

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EMPOCABAL ESP – EICE

1. OBJETIVO

Identificar, analizar y gestionar los riesgos asociados a la seguridad de la información en EMPOCABAL ESP–EICE, con el fin de implementar controles que permitan reducir la probabilidad de incidentes y proteger los activos de información institucional.

2. ALCANCE

La presente matriz aplica a todos los activos de información relacionados con:

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

3. CRITERIOS DE VALORACIÓN

Probabilidad

Baja (1) – Poco probable

Media (2) – Puede ocurrir ocasionalmente

Alta (3) – Ocurre con frecuencia

Impacto

Bajo (1) – Afectación mínima al proceso

Medio (2) – Afecta la operación de un área

Alto (3) – Afecta la operación institucional o información sensible

Nivel de Riesgo

Se calcula multiplicando:

Probabilidad × Impacto

Resultado:

1 – 2 Riesgo Bajo

3 – 4 Riesgo Medio

6 – 9 Riesgo Alto

4. MATRIZ DE RIESGOS

Riesgo 1

Activo: Sistemas de Información

Amenaza: Acceso no autorizado

Vulnerabilidad: uso indebido de credenciales

Probabilidad: Media

Impacto: Alto

Nivel de riesgo: Alto

Controles

- uso de credenciales personales
- cambio periódico de contraseñas
- control de accesos por perfiles

Responsable: Coordinación de Sistemas

Riesgo 2

Activo: Equipos de cómputo

Amenaza: infección por malware

Vulnerabilidad: descarga de software no autorizado

Probabilidad: Media

Impacto: Medio

Nivel de riesgo: Medio

Controles

- antivirus actualizado
- restricción de instalación de software
- monitoreo de equipos

Responsable: Coordinación de Sistemas

Riesgo 3

Activo: Bases de datos institucionales

Amenaza: pérdida de información

Vulnerabilidad: fallas de hardware o eliminación accidental

Probabilidad: Baja

Impacto: Alto

Nivel de riesgo: Medio

Controles

- copias de seguridad periódicas
- almacenamiento seguro
- procedimientos de recuperación

Responsable: Coordinación de Sistemas – proveedores software externo

Riesgo 4

Activo: Información institucional

Amenaza: fuga de información

Vulnerabilidad: uso de correos personales o dispositivos externos

Probabilidad: Media

Impacto: Alto

Nivel de riesgo: Alto

Controles

- política de clasificación de información
- control de acceso a documentos
- sensibilización a usuarios

Responsable: Direcciones

Riesgo 5

Activo: Infraestructura tecnológica

Amenaza: interrupción de servicios

Vulnerabilidad: fallas eléctricas o problemas de red

Probabilidad: Baja

Impacto: Alto

Nivel de riesgo: Medio

Controles

- monitoreo de infraestructura
- mantenimiento preventivo
- respaldo de servicios

Responsable: Coordinación de Sistemas

Riesgo 6

Activo: Red institucional

Amenaza: conexión de dispositivos inseguros

Vulnerabilidad: uso de equipos personales sin controles

Probabilidad: Media

Impacto: Medio

Nivel de riesgo: Medio

Controles

- política de uso de equipos personales
- verificación de antivirus
- restricción de acceso a red

Responsable: Coordinación de Sistemas

5. TRATAMIENTO DE RIESGOS

Los riesgos identificados deberán gestionarse mediante:

- implementación de controles técnicos
- actualización de políticas de seguridad
- capacitación a usuarios
- monitoreo permanente de la infraestructura tecnológica

6. SEGUIMIENTO

La matriz de riesgos deberá revisarse:

- anualmente
- cuando se implementen nuevos sistemas
- cuando ocurran incidentes de seguridad relevantes

7. RESPONSABLES

Gerencia

Aprobar las políticas institucionales relacionadas con seguridad de la información.

Coordinación de Sistemas

Implementar controles tecnológicos para reducir los riesgos identificados.

Direcciones

Gestionar adecuadamente la información que producen y administran.

Usuarios

Cumplir las políticas de seguridad de la información.

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 tres (3) años, o cuando se presenten cambios significativos en los procesos, en la infraestructura tecnológica o en la normativa aplicable.