



# **Procedimiento de contacto con grupos de interés especial**

**PROYECTO: SOFTWARE PARA LA CREACIÓN DE LA APLICACIÓN “ALERTA MUJER”**

**INTEGRANTES:  
LUIS DAVID CONDE SANCHEZ  
FREINIER CARDONA PEREZ  
ANDRES FELIPE CUELLAR GOMEZ**

**INSTRUCTOR:  
Javier Humberto Pinto Diaz**

**SERVICIO NACIONAL DE APRENDIZAJE –  
SENA  
ANALISIS Y DESARROLLO DE  
SOFTWARE – 3145555**

**2025**

## TABLA DE CONTENIDO

- 1. Propósito**
- 2. Alcance**
- 3. Matriz de Grupos de Interés Especial**
- 4. Procedimiento de Contacto y Escalabilidad**
  - 4.1 Escenario 1: Recolección de Inteligencia (Input)
  - 4.2 Escenario 2: Respuesta a un Incidente (Output)
- 5. Revisión y Mantenimiento**

# Procedimiento de Contacto con Grupos de Interés Especial (Control 5.6)

Versión	Fecha	Propietario del Proceso	Control ISO 27001
1.0	2025-10-02	Líder del Proyecto / Administrador de Operaciones (DevOps)	5.6 Contacto con grupos de interés especial

## 1. Propósito

Establecer los canales y protocolos de comunicación bidireccional con entidades y comunidades externas e internas relevantes. Este procedimiento tiene dos objetivos principales:

1. **Obtener Inteligencia de Amenazas (Control 5.7):** Recolectar información sobre vulnerabilidades y nuevas técnicas de ataque que puedan afectar la tecnología de "Alerta Mujer" (Android, servidor, BD).
2. **Coordinación de Respuesta:** Asegurar la escalabilidad adecuada en caso de un incidente grave, priorizando la **seguridad y la estabilidad de la infraestructura del SENA** y la protección de la imagen institucional.

## 2. Alcance

Este procedimiento es de aplicación obligatoria para el **Líder del Proyecto**, el **Docente Guía/Supervisor** y el **Administrador de Operaciones (DevOps)** del proyecto "Alerta Mujer".

## 3. Matriz de Grupos de Interés Especial

Los contactos se clasifican por su prioridad y su rol en el ciclo de seguridad:

<b>Categoría</b>	<b>Nombre del Grupo de Interés</b>	<b>Razón del Contacto</b>	<b>Frecuencia de Revisión</b>
<b>A. Interno Crítico</b>	<b>Equipo de Seguridad Informática del SENA</b>	Notificación obligatoria e inmediata en caso de ataque DDoS, intrusión en el servidor o uso anómalo de recursos de red institucional.	Trimestral (Verificación de contactos)
<b>B. Formación/Gobernanza</b>	Docente Guía / Supervisor del Proyecto	Revisión y aprobación de la respuesta a incidentes, y validación de las estrategias de mitigación.	Cada Incidente o Alerta Crítica
<b>C. Inteligencia Externa</b>	OWASP Mobile Security Project / NIST NVD (CVEs)	Obtención de boletines y alertas sobre vulnerabilidades en plataformas móviles (Android) y librerías de <i>backend</i> .	Semanal (Monitoreo)
<b>D. Respuesta Legal</b>	Policía Cibernética [Autoridad Local de Colombia]	Notificación oficial solo en caso de violación de la Ley de Protección de Datos Personales o ataque masivo, previa autorización del SENA.	Anual (Verificación de contactos)

## 4. Procedimiento de Contacto y Escalabilidad

El flujo de información se divide en dos escenarios: Recolección y Respuesta.

### 4.1. Escenario 1: Recolección de Inteligencia (Input)

1. **Monitoreo (DevOps):** El Administrador de Operaciones revisa las fuentes de la Categoría C (**Inteligencia Externa**) al menos una vez por semana.
2. **Análisis (DevOps/Líder):** Si se identifica una vulnerabilidad (CVE) aplicable a las librerías o al entorno de "Alerta Mujer" (ej. en la base de datos o en la versión de Android), se registra como un **Riesgo Prioritario** (Control 5.7).
3. **Diseminación Interna:** La amenaza y la mitigación recomendada se comunican inmediatamente al equipo de **Desarrollo** para su corrección (Control 8.27).

### 4.2. Escenario 2: Respuesta a un Incidente (Output)

Si el proyecto "Alerta Mujer" sufre una anomalía de seguridad o un ataque confirmado (ej. caída del servidor por DDoS o detección de intrusión), se sigue este protocolo estricto:

Fase	Tarea	Responsable	Contacto	Tiempo Máximo
1. Contención	Mitigación inicial y contención de la amenaza (ej. apagar el servidor, bloquear la IP).	DevOps	Ninguno (Acción Técnica Inmediata)	15 Minutos
2. Escalamiento Formativo	Notificación inmediata del incidente, su impacto potencial y las acciones tomadas.	Líder del Proyecto	Docente Guía (B)	30 Minutos
3. Notificación Institucional	Reporte del incidente al equipo interno	Líder del Proyecto	Equipo de Seguridad del SENA (A)	1 Hora

	para verificar el impacto en la red SENA.			
<b>4. Decisión Externa</b>	El Docente Guía y el Equipo SENA deciden si el incidente justifica notificar a las <b>Autoridades Legales (D)</b> .	Docente Guía / Líder	Policía Cibernética	Depende de la Gravedad

## 5. Revisión y Mantenimiento

1. **Verificación de Contactos:** La Matriz de Grupos de Interés Especial (Sección 3) debe ser validada por el Líder del Proyecto y el Docente Guía al inicio de cada nuevo ciclo formativo o **cada 6 meses**.
2. **Evidencia de Cumplimiento:** Los correos electrónicos o las actas de reuniones que demuestren el intercambio de información con los grupos A, B y C servirán como evidencia de que este control está aplicado y en funcionamiento.

LIDER DEL PROYECTO.

EQUIPO DE TRABAJO.

EQUIPO DE TRABAJO.