

SOC-T (Centro de Operaciones de Seguridad Transfronterizo)



Situación actual de ciberseguridad.



Vulnerabilidades principales

- La mayoría de las PYMES carece de sistemas de prevención sólidos
- Gran parte de las organizaciones considera que su personal no tiene formación en ciberseguridad
 - Muchas usan tecnologías sin actualizar
- Son objetivo frecuente para atacar a empresas mayores a través de la cadena de suministro

Tendencias de amenazas

- Aumento del phishing avanzado: afecta a más de la mitad de los usuarios, y es la principal preocupación
 - Aparición de nuevas operaciones de ransomware como servicio
 - Crecen los ataques a proveedores en cadenas de suministro.
 - Se utiliza IA para lanzar ataques más sofisticados.

¿Qué vamos a aprender?

1. ¿Cómo proteger el futuro digital de su negocio?

2. Enfoque en NIS2 y GDPR



Nuestro Mundo Digital: Oportunidades y Riesgos Inevitables

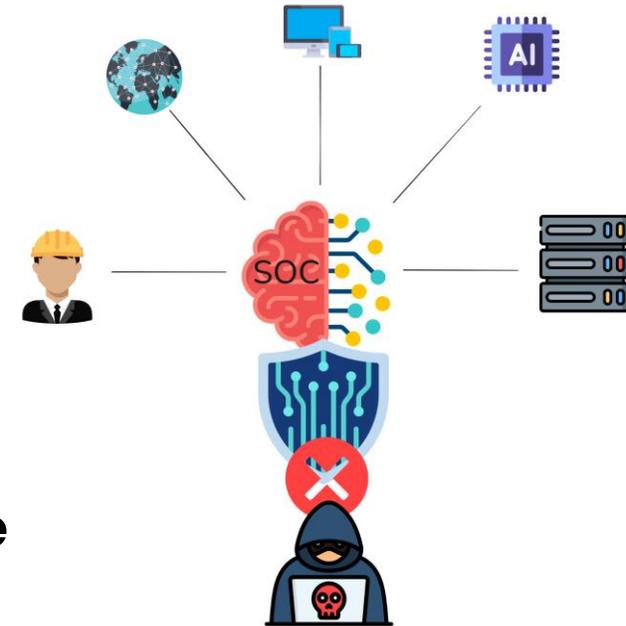


- Las empresas dependen fundamentalmente de la información y la tecnología para su funcionamiento diario
- La transformación digital ha expandido el panorama de amenazas
- Incremento constante de ciberataques sofisticados, con preocupación por el phishing avanzado y el ransomware
- Pérdida de información o acceso a ella puede paralizar su negocio



Entendiendo el SOC: Un Centro de Operaciones de Seguridad

- Un SOC (Security Operations Center) es un equipo de profesionales especializados
- Utiliza tecnologías avanzadas para monitorear, detectar, analizar y responder a amenazas en tiempo real
- Su misión principal es actuar como la primera línea de defensa contra ciberataques que podrían paralizar un negocio
- Protege los activos digitales de una organización, como sistemas, redes y datos, mediante una supervisión continua

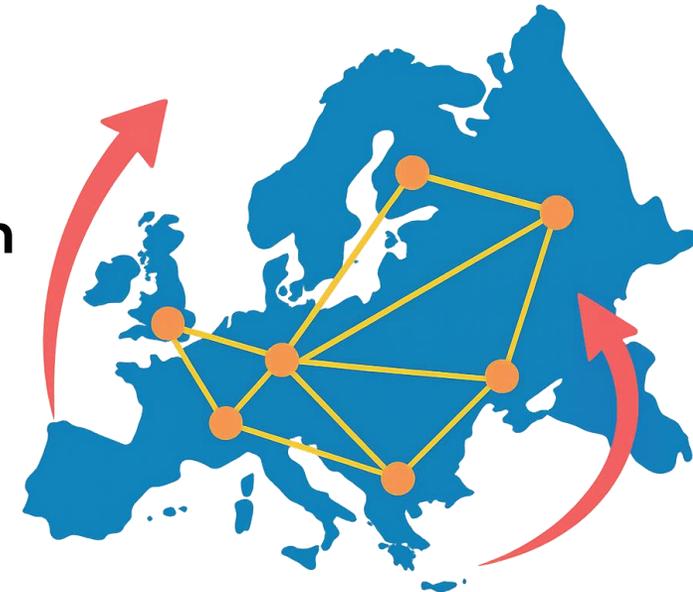




La Ciberseguridad No Conoce Fronteras: El Impulso de la UE



- **A pesar de los SOC tradicionales, Europa sufrió una "pandemia de ransomware" que la red de CSIRT existente no pudo detener**
- **Esto impulsó la necesidad de focalizar la detección en los SOC y crear una red europea de SOCs**
- **Así surge el concepto de SOC Transfronterizo, impulsado por la UE**
- **Este nuevo modelo conecta centros de seguridad de distintos países para hacer frente a amenazas globales de forma coordinada**



SOC Transfronterizo: Beneficios Estratégicos y Operacionales

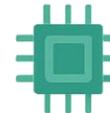
- Alcance geográfico y recursos ampliados
- Inteligencia de amenazas compartida
- Detección temprana mejorada
- Respuesta coordinada a incidentes
- Tecnología avanzada
- Protección 24/7 sin coste de personal interno adicional

Alcance geográfico y recursos ampliados, Acceso a una red europea y más capacidades



Inteligencia de amenazas compartida

Detección temprana mejorada



Tecnología avanzada



Tecnología avanzada



Respuesta coordinada a incidentes



Protección 24/7 sin coste de personal interno adicional

Optimización de Recursos y Retorno de la Inversión



Democratización de la ciberseguridad avanzada

Facilita el acceso a tecnologías y conocimientos que antes solo estaban al alcance de grandes empresas



Detección temprana mejorada

Al integrarse en una red europea, permite identificar amenazas antes de que lleguen a España

Coste-eficiencia

El uso compartido de recursos y conocimientos entre países disminuye considerablemente los costes de implementación para cada entidad

NIS2: Elevando el Estándar de Ciberseguridad en la UE



◆ Nuevo NIS2
● Más tipos en NIS2

NIS2: Elevando el Estándar de Ciberseguridad en la UE



Servicios postales
y de mensajería



Gestión de
residuos



Fabricación, producción y
distribución de sustancias
y mezclas químicas

◆ Nuevo NIS2



Producción,
transformación
y distribución de
alimentos



Fabricación de:

- Productos sanitarios y diagnóstico in vitro.
- Productos informáticos, electrónicos y ópticos.
- Material eléctrico.
- Maquinaria y equipo ncop.
- Vehículos de motor, remolques y semirremolques.
- Otro material de transporte.



Organismos
de investigación



Proveedores de
servicios digitales

- Proveedores de mercados en línea.
- Motores de búsqueda en línea.

◆ Plataformas de RRSS.

Marco Normativo Europeo: La Directiva NIS2

- La Directiva NIS2 busca un alto nivel común de ciberseguridad en toda la UE, imponiendo obligaciones a entidades públicas y privadas de sectores críticos
- Amplía significativamente el ámbito de aplicación, incluyendo más sectores
- Afecta generalmente a medianas y grandes empresas, y en algunos casos, sin importar su tamaño
- Establece la obligación de gestionar riesgos de ciberseguridad con medidas técnicas, operativas y organizativas
- Fija plazos estrictos para la notificación de incidentes significativos
- Endurece las sanciones en caso de incumplimiento, incluyendo multas administrativas y prohibiciones temporales para directivos



Alineando su Organización con NIS2 a través del SOC

- Un SOC Transfronterizo ayuda a cumplir con las medidas de gestión de riesgos de NIS2

Artículo 21.2 a

Políticas de seguridad y análisis de riesgos de los sistemas de información

- ♦ Marco de gobierno de la ciberseguridad.
- ♦ Roles y responsabilidades.
- ♦ Postura de ciberseguridad.
- ♦ Medidas para mitigar los riesgos.

Artículo 21.2 b

Gestión de incidentes

- ♦ Detección, notificación y respuesta.
- ♦ Planes y procedimientos.

Artículo 21.2 c

Continuidad de las actividades, copias de seguridad, recuperación en caso de catástrofe y gestión de crisis

- ♦ Desarrollo de planes (crisis, continuidad, contingencias) que aseguren continuidad en caso de incidente.
- ♦ Realizar formación y simulacros de continuidad de negocio.

Artículo 21.2 h

Políticas y procedimientos de criptografía y cifrado

- ♦ Utilizar cifrado para preservar integridad, confidencialidad y autenticidad de los datos.
- ♦ Implementar prácticas de gestión de claves.
- ♦ Pruebas y formación sobre cifrado.

Artículo 21.2 i

Seguridad de los RRHH, políticas de control de acceso y gestión de activos

- ♦ Procedimientos para empleados con acceso a información sensible.
- ♦ Formación y pruebas sobre control de acceso.
- ♦ Evaluar las medidas sobre el inventario de activos.

Artículo 21.2 d

Seguridad de la cadena de suministro y relaciones con proveedores y prestadores de servicios directos

- ♦ Evaluar riesgos de ciberseguridad en la cadena de suministro.
- ♦ Medidas de mitigación.
- ♦ Evaluar riesgos e impactos en la cadena de suministro.

Artículo 21.2 e

Seguridad en la adquisición, desarrollo y mantenimiento de redes y de información. Gestión y divulgación de vulnerabilidades

- ♦ Escaneo de vulnerabilidades, y test de penetración regulares.
- ♦ Medidas de mitigación de vulnerabilidades.
- ♦ Ciberhigiene y formación frecuentes.

Artículo 21.2 f

Políticas y procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad

- ♦ Políticas y procedimientos de evaluación de medidas.
- ♦ Auditorías y pruebas frecuentes.

Artículo 21.2 g

Prácticas básicas de ciberhigiene y formación en ciberseguridad

- ♦ Programa integral de formación y concienciación.
- ♦ Formación continua.
- ♦ Formación y testeos aplicados para reforzar lo aprendido.

Artículo 21.2 j

Autenticación multifactorial o continua, comunicaciones de voz y sistemas seguros de comunicaciones de emergencia

- ♦ Implementar 2FA o autenticación continua, para voz, video, texto y comunicaciones.

Otros Marcos Clave: GDPR y DORA



- Un SOC contribuye a la protección de datos personales mediante la detección y prevención de brechas de seguridad
- Facilita la notificación de incidentes de datos a las autoridades y afectados en los plazos establecidos, un requisito clave de GDPR
- SOC es fundamental para la resiliencia operativa digital exigida por DORA en el sector financiero
- Ayuda a identificar, proteger, detectar, responder y recuperarse de incidentes relacionados con las TIC, pilares de DORA



Servicio gratuito y confidencial, disponible de 08:00 am a 11:00 pm los 365 días del año.

TU AYUDA EN CIBERSEGURIDAD

017

Teléfono 017

WhatsApp 900 116 117

Telegram @INCIBE017

Formulario web

Atención presencial

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE CASTILLA Y LEÓN MINISTERIO DE TRANSFORMACIÓN DIGITAL

Plan de Recuperación, Transformación y Resiliencia

España digital 2026

incibe INSTITUTO NACIONAL DE CIBERSEGURIDAD



Operativa del SOC Transfronterizo: Detección Proactiva de Amenazas

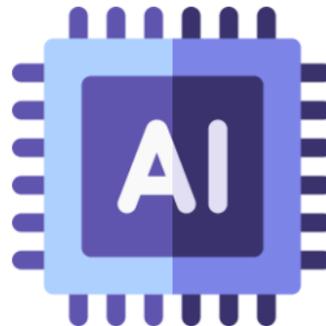


Monitorización continua 24/7

Análisis y correlación de eventos

Detección proactiva de amenazas

Inteligencia artificial y Machine Learning

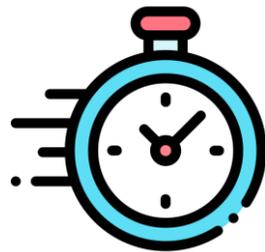


Operativa del SOC Transfronterizo: Respuesta Rápida y Recuperación

Gestión de incidentes

Análisis forense

Sistemas automatizados



Tecnologías Clave Implicadas en el SOC Transfronterizo



Plataformas SIEM

Inteligencia artificial y machine learning

Sistemas SOAR



Herramientas de análisis forense digital

**Plataformas de intercambio de
inteligencia de amenazas**

**Tecnologías de detección y respuesta
extendida (XDR)**



Casos prácticos. Ejemplos de uso del SOC Transfronterizo.

Caso 1

Protección frente a ransomware

Caso 2

Soporte ante brechas de datos

Caso 3

Cumplimiento normativo RGPD

Implementación práctica. Proceso de evaluación inicial.

Paso 1: Auditoría de ciberseguridad

- Evaluación de activos críticos
- Identificación de vulnerabilidades
 - Análisis de riesgos

Paso 2: Análisis de necesidades

- Determinación del nivel de protección requerido
- Identificación de requisitos normativos
- Evaluación del presupuesto disponible

Paso 3: Selección del modelo SOC-T

- Evaluación de proveedores certificados
 - Comparación de servicios y precios
 - Análisis de SLA y garantías



El Proceso de Implementación de un SOC Transfronterizo



Paso 1: Auditoría de ciberseguridad

- Evaluación de activos críticos
- Identificación de vulnerabilidades
 - Análisis de riesgos

Paso 2: Análisis de necesidades

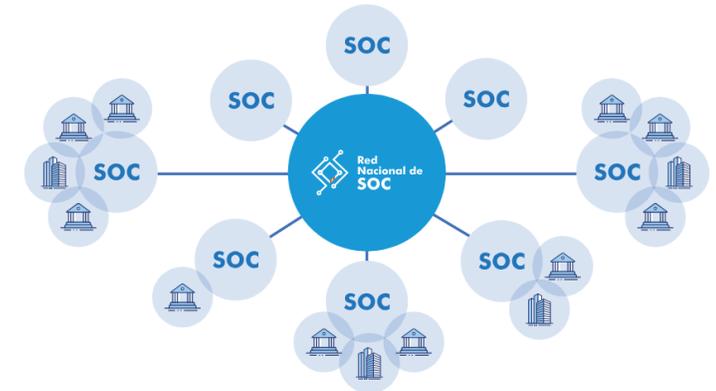
- Determinación del nivel de protección requerido
- Identificación de requisitos normativos
- Evaluación del presupuesto disponible

Paso 3: Selección del modelo SOC-T

- Evaluación de proveedores certificados
- Comparación de servicios y precios
 - Análisis de SLA y garantías
- Considerar SOC interno, externo o híbrido

La Red Nacional de SOC (RNS) y la Cooperación Europea

- La Red Nacional de SOC (RNS) integra a todos los SOC en España, tanto públicos como privados, impulsada por el CCN-CERT
- Su objetivo es impulsar la protección mediante el bloqueo casi inmediato de actividades anómalas detectadas en cualquier punto de la Red
- La RNS se alinea con la Estrategia de Ciberseguridad de la UE de 2020, que promueve una red europea de SOC basada en IA
- Fomenta el intercambio de Indicadores de Ataque (IOA) e Indicadores de Compromiso (IOC) entre miembros, bajo la premisa de "solo compartir lo que yo mismo estoy ya bloqueando"
- Beneficios de participar en la RNS incluyen el acceso inmediato a IOA/IOC y, para entidades proveedoras, un mejor posicionamiento en contrataciones públicas



La Red Nacional de SOC (RNS)



- <https://rns.ccn-cert.cni.es/red-nacional-soc>

Listado de entidades

Listado de entidades adheridas

Mostrar 5 registros

Logotipo	Entidad	Tipo	Nivel de participación	Fecha de renovación
	4Elitech - CSIRT	Entidad proveedora	Oro	01-10-2025
	A3Sec Grupo SL	Entidad proveedora	Oro	01-10-2025
	Accenture	Entidad proveedora	Oro	01-10-2025
	Advens Cybersecurity	Entidad proveedora	Oro	01-10-2025
	Aiuken Cybersecurity	Entidad proveedora	Oro	01-10-2025

Mostrando 1 a 5 de 267 registros

Anterior 1 2 3 4 5 ... 54 Siguiente



RECURSOS ADICIONALES: INCIBE

- <https://catalogo.incibe.es/search>

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD

INICIO / EMPRESAS / Herramientas de ciberseguridad / Catálogo de empresas y soluciones de ciberseguridad / Buscador de empresas

Buscador

Busca empresas y soluciones

Filtrados por [quitar todos](#)

Proveedores De Seguridad Gestionada Cumplimiento Legal Y Normativo

¿Qué empresa buscas?

Tipo de empresa

- Consultoría/integrador
- Fabricante
- Mayorista/distribuidor
- Proveedores De Seguridad Gestionada
- Proveedores Especializados Locales
- Revendedor De Valor Añadido (Var)

Sede de empresa

¿Qué solución necesitas?

Categoría

- Anti-fraude
- Anti-malware

15 empresas

0Invader

Empresa
0Invader Cybersecurity S.L

Listado
Soluciones (2)

Akuda

Empresa
Akuda Cyberseguridad

Servicio gratuito y confidencial, disponible de 08:00 am a 11:00 pm los 365 días del año.

TU AYUDA EN CIBERSEGURIDAD

Teléfono 017
WhatsApp 900 116 117
Telegram @INCIBE017
Formulario web
Atención presencial

Financiado por la Unión Europea NextGenerationEU

Comunidad de Castilla y León MINISTERIO DE TRANSFORMACIÓN DIGITAL

Plan de Recuperación, Transformación y Resiliencia

España digital 2026

incibe INSTITUTO NACIONAL DE CIBERSEGURIDAD

RECURSOS ADICIONALES: INCIBE



- <https://adl.incibe.es/>



Herramienta de Autodiagnóstico

Conoce tus riesgos en cinco minutos

Las empresas dependen para su funcionamiento de la información y de la tecnología: ordenadores, teléfonos móviles y tabletas, bases de datos, líneas de comunicaciones...

Pero, ¿has pensado alguna vez en lo que ocurriría si, de repente, perdistes la información de tu negocio o la capacidad de acceder a ella? Seguro que tu empresa está expuesta a amenazas que ni siquiera imaginas.

¿Quieres gestionar la seguridad de tu negocio?

Te proponemos una evaluación inicial del riesgo de seguridad de tu negocio en función de cómo utilizas la tecnología: correo electrónico, página web, tabletas, smartphones, etc.

Reflexiona sobre estas sencillas cuestiones para conocer el estado de ciberseguridad de tu empresa y cuáles son los riesgos que te afectan. Así sabrás por dónde empezar a mejorar.

Debe aceptar las cookies de recaptcha para poder continuar.

[Aceptar todas las cookies](#) o [gestionar cookies](#)

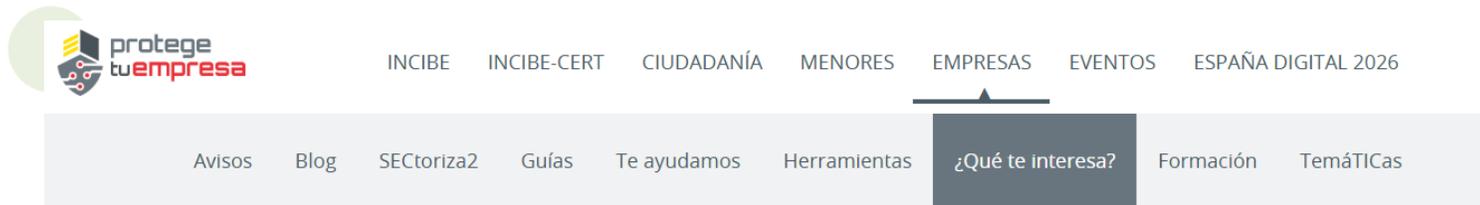
▶ Calcula el riesgo de tu negocio

Esta herramienta es un primer paso para mejorar la ciberseguridad de tu negocio. Si necesitas más información consulta el apartado [Protege tu empresa. ¿Qué te interesa?](#)

- <https://www.incibe.es/empresas/que-te-interesa>

RECURSOS ADICIONALES: INCIBE

- <https://www.incibe.es/empresas/que-te-interesa>



entidad y proteger su principal activo: la información.
Haga de la ciberseguridad su valor diferencial.



Conclusión y Puntos clave

Las ciber amenazas no distinguen entre grandes empresas y PYMES

El SOC Transfronterizo ofrece protección europea coordinada con recursos compartidos

Los beneficios económicos superan ampliamente la inversión requerida

El cumplimiento normativo se simplifica significativamente

El tiempo es crítico

ic3cyl
competitividad
empresarial



Gracias por su atención

