“Al momento de la auditoría no se encontró documentado un plan de copias de seguridad. Tampoco encontramos ningún documento o flujo que nos indiquen como se realizan las copias de seguridad. Esto es totalmente necesario para conseguir la certificación de la ISO 27001 y para garantizar el buen funcionamiento. Por este motivo, hemos realizado una estructura de plan de copias de seguridad para la sede de Barcelona que es el siguiente:”

Plan de Copias de Seguridad

TechSys Solutions S.L. – Sede Barcelona

1. Introducción

- **Objetivo:** Garantizar la disponibilidad e integridad de los datos críticos mediante un sistema de copias de seguridad.
- **Alcance:** Aplica a servidores locales y virtualizados, bases de datos, sistemas cloud, estaciones de trabajo críticas y claves criptográficas gestionadas por HSM en la sede de Barcelona.
- **Normativas:** ISO 27001, RGPD.

2. Roles y Responsabilidades

- **Responsable del plan:** Departamento IT Barcelona.
- **Operadores de respaldo:** Técnicos designados.
- **Aprobación de restauraciones:** Responsable de Operaciones.
- **Usuarios:** Obligados a almacenar datos críticos en unidades sujetas a backup.

3. Alcance de las Copias

- **Incluidos:**
    - Servidores Cisco UCS C240 M6.
    - Servidor 1 (backup), Servidor 2 (apps).

    - Bases de datos de clientes, facturación y proyectos.
    - Documentación compartida en la nube.
    - Equipos clave de consultoría, soporte y dirección.
    - Claves y configuraciones gestionadas en HSM.

4. Frecuencia y Tipo de Backups

- Backup completo: semanal (sábado noche).
- Backup incremental: diario (lunes a viernes, 22:00).
- Backup crítico de bases de datos: cada 4 h.
- Retención: 5 versiones completas.

5. Herramientas y Procedimientos

- **Software:** Veeam Backup & Replication.
- **Destino:**
    - Local: Servidor 1 en Barcelona.
    - Off-site: nube corporativa geográficamente separada.
- **Cifrado:** Backups cifrados en tránsito y reposo mediante claves HSM. Uso de "key wrapping" para tokens USB.
- **Verificación:** Pruebas de restauración mensuales + restauración de claves semestral.

6. Restauración

- Prioridad:
    1. VPN y correo electrónico.

2. Bases de datos.
3. Documentación cloud.
4. Sistemas internos.

- Autorización previa requerida.
- Registro obligatorio en bitácora de incidentes.

7. Almacenamiento y Custodia

- **Ubicaciones:** Servidor 1 (on-premise) + nube segura.
- **Custodia física:** Acceso dual, control biométrico.
- **Custodia lógica:** Acceso restringido por rol (RBAC), etiquetado y versionado.

8. Revisiones y Simulacros

- Revisiones anuales o tras cambios críticos.
- Simulacros de restauración y fallos incluidos en DRP.

9. Integración con el SGSI

- Este plan se alinea con el Sistema de Gestión de Seguridad de la Información y el Plan de Continuidad del Negocio.
- Actualización coordinada con el RSI y el Comité de Seguridad.

10. Anexos

- Inventario de sistemas respaldados.
- Cronograma de tareas de backup.
- Formato de registro de restauraciones.
- Resultados de últimas pruebas de recuperación.