Playbook de Respuesta ante Ransomware

TechNova Solutions S.L.

1. Introducción

Este documento describe el protocolo oficial de TechNova Solutions S.L. ante un ataque de ransomware. El propósito es garantizar una respuesta rápida, coordinada y efectiva para minimizar el impacto, restaurar la operativa sin ceder al chantaje y reforzar la seguridad posterior al incidente.

- Ámbito de aplicación: Sistemas, empleados y activos digitales.
- Frecuencia de revisión: Semestral o tras un incidente grave.

2. Escenario

Se detectan archivos cifrados, bloqueo del acceso a sistemas críticos y un mensaje de rescate.

Ejemplo:

El lunes a las 08:00h, varios empleados reportan que sus archivos presentan una extensión .locky. Al reiniciar los equipos, aparece una nota exigiendo 3 BTC por la recuperación de los datos.

3. Objetivos

- ☑Contener el ataque inmediatamente.
- ☑Recuperar la operativa sin pagar rescate.
- ☑Preservar evidencias para análisis forense.
- ☑Notificar a las autoridades si procede.
- ☑Reforzar la seguridad post-incidente.
- ☑Asegurar la comunicación efectiva durante la crisis.

4. Roles y Responsabilidades

Rol	Responsabilidad
Empleado	Reportar incidentes al área de IT.
IT	Aislar equipos afectados, ejecutar acciones de contención.
CISO / DPO	Coordinar respuesta, evaluar impacto y decidir notificación.
Legal	Asesorar legalmente y redactar notificaciones.
Infraestructura	Verificar sistemas y aplicar refuerzos.
Proveedor de Hosting	Bloquear tráfico malicioso y colaborar en mitigación.
Responsable de Backups	Restaurar datos desde copias limpias.
Comunicación	Coordinar mensajes internos y externos.

5. Procedimiento de Respuesta

Fase 1: Contención Inmediata

- ☑Aislar el sistema afectado (desconectar red/VPN).
- ☑Desactivar sincronización con backups.
- ☑Notificar al equipo de respuesta a incidentes.
- ☑Capturar evidencia forense (imágenes de disco, logs).

Fase 2: Análisis y Erradicación

- ☑Analizar el malware en un entorno seguro (https://any.run).
- ☑Eliminar amenazas con herramientas EDR/AV (ej. Bitdefender, CrowdStrike).
- ☑Revisar red interna y endpoints para detectar propagación.

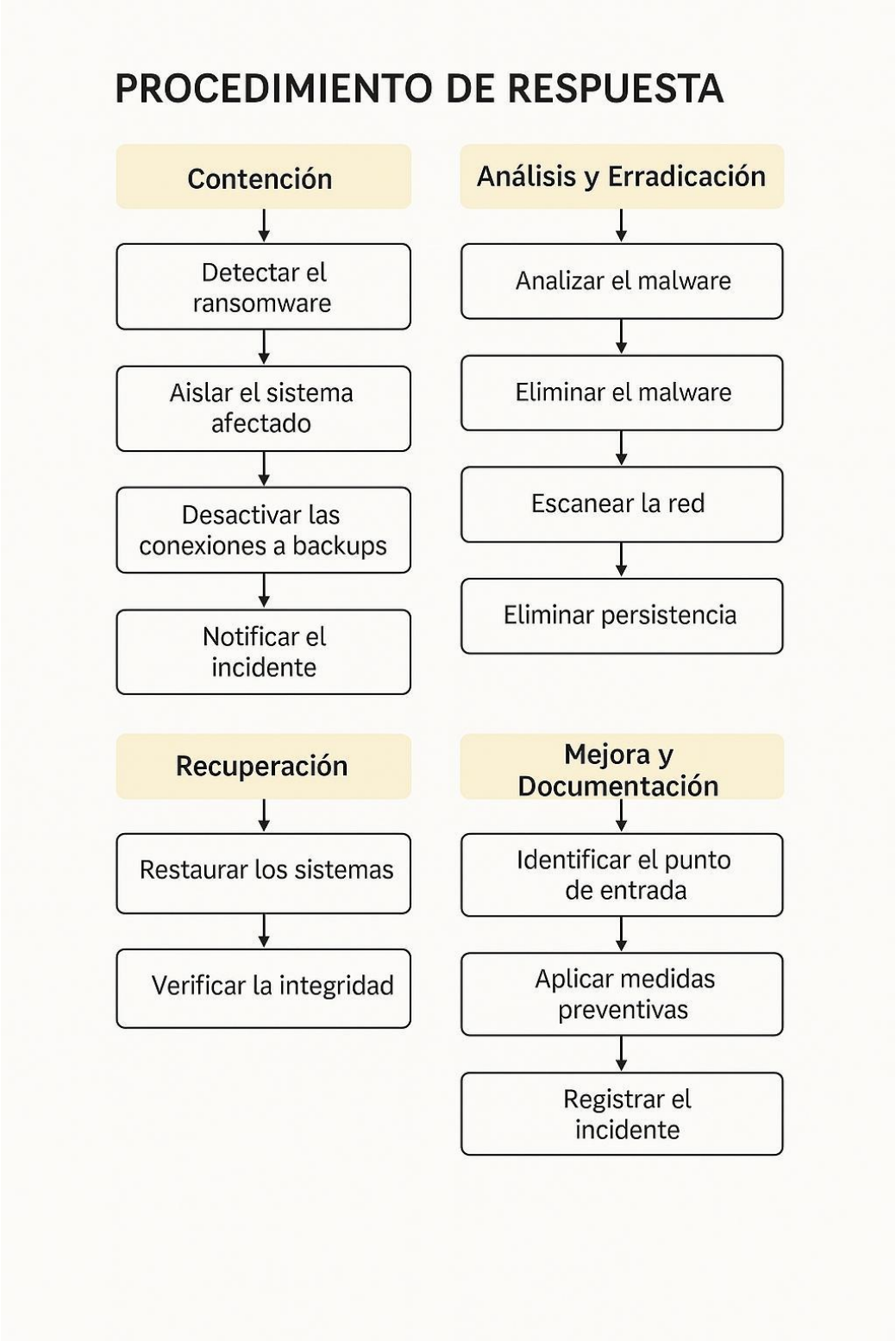
Fase 3: Recuperación

- ☑Restaurar datos desde backups limpios.
- ☑Verificar integridad y funcionamiento del sistema.
- ☑Reinstalar sistemas críticos si es necesario.

Fase 4: Mejora Continua

- ☑Identificar el punto de entrada del ataque.
- ☑Actualizar políticas de acceso y segmentación de red.
- ☑Documentar lecciones aprendidas y actualizar este playbook.

6. Diagrama de Flujo del Procedimiento



7. Herramientas Recomendadas

Fase	Herramienta	Función
Contención inmediata	Wazuh(SIEM)	Detecta la actividad sospechosa automáticamente (https://wazuh.com)
Contención inmediata	FTK Imager	Genera imágenes forenses de los discos infectados (https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81)
Contención inmediata	Firewall/Control de red (PfSense, Fortinet)	Aisla segmentos comprometidos inmediatamente (https://www.pfsense.org/) (https://www.fortinet.com/)
Análisis y erradicación	Any.Run (sandbox dinámica)	Análisis dinámico del malware en entorno seguro (https://any.run)
Análisis y erradicación	VirusTotal	Identificación del malware por firmas y hash (https://www.virustotal.com)
Análisis y erradicación	Bitdefender EDR	Detecta y elimina el ramsoware Locky en los endpoints (https://www.bitdefender.es)
Análisis y erradicación	EDR + Wazuh (revisión completa de edpoints y logs)	Se asegura de que no quede persistencia del atacante
Recuperación	Rubrik (Backup empresarial seguro)	Se restauran sistemas desde copias limpias anteriores al ataque https://www.rubrik.com)
Mejora continua	MXToolbox (cabeceras email)	Analiza posibles emails de phising inicial (https://mxtoolbox.com/EmailHeaders.aspx)

8. Notificación a Autoridades

Debe realizarse cuando:
- Se comprometan datos personales.
- El impacto sea grave o de carácter público.

Organismos:
- INCIBE-CERT: https://www.incibe-cert.es
- AEPD: https://www.aepd.es

Datos requeridos:
- Fecha, hora y responsable.
- Tipo de incidente.
- Medidas adoptadas.
- Nº de expediente.

Ejemplo ficticio de notificación detallada.

Fecha y hora del incidente	Lunes, 15 de abril de 2025, 08:00h (detección inicial)
Responsable del informe	María López, DPO - TechNova Solutions S.L.
Tipo de incidente	Ransomware Locky (SHA256: a3b1c5d8e9f...); archivos con extensión .locky
Alcance	20 estaciones de trabajo y 3 servidores de archivos cifrados
Metodología de detección	Alerta generada por Wazuh (regla ID 1001) a las 08:02h
Medidas adoptadas	- Aislamiento de red a las 08:05h- Captura forense con FTK Imager a las 08:10h- Análisis dinámico en Any.Run y VirusTotal- Eliminación de malware con Bitdefender EDR- Restauración desde backups limpios con Rubrik a las 10:30h
Artefactos y C2	Dominio malicioso hxxp://malicious.example.com; IP C2: 192.0.2.45
Evaluación preliminar	Posible exfiltración de datos personales de 500 clientes (nombres, e-mails, historial de servicio)
Número de expediente	INC-2025-0425-001

9. Prevención y Formación

- ☑Simulacros trimestrales de ransomware.
- ☑Formación continua sobre phishing y contraseñas.
- ☑Modelo de acceso Zero Trust y políticas de privilegio mínimo.
- ☑Autenticación multifactor (MFA) obligatoria.
- ☑Actualización regular de software y sistemas.

10. Bibliografía

1. INCIBE. (2024). Guía de actuación ante ransomware. https://www.incibe.es
2. CCN-CERT. (2023). Buenas prácticas ante ransomware. https://www.ccn-cert.cni.es
3. Digital Guardian. (s.f.). Ransomware Protection Guide. https://www.digitalguardian.com
4. Cofense. (s.f.). Threat Intelligence Platform. https://cofense.com