Playbook de Respuesta ante Fuga de Datos

1. Introducción

Este documento describe el protocolo oficial de TechNova Solutions S.L. ante una fuga de datos. Su propósito es garantizar una respuesta rápida, coordinada y eficaz para minimizar el impacto, contener la brecha de seguridad, cumplir con las obligaciones legales y prevenir futuras filtraciones.

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

2. Escenario

Se detecta una transferencia no autorizada de datos sensibles desde el servidor web hacia una IP externa.

Ejemplo:
El miércoles a las 10:00h, el equipo de seguridad detecta una actividad inusual en los logs del servidor. Una API expuesta públicamente fue explotada para extraer una base de datos que contiene información personal de clientes (nombres, correos electrónicos y direcciones).

3. Objetivos

☑Contener inmediatamente la fuga de información.
☑Proteger los datos afectados y evitar mayor exposición.
☑Preservar evidencias para análisis forense.
☑Notificar a los organismos reguladores y a los afectados si procede.
☑Reforzar los sistemas y procesos implicados.
☑Documentar el incidente y las lecciones aprendidas.

4. Roles y Responsabilidades

Rol	Responsabilidad
Empleado	Reportar actividad sospechosa al área de IT.
IT	Aislar el sistema afectado y colaborar con el análisis.
CISO / DPO	Coordinar respuesta, evaluar impacto y decidir notificación.
Legal	Asesorar legalmente y redactar comunicaciones oficiales.
Infraestructura	Auditar los sistemas implicados y aplicar refuerzos.
Proveedor Cloud/Web	Colaborar en la mitigación del incidente.
Comunicación	Coordinar mensajes internos y externos.

5. Procedimiento de Respuesta

Fase 1: Contención Inmediata

☑Aislar el sistema comprometido (firewall, desconexión de red).
☑Cambiar credenciales afectadas.
☑Revocar claves API expuestas.
☑Notificar al equipo de respuesta a incidentes.
☑Capturar evidencia (logs, volcados de memoria, tráfico de red).

Fase 2: Análisis y Erradicación

☑Revisar logs y tráfico para identificar el vector de ataque.
☑Usar herramientas forenses y EDR para detectar persistencia.
☑Eliminar accesos no autorizados.
☑Parchear vulnerabilidades detectadas.

Fase 3: Recuperación

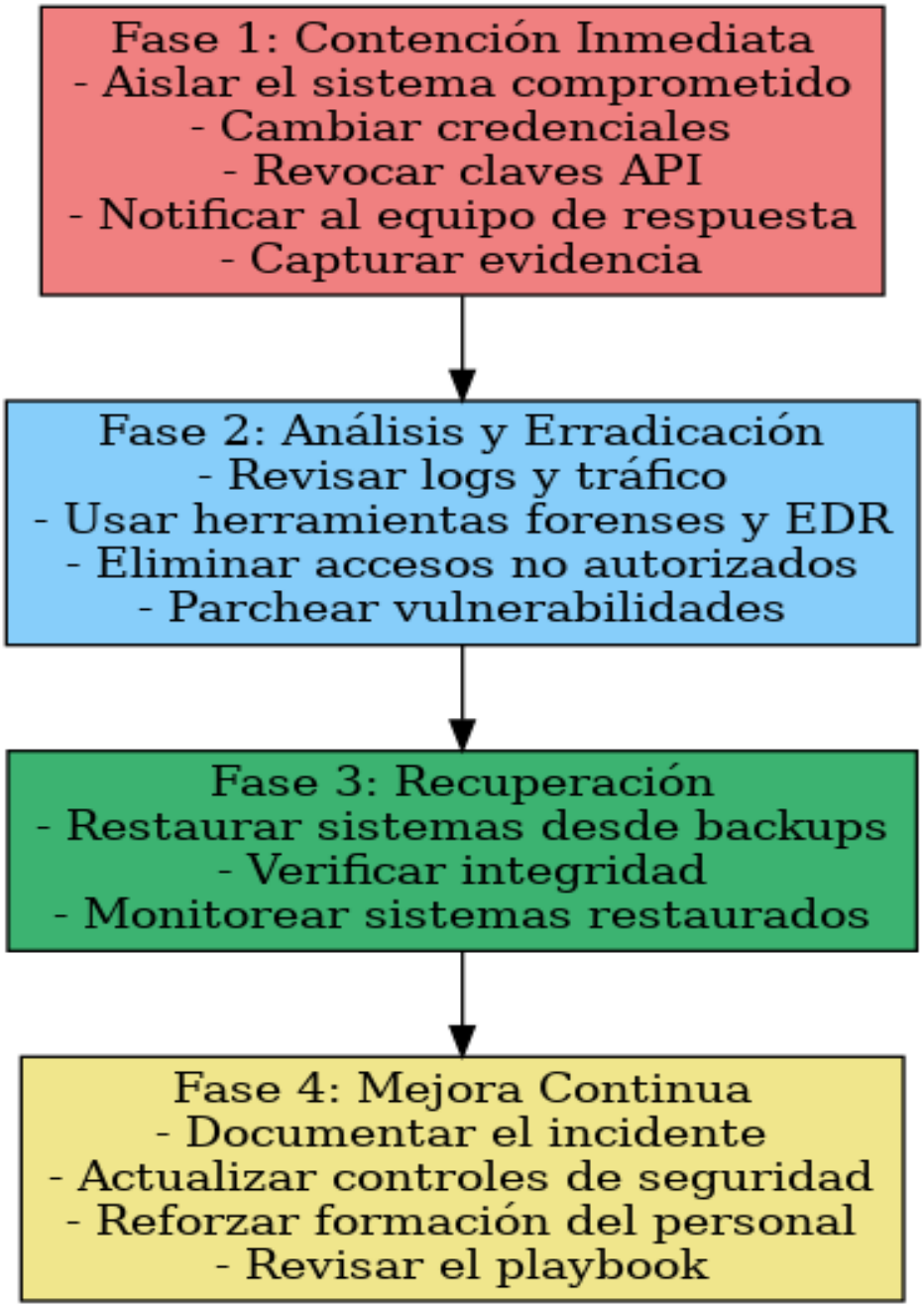
☑Restaurar sistemas desde backups previos al incidente.
☑Verificar integridad y seguridad antes de reactivar servicios.
☑Monitorear sistemas restaurados.

Fase 4: Mejora Continua

☑Documentar el incidente y las acciones tomadas.
☑Actualizar controles de acceso y seguridad.
☑Reforzar la formación del personal.
☑Actualizar este playbook si procede.

6. Diagrama de Flujo del Procedimiento

A continuación se muestra el diagrama de flujo del procedimiento de respuesta:



7. Herramientas Recomendadas

Fase	Herramienta	Uso	Enlace
Contención Inmediata	Wazuh	Detección inicial del incidente y alertas de seguridad	https://wazuh.com
Contención Inmediata	Bitwarden	Revocación y gestión segura de credenciales	https://bitwarden.com
Análisis y Erradicación	Wireshark	Análisis de tráfico de red y detección de fuga	https://www.wireshark.org
Análisis y Erradicación	Any.Run	Análisis dinámico del comportamiento de archivos sospechosos	https://any.run
Análisis y Erradicación	FTK Imager	Captura de evidencia forense (discos, memoria)	https://www.exterro.com/ftk-product-downloads/
Recuperación	Graylog	Revisión de logs para confirmar restauración limpia	https://www.graylog.org
Mejora Continua	OWASP API Security	Guías para reforzar seguridad de APIs vulnerables	https://owasp.org/www-project-api-security/

8. Notificación a Autoridades

Debe realizarse cuando:
- Se comprometan datos personales.
- La fuga tenga un impacto significativo o público.

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

Este es un ejemplo de cómo se debe documentar y notificar una fuga de datos personales conforme a las directrices de la AEPD e INCIBE.

Fecha y hora del incidente	Miércoles, 24 de abril de 2025, 10:00h
Responsable del informe	María López, DPO - TechNova Solutions S.L.
Tipo de incidente	Fuga de datos personales por explotación de API (SHA256: 9a3c5f...1de)
Alcance	Base de datos con 3.200 registros extraída (nombre, email, dirección)
Metodología de detección	Alerta generada por Wazuh (regla ID 3002) y análisis de logs en Graylog
Medidas adoptadas	- Aislamiento del servidor afectado- Cambios de credenciales- Revocación de API keys- Captura forense con FTK Imager- Análisis de tráfico con Wireshark- Notificación a AEPD e INCIBE
Artefactos y C2	IP origen: 203.0.113.77Dominio malicioso: hxxps://leakapi.example.com
Evaluación preliminar	Riesgo alto de afectación a la privacidad de los usuarios (nivel 4 según RGPD)

9. Prevención y Formación

☑Simulacros de fuga de datos semestrales.
☑Auditorías de seguridad periódicas.
☑Control de acceso basado en roles (RBAC).
☑Políticas de retención y cifrado de datos.
☑Formación continua sobre manipulación segura de datos.
☑MFA obligatorio para servicios críticos.

10. Bibliografía

1. INCIBE. (2024). Guía de actuación ante fugas de datos. https://www.incibe.es
2. AEPD. (2023). Brechas de seguridad. https://www.aepd.es
3. OWASP. (2024). Guía de seguridad para APIs. https://owasp.org
4. ENISA. (2023). Incident Handling Guide. https://www.enisa.europa.eu