1. Propósito

Establecer un procedimiento integral para la identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos asociados a la seguridad de la información en **la organización**, asegurando su adecuada gestión y alineación con los objetivos del SGSI.

2. Alcance

Aplica a todos los activos, procesos, servicios y áreas incluidos en el **DOC 001 Alcance del SGSI**, considerando riesgos internos y externos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Cláusulas 6.1 y 8.
- **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 adverso.
Tratamiento de riesgo	Selección e implementación de medidas para modificar el riesgo.
Monitoreo	Supervisión continua y revisión periódica del estado del riesgo y controles aplicados.

5. Procedimiento

Paso	Actividad	Descripción	Responsable	Registro
1	Identificación	Detectar riesgos mediante análisis del contexto, activos, amenazas y vulnerabilidades.	Responsable SGSI / Equipos técnicos	FOR 001, informes
2	Análisis	Evaluar probabilidad e impacto para determinar nivel de riesgo.	Equipo de Riesgos	Matriz de riesgos (DOC 018)
3	Evaluación	Priorizar riesgos según criterios definidos y contexto organizacional.	Equipo de Riesgos	Matriz priorizada
4	Tratamiento	Definir y aplicar controles y medidas para mitigar o gestionar riesgos.	Responsable SGSI / Áreas responsables	FOR 002

5	Monitoreo	Supervisar la eficacia del tratamiento y cambios en riesgos.	Responsable SGSI	Reportes de seguimiento
6	Revisión	Actualizar registros y procedimientos basados en resultados y cambios.	Comité de Seguridad	FOR 017, actas

6. Roles y Responsabilidades

Rol	Responsabilidades
Responsable del SGSI	Coordinar todo el proceso de gestión de riesgos.
Equipo de Riesgos	Realizar análisis, evaluación y seguimiento.
Áreas responsables	Implementar controles y reportar estado.
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 entre revisiones	Días entre evaluaciones	≤ 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