

# Cuestionario previo para recolección de información en proyectos de Gestión de la Seguridad con OSSIM



Áudea Seguridad de la Información, S.L.  
C/ Playa de Liencres, 2 Edif. Londres, Bajo, Ofic. 6  
28230 Las Rozas – Madrid  
Tel. 91 745 11 57 - Fax: 91 636 63 96  
<http://www.audea.com>  
[audea@audea.com](mailto:audea@audea.com)

## 1. Formulario de Dimensionamiento

### 1.1. Tipo de Proyecto

La solución de Seguridad Gestionada de Áudea incluye 3 tipos de funcionalidades. Es necesario detectar cuales de ellas son necesarias para decidir el tipo de proyecto.

Las funcionalidades son:

1. **SIM: Análisis de Seguridad.** El SIM incluye el motor de correlación, cuadros de mando y consolas para el análisis de la seguridad. El SIM almacena en base de datos SQL teniendo una respuesta rápida pero un almacenamiento limitado (2 a 4 semanas de logs).
2. **SEM: Almacenamiento Masivo Legal.** El SEM permite almacenar grandes volúmenes de datos (años de logs o Terabytes) y almacena los logs en formato natural y con firma digital sirviendo como evidencia legal. Las consultas al SEM pueden ser lentas.
3. **Sondas: Detectores de Seguridad.** Tanto el SIM como el SEM se alimentan de logs de los sistemas del cliente y/o de las Sondas de OSSIM. Las sondas incluyen detectores y monitores que analizan el tráfico de la red.

Funcionalidad	Sí / No
<b>SIM</b>	
<b>SEM</b>	
<b>Sonda</b>	



### 1.3. Recolección

Los sistemas a recolectar serían:

Nombre de la Oficina – Dirección Física	Nombre del Producto	Versión	Logs Diarios	Throughput Medio
			En Mbps	En Mbps

#### Instrucciones/Notas

- Todos los datos son estimativos para permitir dimensionar el hardware, no siendo necesario un dato exacto.
- En caso de no contar con el dato de Logs Diarios será necesario contar con el dato de Throughput Medio