# 03_11_Formatos_Plantillas de registro de incidentes_Barcelona

**Resumen ejecutivo**
Como TechSys no nos ha facilitado ninguna plantilla de registro de incidentes en Barcelona que cumplan con la normativa, adjuntamos unas plantillas para que las utilicen.

**Objetivo**
Este documento se realiza para evaluar, mejorar y documentar las plantillas de registro de incidentes existentes para la sede de Barcelona.

**Documentación aportada**
TechSys solo ha aportado un registro de incidencias referente al período 2024-2025. Este registro, en Excel y con formato de tabla, resulta bastante rudimentario y no cumple con todas las especificaciones y requisitos exigidos por normativa y buenas prácticas de ciberseguridad en materia de gestión y trazabilidad de incidentes.

**Hallazgos principales**

- La plantilla entregada es básica: contiene campos elementales como identificador, fecha, sistema afectado y tipo de incidente, pero carece de apartados para detallar medidas correctivas, responsables de cierre, lecciones aprendidas y propuestas de mejora para el Sistema de Gestión de Seguridad de la Información.
- No existe una división clara entre la notificación inicial del incidente, las acciones técnicas tomadas y el informe final post-incidente.
- La trazabilidad de la resolución y el seguimiento queda incompleta, lo que pone en riesgo la capacidad de respuesta efectiva y dificulta la presentación de evidencia ante auditorías o ante requerimientos legales.

**Medidas de mejora propuestas**
Para subsanar estas carencias y contribuir a que TechSys cumpla con la regulación y las mejores prácticas internacionales (ISO 27001, RGPD y LOPDGDD), hemos elaborado unas plantillas de registro de incidentes estandarizadas, compuestas por tres bloques claves:

1. **Registro Inicial del Incidente**
    - Identificación del incidente, fecha/hora de detección, origen, sistema afectado, tipo y descripción del incidente, nivel de severidad, estado actual y responsable asignado.
2. **Acciones Técnicas y Contención**
    - Medidas de contención aplicadas, fecha/hora, estado de erradicación, detalles técnicos, restauración del servicio y verificación post-restauración.
3. **Informe Post-Incidente**
    - Causa raíz técnica y organizativa, impacto sobre la operación y la legalidad, tiempo de inactividad, lecciones aprendidas, cambios propuestos al SGSI, fecha de cierre y validación final por responsables y comités.

Estas plantillas permiten cubrir el ciclo completo de gestión de un incidente, desde la notificación inicial hasta el cierre y la mejora continua, asegurando trazabilidad, transparencia y alineación con lo exigido por normativas y estándares aplicables a empresas tecnológicas y consultoras.

**Conclusión**

Se recomienda la adopción inmediata de estas plantillas que les facilitamos como medida correctiva prioritaria. Este paso fortalecerá la gestión interna de incidentes, mejorará la capacidad de respuesta y permitirá cumplir con los requisitos regulatorios que la empresa debe observar en la sede de Barcelona.