**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**
**EMPOCABAL ESP – EICE**

## 1. OBJETIVO

Establecer el plan institucional para fortalecer la seguridad y privacidad de la información en EMPOCABAL ESP–EICE, mediante la implementación de controles, políticas y procedimientos que permitan proteger los activos de información de la entidad y garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.

## 2. ALCANCE

El presente plan aplica a:

- Funcionarios de planta
- Directivos
- Contratistas
- Proveedores con acceso a información institucional
- Terceros que utilicen recursos tecnológicos de la entidad

Incluye todos los activos de información relacionados con:

- Sistemas de información
- Infraestructura tecnológica
- Bases de datos
- Equipos de cómputo
- Redes institucionales
- Documentos digitales institucionales

## 3. MARCO NORMATIVO

El Plan de Seguridad y Privacidad de la Información se fundamenta en:

- Ley 1581 de 2012 – Protección de Datos Personales
- Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública
- Ley 594 de 2000 – Ley General de Archivos
- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC

• Modelo Integrado de Planeación y Gestión – MIPG
• Lineamientos de Seguridad Digital del Gobierno Nacional
• Modelo de Seguridad y Privacidad de la Información (MSPI)

## 4. OBJETIVOS ESPECÍFICOS

• Fortalecer la protección de los activos de información institucional.
• Reducir riesgos asociados al manejo de información digital.
• Implementar buenas prácticas de seguridad informática.
• Garantizar el acceso controlado a la información institucional.
• Establecer mecanismos para la gestión de incidentes de seguridad.
• Cumplir con los lineamientos de Gobierno Digital.

## 5. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de seguridad de la información en EMPOCABAL se fundamentará 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 el desarrollo de las funciones institucionales.

Trazabilidad
Todas las acciones realizadas sobre los sistemas deberán poder ser identificadas.

Responsabilidad
Cada dependencia será responsable de la información que genera y administra.

## 6. COMPONENTES DEL PLAN

El Plan de Seguridad y Privacidad de la Información se implementará mediante los siguientes componentes:

1. Política Institucional de Seguridad de la Información
2. Modelo de Clasificación de la Información
3. Política de Uso de Equipos Personales
4. Protocolo de Gestión de Incidentes de Seguridad
5. Cláusulas contractuales de seguridad de la información
6. Control de accesos a sistemas institucionales
7. Gestión de copias de seguridad
8. Monitoreo de infraestructura tecnológica

## 7. RESPONSABILIDADES

Gerencia
Aprobar las políticas institucionales relacionadas con seguridad de la información.

Coordinación de Sistemas
Administrar la infraestructura tecnológica y aplicar controles técnicos de seguridad.

Dependencias
Garantizar el manejo adecuado de la información que generan.

Usuarios
Utilizar adecuadamente los sistemas institucionales y cumplir las políticas de seguridad.

## 8. GESTIÓN DE RIESGOS

La entidad promoverá la identificación y gestión de riesgos asociados a la seguridad de la información mediante:

- identificación de activos de información
- identificación de amenazas
- análisis de vulnerabilidades
- implementación de controles de seguridad

## 9. GESTIÓN DE INCIDENTES

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

## 10. CONTROLES DE SEGURIDAD

Entre los controles de seguridad institucional se contemplan:

- control de accesos a sistemas
- uso de credenciales personales
- implementación de antivirus
- copias de seguridad periódicas
- actualización de sistemas
- monitoreo de infraestructura tecnológica
- control de dispositivos externos

## 11. CAPACITACIÓN Y CULTURA DE SEGURIDAD

La entidad promoverá actividades de sensibilización orientadas a fortalecer la cultura de seguridad de la información entre funcionarios y contratistas.

Estas actividades podrán incluir:

- capacitaciones internas
- difusión de políticas institucionales
- campañas de buenas prácticas de seguridad digital

## 12. SEGUIMIENTO Y MEJORA

La implementación del presente plan será objeto de seguimiento institucional con el fin de:

- evaluar su efectividad
- identificar oportunidades de mejora
- actualizar los controles de seguridad

## 13. VIGENCIA

El presente Plan de Seguridad y Privacidad de la Información 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

**Política de Seguridad de la Información**
**EMPOCABAL ESP – EICE**

**1. Control de versiones**

| Versión | Fecha | Descripción del cambio | Responsable |
|---|---|---|---|
| 1.0 | Marzo 2026 | Creación del documento | Coordinación de Sistemas |

**2. Elaboración, revisión y aprobación**

| Rol | Nombre | Cargo | Firma | Fecha |
|---|---|---|---|---|
| **Elaboró** | John Jairo Castañeda | Coordinador de Sistemas | | |
| **Revisó** | | | | |
| **Aprobó** | | Gerente | | |

**3. Control de distribución**

Este documento es propiedad de EMPOCABAL ESP – EICE y su contenido está destinado para uso institucional.
La distribución de este documento será controlada por la Coordinación de Sistemas, quien garantizará que las versiones vigentes estén disponibles para las dependencias que lo requieran.
Las copias impresas de este documento se consideran copias no controladas, salvo que estén debidamente identificadas como tales.

**4. Vigencia y actualización**

La presente Política de Seguridad de la Información entra en vigencia a partir de su aprobación por la Gerencia de EMPOCABAL ESP – EICE y deberá ser revisada al menos una vez cada dos (3) años, o cuando se presenten cambios significativos en los procesos, en la infraestructura tecnológica o en la normativa aplicable.