Plan de Respuesta a Incidentes de Seguridad (IRP)

TechSys Solutions S.L.

Sede Barcelona

1. Introducción
Este plan define las fases, responsabilidades y procedimientos para detectar, responder y resolver incidentes de seguridad que puedan afectar la sede de Barcelona. Se integra con el SGSI, el Plan de Continuidad del Negocio y el DRP local.

2. Objetivos

- Minimizar el impacto operativo, legal y reputacional.
- Asegurar la respuesta coordinada ante incidentes.
- Documentar lecciones aprendidas y acciones de mejora.

3. Alcance
Aplica a todos los sistemas, empleados y datos gestionados desde la sede de Barcelona, incluyendo equipos locales, entornos virtualizados, nube y dispositivos en teletrabajo autorizados.

4. Clasificación de Incidentes

- Malware / Ransomware.
- Acceso no autorizado.
- Pérdida de datos / dispositivo.
- Phishing y suplantación.
- Vulnerabilidad explotada.
- Fallos de disponibilidad o denegación de servicio.

5. Fases de Respuesta

1. **Detección y notificación:** por SIEM o usuario. Canal seguro (correo seguro, Jira, interno).

2. **Clasificación:** por impacto (Bajo / Medio / Alto / Crítico) y urgencia.
3. **Contención:** según el tipo de incidente (aislar equipo, revocar accesos, etc).
4. **Erradicación:** limpieza de malware, cierre de vulnerabilidades.
5. **Recuperación:** restauración desde backups, configuración, validación.
6. **Análisis forense:** si aplica (uso de Volatility, Autopsy, etc).
7. **Informe y mejora:** informe post-incidente, revisión con RSI y Comité.

6. Roles y Responsabilidades

- **Responsable de Seguridad de la Información (RSI):** dirige la respuesta, comunica con Dirección.
- **Departamento IT:** ejecución técnica, contención, recuperación.
- **DPO:** notifica a la AEPD si hay datos personales.
- **Comité de Seguridad:** evaluación de impacto alto/crítico.
- **Usuarios:** primera línea de detección, deben informar inmediatamente.

7. Integración con SIEM y DRP

- Logs enviados al SIEM central para correlación y alerta automática.
- Las acciones de respuesta están coordinadas con el DRP (prioridad: VPN, correo, bases de datos).

8. RTO y RPO por Proceso Crítico *(según BIA)*

Proceso	**RTO (h)**	**RPO (h)**
Soporte telefónico y en vivo	≤ 8	≤ 4
Gestor de proyectos	≤ 8	≤ 8
Consultas y reclamos	≤ 24	≤ 8
Análisis empresarial	≤ 24	≤ 8

9. Comunicaciones en Incidentes

- Internas: correo seguro, canal Jira, notificaciones SIEM.
- Externas: comunicación oficial por parte del Responsable de Comunicaciones. Se puede requerir notificación a clientes o autoridades.
- Plantillas predefinidas para reportes internos y externos.

10. Plantillas

- **Registro de incidente:** ID, tipo, sistemas afectados, medidas tomadas, fecha, responsable.
- **Informe post-incidente:** resumen, causa raíz, impacto, resolución, acciones preventivas, lecciones aprendidas.

11. Mantenimiento del Plan

- Revisado anualmente o tras incidentes críticos.
- Simulacros semestrales con participación de IT y Seguridad.
