Informe Técnico

Proyecto Final de Ciberseguridad – Fase 3

Plan de Respuesta a Incidentes y SGSI (ISO/IEC 27001)

Autor: Carlos Navarro

Entidad: 4Geeks Academy

Fecha: 29/09/2025

Índice

1. Objetivo

Diseñar un Plan de Respuesta a Incidentes (PRI) robusto, alineado con NIST SP 800■61, y un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO/IEC 27001, para garantizar detección temprana, contención eficaz, erradicación completa, recuperación controlada y mejora continua tras cada incidente.

2. Plan de Respuesta a Incidentes (NIST SP 800-61)

2.1 Cuadro del Plan de Respuesta (NIST)

Fase	Objetivo	Acciones clave
Preparación	Establecer capacidades para gestionar incidentes.	• Definir CSIRT y roles. • Políticas y procedimientos aprobados. • SIEM/EDR/IDS, backups y pruebas. • Inventario de activos y clasificación. • Formación y simulacros (table■top).
Detección y análisis	Identificar eventos, confirmar incidentes y priorizar.	• Monitoreo SIEM 24/7 y correlación. • Revisión de logs (Apache, SSH, MySQL). • Clasificar severidad (Sev1■Sev4). • Preservar evidencia (forense).
Contención	Limitar el alcance e impacto del incidente.	• Aislar host/servicio afectado. • Reglas de firewall temporales. • Rotación inmediata de credenciales. • Segmentación y bloqueo IOC.
Erradicación	Eliminar causa raíz y artefactos maliciosos.	• Borrar backdoors/cuentas. • Parches de seguridad (Apache, kernel, etc.). • Reforzar configuración (SSH, Apache, MySQL).
Recuperación	Restaurar operaciones seguras y monitorizar.	• Restaurar desde backups verificados. • Validaciones de integridad y pruebas. • Monitoreo reforzado 14 días.
Lecciones aprendidas	Mejora continua del programa de seguridad.	• Informe post■mortem y causa raíz. • Actualizar políticas/runbooks. • Acciones preventivas y métricas (MTTD/MTTR).

2.2 Matriz de severidad y SLA (tiempos objetivo)

Severidad	Ejemplos	Detección	Contención	Erradicación	RTO
Sev1 (Crítico)	RCE, ransomware activo, fuga de datos confirmada	≤ 15 min	≤ 60 min	≤ 24 h	≤ 4 h
Sev2 (Alto)	Explotación limitada, escalado de privilegios	≤ 30 min	≤ 4 h	≤ 48 h	≤ 8 h
Sev3 (Medio)	Intentos de intrusión sin impacto	≤ 4 h	≤ 24 h	≤ 5 días	≤ 24 h
Sev4 (Bajo)	Eventos informativos / falsos positivos	≤ 1 día	Planificado	Planificado	N/A

2.3 RACI del equipo de respuesta

Actividad	Líder IR	CISO	SysAdmin	DevOps	Legal	PR/Comms	Soporte TI
Detección y análisis	R	A	C	C	-	I	I
Contención inicial	R	A	R	C	-	I	I
Erradicación técnica	C	A	R	R	-	I	I
Recuperación	C	A	R	R	-	I	I
Notificación regulatoria	I	A	-	-	R	C	I
Comunicaciones externas	I	A	-	C	C	R	I
Lecciones aprendidas	R	A	C	C	C	I	I

2.4 Flujo de escalado y comunicación

1) Analista SOC detecta evento → valida en SIEM y clasifica severidad.
2) Escala al Líder IR (Sev2+) y notifica a CISO (Sev1).
3) Líder IR convoca CSIRT, asigna responsables y arranca registro de evidencias.
4) PR/Comms y Legal se activan sólo si hay impacto reputacional o regulatorio.
5) Cierre formal: informe post■incidente, lecciones aprendidas y acciones preventivas.

3. Protección de datos y continuidad

• Backups: incrementales diarios y completos semanales, con pruebas de restauración mensuales.
• Cifrado: LUKS/BitLocker en reposo; TLS 1.3 en tránsito; gestión de claves centralizada.
• Acceso: mínimo privilegio, MFA, revisión trimestral de cuentas y secretos; rotación de claves.
• Continuidad: RPO 24h, RTO 4h; planes de BCP/DRP probados con simulacros semestrales.

4. SGSI (ISO/IEC 27001)

• Análisis de riesgos (ISO 27005): activos, amenazas, vulnerabilidades, impacto y tratamiento.
• Políticas: contraseñas y autenticación, uso aceptable, clasificación y manejo de la información.
• Operación: parches mensuales, escaneo de vulnerabilidades, auditorías internas anuales y KPIs (MTTD/MTTR).
• Controles: A.9 (accesos), A.12 (operativa), A.17 (continuidad), A.18 (cumplimiento y evidencias).

5. Entregables

• Diagrama de red (Packet Tracer/draw.io) con DMZ, WAF, bastión y segmentación.
• Informe de pentesting (Fase 2) y de incidente (Fase 1).
• Plan BCP/DRP actualizado y probado.
• Presentación ejecutiva para gerencia (resumen, impacto, roadmap).

6. Conclusión

El presente plan ofrece un marco operativo sin ambigüedades, con responsabilidades claras (RACI), objetivos de tiempo medibles (SLA) y un cuadro NIST completo y aplicable. Con ello, la

organización refuerza su capacidad para prevenir, detectar, responder y recuperarse de incidentes de seguridad con garantías.