

**Procedimiento de Requisitos de Auditoría de Sistemas de Infiormación**

### 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

### Propósito y Alcance

* 1. **Propósito**

### Alcance

1. **Principio CRÍTICO: No Interfierencia**

### Procedimiento de Planificación y Ejecución de la Auditoría

* 1. **Fase de Planificación (Obligatoria)**

### Fase de Ejecución y Monitoreo

* 1. **Uso del Entorno de Prueba (Prioridad)**

### Evidencia de Cumplimiento

**Procedimiento de Requisitos de Auditoría de Sistemas de Infiormación (Control 5.34)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Propietario del Proceso** | **Control ISO 27001** |
| 1.0 | 2025-10-02 | Líder del Proyecto / Docente Guía | 5.34 Requisitos de auditoría de los sistemas de información |

# Propósito y Alcance

## Propósito

Establecer las directrices de planificación, autorización y ejecución para cualquier actividad de evaluación o auditoría (interna o externa) realizada sobre los sistemas de información del proyecto "Alerta Mujer". El objetivo principal es **proteger la integridad y la disponibilidad (RNF1.1)** de los sistemas de **Producción** durante las pruebas.

## Alcance

Aplica a:

1. Las **Pruebas de Resiliencia** y **Pruebas de Penetración Básicas** descritas en el **Control 5.33**.
2. Cualquier auditoría de seguridad o cumplimiento (ej. revisiones de código, escaneos de red) solicitada por el Docente Guía o el Equipo de Seguridad del SENA.
3. Todos los activos de Software (SW-001) y Hardware (HW-001) en producción.

# Principio CRÍTICO: No Interfierencia

El principio fundamental de este control es **evitar cualquier interrupción del servicio** que afecte a las usuarias, dada la naturaleza crítica de "Alerta Mujer".

|  |  |  |
| --- | --- | --- |
| **Acción Prohibida** | **Responsable de Monitoreo** | **Justificación** |
| Ejecutar herramientas de escaneo de vulnerabilidades sin notificar al **DevOps**. | DevOps | Riesgo de Denegación de Servicio (DDoS) involuntario. |
| Acceder a los datos  **CONFIDENCIALES (INF-**  **001)** de Producción sin el consentimiento formal del Docente Guía. | Líder del Proyecto | Riesgo de fuga o violación de la política de privacidad (Control 5.28). |
| Realizar cambios de configuración en **HW-001** (Servidor de Producción) durante una auditoría. | DevOps | Riesgo de inestabilidad y dificultad para rastrear la causa de un fallo. |

# Procedimiento de Planifiicación y Ejecución de la Auditoría

El **Líder del Proyecto** actúa como el punto de contacto entre el auditor/evaluador (que puede ser un Desarrollador o el Docente Guía) y el **DevOps** (dueño del sistema de Producción).

## Fase de Planifiicación (Obligatoria)

Antes de iniciar cualquier prueba, se debe completar un Plan de Auditoría formal:

* + 1. **Definición de Objetivos:** El Líder del Proyecto debe definir exactamente qué se va a probar (ej. "Solo el módulo de autenticación" o "Prueba de *backup* y restauración").
    2. **Definición del Alcance:** Especificar la IP, el rango de puertos, los activos (ej. solo BD, no el *front-end*) y el tipo de tráfico (ej. solo 10 peticiones/segundo) para limitar el impacto potencial.
    3. **Rol del Auditor:** Definir los permisos y credenciales que tendrá el auditor. Para pruebas de seguridad, se debe usar una cuenta de prueba sin privilegios administrativos (Control 8.2).
    4. **Ventana de Ejecución:** La auditoría o prueba **debe programarse fuera del horario pico de uso** (ej. de 1:00 AM a 5:00 AM) para minimizar el impacto. El Docente Guía debe

aprobar esta ventana.

## Fase de Ejecución y Monitoreo

* + 1. **Notificación:** El DevOps debe ser notificado al menos **48 horas** antes del inicio de la Ventana de Ejecución.
    2. **Monitoreo Activo:** Durante la prueba, el **DevOps** debe monitorear activamente la carga del servidor (CPU, Memoria, I/O de la BD) y la latencia para detectar inmediatamente cualquier indicio de sobrecarga o fallo.
    3. **Protocolo de Detención:** Si el monitoreo indica que el consumo de recursos supera el **75% de la capacidad** del servidor, el DevOps tiene la **autoridad inmediata** para detener la prueba, notificar al Líder del Proyecto y registrar el evento como un incidente (Control 5.24).

## Uso del Entorno de Prueba (Prioridad)

* + 1. **Requisito:** Siempre que sea posible, las pruebas de seguridad y auditoría se deben realizar en el entorno de **Pruebas o Staging** (Control 8.31) para replicar la producción sin arriesgar el servicio crítico.
    2. **Datos:** El auditor solo puede usar datos de prueba **anonimizados o enmascarados**

(Control 8.33).

# Evidencia de Cumplimiento

La evidencia de que el Control 5.34 está implementado incluye:

* + El **Plan de Auditoría** formal, firmado por el Líder del Proyecto y aprobado por el Docente Guía.
  + Los **registros de *logging*** del servidor y el monitoreo que demuestren que el DevOps estuvo activo durante la ejecución de la prueba.
  + El **Reporte Final de Auditoría**, que debe incluir la fecha, la hora de inicio/fin y la confirmación de que no hubo interrupciones del servicio.

LIDER DEL PROYECTO. EQUIPO DE TRABAJO. EQUIPO DE TRABAJO.