MANUAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN
EMPOCABAL ESP – EICE

---

1. OBJETIVO

Establecer el marco institucional para la gestión de la seguridad de la información en EMPOCABAL ESP–EICE, mediante la definición de políticas, lineamientos, responsabilidades y controles orientados a proteger los activos de información de la entidad.

---

2. ALCANCE

El Sistema de Seguridad de la Información aplica a:

- funcionarios de planta
- directivos
- contratistas
- proveedores con acceso a sistemas institucionales
- terceros que utilicen recursos tecnológicos de la entidad

Incluye todos los activos relacionados con:

- sistemas de información
- infraestructura tecnológica
- bases de datos
- redes institucionales
- documentos digitales institucionales

---

3. MARCO NORMATIVO

El Sistema de Seguridad de la Información se fundamenta en:

- Ley 1581 de 2012 – Protección de Datos Personales
- Ley 1712 de 2014 – Transparencia y Acceso a la Información
- Ley 594 de 2000 – Ley General de Archivos
- Decreto 1078 de 2015 – Sector TIC
- Modelo Integrado de Planeación y Gestión (MIPG)
- Lineamientos de Gobierno Digital del Gobierno Nacional
- Modelo de Seguridad y Privacidad de la Información (MSPI)

4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información en EMPOCABAL se basa en los siguientes principios:

Confidencialidad
La información solo podrá ser conocida por personas autorizadas.

Integridad
La información deberá mantenerse completa y protegida contra modificaciones no autorizadas.

Disponibilidad
La información deberá estar disponible cuando sea requerida para la operación institucional.

Trazabilidad
Las acciones realizadas sobre los sistemas deberán poder ser identificadas.

Responsabilidad
Cada dependencia será responsable del manejo de la información que produce.

---

5. ESTRUCTURA DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Seguridad de la Información de EMPOCABAL está conformado por los siguientes documentos institucionales:

1. Política Institucional de Seguridad de la Información.
2. Plan de Seguridad y Privacidad de la Información.
3. Modelo de Clasificación de la Información.
4. Protocolo de Gestión de Incidentes de Seguridad de la Información.
5. Política de Copias de Seguridad de la Información.
6. Política de Uso de Equipos Personales.
7. Inventario de Activos de Información.
8. Matriz de Riesgos de Seguridad de la Información.
9. Cláusula de Seguridad de la Información para contratos y contratistas.

6. RESPONSABILIDADES

Gerencia

• aprobar las políticas institucionales
• promover la cultura de seguridad de la información

Coordinación de Sistemas

• administrar la infraestructura tecnológica
• implementar controles técnicos de seguridad
• gestionar incidentes tecnológicos
• administrar accesos a sistemas institucionales

Dependencias

• custodiar la información que generan
• aplicar las políticas institucionales de seguridad

Usuarios

• utilizar adecuadamente los sistemas institucionales
• proteger sus credenciales de acceso
• reportar incidentes de seguridad

---

7. GESTIÓN DE RIESGOS

La entidad deberá identificar y gestionar los riesgos asociados a la seguridad de la información mediante:

• identificación de activos de información
• análisis de amenazas
• evaluación de vulnerabilidades
• implementación de controles de seguridad

---

8. GESTIÓN DE INCIDENTES

Los incidentes de seguridad serán gestionados conforme al **Protocolo Institucional de Gestión de Incidentes de Seguridad de la Información**, el cual define los procedimientos para la identificación, reporte, contención y recuperación de incidentes.

9. CONTROL DE ACCESOS

El acceso a los sistemas institucionales se gestionará mediante:

- credenciales personales
- perfiles de usuario
- autorización por parte de las dependencias responsables

---

10. COPIAS DE SEGURIDAD

La información institucional será protegida mediante procesos de respaldo definidos en la **Política de Copias de Seguridad de la Información**.

---

11. CAPACITACIÓN Y CULTURA DE SEGURIDAD

EMPOCABAL promoverá actividades orientadas a fortalecer la cultura de seguridad de la información entre funcionarios y contratistas mediante:

- capacitaciones
- difusión de políticas institucionales
- campañas de sensibilización

---

12. SEGUIMIENTO Y MEJORA

El Sistema de Seguridad de la Información será objeto de seguimiento institucional con el fin de:

- evaluar la efectividad de los controles implementados
- identificar oportunidades de mejora
- actualizar las políticas y procedimientos

---

13. VIGENCIA

El presente manual entrará en vigencia una vez sea aprobado por la **Gerencia de EMPOCABAL ESP – EICE** y deberá revisarse periódicamente o cuando se presenten cambios en la infraestructura tecnológica o en la normativa aplicable.

CONTROL Y APROBACIÓN DEL DOCUMENTO

Versión: 1.0
Fecha: Marzo 2026

Elaboró
John Jairo Castañeda
Coordinador de Sistemas

Revisó

Aprobó
Gerente
EMPOCABAL ESP – EICE