1. Propósito

Establecer un procedimiento sistemático para seleccionar y aplicar las medidas adecuadas que permitan tratar los riesgos identificados en la evaluación de riesgos de seguridad de la información, con el fin de reducirlos a niveles aceptables alineados con los objetivos de **la organización** y su SGSI.

2. Alcance

Aplica a todos los riesgos documentados en el **FOR 001 Registro de Evaluación de Riesgos** y priorizados en la matriz de riesgos (**DOC 018 Matriz de Riesgo 2025**), considerando activos, procesos y servicios incluidos en el **DOC 001 Alcance del SGSI**.

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Cláusulas 6.1 y 8.3.
- **POL 001 Política de Seguridad de la Información**.
- **PRO 001 Evaluación de Riesgos de Seguridad de la Información**.
- **FOR 002 Registro de Evaluación y Tratamiento de Riesgos**.
- **DOC 008 Estrategia de Seguridad de la Información**.

4. Definiciones

Término	Descripción
Tratamiento de riesgo	Selección y aplicación de medidas para modificar el riesgo.
Medidas de control	Acciones o mecanismos para mitigar, transferir, aceptar o evitar un riesgo.
Nivel aceptable de riesgo	Umbral definido por la organización para la aceptación del riesgo residual.

5. Procedimiento

Paso	Actividad	Descripción	Responsable	Registro
1	Revisión de riesgos	Revisar riesgos identificados y priorizados en la evaluación previa.	Responsable SGSI / Equipo de Riesgos	FOR 001, DOC 018
2	Selección de opciones de tratamiento	Considerar: mitigación, transferencia, aceptación o evitación según criterios y costos.	Equipo de Riesgos / Dirección General	Informe de opciones
3	Diseño de controles	Definir controles técnicos, organizativos y legales aplicables.	Responsable SGSI / Áreas Técnicas	Planes de control
4	Aprobación del plan	Presentar plan de tratamiento a la dirección para	Dirección General	Acta de aprobación

		aprobación formal.		
5	Implementación	Ejecutar las acciones y controles definidos para tratar los riesgos.	Áreas responsables	Evidencias de implementación
6	Monitoreo y revisión	Evaluar la efectividad del tratamiento y actualizar el registro de riesgos.	Responsable SGSI	FOR 002 actualizado
7	Comunicación	Informar a partes interesadas sobre el estado y resultados del tratamiento.	Responsable SGSI	Reportes internos

6. Opciones de Tratamiento de Riesgos

- **Mitigación:** Implementar controles para reducir probabilidad o impacto.
- **Transferencia:** Delegar riesgo a terceros mediante contratos o seguros.
- **Aceptación:** Asumir el riesgo residual dentro de niveles definidos.
- **Evitación:** Eliminar la causa del riesgo o cesar la actividad asociada.

7. Roles y Responsabilidades

Rol	Responsabilidades
Responsable del SGSI	Coordinar el proceso y mantener actualizado el registro de riesgos y controles.
Equipo de Riesgos	Analizar opciones y diseñar controles.
Dirección General	Aprobar planes y asignar recursos.
Áreas responsables	Implementar y mantener controles aplicados.

8. Indicadores de Desempeño (KPI)

Indicador	Fórmula	Meta
% riesgos tratados vs identificados	(Riesgos tratados / Total identificados) × 100	100 %
Tiempo promedio de implementación	Σ días implementación / Nº controles	≤ 60 días
% eficacia de controles	(Controles efectivos / Total controles) × 100	≥ 95 %

9. Documentación Relacionada

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

- **DOC 008 Estrategia de Seguridad de la Información**.

Historial de Versiones

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