PROTOCOLO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
EMPOCABAL ESP – EICE

1. OBJETIVO

Establecer el procedimiento institucional para **identificar, reportar, gestionar y responder ante incidentes de seguridad de la información**, con el fin de proteger los activos de información de EMPOCABAL ESP–EICE y garantizar la continuidad de los servicios institucionales.

2. ALCANCE

Este protocolo aplica a:

- Funcionarios de planta
- Contratistas
- Directivos
- Proveedores con acceso a sistemas
- Terceros que utilicen recursos tecnológicos institucionales

Incluye incidentes relacionados con:

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

3. DEFINICIÓN DE INCIDENTE DE SEGURIDAD

Se considera **incidente de seguridad de la información** cualquier evento que pueda comprometer:

- la **confidencialidad**
- la **integridad**
- la **disponibilidad**
- la **trazabilidad**

de la información institucional.

4. EJEMPLOS DE INCIDENTES

Se consideran incidentes, entre otros:

Acceso no autorizado

- Uso indebido de credenciales
- Acceso a carpetas restringidas
- Uso de cuentas de otros usuarios

Malware o virus

- Equipos infectados
- Archivos maliciosos
- Ransomware

Pérdida de información

- Eliminación accidental de archivos

- Daño de discos duros
- Pérdida de bases de datos

Fuga de información

- Envío de documentos sensibles a externos
- Uso de correos personales para información institucional
- Copia no autorizada de información

Fallas tecnológicas

- caída de servidores
- interrupción de sistemas
- pérdida de conectividad

5. RESPONSABLES

Coordinación de Sistemas

Será responsable de:

- evaluar el incidente tecnológico
- aplicar medidas de contención
- recuperar servicios tecnológicos
- analizar registros del sistema
- implementar controles preventivos

La Coordinación de Sistemas **no será responsable del contenido o veracidad de la información gestionada por las dependencias.**

Direcciones

Cada dirección será responsable de:

- custodiar la información que produce
- reportar incidentes inmediatamente
- colaborar en la investigación del incidente

Usuarios

Todo usuario deberá:

- reportar inmediatamente incidentes detectados
- no ocultar eventos de seguridad
- seguir las instrucciones de la Coordinación de Sistemas

6. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

Paso 1 – Identificación

El incidente puede ser detectado por:

- usuarios
- coordinadores de área
- sistemas de monitoreo
- la Coordinación de Sistemas

Paso 2 – Reporte
El incidente deberá reportarse **de inmediato a la Coordinación de Sistemas**, mediante:

- correo institucional
- llamada directa
- mesa de soporte técnico

La información mínima del reporte deberá incluir:

- usuario que reporta
- área
- equipo afectado
- descripción del incidente
- hora aproximada del evento

Paso 3 – Evaluación
La Coordinación de Sistemas evaluará:

- tipo de incidente
- alcance del problema
- riesgo para la información
- impacto en los servicios institucionales

Paso 4 – Contención
Se podrán aplicar medidas como:

- aislamiento del equipo afectado
- bloqueo de cuentas
- desconexión de red
- suspensión temporal de accesos

Paso 5 – Recuperación
Se ejecutarán acciones como:

- restauración desde copias de seguridad
- limpieza de malware
- recuperación de servicios
- restablecimiento de sistemas

Paso 6 – Registro del incidente
Todo incidente deberá registrarse con:

- fecha
- tipo de incidente
- área afectada
- acciones tomadas
- responsables

Este registro permitirá mejorar los controles de seguridad.

7. CLASIFICACIÓN DE INCIDENTES

Los incidentes se clasificarán en tres niveles:

Nivel Bajo

Impacto mínimo.

Ejemplo:

- archivo eliminado accidentalmente.

Nivel Medio

Afecta procesos internos.

Ejemplo:

- equipo infectado con virus
- acceso indebido a carpeta interna

Nivel Alto

Afecta la operación institucional o información sensible.

Ejemplo:

- fuga de información
- ransomware
- caída de servidores

8. MEDIDAS PREVENTIVAS

Para reducir incidentes se deberán aplicar:

- uso de antivirus actualizado
- credenciales personales
- copias de seguridad
- control de accesos
- actualización de sistemas
- cumplimiento de políticas de seguridad

9. CONFIDENCIALIDAD DEL INCIDENTE

La información relacionada con incidentes de seguridad **tendrá carácter reservado**, y solo podrá ser conocida por:

- Gerencia
- Coordinación de Sistemas
- Dependencias involucradas
- organismos de control cuando sea requerido

10. MARCO NORMATIVO

Este protocolo 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
- Modelo Integrado de Planeación y Gestión – MIPG
- Lineamientos de Seguridad Digital del Gobierno Nacional

11. VIGENCIA

El presente protocolo entrará en vigencia una vez sea aprobado por la **Gerencia de EMPOCABAL ESP – EICE** y deberá revisarse al menos cada **dos años** 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.