# Centros de Operaciones de Ciberseguridad

## Ningún organismo escapa hoy de la amenaza de un ciberataque

En cuestión de minutos una organización puede ser víctima del robo y destrucción de la información de toda su entidad.

Las pérdidas y la repercusión que para una organización tendría ser víctima de un ciberincidente podrían ser irreversibles.

Los desafíos y amenazas en ciberseguridad son cada vez más numerosos y complejos, técnicamente más avanzados y con mayor capacidad de impacto.

Cualquier organización debe estar preparada para prevenir, detectar y responder a un posible ciberataque.

## SOC: ciberseguridad integral y horizontal

Los Centros de Operaciones de Ciberseguridad (SOC) son la respuesta a este paradigma. Proporcionan servicios horizontales de prevención, detección, cibervigilancia, protección y respuesta a todas las áreas de una organización y ante cualquier tipo de amenaza.

La implementación de los SOC ha de ser una prioridad estratégica para cualquier organismo de la Administración Pública como medida urgente para reforzar sus políticas y estrategia de seguridad.

## SOC Entidades Locales

La arquitectura y dimensión de los Centros de Operaciones de Ciberseguridad (SOC) es flexible y atiende al tipo de organización en la que se integra: pequeñas entidades o vSOC (virtual).

El objetivo de los SOC Locales es dar seguridad de forma centralizada a conjuntos de organismos o ayuntamientos pequeños.

## Red Nacional de SOC

Todos los Centros de Operaciones de Ciberseguridad que se desplieguen en este ámbito formarán parte de la Red Nacional de Centros de Operaciones de Ciberseguridad, en la que el CCN ya está trabajando, y que integrará a una amplia tipología de SOCs.

La coordinación de todos los SOCs integrados en esta red nacional se llevará a cabo a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

## SUPUESTO DE INSTALACIÓN Y DESPLIGUE DE UN SOC ENTIDADES LOCALES

Centraliza y ofrece servicios de ciberseguridad horizontal a un máximo de **20 organismos***

Cubre la ciberseguridad de los puestos de trabajo de **5.000 usuarios**

| | Servicios iniciales | Servicios avanzados |
|---|---|---|
| Tipo de **servicios** | • Auditoria inicial<br>• Revisión<br>• Formación de equipo de seguridad<br>• Instalación de soluciones y SW de defensa<br>• Instalación de solución específica de protección contra el ransomware<br>• Apoyo para la adecuación al ENS<br>• Equipo de búsqueda de incidentes de seguridad | Servicios del SOC Inicial<br>+<br>• Implementación de listas blancas<br>• Instalación de herramienta avanzada de detección de anomalías en equipos de usuario<br>• Auditorías recursivas y de código<br>• Servicio de monitorización de los sistemas<br>• Vigilancia digital<br>• Apoyo a la implementación del ENS |
| **Coste** aproximado y orientativo de instalación | **600.000 €** | **1.000.000 €** |
| **Coste** servicio anual | **150.000 €** | **250.000 €** |

* El coste asociado a cada SOC no varía en función del número de organismos al que dé servicio. Es decir, dar servicios de ciberseguridad a 20 organismos tendría un coste similar que ofrecerlo solo a dos.