

1. Propósito

Establecer el procedimiento para la comunicación oportuna, clara y estructurada de los incidentes de seguridad de la información en **la organización**, garantizando una respuesta eficaz y la minimización del impacto.

2. Alcance

Aplica a todos los empleados, contratistas, proveedores y terceros que detecten o sean afectados por incidentes relacionados con la seguridad de la información dentro del alcance definido en el **DOC 001 Alcance del SGSI**.

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Controles 5.24 a 5.27.
- **POL 001 Política de Seguridad de la Información.**
- **PRO 002 Gestión de Incidentes.**
- **FOR 031 Registro de Comunicado de Incidente y Seguimiento.**

4. Definiciones

Término	Descripción
Incidente de seguridad	Evento que compromete la confidencialidad, integridad o disponibilidad de la información.
Comunicación de incidente	Proceso formal de reporte y notificación de incidentes.
Equipo de Respuesta a Incidentes (ERI)	Grupo encargado de la gestión y resolución de incidentes.

5. Procedimiento

Paso	Actividad	Descripción	Responsable	Registro
1	Detección	Identificar el incidente o anomalía relacionada con seguridad.	Todos los usuarios	Reportes iniciales
2	Reporte inmediato	Comunicar el incidente al Responsable del SGSI o al ERI utilizando canales definidos (correo, línea telefónica, formulario digital).	Afectados / Testigos	FOR 031 Registro de Comunicado
3	Registro formal	Documentar detalles del incidente en el FOR 031 , incluyendo fecha, hora, descripción y personas involucradas.	Responsable SGSI / ERI	FOR 031 completo
4	Evaluación inicial	Clasificar el incidente según su impacto y urgencia para priorizar respuesta.	ERI	Informe preliminar
5	Comunicación interna	Informar a las áreas afectadas y dirección	Responsable SGSI	Comunicados internos

