# INFORME TÉCNICO DE SEGURIDAD – FASE 3: PLAN DE RESPUESTA A INCIDENTES (NIST) Y SISTEMA DE GESTIÓN DE SEGURIDAD (ISO 27001)

Proyecto Final de Ciberseguridad

Elaborado por: Santiago Rivero

Fecha: Enero 2026

# 1. INTRODUCCIÓN

La presente Fase 3 del proyecto final tiene como objetivo el diseño de un Plan de Respuesta a Incidentes (PRI) basado en la guía NIST SP 800-61 Rev. 2, así como el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001.

Este informe se fundamenta en el incidente previamente analizado en las Fases 1 y 2, donde un servidor crítico fue comprometido mediante malas configuraciones de servicios expuestos. A partir de este escenario, se define cómo la organización debe prepararse, responder y recuperarse ante incidentes similares, y cómo establecer un marco de seguridad continuo para prevenir su recurrencia.

# 2. OBJETIVOS DE LA FASE 3

- Diseñar un Plan de Respuesta a Incidentes conforme al NIST SP 800-61.
- Establecer procedimientos claros para identificación, contención, erradicación y recuperación.
- Definir mecanismos de protección de datos críticos.
- Diseñar un SGSI alineado con ISO 27001.
- Reducir el impacto y la probabilidad de futuros incidentes de seguridad.

# 3. PLAN DE RESPUESTA A INCIDENTES (NIST SP 800-61)

## 3.1 Preparación

La fase de preparación es fundamental para reducir el impacto de un incidente de seguridad. La organización debe contar con:

- Políticas de seguridad documentadas y aprobadas.
- Inventario actualizado de activos críticos.
- Procedimientos de respaldo y recuperación.
- Capacitación básica del personal en seguridad.
- Herramientas de monitoreo y registro de eventos (logs).

Ejemplos de controles implementados:

- Centralización de logs mediante `journalctl`.
- Configuración de firewalls (UFW).
- Endurecimiento de servicios como SSH, Apache y MySQL.

## 3.2 Identificación

En esta etapa se detecta y confirma la ocurrencia de un incidente de seguridad.

Fuentes de detección:

- Logs del sistema (`journalctl`).
- Alertas de servicios de seguridad (Fail2Ban).
- Escaneos de integridad y malware (`chkrootkit`, `rkhunter`).
- Reportes de usuarios o administradores.

Ejemplos de comandos utilizados:

```bash
sudo journalctl -u ssh
sudo journalctl | grep "Accepted"
sudo chkrootkit

sudo rkhunter --check
```

## 3.3 Contención

El objetivo de la contención es limitar el alcance del incidente y evitar su propagación.

Acciones de contención a corto plazo:

- Deshabilitar servicios comprometidos.
- Bloquear direcciones IP maliciosas.
- Restringir accesos sospechosos.

Ejemplos prácticos:

```bash
sudo systemctl stop vsftpd

sudo ufw deny from <192.168.0.134>
```


## 3.4 Erradicación

En esta fase se eliminan las causas raíz del incidente.

Acciones de erradicación:

- Eliminación de usuarios no autorizados.
- Cambio de credenciales comprometidas.
- Corrección de configuraciones inseguras.
- Aplicación de parches y actualizaciones.

Ejemplos:

```bash
sudo deluser usuario_sospechoso
sudo mysql -u root -p

ALTER USER 'usuario'@'localhost' IDENTIFIED BY 'PasswordFuerte';
```

### 3.5 Recuperación

La recuperación busca restaurar la operación normal del sistema de forma segura.

Acciones realizadas:

- Restauración desde respaldos verificados.
- Reinicio controlado de servicios.
- Monitoreo reforzado posterior al incidente.

```bash
sudo systemctl start apache2

sudo systemctl start ssh
```

### 3.6 Lecciones Aprendidas

Tras la resolución del incidente, se debe realizar una revisión para:

- Documentar el incidente.
- Evaluar la efectividad de la respuesta.
- Mejorar controles y procedimientos.
- Actualizar el plan de respuesta.

## 4. RESPUESTA A UN ATAQUE SIMILAR FUTURO

Ante un ataque similar al analizado (explotación de servicios mal configurados), la organización:

- Detectaría el incidente mediante monitoreo y alertas.
- Aislaría los servicios afectados de inmediato.
- Aplicaría controles de hardening previamente definidos.
- Restauraría sistemas desde respaldos confiables.
- Notificaría a las partes interesadas según políticas internas.

Esto reduce significativamente el impacto y el tiempo de recuperación.

# 5. MECANISMOS DE PROTECCIÓN DE DATOS

## 5.1 Respaldos (Backups)

- Respaldos automáticos diarios de información crítica.
- Almacenamiento fuera del sistema principal.
- Pruebas periódicas de restauración.

## 5.2 Cifrado de Datos

- Cifrado de discos y bases de datos sensibles.
- Uso de protocolos seguros (SSH, HTTPS).

## 5.3 Controles de Acceso

- Principio de mínimo privilegio.
- Autenticación fuerte.
- Uso de claves SSH en lugar de contraseñas.

# 6. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI – ISO 27001)

## 6.1 Contexto de la Organización

La organización gestiona información crítica relacionada con operaciones internas y plataformas digitales. La pérdida de confidencialidad, integridad o disponibilidad podría generar impactos operativos y reputacionales.

## 6.2 Análisis de Riesgos

Identificación de riesgos:

- Accesos no autorizados.
- Exposición de servicios.
- Pérdida de datos.

Evaluación:

- Probabilidad: Media
- Impacto: Alto
- Riesgo: Alto

## 6.3 Políticas de Seguridad

- Política de control de accesos.
- Política de gestión de incidentes.
- Política de respaldos y recuperación.
- Política de actualizaciones y parches.

## 6.4 Controles ISO 27001 Aplicables (Anexo A)

- A.5 Políticas de seguridad de la información.
- A.8 Gestión de activos.
- A.9 Control de accesos.
- A.12 Seguridad en las operaciones.
- A.16 Gestión de incidentes de seguridad.

## 6.5 Plan de Mejora Continua

- Auditorías internas periódicas.
- Revisión anual del SGSI.

- Actualización de controles y políticas.
- Capacitación continua del personal.

# 7. CONCLUSIÓN

La Fase 3 consolida el proyecto final al proporcionar un enfoque estructurado y normativo para la gestión de incidentes y la protección de la información. La adopción de un Plan de Respuesta a Incidentes basado en NIST SP 800-61 y un SGSI conforme a ISO 27001 permite a la organización mejorar su postura de seguridad, responder de forma efectiva ante incidentes y reducir significativamente el riesgo de futuros compromisos.