del laboratorio ambiental y sus sistemas

11. Evaluación del desempeño

Incluye:

- Auditorías internas semestrales
- Informes al Comité Institucional
- Revisión por la Dirección General
- Evaluación de indicadores de seguridad
- Seguimiento a brechas detectadas

12. Mejoramiento continuo

La Corporación Autónoma Regional del Atlántico – C.R.A. aplicará:

- Acciones correctivas
- Actualización permanente del plan de riesgos
- Lecciones aprendidas de incidentes
- Retroalimentación de usuarios
- Ajustes a políticas y procedimientos

13. Anexos institucionales

Se adjuntan:

1. Plantilla inventario de activos
2. Plantilla matriz de riesgos
3. Declaración de aplicabilidad
4. Procedimiento de gestión de incidentes
5. Formato de clasificación de activos
6. Mapa de procesos de la C.R.A. vinculado al MSPI
7. Roles y responsabilidades
8. Modelo de política institucional MSPI
9. Lista de sistemas de información de la C.R.A.
10. Lineamientos de gestión documental y seguridad digital