1. Propósito

Establecer un procedimiento sistemático para identificar, evaluar, tratar y monitorear tanto los riesgos como las oportunidades que puedan afectar el logro de los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) en **la organización**, promoviendo la mejora continua y la resiliencia organizacional.

2. Alcance

Aplica a todos los procesos, actividades, activos, servicios y áreas definidos en el **DOC 001 Alcance del SGSI**, considerando factores internos y externos que puedan influir positiva o negativamente en la seguridad de la información.

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Cláusulas 4.1, 6.1 y 10.1.
- **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 un evento afecte negativamente los objetivos del SGSI.
Oportunidad	Circunstancia que puede mejorar el desempeño o eficacia del SGSI.
Tratamiento	Acciones para abordar riesgos u oportunidades mediante mitigación, aceptación, transferencia, evitación o explotación.

5. Procedimiento

Paso	Actividad	Descripción	Responsable	Registro
1	Identificación	Detectar riesgos y oportunidades a partir de análisis del contexto, partes interesadas, auditorías y eventos.	Responsable SGSI / Áreas	Informes, registros
2	Evaluación	Analizar la probabilidad, impacto y nivel de prioridad de riesgos y oportunidades.	Equipo de Riesgos	FOR 001, FOR 002
3	Planificación	Definir y aprobar estrategias y acciones para tratar riesgos y aprovechar oportunidades.	Dirección General / Comité de Seguridad	Planes documentados

4	Implementación	Ejecutar las acciones acordadas y asignar responsables y recursos.	Áreas responsables	Evidencias, informes
5	Monitoreo y seguimiento	Revisar la efectividad del tratamiento y actualizar registros.	Responsable SGSI	FOR 002 actualizado
6	Comunicación	Informar a las partes interesadas sobre el estado y resultados.	Responsable SGSI	Reportes y comunicaciones

6. Roles y Responsabilidades

Rol	Responsabilidades
Responsable del SGSI	Coordinar la gestión integral de riesgos y oportunidades.
Equipo de Riesgos	Realizar análisis y proponer tratamientos.
Dirección General	Aprobar planes y asignar recursos.
Áreas responsables	Implementar acciones y reportar resultados.

7. Indicadores de Desempeño (KPI)

Indicador	Fórmula	Meta
% riesgos y oportunidades gestionados	(Gestiones realizadas / Total identificados) × 100	100 %
Tiempo promedio de implementación	Σ días implementación / Nº acciones	≤ 60 días
% eficacia del tratamiento	(Tratamientos efectivos / Total) × 100	≥ 95 %

8. Documentación Relacionada

- **FOR 001 Registro de Evaluación de Riesgos**.
- **FOR 002 Registro de Evaluación y Tratamiento de Riesgos**.

Historial de Versiones

Versión	**Fecha**	**Asiento**	**Aprueba**
001	01.02.2024	Original	CEO