1. Propósito

Establecer un proceso sistemático y eficaz para la identificación, registro, análisis, tratamiento y seguimiento de no conformidades en el Sistema de Gestión de Seguridad de la Información (SGSI) de **la organización**, asegurando la implementación de acciones correctivas oportunas para eliminar causas y prevenir recurrencias.

2. Alcance

Este proceso abarca todas las no conformidades detectadas en los controles, procedimientos, procesos y actividades del SGSI, derivadas de auditorías, incidentes, revisiones por la dirección, evaluaciones internas o externas, y cualquier otra fuente.

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Cláusula 10.1 No conformidades y acciones correctivas.
- **POL 001 Política de Seguridad de la Información**.
- **FOR 008 Registro de No Conformidades**.
- **PSC 004 Auditoría Interna**.
- **PSC 005 Revisión por la Dirección**.

4. Descripción del Proceso

Actividad	Descripción	Responsable	Evidencia / Registro
Detección	Identificación de no conformidades mediante auditorías, incidentes o revisiones.	Auditor Interno / Usuarios / Responsable SGSI	Informes, registros FOR 008
Registro	Documentar la no conformidad en el **FOR 008 Registro de No Conformidades** con detalles, impacto y evidencias.	Responsable SGSI / Auditor Interno	FOR 008
Evaluación	Analizar la causa raíz y determinar la gravedad y alcance.	Responsable SGSI / Equipo de Mejora	Informe de análisis
Planificación de acciones	Definir acciones correctivas específicas, responsables y plazos.	Responsable SGSI / Áreas involucradas	Plan de acción documentado
Implementación	Ejecutar las acciones correctivas conforme a lo planificado.	Áreas responsables	Evidencias de implementación
Verificación	Confirmar la efectividad de las acciones y cierre de la no conformidad.	Auditor Interno / Responsable SGSI	Informe de cierre
Seguimiento	Monitorear para asegurar la no recurrencia y actualizar registros.	Responsable SGSI	Registros FOR 008 actualizados

5. Flujo del Proceso

1. Detección y reporte de no conformidad.

2. Registro formal y análisis de causa raíz.
3. Planificación y aprobación de acciones correctivas.
4. Implementación y seguimiento de acciones.
5. Verificación y cierre formal.
6. Retroalimentación y mejora continua.

6. Roles y Responsabilidades

Rol	Responsabilidades
Usuarios	Reportar no conformidades y colaborar en la investigación.
Auditor Interno	Detectar no conformidades y verificar acciones correctivas.
Responsable del SGSI	Coordinar el proceso, análisis y cierre.
Áreas responsables	Ejecutar y evidenciar acciones correctivas.
Comité de Seguridad	Supervisar seguimiento y eficacia del proceso.

7. Indicadores de Desempeño (KPI)

Indicador	Fórmula	Meta
Tiempo medio de cierre de no conformidades	Σ días cierre / Nº no conformidades	≤ 30 días
% de no conformidades con acciones verificadas	(No conformidades cerradas / Total) × 100	≥ 95 %
Nº de recurrencias de no conformidades	Conteo anual	Tendencia descendente

8. Cumplimiento y Control

El proceso está sujeto a auditorías regulares y revisión por la dirección, asegurando la eficacia y mejora continua del SGSI.

9. Mejora Continua

Los resultados y aprendizajes de las no conformidades fortalecen las políticas, controles y procedimientos de seguridad.

Historial de Versiones

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