1. Propósito

Establecer el procedimiento sistemático para identificar, analizar y evaluar los riesgos relacionados con la seguridad de la información en **la organización**, permitiendo priorizar su tratamiento conforme a criterios definidos y alineados con los objetivos del SGSI.

2. Alcance

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

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Cláusulas 6.1 y 8.2.
- **POL 001 Política de Seguridad de la Información**.
- **DOC 018 Matriz de Riesgo 2025**.
- **PRO 002 Tratamiento de Riesgos de Seguridad de la Información**.
- **FOR 001 Registro de Evaluación de Riesgos**.

4. Definiciones

Término	Descripción
Riesgo	Posibilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo.
Activo	Elemento con valor para la organización que requiere protección.
Amenaza	Evento o acción potencial que puede comprometer un activo.
Vulnerabilidad	Debilidad que puede ser explotada por una amenaza.
Impacto	Consecuencia negativa sobre la organización si se materializa el riesgo.

5. Procedimiento

Paso	Actividad	Descripción	Responsable	Registro
1	Preparación	Definir el contexto, alcance y criterios para la evaluación.	Responsable SGSI	Documentos de planificación
2	Identificación de activos	Listar y caracterizar activos relevantes según **FOR 027 Inventario de Activos**.	Propietarios de activos	Inventario actualizado
3	Identificación de amenazas	Detectar amenazas potenciales internas y	Responsable SGSI / Equipos técnicos	Informe de amenazas

		externas para cada activo.		
4	Identificación de vulnerabilidades	Analizar debilidades existentes que puedan ser explotadas.	Responsable SGSI / Equipos técnicos	Informe de vulnerabilidades
5	Análisis del riesgo	Evaluar la probabilidad y el impacto de cada riesgo identificado.	Equipo de Riesgos	Matriz de riesgos preliminar
6	Evaluación del riesgo	Comparar los riesgos con los criterios definidos para priorizar.	Equipo de Riesgos	Matriz de riesgos priorizada (DOC 018)
7	Documentación	Registrar los resultados en el **FOR 001 Registro de Evaluación de Riesgos**.	Responsable SGSI	FOR 001 completo
8	Comunicación	Informar a la dirección y áreas involucradas sobre los riesgos prioritarios.	Responsable SGSI	Reporte de evaluación

6. Metodología

Se utiliza un enfoque cualitativo y cuantitativo que considera la probabilidad de ocurrencia y el impacto potencial, categorizando los riesgos en niveles (bajo, medio, alto). Se aplica la matriz de riesgos establecida en el **DOC 018 Matriz de Riesgo 2025**.

7. Roles y Responsabilidades

Rol	Responsabilidades
Responsable del SGSI	Coordinar la evaluación, consolidar resultados y reportar.
Propietarios de activos	Proveer información y validar activos y riesgos asociados.
Equipo de Riesgos	Realizar análisis técnico y priorización.
Dirección General	Revisar y aprobar criterios y resultados.

8. Indicadores de Desempeño (KPI)

Indicador	Fórmula	Meta
% activos evaluados	(Activos evaluados / Total activos) × 100	100 %
Nº riesgos identificados revisados anualmente	Conteo anual	100 % cobertura

Tiempo medio para reporte de evaluación	Horas / evaluación	≤ 72 h

9. Documentación Relacionada

- **FOR 001 Registro de Evaluación de Riesgos**.
- **DOC 018 Matriz de Riesgo 2025**.
- **PRO 002 Tratamiento de Riesgos de Seguridad de la Información**.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO