1. Propósito

Establecer un procedimiento integral para la identificación, evaluación, tratamiento, monitoreo y revisión continua de los riesgos relacionados con la seguridad de la información en **la organización**, asegurando su gestión efectiva y alineada con los objetivos del SGSI.

2. Alcance

Aplica a todos los procesos, activos, servicios y áreas incluidos en el **DOC 001 Alcance del SGSI**, considerando amenazas internas y externas, vulnerabilidades y posibles impactos.

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Cláusulas 6.1, 8.2 y 8.3.
- **PRO 001 Evaluación de Riesgos de Seguridad de la Información**.
- **PRO 002 Tratamiento de Riesgos de Seguridad de la Información**.
- **FOR 001 Registro de Evaluación de Riesgos**.
- **FOR 002 Registro de Evaluación y Tratamiento de Riesgos**.

4. Definiciones

Término	Descripción
Riesgo	Posibilidad de que una amenaza explote una vulnerabilidad causando un impacto negativo.
Tratamiento de riesgo	Medidas para modificar el riesgo mediante mitigación, transferencia, aceptación o evitación.
Monitoreo	Supervisión continua de los riesgos y la efectividad de las medidas implementadas.

5. Procedimiento

Paso	Actividad	Descripción	Responsable	Registro
1	Identificación	Detectar riesgos mediante análisis del contexto, activos y eventos previos.	Responsable SGSI / Equipos técnicos	FOR 001, informes
2	Evaluación	Analizar probabilidad e impacto para determinar nivel de riesgo.	Equipo de Riesgos	Matriz de riesgos (DOC 018)
3	Tratamiento	Seleccionar y aplicar medidas para controlar riesgos prioritarios.	Responsable SGSI / Áreas responsables	FOR 002
4	Monitoreo	Realizar seguimiento y reevaluación periódica de riesgos y controles.	Responsable SGSI	Reportes y registros
5	Revisión	Actualizar el proceso y registros en función de resultados y cambios.	Comité de Seguridad	Actas y FOR 017

6. Roles y Responsabilidades

Rol	Responsabilidades

Responsable del SGSI	Coordinar gestión integral de riesgos.
Equipo de Riesgos	Ejecutar análisis y seguimiento.
Áreas responsables	Implementar controles y reportar cambios.
Dirección General	Aprobar criterios y asignar recursos.

7. Indicadores de Desempeño (KPI)

Indicador	Fórmula	Meta
% riesgos gestionados	(Riesgos gestionados / Total identificados) × 100	100 %
% controles efectivos	(Controles efectivos / Total aplicados) × 100	≥ 95 %
Tiempo promedio de actualización	Días entre revisiones	≤ 365 días

8. Documentación Relacionada

- **FOR 001 Registro de Evaluación de Riesgos**.
- **FOR 002 Registro de Evaluación y Tratamiento de Riesgos**.
- **DOC 018 Matriz de Riesgo 2025**.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO