SOC-T (Centro de Operaciones de Seguridad Transfronterizo)

Centr@Tec
Servicios Avanzados de Innovación para Pymes

AIR INSTITUTE

icecyl competitividad empresarial

Junta de Castilla y León

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?

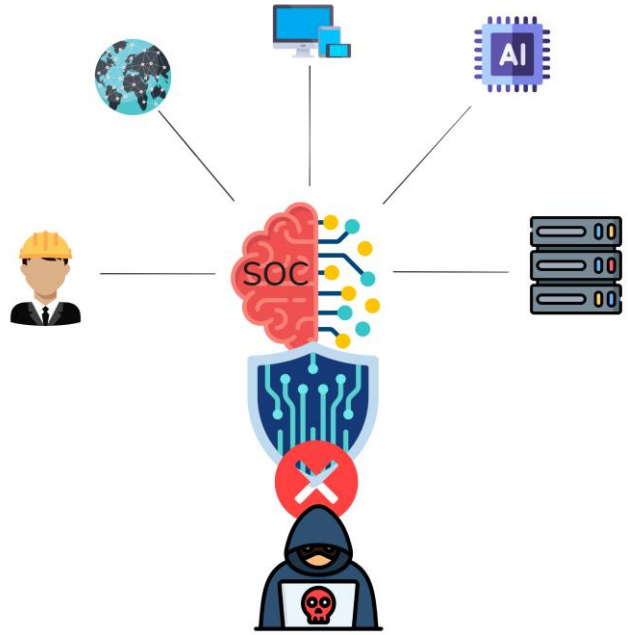
2. Enfoque en NIS2 y GDPR

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

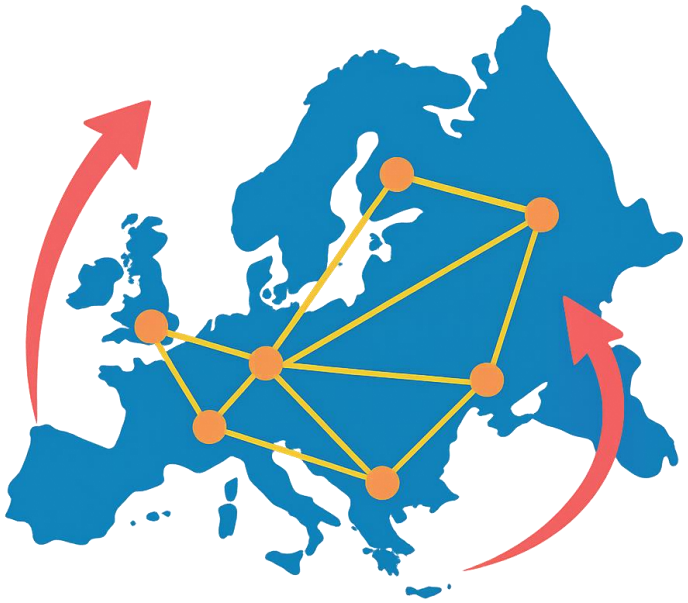
Entendiendo el SOC: Un Centro de Operaciones de Seguridad

- 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

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

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**

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

Operativa del SOC Transfronterizo: Detección Proactiva de Amenazas

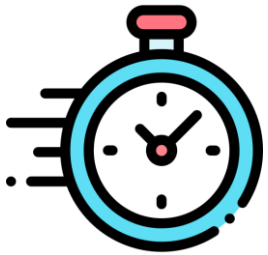
- Monitorización continua 24/7
- Análisis y correlación de eventos
- Detección proactiva de amenazas
- Inteligencia artificial y Machine Learning

Operativa del SOC Transfronterizo: Respuesta Rápida y Recuperación

Gestión de incidentes

Análisis forense

Sistemas automatizados



Tecnologías Clave Implicadas en el SOC Transfronterizo

- Plataformas SIEM
- Herramientas de análisis forense digital
- Inteligencia artificial y machine learning
- Plataformas de intercambio de inteligencia de amenazas
- Sistemas SOAR
- 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

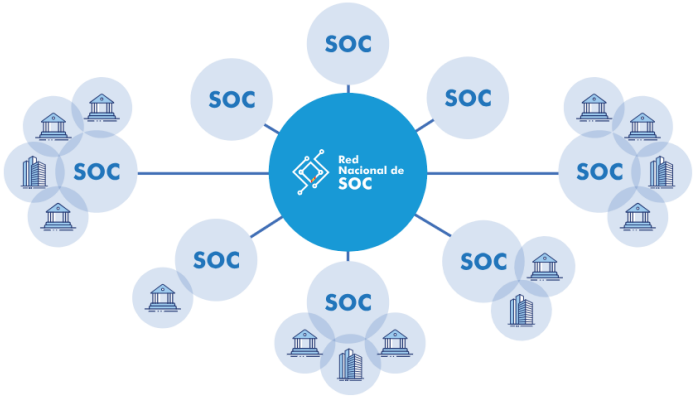
- Determinación del nivel de protección requerido
- Identificación de requisitos normativos
- Evaluación del presupuesto disponible

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 SOCs 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 SOCs 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

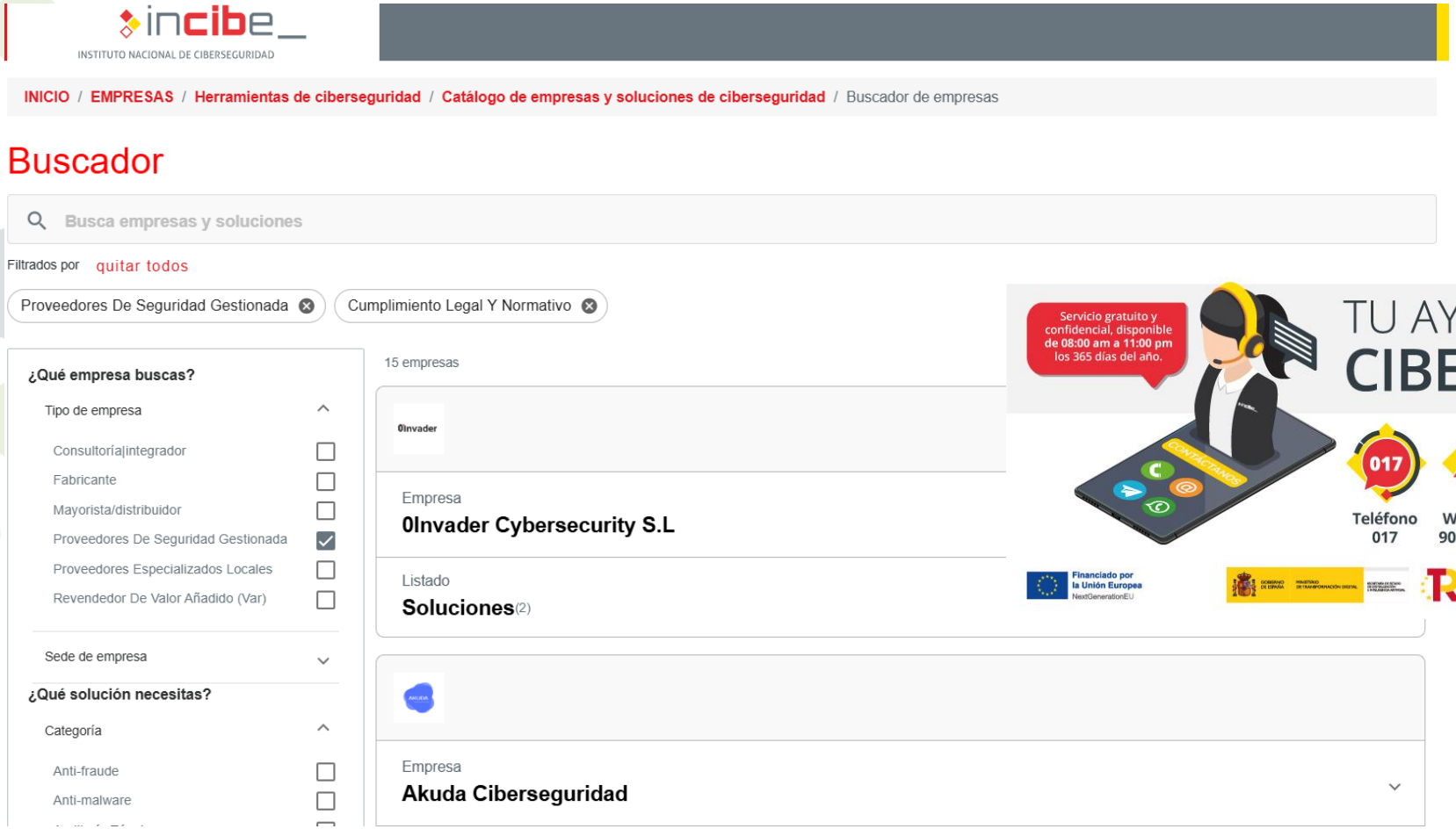
Mostrar 5 registros Buscar:

Logotipo	Entidad	Tipo	Nivel de participación	Fecha de renovación
4Elitech	4Elitech – CSIRT	Entidad proveedora	Oro	01-10-2025
a3Sec	A3Sec Grupo SL	Entidad proveedora	Oro	01-10-2025
accenture	Accenture	Entidad proveedora	Oro	01-10-2025
aDvens	Advens Cybersecurity	Entidad proveedora	Oro	01-10-2025
Aiuken Cybersecurity	Aiuken Cybersecurity	Entidad proveedora	Oro	01-10-2025

Mostrando 1 a 5 de 267 registros Anterior 1 2 3 4 5 … 54 Siguiente

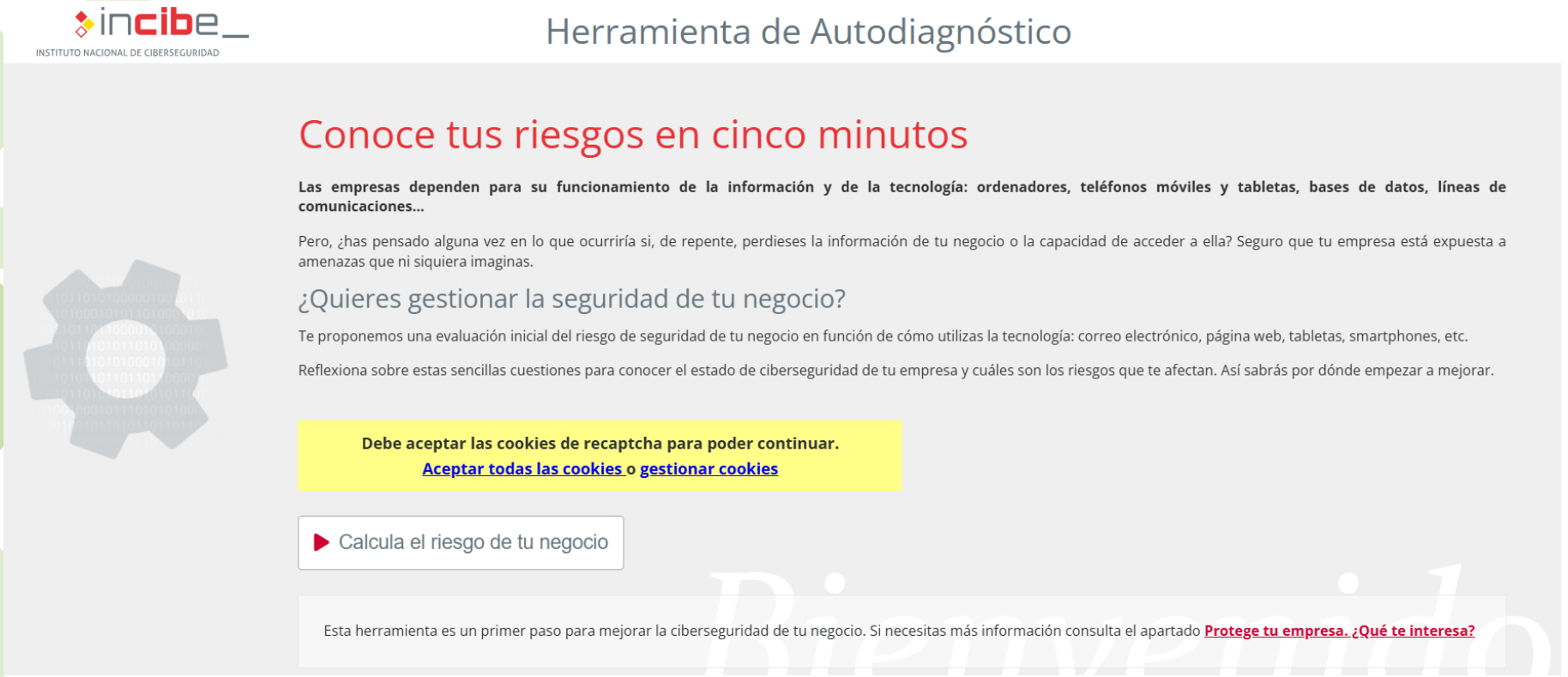
RECURSOS ADICIONALES: INCIBE

- **https://catalogo.incibe.es/search**



RECURSOS ADICIONALES: INCIBE

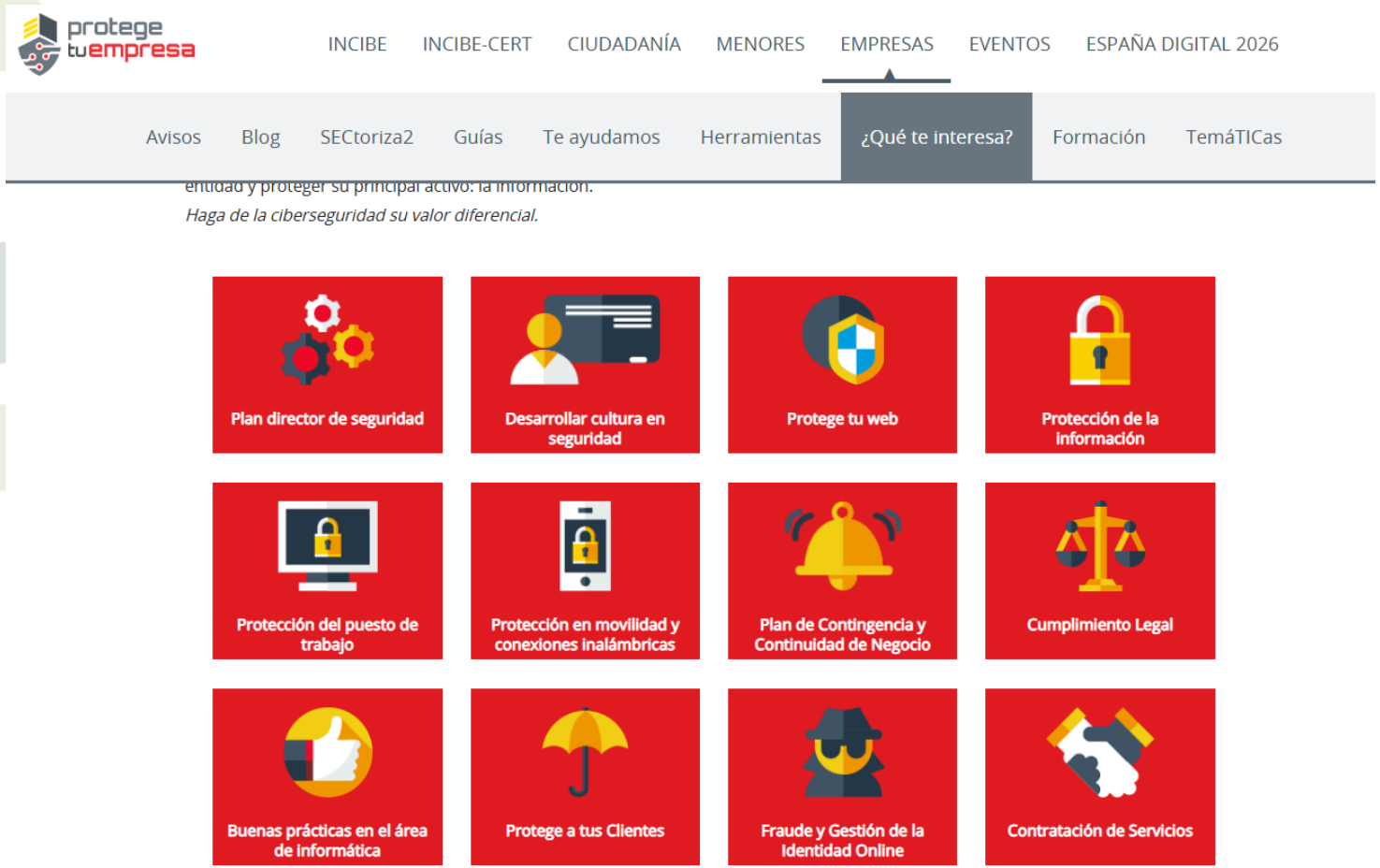
- **https://adl.incibe.es/**



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

RECURSOS ADICIONALES: INCIBE

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



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

Gracias por su atención