FERCHAU

CIBERSEGURIDAD PARA DIRECTIVOS

¿INVERTIMOS?

PONENTE

NÉSTOR JARQUE



Responsable del Departamento de Ciberseguridad en FERCHAU Spain

- Analista en Ciberinteligencia (UFV).
- Analista Internacional en Cibercrimen y Ciberdelito (ITE).
- Ingeniero técnico en informática (UTA).
- Perito Judicial en Informática Forense (UI1).
- Docente universitario (UNIR).
- Colaboración con las fuerzas de seguridad y,
- Más de 65 certificaciones.

Néstor Jarque

ESTRUCTURA

01

La situación en España

Datos y tendencias que muestran cómo ha evolucionado el riesgo digital en el entorno empresarial.

02

Manos a la obra

Desde FERCHAU Spain hemos realizado unos de los programas más amplio y exitoso de España en materia de Ciberseguridad.

03

Cómo mejorar la gobernanza y cultura

Compartiremos acciones concretas, fáciles de implementar, que puedes poner en marcha hoy mismo para reducir drásticamente el riesgo

04

La ciberseguridad como decisión estratégica

Cómo abordar la inversión y la cultura de ciberseguridad desde la dirección de la empresa.

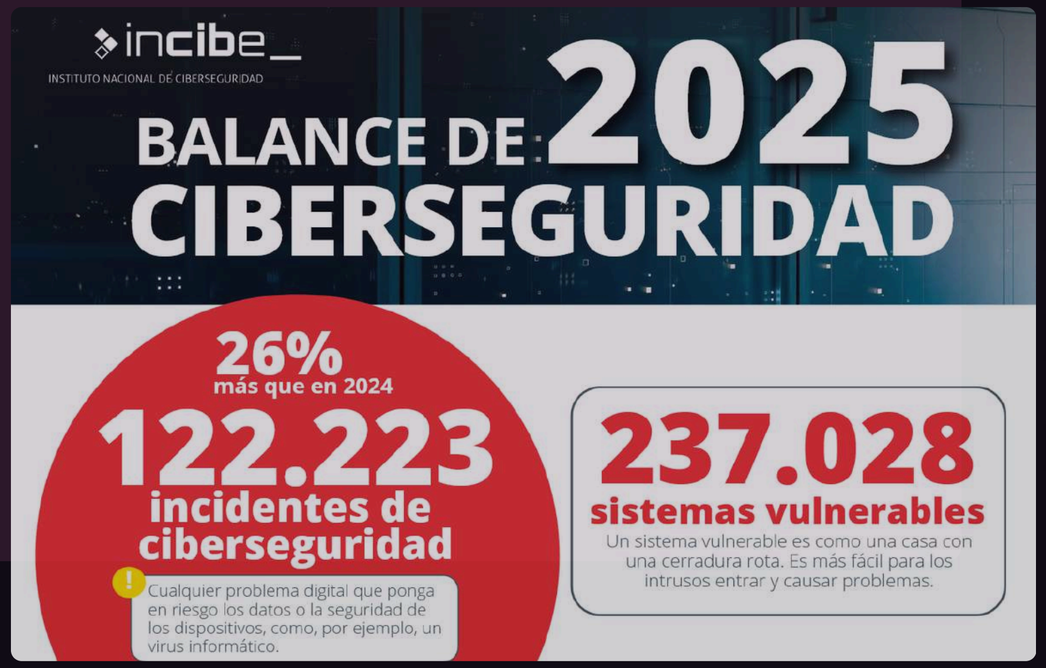
¿QUÉ SE ENTIENDE POR CIBERSEGURIDAD PARA PYMES?

La ciberseguridad es cuidar lo que más valoramos en lo digital: nuestra información, nuestro trabajo y la confianza de nuestros clientes.

Hoy, cualquier empresa —**grande o pequeña**— HA SIDO ciberatacada.
Y muchas veces, las pymes son las más vulnerables… no por lo que tienen, sino por lo que no tienen: **CIBERSEGURIDAD**.

Protegerse no es solo cosa de “gastos”. Es sentido común, es prevenir, y sobre todo, es cuidar el esfuerzo de años.

LA CIBERSEGURIDAD EN LAS PYMES ESPAÑOLAS



01 45% más que el 2024



02 Robo de información



03 Dispositivos IoT



FUENTE DE INFORMACIÓN

01

pymes que cierran

El 60% de las pymes que son víctimas de ciberataques con malware se ven obligadas a cerrar sus puertas en un plazo de seis meses.

Enlace: directivosygerentes.es

02

El reto de la IA

España registra la primera brecha de seguridad provocada por un agente de IA.

Enlace: elEconomista.es

03

Ciberataques

Las empresas españolas registran una media de 2.192 ataques semanales en agosto.

~14 Ciberatques por hora

Enlace: cybersecuritynews.com

04

Aumentar la inversión

Aumentar la inversión en seguridad, prioridad para el 51 % de las pymes españolas en 2024. Porcentaje que sitúa a España por delante de países como Italia (46 %), Alemania (43 %) o Francia (37 %).

Enlace: revistapymes.es

MANOS A LA OBRA

PROGRAMA DE ACELERACIÓN EN CIBERSEGURIDAD

FERCHAU

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

+100 PYMES ESPAÑOLAS

¿Cuáles son nuestras conclusiones?



¿POR QUÉ LAS PYMES SON EL BLANCO FAVORITO DE LOS CIBERDELINCUENTES?

Los ciberdelincuentes ya no buscan solo grandes empresas. Buscan **blancos fáciles**, y las pymes, por su menor nivel de protección y de consciencia, se han convertido en uno de sus objetivos preferidos.

98,3%



Datos valiosos y acceso a terceros

Aunque sean pequeñas, manejan información crítica de clientes, proveedores y empleados.

92,9%



Falta de formación interna

Eempleados que no saben reconocer un correo falso o un enlace peligroso

56,3%



El mito: “A mí no me va a pasar”

Las microempresas españolas asumen un coste medio anual de casi 30.000 euros por incidentes cibernéticos. Fuente

De acuerdo con datos proporcionados por Ayesa, el coste medio de un ciberataque en pymes alcanza los 75.000 euros.

CUMPLIMIENTO DE LOS OPERADORES ESENCIALES

Infraestructuras críticas (OT):

401

operadores esenciales e importantes*

Empresas o servicios que son muy importantes para el funcionamiento diario de la sociedad. Incluye sectores, como la energía, el agua o las comunicaciones.

- Infraestructuras críticas
- Impacto en la cadena (suministro, industria, energía, farmacia, etc.)
- Riesgo sistémico.

34% Banca

14% Transporte

8% Energía



7% Infraestructura de los mercados financieros

6% Aseguradoras y fondos de pensiones

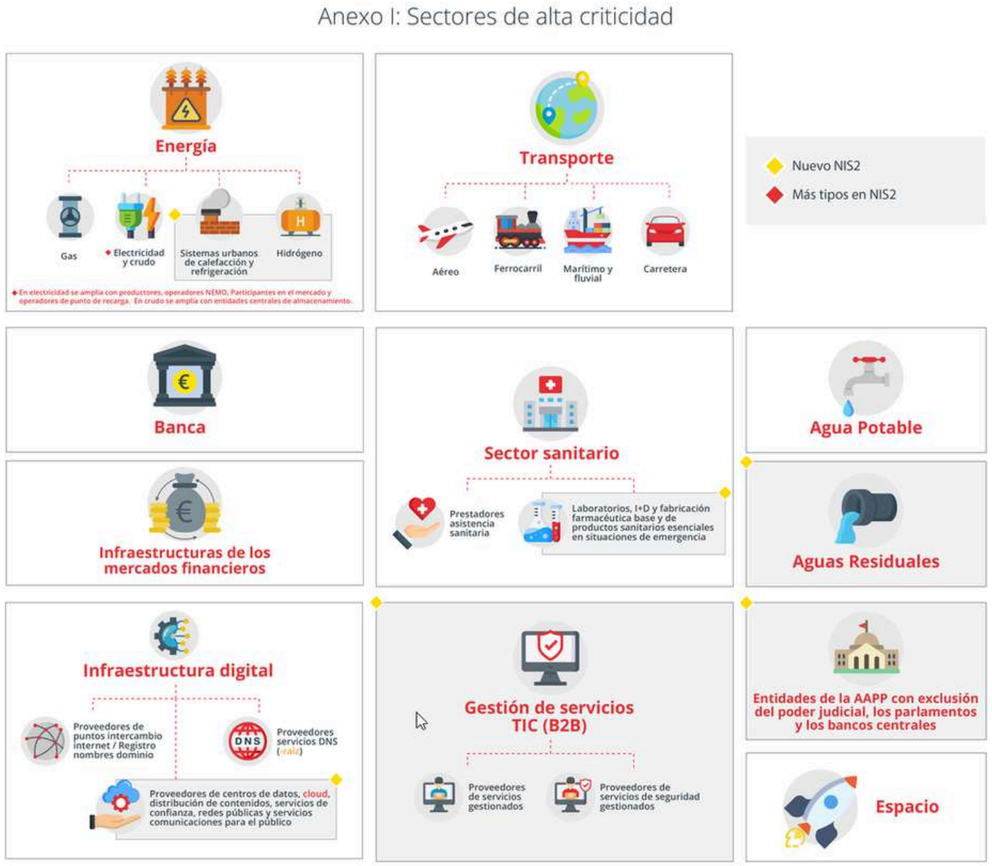
*Entidades alineadas con la terminología de la directiva NIS2

FUENTE: INCIBE

¿Nuestra empresa es un operador esencial?



OPERADORES ESENCIALES E IMPORTANTES



FUENTE: INCIBE



FUENTE: INCIBE



OPERADORES ESENCIALES E IMPORTANTES

¿Estoy obligado si soy PYME?

Por defecto NIS2 **no aplica a microempresas y pequeñas empresas** (menos de 50 empleados y ≤ 10 M€ facturación), salvo excepciones tasadas:

- Proveedores únicos de un servicio en el Estado miembro
- Operadores de DNS, TLD, registros de nombres de dominio
- Proveedores cualificados de servicios de confianza
- Entidades cuya interrupción afecte a la seguridad pública
- Administraciones públicas

Si tu empresa **suministra a una entidad obligada NIS2**, no estás bajo NIS2 directamente, pero tu cliente debe **gestionar el riesgo de su cadena de suministro**: **en la práctica, te exigirán contractualmente medidas equivalentes.**

Implica:

- Gestión del riesgo de ciberseguridad.
- Notificación obligatoria de incidentes.
- Responsabilidad del órgano de dirección.

Por lo tanto:

La responsabilidad de la ciberseguridad pasa del departamento IT/Cyber al comité de dirección.



QUÉ NOS ESPERA PARA EL 2026

Este año confirmará que el coste de la inacción superará cualquier inversión preventiva.

01

NIS2 será obligatoria en España

Las organizaciones que comiencen su adaptación desde ahora contarán con una ventaja competitiva. La NIS2 marcará la diferencia entre quienes conciben la ciberseguridad como una estrategia esencial y quienes la consideran un mero coste operativo.

"Las multas podrán alcanzar los 10 millones de euros o el 2 % de la facturación anual global."

02

Superficie de ataque e IA

La superficie de ataque sigue creciendo con desafíos complejos como: La interdependencia, más IoT, privacidad, propiedad de los datos, entre otros.

El avance de la IA en todos los ámbitos trae consigo una sofisticada y gran amenaza en malware. Los Ciberdelincuentes trabajan con IA dedicadas a perfeccionar los ataques según entorno.
Ejemplo: PROMPTFLUX

03

"Confianza" como Vector de Ataque

La **confianza** que se construye con clientes y proveedores es un **activo valioso**, pero también frágil. Si los socios comerciales no invierten en ciberseguridad, pueden convertirse en un vector de ataque que afecte tu reputación. Es vital integrar la ciberseguridad como un elemento fundamental en todas las relaciones comerciales para blindar tu imagen y evitar que los riesgos externos comprometan el éxito y la confianza de tu empresa.

CÓMO MEJORAR LA GOBERNANZA Y CULTURA

CONCIENCIA

Conciencia en Ciberseguridad

- Si crees que no eres un objetivo, ya eres vulnerable.
- Y si decides no actuar, lo estás decidiendo también por tu equipo, tus clientes/proveedores y tu reputación.

La ciberseguridad empieza en la conciencia directiva con decisiones estratégicas.

Ciberseguridad no es solo protección, es cumplimiento

Las normativas como NIS2, RGPD o ENS convierten la ciberseguridad en una obligación empresarial.

- Sanciones económicas.
- Pérdida de contratos.
- Impacto reputacional.

INVERSIÓN

Cultura de ciberseguridad

La mayoría de incidentes comienzan con errores humanos.

- Formación y concienciación.
- Procesos claros.
- Responsabilidad compartida.

Lo que inviertes lo ganas en oportunidades

La ciberseguridad no solo reduce riesgos:

- **Genera confianza** con clientes y partners.
- Facilita trabajar con grandes empresas.
- Abre nuevas **oportunidades de negocio.**

La pregunta del millón:

¿Cuánto debo invertir?



¿CÓMO DECIDIR LA INVERSIÓN EN CIBERSEGURIDAD?

Depende principalmente de:

- **Nivel de riesgo y madurez de la organización.**
- **El sector y las obligaciones regulatorias.**
- **Los activos críticos.**
- **El impacto que tendría un incidente en el negocio.**

Antes de invertir en tecnología es clave:

- **Realizar un análisis de riesgos.**
- **Impulsar la cultura de ciberseguridad desde la dirección.**
- **Concienciar a toda la organización.**

Reformulación de la pregunta...

No es cuánto invertir, sino ¿Qué riesgos estamos dispuestos a asumir si no invertimos?

PREGUNTAS



FERCHAU

¡GRACIAS!



Contacto

Néstor Jarque