

1. Propósito

Definir el procedimiento para planificar, implementar y supervisar los controles de seguridad de la información en **la organización**, asegurando que los controles sean efectivos para mitigar riesgos y cumplir con los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI).

2. Alcance

Aplica a todos los controles técnicos, físicos y administrativos establecidos para proteger los activos, procesos y servicios incluidos en el **DOC 001 Alcance del SGSI**.

3. Referencias Normativas y Documentales


- ISO/IEC 27001:2022 — Controles del Anexo A aplicables.
- **POL 001 Política de Seguridad de la Información.**
- **PRO 001 Evaluación de Riesgos.**
- **PRO 002 Tratamiento de Riesgos.**
- **FOR 005 Registro de Controles Implementados.**

4. Definiciones

Término	Descripción
Control de seguridad	Medida implementada para gestionar riesgos y proteger la información.
Planificación de controles	Selección y diseño de controles según riesgos y necesidades.
Ejecución de controles	Implementación operativa y monitoreo continuo de los controles.

5. Procedimiento

Paso	Actividad	Descripción	Responsable	Registro
1	Selección de controles	Basar la selección en la evaluación y tratamiento de riesgos, normativa y mejores prácticas.	Responsable SGSI / Equipo de Riesgos	Plan de controles
2	Diseño y documentación	Definir alcance, métodos, responsabilidades y criterios de éxito para cada control.	Responsable SGSI / Responsable TI	Documentación técnica
3	Aprobación	Validar y aprobar la planificación de controles por la dirección y comité de seguridad.	Dirección General / Comité de Seguridad	Actas de aprobación
4	Implementación	Ejecutar la instalación y configuración de controles técnicos, físicos y administrativos.	Responsable TI / Áreas involucradas	FOR 005 Registro de Controles Implementados

	Sistemas de gestión de la seguridad de la información	Rev. 1
	PRO 008 — Procedimiento de Planificación y Ejecución de Controles	Aprobada: 01.05.2024
	Crea: COF Aprueba: CEO	Página 2 de 2

5	Monitoreo y mantenimiento	Supervisar el funcionamiento, realizar pruebas y mantener actualizados los controles.	Responsable TI / Responsable SGSI	Informes de monitoreo
6	Evaluación de eficacia	Realizar auditorías y revisiones para verificar la efectividad de los controles.	Auditor Interno / Responsable SGSI	Informes de auditoría

6. Roles y Responsabilidades

Rol	Responsabilidades
Responsable del SGSI	Coordinar planificación y seguimiento de controles.
Responsable de TI	Implementar, monitorear y mantener controles técnicos.
Comité de Seguridad	Aprobar planes y evaluar resultados.
Auditor Interno	Verificar cumplimiento y eficacia.
Propietarios de activos	Colaborar en la implementación y seguimiento.

7. Indicadores de Desempeño (KPI)

Indicador	Fórmula	Meta
% controles implementados vs planificados	$(\text{Controles implementados} / \text{Total planificado}) \times 100$	100 %
% controles efectivos según auditoría	$(\text{Controles efectivos} / \text{Total evaluados}) \times 100$	≥ 95 %
Tiempo promedio para corrección de controles deficientes	$\Sigma \text{ días} / \text{N}^{\circ} \text{ controles}$	≤ 30 días

8. Cumplimiento y Control

El proceso es objeto de auditorías periódicas para garantizar la correcta planificación, ejecución y mantenimiento de los controles.

9. Mejora Continua

Los hallazgos de auditorías y monitoreo permiten actualizar y optimizar los controles y su gestión.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO