

# Logs y Evidencias para Auditoría Técnica

## TechSys Solutions S.L.

### Sede Barcelona

**Aclaración:**

No disponemos de información sobre logs recogidos pero en caso de tenerlos, se deberían gestionar siguiendo este documento.

#### 1. Objetivo

El objetivo de este documento es compilar registros y evidencias técnicas que respalden el cumplimiento de los controles de seguridad definidos por la organización. Estas evidencias servirán como soporte para auditorías técnicas internas o externas, específicamente en la sede de Barcelona.

---

#### 2. Alcance

Este informe abarca los sistemas, dispositivos, aplicaciones y servicios desplegados en la sede de Barcelona. Incluye logs generados por servidores, dispositivos de red, firewalls, sistemas IDS/IPS, estaciones de trabajo, soluciones antivirus y cualquier otro componente identificado como relevante en el mapa de activos.

---

#### 3. Fuentes de Log Incluidas

A continuación se relacionan las fuentes de log contempladas para la auditoría. Se debe especificar ubicación, rango temporal y tipo de eventos registrados.

Fuente	Ubicación/Dispositivo	Periodo Cubierto	Tipo de Evento

---

## **4. Evidencias Relevantes**

En esta sección se deben documentar las evidencias consideradas relevantes para la auditoría. Cada evidencia debe incluir una descripción del evento, el origen del registro, la fecha y hora del suceso, los sistemas implicados y las acciones asociadas.

---

## **5. Verificación de Integridad**

Se deben detallar los métodos aplicados para garantizar la integridad de los registros recopilados, como el uso de funciones hash o controles de acceso. Es importante asegurar que los archivos no fueron modificados desde su generación.

---

## **6. Análisis y Conclusiones**

Aquí se incluye una síntesis del análisis realizado sobre los logs recolectados. Deben destacarse hallazgos, desviaciones respecto a la política de seguridad, eventos sospechosos o críticos y cualquier recomendación técnica para su mitigación o seguimiento.