

# Fase 3: Plan de respuesta de incidentes y certificación

## 1. Plan de Respuesta a Incidentes

El plan está diseñado para actuar con precisión ante cualquier compromiso, estructurándose en cuatro fases críticas:

### A. Detección y Análisis

**Monitoreo Centralizado:** Uso de herramientas **EDR** conectadas a un **SIEM** para obtener visibilidad total de la infraestructura.

**Sistemas de Prevención:** Implementación de **IDS/IPS** para identificar y bloquear intrusiones antes de que escalen.

**Vigilancia 24/7:** Monitoreo continuo de toda la infraestructura crítica para detectar anomalías en tiempo real.

### B. Contención

**Aislamiento:** Identificación rápida y aislamiento de cualquier equipo que muestre señales de compromiso para evitar el movimiento lateral.

**Preservación de Evidencia:** Realización de adquisiciones de datos "en caliente" para asegurar que la evidencia forense no se pierda al apagar el sistema.

### C. Erradicación

**Limpieza de Amenazas:** Eliminación total de componentes maliciosos, puertas traseras y tareas programadas por el atacante.

**Saneamiento de Identidad:** Ejecución de un cambio forzado de todas las contraseñas que pudieron verse afectadas durante el incidente.

## D. Recuperación

**Restauración Segura:** Los sistemas se recuperan a partir de copias de seguridad verificadas y libres de malware.

**Verificación Post-Incidente:** Antes de volver a producción, se realiza una auditoría exhaustiva del funcionamiento y seguridad del sistema.

## 2. Prevención de Recurrencia y Protección de Datos (DLP)

Para evitar que un ataque de fuerza bruta o de permisos mal configurados se repita, se han establecido los siguientes controles de seguridad de datos:

Mecanismo	Estrategia de Implementación
<b>Datos en Reposo</b>	Uso de cifrado de credenciales y aplicación de permisos restrictivos (como el <b>600</b> en archivos críticos).
<b>Datos en Tránsito</b>	Obligatoriedad del uso de canales cifrados como <b>SSH/SFTP</b> .
<b>Control de Acceso</b>	Eliminación completa del protocolo <b>FTP</b> por su falta de seguridad inherente.

## 3. SGSI conforme a ISO 27001

El **Sistema de Gestión de Seguridad de la Información (SGSI)** se apoya en políticas de continuidad y análisis de riesgos constantes:

### Política de Respaldos (Backups)

La continuidad del negocio se garantiza mediante una estrategia de respaldo automatizada y robusta:

**Frecuencia:** Copias diarias de la base de datos y respaldos semanales de los ficheros web.

**Automatización:** Implementación de tareas vía **cron** para asegurar la consistencia de los datos sin intervención humana.

**Regla de Oro (Off-site):** Al menos una copia de seguridad se almacena fuera del servidor principal para proteger la información contra ataques de **ransomware**.

## Monitorización Activa

Como medida de prevención proactiva, se ha desplegado **Fail2Ban** con políticas de bloqueo automático

**Umbral de Intrusión:** Bloqueo tras 3 intentos fallidos de inicio de sesión.

**Respuesta Automática:** Integración con `iptables` para rechazar IPs atacantes en tiempo real sin intervención manual.

---

Con la implementación de este Plan de Respuesta y el SGSI, la organización no solo corrige las vulnerabilidades del pasado, sino que establece un marco de mejora continua bajo estándares internacionales.