smart-team.tech

SMART TEAM · INSIGHTS · ESTUDIO SECTORIAL

Ciberseguridad 2030: las 25 tendencias que una empresa española debe decidir ya

25 TENDENCIAS ANALIZADAS



Smart Team · smart-team.tech
2026-09-20 · Equipo de Análisis de Smart Team

Guía de lectura: cómo está construido este estudio

Cada una de las 25 fichas sigue el mismo formato: un titular, un párrafo de tesis con la decisión que la tendencia plantea a la dirección, un bloque de evidencia documental con cifras y fuentes enlazadas, y un panel de evaluación con tres magnitudes:

- **Impacto de mercado (1-5)**: magnitud esperada del efecto de la tendencia sobre las decisiones, presupuestos o riesgos de una empresa española mediana en el horizonte 2026-2030.
- **Nivel de confirmación (1-5)**: solidez y convergencia de la evidencia disponible. Un 5 indica datos oficiales o concordancia de varias fuentes independientes; un 3, señales consistentes pero todavía parciales.
- **Índice medio**: media aritmética simple de las dos magnitudes anteriores. Sirve para comparar tendencias heterogéneas, no para sustituir el juicio directivo.

Con ese índice se construye el **orden de prioridad global (01-25)**, de mayor a menor. Cuando dos fichas empatan en índice, el desempate es editorial y favorece a la tendencia que exige una actuación más inmediata. El ranking ordena la agenda; no sustituye el diagnóstico de cada organización.

CÓMO LEER

25 tendencias de ciberseguridad hacia 2030 para la empresa española: amenazas, NIS2, ENS, AI Act, Zero Trust y talento, con datos de INCIBE, ENISA e ISACA.

Índice del estudio

01	Guía de lectura: cómo está construido este estudio	2
02	Contexto de mercado: los números que enmarcan la década	4
03	Bloque I · Señales de mercado: la economía española de la ciberseguridad	6
04	Bloque II · El mapa de amenazas: volumen récord, precisión e inteligencia artificial	12
05	Bloque III · El coste real para la empresa mediana	18
06	Bloque IV · El marco regulatorio: de carga administrativa a palanca competitiva	24
07	Bloque V · Arquitectura 2030: decisiones de modelo y de tecnología	30
08	Del ranking a la agenda: cómo aplicar las prioridades según el punto de partida	36
09	Ocho hipótesis de trabajo hacia 2030	37
10	Síntesis ejecutiva	39
11	Fuentes principales	40



Contexto de mercado: los números que enmarcan la década

Antes de entrar en las fichas, conviene fijar los indicadores estructurales que atraviesan todo el análisis:

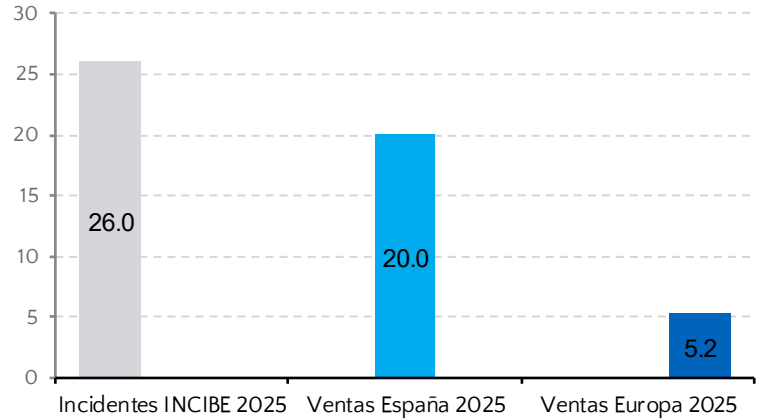
Indicador	Valor	Fuente
Facturación de la industria española de ciberseguridad (2024)	**6.351 M€ (4,65% del sector TIC)**	INCIBE–CONETIC
Posición de España en el mercado europeo	**4.º mercado (12% de la facturación continental)**	INCIBE–CONETIC
Incidentes gestionados por INCIBE en 2025	**122.223 (+26% interanual)**	España Digital / INCIBE
Crecimiento de ventas de soluciones en España (2025)	**+20% interanual (Europa: +5,2%)**	Context / Channel Partner
Empleo en el sector (2025)	**164.761 profesionales (25,55% del empleo TIC)**	INCIBE–CONETIC
Previsión de crecimiento anual del empleo (2026-2029)	**+14,25% (hasta 282.157 empleos)**	INCIBE–CONETIC
Pymes españolas que sufrieron algún ataque en el último año	**6 de cada 10**	Hiscox, Informe de Ciberpreparación 2025
Coste medio estimado de un incidente grave para una pyme	**~75.000 €**	Estimaciones sectoriales recogidas por INCIBE – Protege tu empresa

Lectura combinada: oferta, amenaza y regulación

La conclusión del contexto de mercado

La lectura combinada es inequívoca: la oferta crece a doble dígito, la amenaza crece aún más deprisa y la presión regulatoria elimina la opción de la inacción. España es, a la vez, uno de los mercados de defensa más dinámicos de Europa y uno de los territorios más castigados por la actividad delictiva.

Crecimiento interanual: amenaza y mercado (%)



Fuente: INCIBE / España Digital; Context–Channel Partner. Cifras citadas en el cuerpo del texto.

BLOC I

Señales de mercado: la economía española de la ciberseguridad

El primer bloque examina el lado de la oferta y de la demanda. Entender cómo se estructura el mercado que vende protección es tan relevante para el comprador como entender la amenaza: determina precios, modelos de contratación y poder de negociación.

01 La ciberseguridad se consolida como industria estratégica en España

02 La demanda española crece a un ritmo muy superior al europeo

03 El gasto migra del producto al servicio gestionado

04 Un ecosistema atomizado: más oferta, más responsabilidad de selección

05 La presión del empleo ciber anticipa el encarecimiento de la protección



01 La ciberseguridad se consolida como industria estratégica en España

Tendencia 01 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El sector que protege a la economía española ha alcanzado una escala que lo convierte en interlocutor estructural de cualquier empresa mediana: ya no es un nicho técnico, sino una industria con peso macroeconómico propio. Para el demandante, esto se traduce en madurez de la oferta, estabilidad de los proveedores y, también, en la necesidad de aprender a comprar servicios de seguridad con el mismo rigor con que se compran otros servicios críticos.

Evidencia documental. El *Estudio sobre la industria de la ciberseguridad en España 2025*, elaborado por el Instituto Nacional de Ciberseguridad y la Confederación CONETIC a partir de una encuesta a 517 empresas, cifra la facturación del sector en **6.351 millones de euros en 2024**, equivalentes al 4,65% de todos los ingresos del sector TIC nacional. El dato sitúa a España como el **cuarto mercado europeo** de ciberseguridad, con una cuota cercana al 12% de la facturación continental y al 2,8% de la mundial, por delante de economías comparables. El tejido suma 3.431 empresas activas, el 4,47% de las compañías tecnológicas del país, y el mercado ha crecido aproximadamente un 70% desde 2020. En los últimos cinco años se han constituido 403 nuevas compañías de ciberseguridad, que ya concentran el 12% de la facturación total, lo que evidencia un dinamismo emprendedor inusual.

La presencia internacional de las firmas españolas es especialmente destacada en Portugal, Colombia, Alemania, Brasil y Chile. Para una empresa mediana, la conclusión práctica es que el mercado nacional ofrece hoy capacidad probada y competencia real: negociar servicios de seguridad en 2026 no se parece a hacerlo en 2019, cuando la oferta era escasa y concentrada. La consolidación del sector también reduce el riesgo de contraparte: la probabilidad de que un proveedor especializado desaparezca a mitad de contrato es menor en un mercado que crece y se profesionaliza.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	19/25

Fuentes: INCIBE y CONETIC presentan las conclusiones del estudio

02 La demanda española crece a un ritmo muy superior al europeo

Tendencia 02 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. Mientras el mercado europeo de ciberseguridad avanza a un ritmo moderado, la demanda española se comporta como un valor atípico al alza. Para el comprador, este diferencial tiene una consecuencia concreta: la competencia por los mejores proveedores, perfiles y ventanas de servicio se endurecerá, y quien retrase sus decisiones encontrará un mercado más caro y con menos disponibilidad.

Evidencia documental. Los datos de la consultora Context, que mide las ventas reales a través de los mayoristas de TI del continente, muestran que las ventas de soluciones de ciberseguridad en Europa crecieron un **5,2% en 2025**, un ejercicio de dos mitades muy distintas: impulso sólido en el primer semestre y retrocesos del 3% y el 1,8% en los dos últimos trimestres, lastrado por Alemania y Reino Unido. Frente a ese enfriamiento, **España registró un aumento del 20%** en el gasto en ciberseguridad a lo largo de todo 2025, solo superada por Polonia (+59%) y por delante de Italia (+15%). Los motores del crecimiento europeo se han desplazado al sur y al este del continente.

Por segmentos, la seguridad de redes mantiene el mayor volumen de negocio, pero la seguridad de datos fue el segmento más dinámico del año a escala europea, con un avance en torno al 13%, señal de que la preocupación se desplaza del perímetro hacia la información misma. El diferencial español no es coyuntural: responde a la combinación de una digitalización empresarial acelerada, la presión del marco regulatorio europeo y una concienciación creciente tras años de incidentes mediáticos. La empresa mediana que planifique presupuestos plurianuales debe asumir que la inflación del sector —en servicios y en salarios especializados— será superior a la del resto de partidas tecnológicas.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	10/25

Fuentes: Context vía Channel Partner, febrero de 2026

03 El gasto migra del producto al servicio gestionado

Tendencia 03 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. La partida dominante del gasto en ciberseguridad ya no es la compra de tecnología, sino la contratación de servicios gestionados. El modelo MSSP (*Managed Security Service Provider*) se ha convertido en la vía principal por la que las empresas medianas acceden a capacidades que no pueden construir internamente, y esta migración redefine lo que significa "tener seguridad": de poseer herramientas a consumir un resultado operativo.

Evidencia documental. La estructura del mercado español refleja este giro: las empresas de consultoría y servicios acaparan aproximadamente el **70% del negocio del sector**, según el análisis sectorial del Observatorio DBK de Informa, muy por encima del peso de la distribución de producto. La lógica económica es clara para una organización de 50 a 250 empleados: mantener un equipo interno capaz de monitorizar, detectar y responder las 24 horas exigiría un mínimo de cuatro o cinco perfiles senior, cuyo coste salarial anual supera con facilidad el precio de un contrato de servicios gestionados de alcance completo. El informe de la industria de INCIBE y CONETIC confirma que el grueso de las 3.431 empresas del sector se dedica a servicios y no a fabricación.

Para el demandante, la tendencia plantea dos tareas: aprender a evaluar proveedores gestionados (alcance real del servicio, tiempos de respuesta comprometidos, visibilidad sobre lo que ocurre) y evitar la dependencia ciega, conservando internamente al menos la capacidad de gobierno del riesgo. El servicio gestionado traslada la ejecución, no la responsabilidad: la propiedad del riesgo sigue siendo de la empresa contratante, como subraya el propio marco regulatorio europeo. Esta distinción, trivial en apariencia, es la que separa una externalización sana de una delegación temeraria.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	16/25

04 Un ecosistema atomizado: más oferta, más responsabilidad de selección

Tendencia 04 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El sector español de ciberseguridad es, en su mayor parte, un archipiélago de especialistas pequeños. Esta atomización es una ventaja para la empresa mediana —oferta cercana, flexible y asequible— pero también una carga: la calidad es heterogénea y la diligencia en la selección del proveedor se convierte en parte del propio programa de seguridad.

Evidencia documental. El estudio de INCIBE y CONETIC dibuja una estructura empresarial muy fragmentada: el **45% de las compañías del sector son microempresas**, el 8% son autónomos y solo el 5% son grandes corporaciones. En otras palabras, la mitad de la oferta española de ciberseguridad está formada por firmas de menos de diez personas. Las 403 empresas creadas en los últimos cinco años ya facturan el 12% del total, lo que indica una rotación elevada de actores. Para el comprador esto tiene lecturas enfrentadas. En positivo, el tejido de especialistas locales permite encontrar servicios a medida —auditorías puntuales, acompañamiento normativo, respuesta a incidentes— sin las tarifas de las grandes consultoras.

En negativo, la barrera de entrada al sector es baja y el término "ciberseguridad" no está protegido: conviene exigir credenciales verificables (certificaciones del equipo, referencias de clientes comparables, seguros de responsabilidad, cumplimiento del propio Esquema Nacional de Seguridad cuando aplique). La tendencia apunta a una profesionalización gradual impulsada por la demanda: las empresas medianas empiezan a pedir a sus proveedores de seguridad las mismas garantías que sus propios clientes les piden a ellas. El dato adicional de que el 42% de las empresas del sector recibe avisos del servicio de Alerta Temprana de INCIBE muestra una maduración del ecosistema en su conjunto.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	20/25

05 La presión del empleo ciber anticipa el encarecimiento de la protección

Tendencia 05 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El sector de la ciberseguridad es hoy uno de los grandes motores de empleo tecnológico en España, pero su crecimiento convive con una escasez crónica de profesionales. Para la empresa mediana, el indicador laboral funciona como un barómetro de precios: mientras el empleo del sector crezca a doble dígito con ofertas sin cubrir, el coste de los servicios de seguridad seguirá tensionado al alza.

Evidencia documental. Según el estudio de INCIBE y CONETIC, la ciberseguridad emplea actualmente a **164.761 personas en España**, el 25,55% de todo el empleo del sector TIC. Entre 2021 y 2025 el número de profesionales creció un **35,14%**, al pasar de 122.284 a 165.256 empleados. Y la proyección no se modera: el estudio anticipa un crecimiento anual del **14,25% entre 2026 y 2029**, lo que situaría el empleo del sector en torno a **282.157 personas** al final del período. Pese a ese ritmo de contratación, la demanda sigue sin cubrirse: el propio análisis del sector constata que cerca de cuatro ofertas de empleo compiten por cada profesional disponible, y la presencia femenina apenas supera el 20%, lo que evidencia un margen de incorporación todavía amplio.

La lectura para el demandante es directa. Los salarios de los perfiles de seguridad seguirán creciendo por encima de la media TIC, lo que hará aún menos viable construir capacidad interna y más dependiente a las empresas medianas del mercado de servicios. Planificar el presupuesto de seguridad a tres años sin contemplar esta inflación estructural equivale a infraestimarlo de forma sistemática. La tendencia también sugiere oportunidad: las empresas que formen internamente a personal propio en competencias básicas de seguridad reducirán su exposición a un mercado laboral en tensión permanente.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
3/5	4/5	3,5	21/25

BLOC II

El mapa de amenazas: volumen récord, precisión e inteligencia artificial

El segundo bloque describe contra qué se compite realmente. Los datos de 2025 muestran una escalada en frecuencia y una mutación cualitativa: la IA ha industrializado la ingeniería social y abaratado la sofisticación.

06 El incidente se normaliza: volumen récord y crecimiento estructural

07 Phishing industrializado con IA: la puerta de entrada dominante

08 Ransomware: menos frecuente, más letal

09 La cadena de suministro se convierte en vector prioritario

10 Deepfakes ejecutivos y desviación de pagos: el fraude con voz de dirección



06 El incidente se normaliza: volumen récord y crecimiento estructural

Tendencia 06 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. Los incidentes de ciberseguridad en España han dejado de ser acontecimientos excepcionales para convertirse en ruido de fondo de la actividad económica. La dirección que todavía planifica como si el incidente fuera una posibilidad remota está gestionando con estadísticas de otra década: la pregunta operativa ya no es *si* ocurrirá, sino cuándo y con qué capacidad de respuesta se llegará a ese momento.

Evidencia documental. El balance oficial de INCIBE, publicado en febrero de 2026, fijó en **122.223 los incidentes gestionados en 2025**, un **26% más** que el año anterior y la cifra más alta de la serie. La trayectoria es de aceleración sostenida: 83.517 incidentes en 2023, 97.348 en 2024 (+16,6%) y el nuevo récord de 2025. En paralelo, INCIBE-CERT detectó y notificó **237.028 sistemas vulnerables** susceptibles de explotación, y la línea gratuita de ayuda 017 atendió 142.767 consultas, un 45% más, de las que el 51% llegaron cuando el daño ya se había producido. La presión sobre el tejido empresarial es especialmente intensa: en 2024 el 32,4% de los incidentes (31.540) afectó a empresas, pymes, micropymes y autónomos, y la evolución de 2025 mantiene ese peso.

Los datos de Check Point Research aportan la lectura de frecuencia: las organizaciones españolas sufrieron una media de **1.968 ciberataques semanales a lo largo de 2025**, un 70% más que en 2023, cifra que se mantuvo en torno a los 2.000 semanales en los primeros meses de 2026. La conclusión para la planificación es que el presupuesto de seguridad debe diseñarse asumiendo incidentes recurrentes, no un evento único.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
5/5	5/5	5,0	01/25

Fuentes: Balance de INCIBE 2025 vía España Digital y Check Point Security Report 2026

07 Phishing industrializado con IA: la puerta de entrada dominante

Tendencia 07 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El phishing ha dejado de ser un correo mal redactado reconocible a simple vista. La IA generativa ha convertido la suplantación en un producto industrial —sin faltas, personalizado, multicanal— y lo ha consolidado como el vector inicial de la mayoría de intrusiones. La defensa clásica basada en "enseñar a detectar correos sospechosos" resulta insuficiente frente a mensajes que ya no parecen sospechosos.

Evidencia documental. El *ENISA Threat Landscape 2025*, que analiza 4.875 incidentes europeos entre julio de 2024 y junio de 2025, sitúa el phishing como vector de intrusión inicial en torno al **60% de los casos**, muy por delante de la explotación de vulnerabilidades (21,3%). El mismo informe estima que **más del 80% de las campañas de phishing analizadas ya incorporan contenido generado o mejorado con IA**, y documenta la maduración del *phishing-as-a-service*, que pone campañas sofisticadas al alcance de actores sin conocimientos técnicos. El salto cuantitativo quedó marcado por el *State of Phishing Report 2023* de SlashNext, que midió un incremento del **1.265% en correos de phishing maliciosos** desde el lanzamiento de ChatGPT, junto a un aumento del 967% del robo de credenciales.

En España, la posición dominante del phishing no es nueva: ya en 2024 superó los 38.000 incidentes y representó el **43,2% de todos los gestionados por INCIBE**, liderando la categoría de fraude online; el balance de 2025 registró **25.133 incidentes de phishing**, la técnica más frecuente dentro de los 45.445 casos de fraude online. En la encuesta *Tech Trends Pulse Poll* de ISACA, el 63% de los profesionales señala la ingeniería social impulsada por IA como la amenaza más significativa, y el 71% afirma que estos ataques son ya más difíciles de detectar. La respuesta exige combinar filtrado avanzado, autenticación resistente al phishing y verificación procedural de instrucciones sensibles, no solo más formación genérica.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
5/5	5/5	5,0	02/25

Fuentes: ENISA Threat Landscape 2025, SlashNext vía Infosecurity Magazine, ISACA Tech Trends Pulse Poll y Balance INCIBE 2025

08 Ransomware: menos frecuente, más letal

Tendencia 08 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El ransomware ha cambiado de patrón: baja en frecuencia relativa pero sube en daño unitario, con doble extorsión —cifrado más amenaza de publicación— como modelo dominante. Para una empresa mediana, un solo episodio puede comprometer la continuidad, y las cifras de recuperación tras pagar el rescate desaconsejan convertir el pago en plan.

Evidencia documental. INCIBE gestionó **392 incidentes de ransomware en 2025** (357 en 2024), una fracción pequeña de los 55.411 casos de malware, pero el *ENISA Threat Landscape 2025* lo identifica de forma consistente como la amenaza de mayor impacto organizativo de Europa, con operaciones cada vez más descentralizadas tras las acciones policiales y un ecosistema de *ransomware-as-a-service* que reduce la barrera de entrada. Check Point documenta el pico histórico de la doble extorsión: cerca de 8.000 organizaciones en todo el mundo vieron sus datos publicados en portales de filtración en 2025, un 50% más interanual, con el cuarto trimestre marcando el máximo de la serie (2.473 víctimas publicadas); España concentra en torno al 2% de los ataques de ransomware global, situándose entre los países europeos más afectados.

La estadística de recuperación es la que debería fijar la política de respuesta: según el Informe de Ciberpreparación de Hiscox 2025, solo el 57% de las pymes que pagaron un rescate recuperaron la totalidad o parte de sus datos. En la encuesta de ISACA, apenas el 7% de los profesionales europeos declara plena confianza en la capacidad de su organización para superar un ataque de ransomware en el próximo año. La consecuencia práctica se concentra en dos palancas: copias de seguridad inmutables con restauración probada y un plan de continuidad ensayado, porque el ataque seguirá ocurriendo pero la dependencia del rescate es opcional.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
5/5	4/5	4,5	04/25

Fuentes: ENISA Threat Landscape 2025, Check Point Security Report 2026, Hiscox 2025 e ISACA Pulse Poll

09 La cadena de suministro se convierte en vector prioritario

Tendencia 09 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. Atacar a una gran corporación a través de su proveedor mediano se ha convertido en método estándar. Esto coloca a la empresa mediana en una doble exposición: puede ser la vía de entrada hacia sus clientes y, a la vez, la víctima de las debilidades de sus propios proveedores. La seguridad de terceros deja de ser una buena práctica para ser requisito contractual y normativo.

Evidencia documental. El *ENISA Threat Landscape 2025* cuantifica los riesgos de cadena de suministro en el **10,6% de las categorías de amenaza** analizadas y subraya el abuso creciente de dependencias legítimas entre organizaciones. En la encuesta europea de ISACA, las vulnerabilidades de la cadena de suministro figuran entre las tres principales preocupaciones de los profesionales (37%), solo por detrás de las amenazas de IA y de la complejidad regulatoria. La Directiva NIS2 incorpora la gestión del riesgo de proveedores como obligación explícita de las entidades afectadas (artículo 21), lo que traslada la exigencia a cualquier empresa que sirva a sectores esenciales o importantes. Los datos de mercado muestran que la práctica ya se ha extendido: según el Informe de Ciberpreparación de Hiscox 2025, el 91% de las pymes realiza comprobaciones de vulnerabilidades al menos una vez por trimestre, una frecuencia impensable hace cinco años, y las grandes corporaciones españolas han empezado a exigir evidencias de seguridad —certificaciones, cuestionarios, auditorías— a sus proveedores medianos como condición de contratación.

Check Point añade un matiz sectorial relevante: uno de cada cuatro ataques internacionales al sector logístico tiene como objetivo una pyme de la cadena, precisamente por su papel de eslabón permeable. La empresa mediana debe actuar en ambos sentidos: documentar su propia postura para no ser descartada por sus clientes y exigir mínimos a quienes tienen acceso a sus sistemas.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	12/25

Fuentes: ENISA Threat Landscape 2025, ISACA Pulse Poll, Directiva NIS2 (EUR-Lex) y Hiscox 2025

10 Deepfakes ejecutivos y desviación de pagos: el fraude con voz de dirección

Tendencia 10 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. La suplantación de identidad de directivos mediante voz e imagen sintéticas ha convertido el fraude de desviación de pagos en la consecuencia económica más frecuente de los ataques a pymes. La defensa ya no es tecnológica en primer lugar: es procedural, porque el objetivo del atacante es que una persona autorizada ejecute voluntariamente la operación fraudulenta.

Evidencia documental. El Informe de Ciberpreparación de Hiscox 2025 identifica las **pérdidas por fraude de desviación de pagos como la consecuencia más frecuente de los ciberataques sufridos por las pymes (53% de los casos)**, por delante de los ataques de denegación de servicio (49%) y del ransomware o extorsión (31%). La técnica conocida como *Business Email Compromise* —correo corporativo comprometido o falsificado que ordena transferencias urgentes— se ha sofisticado con la clonación de voz y los deepfakes de vídeo: la encuesta *AI Pulse Poll* de ISACA revela que el 71% de los profesionales europeos considera que los ataques de ingeniería social impulsados por IA son ya más difíciles de detectar, y el 58% admite que la IA ha degradado gravemente la capacidad de autenticar información digital.

ENISA documenta además la expansión del deepfake hacia campañas de vishing y fraude online en su análisis de 2025, y señala que más del 80% de las campañas de ingeniería social observadas a inicios de 2025 incorporaban ya componentes de IA. En España, el Ministerio del Interior registró en su informe de cibercriminalidad 429.677 fraudes informáticos en 2025, casi nueve de cada diez ciberdelitos conocidos por las fuerzas de seguridad. La medida con mayor retorno es de diseño organizativo: doble aprobación out-of-band para cualquier transferencia o cambio de datos bancarios, con un canal de verificación distinto al que origina la orden.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	11/25

Fuentes: Hiscox 2025, ISACA Pulse Poll, ENISA Threat Landscape 2025 y Ministerio del Interior – Anuarios y estadísticas

BLOC III

El coste real para la empresa mediana

El tercer bloque baja la amenaza al terreno de la cuenta de resultados y de la organización: qué cuesta un incidente, qué probabilidad hay de salir indemne y qué escasez de personas condiciona cualquier estrategia.

11 La factura de un incidente: 75.000 euros y la supervivencia en juego

12 Salir indemne es la excepción estadística

13 El daño invisible: estrés, bajas y deterioro de los equipos

14 La escasez estructural de talento que nadie puede contratar

15 La formación de plantilla como defensa de mayor retorno



11 La factura de un incidente: 75.000 euros y la supervivencia en juego

Tendencia 11 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El coste medio de un ciberataque grave para una pyme española se sitúa en una magnitud que puede absorber el beneficio anual completo de muchas empresas de 50 a 100 empleados. Comparado con ese coste, la inversión anual en prevención deja de ser una partida discutible: es la decisión financiera más asimétrica a favor del gasto que existe hoy en la pyme.

Evidencia documental. Las estimaciones sectoriales recogidas por INCIBE y la prensa económica de referencia sitúan el **coste medio de un incidente grave para una pyme española en torno a 75.000 euros**, una cifra que integra recuperación técnica, interrupción del negocio, daño reputacional y posibles sanciones. Análisis de aseguradoras y consultoras lo descomponen con más detalle: el rescate medio exigido en episodios de ransomware ronda los 45.000 euros, y la parada operativa se prolonga de media cerca de una semana. La consecuencia extrema es la que debería figurar en cualquier consejo de administración: las estimaciones divulgadas por medios de referencia señalan que **el 60% de las pymes que sufre un ciberataque grave no sobrevive a los seis meses siguientes**.

El contraste con el coste de prevenir es brutal: los servicios gestionados de seguridad para una empresa de ese tamaño se mueven en un rango de 300 a 2.000 euros mensuales, es decir, entre uno y dos órdenes de magnitud por debajo del coste de un solo incidente. El Informe de Ciberpreparación de Hiscox 2025 añade que un tercio de las pymes atacadas recibió multas de cuantía suficiente para dañar su salud financiera, lo que introduce al regulador como segundo acreedor del incidente. Para la dirección, el argumento ya no es técnico sino de continuidad: la ciberseguridad es la póliza de existencia de la empresa, y debe presentarse así en la negociación presupuestaria.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
5/5	4/5	4,5	05/25

Fuentes: INCIBE – Protege tu empresa y Hiscox 2025

12 Salir indemne es la excepción estadística

Tendencia 12 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. La narrativa del "ataque sin consecuencias" es estadísticamente marginal: la práctica totalidad de las pymes que sufren un incidente paga algún peaje. Planificar la seguridad asumiendo que el ataque será detectado y neutralizado sin daño es construir sobre el 1% de probabilidad favorable.

Evidencia documental. El dato más contundente del Informe de Ciberpreparación de Hiscox 2025 es que **solo el 1% de las pymes afectadas por ciberataques logró evitar cualquier consecuencia** derivada de los incidentes sufridos en el último año. La distribución de los daños muestra además que no se concentran en una única partida: un 53% de las afectadas registró pérdidas por fraude de desviación de pagos, un 49% sufrió ataques DDoS, un 31% padeció ransomware o extorsión, un 30% detectó mayor dificultad para atraer nuevos clientes y otro 30% provocó la exposición de datos de socios terceros, arrastrando la responsabilidad hacia la cadena comercial.

La frecuencia de exposición tampoco es baja: seis de cada diez pymes españolas sufrieron algún tipo de ataque en el último año según el mismo informe. La lectura estratégica es que el objetivo realista de un programa de seguridad no es la invulnerabilidad —inasequible— sino la reducción del daño esperado: menos probabilidad de entrada, detección más temprana y recuperación más rápida. Este cambio de marco, de la seguridad como escudo a la seguridad como amortiguador, es el que subyace a los marcos de resiliencia que promueven tanto NIS2 como los estándares de gestión. Presupuestar cero daño es una forma encubierta de no presupuestar.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	5/5	4,5	08/25

Fuentes: Hiscox. Informe de Ciberpreparación 2025

13 El daño invisible: estrés, bajas y deterioro de los equipos

Tendencia 13 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El impacto humano de un ciberataque —estrés, bajas médicas, pérdida de confianza interna— es la dimensión menos presupuestada y una de las más persistentes. Las empresas que incorporan la respuesta organizativa y el cuidado de las personas al plan de incidentes acortan la recuperación real, no solo la técnica.

Evidencia documental. El Informe de Ciberpreparación de Hiscox 2025 cuantifica lo que llama el coste invisible de los ataques: el **42% de las pymes reconoce que sus empleados experimentaron altos niveles de estrés** tras sufrir un incidente, el **39% registró un aumento de las bajas por enfermedad** y el **73% detectó efectos negativos en sus equipos** en el periodo posterior. En una organización de 60 personas, una secuela de ese tipo equivale a perder capacidad productiva durante meses justo cuando más se necesita para reconstruir. El fenómeno tiene una segunda derivada: el personal implicado en la gestión del incidente —habitualmente el pequeño equipo de TI o el responsable de sistemas, a menudo una sola persona— concentra la presión, lo que eleva el riesgo de rotación precisamente en el perfil más difícil de reemplazar del mercado laboral actual.

La respuesta no requiere inversión tecnológica: exige que el plan de respuesta a incidentes asigne roles, prevea apoyo externo y establezca comunicación interna honesta, y que los ejercicios de simulación incluyan la dimensión organizativa y no solo la técnica. La tendencia apunta a que las aseguradoras de ciberriesgo empezarán a valorar la madurez de la gestión de crisis empresarial —no solo los controles técnicos— en la fijación de primas, lo que convertirá este coste invisible en una variable económica explícita.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
3/5	4/5	3,5	22/25

Fuentes: Hiscox. Informe de Ciberpreparación 2025

14 La escasez estructural de talento que nadie puede contratar

Tendencia 14 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El freno principal de la ciberseguridad española no está en las herramientas, sino en las personas capaces de operarlas: el mercado necesita el doble de profesionales de los que hay disponibles. Para la empresa mediana, la consecuencia práctica es que "contratar a alguien que se ocupe de esto" es, en la mayoría de los casos, una estrategia inviable, y que el diseño del modelo de seguridad debe partir de esa restricción.

Evidencia documental. El diagnóstico conjunto de INCIBE y el Observatorio Nacional de Tecnología y Sociedad (ONTSI) cifra la demanda de profesionales de ciberseguridad en España en **más de 83.000 puestos**, frente a una oferta de apenas **42.283 profesionales** disponibles en el mercado laboral: una brecha superior a 40.000 personas que no muestra signos de cierre. La dimensión global del problema la documenta el *Global Cybersecurity Skills Gap Report* de Fortinet: el **86% de las organizaciones sufrió al menos una brecha de seguridad** en el último año, y más de la mitad (54% en la edición de 2025, 56% en la de 2026) atribuye esas brechas directamente a la falta de competencias y formación en seguridad; el déficit mundial se estima en 4,8 millones de profesionales.

Gartner aporta la lectura de negocio: solo el **48% de las iniciativas digitales alcanza sus objetivos**, y la escasez de talento figura entre las causas principales del fracaso. Para la empresa de 50 a 250 empleados, las implicaciones son tres: el talento disponible se concentra en grandes corporaciones que pagan mejor; el coste de un equipo interno mínimo es prohibitivo; y la dependencia de proveedores externos es estructural, no coyuntural, lo que eleva la importancia de saber gobernarlos. La salida realista combina externalización de la operación, formación interna del personal existente y automatización de las tareas repetitivas.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	5/5	4,5	09/25

Fuentes: ONTSI, Fortinet Cybersecurity Skills Gap Report y Gartner, encuesta CIO 2025

15 La formación de plantilla como defensa de mayor retorno

Tendencia 15 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. En un contexto de factor humano como vector dominante, la formación y la concienciación de la plantilla ofrecen la mejor relación coste-beneficio de todas las medidas disponibles para una empresa mediana. Pero la evidencia muestra que funciona como programa continuo de cultura, no como curso anual aislado.

Evidencia documental. Los vectores de entrada más frecuentes —phishing, credenciales comprometidas, ingeniería social— explotan decisiones humanas, no fallos técnicos: ENISA sitúa el phishing en el origen del 60% de las intrusiones europeas, y Fortinet identifica la falta de concienciación y formación como la primera causa de brechas a escala global por tercer año consecutivo. El Informe de Ciberpreparación de Hiscox 2025 aporta el dato conductual clave: el **87% de las pymes que sufrieron un ataque invierte ahora en formación** de seguridad, frente al 68% de las que no lo han sufrido, una brecha de casi veinte puntos que describe el patrón reactivo dominante —formarse después del incidente— y, a la vez, la efectividad percibida de la medida por quienes han pasado por él.

La misma fuente indica que el 94% de las pymes está aumentando su inversión en seguridad y protección de datos. Las prácticas con evidencia de eficacia son conocidas y asequibles: simulaciones periódicas de phishing con retroalimentación inmediata, protocolos claros de actuación ante sospechas, ejercicios de respuesta a incidentes con la dirección implicada y refuerzos breves y frecuentes en lugar de sesiones anuales densas. El límite de la medida también debe reconocerse: frente al phishing hiperpersonalizado por IA, la formación reduce la tasa de clic pero no la elimina, por lo que debe combinarse con controles técnicos —autenticación resistente, verificación de pagos— que no dependan del acierto humano.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	17/25

Fuentes: Hiscox 2025, ENISA Threat Landscape 2025 y Fortinet Skills Gap Report

BLOC IV

El marco regulatorio: de carga administrativa a palanca competitiva

El cuarto bloque aborda la regulación europea y española. La clave interpretativa: la norma se aplica aunque el país llegue tarde a transponerla, y quien se adelanta convierte la obligación en argumento comercial.

16 NIS2: aplicable de hecho aunque España llegue tarde

17 La responsabilidad personal de los órganos de dirección

18 ENS: la certificación que abre (o cierra) el mercado público

19 AI Act: la seguridad de la IA entra en el perímetro de cumplimiento

20 El cumplimiento proactivo como argumento comercial



16 NIS2: aplicable de hecho aunque España llegue tarde

Tendencia 16 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. La Directiva NIS2 es el texto que redefine la obligación de ciberseguridad para miles de empresas españolas, incluidas muchas medianas proveedoras de sectores regulados. La tardanza española en transponerla no suspende sus efectos prácticos: los clientes, aseguradoras y auditorías ya aplican sus estándares como referencia de diligencia debida.

Evidencia documental. La Directiva (UE) 2022/2555 (NIS2), publicada en diciembre de 2022, fijó el 17 de octubre de 2024 como fecha límite de transposición. España incumplió el plazo: la Comisión Europea envió carta de emplazamiento el 28 de noviembre de 2024 a 23 Estados miembros, y el 7 de mayo de 2025 elevó dictamen motivado contra 19 de ellos, España incluida; a mediados de 2026 la ley nacional de coordinación y gobernanza de la ciberseguridad seguía en tramitación. El contenido de la directiva, sin embargo, ya opera como estándar de referencia: ámbito ampliado a sectores como energía, transporte, banca, sanidad, infraestructura digital, servicios TIC y administración pública, con umbrales que capturan a empresas medianas proveedoras de esos sectores; obligación de evaluar el riesgo y aplicar medidas técnicas y organizativas proporcionales; **notificación de incidentes significativos con alerta temprana en 24 horas e informe completo en 72 horas**; y un régimen sancionador de hasta **10 millones de euros o el 2% de la facturación mundial** para entidades esenciales.

El balance de INCIBE muestra que la maquinaria de supervisión ya funciona: en 2025 se atendieron 401 incidentes en operadores esenciales e importantes del ámbito NIS2, con la banca (34%), el transporte (14%) y la energía (8%) como sectores más afectados. La empresa mediana debe determinar ya si entra en el perímetro —directamente o por la cadena de sus clientes— porque la adaptación exige meses, no semanas.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
5/5	5/5	5,0	03/25

Fuentes: EUR-Lex, Directiva NIS2, Comisión Europea – política NIS2 y Balance INCIBE 2025

17 La responsabilidad personal de los órganos de dirección

Tendencia 17 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. NIS2 introduce un cambio cualitativo que trasciende lo técnico: la ciberseguridad pasa a ser responsabilidad personal de los órganos de administración, que deben aprobar las medidas de gestión del riesgo, supervisar su aplicación y formarse para ello. El consejo que delegue la seguridad sin supervisarla asume un riesgo jurídico personal.

Evidencia documental. El artículo 20 de la Directiva NIS2 establece que los órganos de dirección de las entidades afectadas "aprueban las medidas de gestión de riesgos de ciberseguridad", "supervisan su aplicación" y "pueden ser considerados responsables del incumplimiento", además de exigir que sus miembros sigan formación específica y periódica. Es la primera vez que el derecho europeo personaliza de forma tan explícita la responsabilidad ciber en la alta dirección, siguiendo la estela del RGPD con los delegados de protección de datos pero yendo un paso más allá en la atribución directa. La evidencia de mercado muestra que la presión ya es real: el *Skills Gap Report* de Fortinet constata que la **mitad de las organizaciones (50% en la edición de 2026, 52% en la de 2025) declara que directivos o miembros de su consejo han afrontado consecuencias —multas e incluso la pérdida del puesto— tras un ciberataque**, y que el foco de los consejos en ciberseguridad se ha intensificado de forma sostenida, aunque el conocimiento efectivo sigue por debajo de la prioridad declarada.

La implicación para una empresa mediana es de gobierno: la seguridad necesita un lugar fijo en el orden del día del consejo o del comité de dirección, indicadores de riesgo comprensibles para perfiles no técnicos y un responsable —interno o externo— con línea directa a la máxima autoridad. Documentar esa supervisión es, en sí mismo, una medida de protección jurídica de los administradores.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
5/5	4/5	4,5	06/25

Fuentes: EUR-Lex, Directiva NIS2 y Fortinet Skills Gap Report

18 ENS: la certificación que abre (o cierra) el mercado público

Tendencia 18 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El Esquema Nacional de Seguridad se ha convertido, por vía contractual, en el billete de acceso al mercado de la administración pública española y a las cadenas de suministro que la sirven. Para una empresa mediana que licita o quiere licitar con el sector público, la certificación ENS no es un proyecto de cumplimiento sino una decisión comercial con retorno directo.

Evidencia documental. El Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad, modernizó el marco heredado de 2010 y amplió su alcance efectivo: aunque su obligación directa recae sobre las administraciones y empresas públicas, su aplicación se extiende a las empresas privadas que prestan servicios o soluciones a entidades del sector público, participan en licitaciones que exigen conformidad ENS o forman parte de la cadena de suministro de organismos públicos. En la práctica, los pliegos de los últimos años han convertido la conformidad ENS en requisito o en criterio de valoración habitual en contratos de servicios digitales, consultoría, ingeniería y logística administrativa. El esquema se estructura en un anexo de medidas organizadas por categorías —organizativas, operacionales y de protección— con tres niveles (básico, medio y alto) asignados según la criticidad de la información tratada, y exige auditoría y certificación periódica por entidades acreditadas, cuyo marco se gestiona a través del portal oficial del ENS del CCN.

Para una empresa de 50 a 100 empleados, la certificación en nivel básico o medio es un proyecto de varios meses que ordena, además, buena parte del programa de seguridad general: análisis de riesgos, políticas, control de accesos, copias, gestión de incidentes y continuidad. La tendencia observada en los pliegos apunta a una exigencia creciente, no a una relajación: esperar a que un concurso estratégico la exija para empezar el proyecto equivale a renunciar a ese concurso.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	5/5	4,5	07/25

Fuentes: BOE, RD 311/2022 y Portal ENS – CCN-CERT

19 AI Act: la seguridad de la IA entra en el perímetro de cumplimiento

Tendencia 19 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. El Reglamento Europeo de Inteligencia Artificial añade una capa nueva a la gestión de seguridad: quien despliega sistemas de IA —propios o de terceros— debe gobernar sus riesgos, su trazabilidad y su ciberseguridad. Para la empresa mediana que ya usa IA generativa en sus procesos, esto exige inventario, política de uso y control, no una homologación burocrática.

Evidencia documental. El Reglamento (UE) 2024/1689 (AI Act), en aplicación escalonada desde agosto de 2024, impone obligaciones diferenciadas por nivel de riesgo: prohibiciones de ciertos usos ya vigentes desde febrero de 2025, requisitos de gobernanza para modelos de propósito general desde agosto de 2025 y obligaciones completas para sistemas de alto riesgo —incluidas exigencias explícitas de ciberseguridad, robustez y trazabilidad— cuya aplicación se completa hacia 2026-2027. El contenido generado por IA está sujeto a obligaciones de etiquetado y transparencia, y los usos en biometría, empleo o servicios esenciales reciben escrutinio reforzado. La dimensión de seguridad es bidireccional: el AI Act exige proteger los sistemas de IA frente a manipulación, y la evidencia de amenazas muestra que la infraestructura de IA ya es objetivo —Check Point analizó en 2026 unos 10.000 servidores del Model Context Protocol y detectó vulnerabilidades en el 40%—, mientras el uso corporativo de IA generativa genera exposición de datos: 1 de cada 27 *prompts* enviados desde redes corporativas implicó riesgo significativo de fuga, según Check Point Research.

ISACA añade que el 87% de los profesionales europeos está preocupado por el uso no autorizado de IA por parte de los empleados. La respuesta proporcional para una empresa mediana es un registro de usos de IA, una política de uso aprobado con reglas sobre datos que no pueden salir del perímetro, y la incorporación de la IA al análisis de riesgos habitual.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
3/5	4/5	3,5	23/25

Fuentes: EUR-Lex, AI Act, Check Point Research e ISACA Pulse Poll

20 El cumplimiento proactivo como argumento comercial

Tendencia 20 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. La madurez demostrable en ciberseguridad —certificaciones, auditorías, seguro de ciberriesgo— se está convirtiendo en criterio de selección en licitaciones, homologaciones de proveedores y procesos de inversión. El cumplimiento deja de ser un centro de costes defensivo para operar como activo comercial: abre mercados y descuenta riesgo.

Evidencia documental. La mecánica ya es visible en tres circuitos distintos. En el público, la conformidad ENS se ha instalado en los pliegos como requisito o valoración, como se ha descrito en la ficha anterior. En el privado, las grandes corporaciones han endurecido la homologación de proveedores: el Informe de Ciberpreparación de Hiscox 2025 muestra que la revisión trimestral de vulnerabilidades y la evaluación de terceros son ya práctica mayoritaria entre las pymes que sobreviven comercialmente a sus clientes grandes. En el asegurador, el mercado de ciberseguros exige niveles mínimos de madurez para suscribir pólizas y ajusta primas a la postura demostrada, una dinámica que premia a quien puede acreditar controles —la penetración del ciberseguro en grandes empresas españolas se estima en torno al 75%, frente a menos del 25% en pymes, lo que deja un margen de diferenciación evidente para quien se anticipe—.

El marco de referencia para estructurar esa madurez sigue siendo la certificación ISO/IEC 27001 como sistema de gestión, complementada por ENS para el mercado público y por la documentación de la adecuación NIS2 cuando el sector lo exige. La tesis de fondo es que, hacia 2030, la pregunta "¿qué certificaciones de seguridad tienes?" figurará en cualquier proceso comercial relevante igual que hoy figura la salud financiera. Adelantarse a esa pregunta es una decisión de posicionamiento, no de cumplimiento.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	18/25

Fuentes: Hiscox 2025, Portal ENS – CCN-CERT y Comisión Europea – NIS2

BLOC V

Arquitectura 2030: decisiones de modelo y de tecnología

El último bloque mira al modelo operativo: qué arquitecturas de defensa se están imponiendo y cuáles son accesibles hoy para una organización de tamaño medio sin transformaciones traumáticas.

21 Zero Trust progresivo: verificar siempre, empezando por la identidad

22 Detección y respuesta automatizada: la IA defensiva se generaliza

23 SOC como servicio: vigilancia continua sin plantilla propia

24 SASE y seguridad en la nube para la empresa híbrida

25 Superficie de ataque, IA agéntica y la carrera hacia 2030



21 Zero Trust progresivo: verificar siempre, empezando por la identidad

Tendencia 21 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. La arquitectura de confianza cero —ningún acceso se concede por defecto, todo se verifica de forma continua— ha sustituido al perímetro como paradigma de referencia. Para la empresa mediana no supone un proyecto de gran envergadura sino una secuencia de decisiones acumulativas que empiezan por la identidad y la autenticación fuerte.

Evidencia documental. El modelo está formalizado en la publicación especial NIST SP 800-207, que define la arquitectura Zero Trust sobre el principio de que ningún recurso es implícitamente confiable por su ubicación en la red. La obsolescencia del perímetro clásico es un hecho documentado: el trabajo híbrido, los servicios en la nube y los dispositivos conectados han disuelto la frontera entre "dentro" y "fuera", y ENISA constata que las intrusiones se producen mayoritariamente por credenciales legítimas robadas —el phishing origina el 60% de los accesos iniciales—, no por asalto al cortafuegos. Los componentes de la transición son conocidos y graduables: autenticación multifactor en todos los accesos críticos (la medida individual con mayor efecto preventivo frente al robo de credenciales), gestión de identidades y accesos con privilegio mínimo, segmentación de red que limite el movimiento lateral de un atacante, y monitorización continua del comportamiento.

El propio balance de INCIBE apoya la urgencia: en 2025 se identificaron 3.849 casos de acceso o sustracción no autorizada de información, la categoría que más creció (un 171%), y buena parte de ellos se apoyó en credenciales comprometidas. La recomendación operativa es una hoja de ruta de doce a veinticuatro meses que empiece por MFA universal y gestión de identidades —capa donde el esfuerzo es menor y el efecto mayor— y avance hacia segmentación y verificación continua según madurez.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	13/25

Fuentes: NIST SP 800-207, ENISA Threat Landscape 2025 y Balance INCIBE 2025

22 Detección y respuesta automatizada: la IA defensiva se generaliza

Tendencia 22 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. La misma IA que ha industrializado el ataque es hoy la única vía realista de sostener la defensa ante el volumen de alertas. Las plataformas de detección y respuesta —EDR/XDR, SIEM, SOAR— han bajado de precio y de requisitos hasta situarse al alcance de la empresa mediana, sobre todo consumidas como servicio.

Evidencia documental. La presión cuantitativa justifica la automatización: con una media cercana a 2.000 ataques semanales por organización en España, según Check Point, ningún equipo pequeño puede revisar manualmente la telemetría que genera. Las estimaciones de los principales fabricantes de plataformas de detección indican que los sistemas con IA resuelven de forma automática en torno al **90% de las alertas de bajo nivel**, liberando la capacidad humana escasa para los casos que realmente la requieren. El stack funcional se ha estabilizado en tres capas complementarias: EDR/XDR para vigilancia y respuesta en puestos y servidores en tiempo real; SIEM para correlación de eventos de múltiples fuentes y detección de patrones anómalos; y SOAR para orquestar respuestas automáticas que reducen el tiempo de reacción de horas a minutos.

ENISA observa en paralelo que los atacantes explotan vulnerabilidades recién publicadas en cuestión de días, lo que hace estructuralmente imposible una defensa a velocidad manual. La encuesta de Fortinet muestra la dirección del gasto: el 97% de las organizaciones (edición de 2025) ya usaba o planeaba usar soluciones de seguridad potenciadas con IA. Para la empresa mediana, la puerta de entrada habitual es el EDR gestionado como servicio, que combina la tecnología con el equipo que la opera, y evita el error frecuente de adquirir herramientas que nadie vigila.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	14/25

Fuentes: Check Point Security Report 2026, ENISA Threat Landscape 2025 y Fortinet Skills Gap Report

23 SOC como servicio: vigilancia continua sin plantilla propia

Tendencia 23 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. La monitorización 24/7, antes patrimonio de grandes corporaciones, se ha democratizado en formato de servicio. Para una empresa mediana, el SOC como servicio o el MSSP es la única vía económicamente razonable de disponer de detección continua y respuesta especializada ante incidentes.

Evidencia documental. La aritmética es contundente: cubrir tres turnos durante todo el año exige un mínimo de cuatro a seis analistas, en un mercado donde la brecha de profesionales supera los 40.000 puestos según el diagnóstico de INCIBE-ONTSI y donde los salarios de seguridad crecen por encima de la media TIC. El mercado ha respondido con la oferta gestionada: las empresas de servicios concentran cerca del 70% del negocio del sector en España según el Observatorio DBK, y el estudio de INCIBE-CONETIC documenta un ecosistema de más de 3.400 firmas donde el servicio gestionado es la modalidad dominante.

La tarifa de mercado para una pyme —entre 300 y 2.000 euros mensuales según alcance— sitúa la vigilancia continua al alcance de prácticamente cualquier empresa con sistemas críticos. La clave de la contratación está en el alcance del compromiso: qué fuentes monitoriza el servicio, qué tiempos de detección y notificación garantiza, si incluye contención activa o solo alerta, y qué ocurre fuera del horario de oficina, precisamente cuando se producen muchos de los ataques. La tendencia hacia 2030 apunta a la convergencia de este servicio con los requisitos de NIS2 —detección, notificación en 24/72 horas—, de modo que el SOC gestionado pasará de capa de defensa a componente de la propia evidencia de cumplimiento.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	4/5	4,0	15/25

Fuentes: ONTSI, Observatorio DBK e INCIBE-CONETIC

24 SASE y seguridad en la nube para la empresa híbrida

Tendencia 24 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. Con aplicaciones y datos ya fuera del centro de datos propio, la seguridad de acceso migra a la nube: el modelo SASE integra conectividad y protección en una capa única que acompaña al usuario esté donde esté. Para la empresa mediana con plantilla híbrida, es la respuesta arquitectónica al perímetro disuelto, aunque su adopción va por detrás de la identidad y la detección.

Evidencia documental. La migración es medible: la mayoría de las empresas españolas de tamaño medio opera ya sobre suites cloud de productividad y aplicaciones SaaS, y los dispositivos remotos y el trabajo híbrido figuran entre los puntos de entrada más habituales de los incidentes, según la evidencia recopilada por INCIBE. El concepto SASE (*Secure Access Service Edge*), formalizado por los analistas de Gartner, integra en una arquitectura cloud funciones de red (SD-WAN) y de seguridad (pasarela web segura, acceso de confianza cero, cortafuegos como servicio), de modo que la política de seguridad se aplica al acceso y no a la ubicación física.

El mercado refleja la transición: la seguridad de redes mantiene el mayor volumen de ventas en Europa, pero el crecimiento se desplaza hacia la protección de datos y de accesos, como muestran los datos de Context. Para una empresa de 50 a 250 empleados, la adopción práctica no exige una arquitectura SASE completa de gran fabricante: los primeros pasos —acceso seguro basado en identidad, protección de navegación, VPN moderna o su sustituto ZTNA— se consumen como servicios modulares. La prioridad relativa de esta ficha es menor porque su valor se materializa cuando las capas anteriores (identidad, endpoints, copias) ya están resueltas; desplegar SASE sobre identidades débiles es sofisticar la fachada de un edificio sin cimientos.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
3/5	3/5	3,0	25/25

Fuentes: INCIBE – Protege tu empresa y Context / Channel Partner

25 Superficie de ataque, IA agéntica y la carrera hacia 2030

Tendencia 25 de 25 · Tesis, evidencia documental y cuadro de priorización

Tesis. Hacia 2030 el pulso entre la IA que ataca y la IA que defiende marcará la década: agentes autónomos en ambos bandos, sobre una superficie de exposición que no deja de crecer. La empresa mediana no controlará esa carrera, pero sí puede controlar dos variables decisivas: conocer continuamente su propia superficie expuesta y gobernar la IA que ya usa.

Evidencia documental. La expansión de la superficie es constatable: INCIBE identificó 237.028 sistemas vulnerables en España en 2025, y el **85% de las botnets detectadas estaba vinculada a dispositivos IoT**, señal de que la exposición crece con cada equipo conectado no gestionado. La disciplina emergente para afrontarla es la gestión continua de la superficie de ataque (EASM): descubrimiento automatizado de activos expuestos —dominios, servicios, certificados, instancias cloud olvidadas— desde la perspectiva del atacante, una capacidad que ya se ofrece como servicio a precios asumibles para la mediana empresa. En el frente de la IA, el *ENISA Threat Landscape 2025* documenta el ecosistema clandestino de modelos maliciosos (WormGPT, FraudGPT) y el uso ofensivo de plataformas legítimas para reconocimiento y evasión, mientras la encuesta de ISACA sitúa las amenazas impulsadas por IA como la principal preocupación del 51% de los profesionales europeos para 2026, con apenas un 14% de organizaciones que se declaran muy preparadas.

La siguiente frontera, ya visible en los análisis de riesgo, son los agentes autónomos: sistemas capaces de ejecutar cadenas completas de ataque —o de defensa— con intervención humana mínima. En gobierno, la figura del CISO se extiende a la empresa mediana en formato virtual, como servicio de dirección de seguridad a tiempo parcial. La agenda 2030 realista para una mediana empresa se resume en continuidad de lo que ya funciona —identidad, copias, detección gestionada, cultura— más dos incorporaciones: visibilidad continua de la superficie propia y gobierno explícito de la IA.

IMPACTO DE MERCADO	CONFIRMACIÓN	MEDIA	PRIORIDAD GLOBAL
4/5	3/5	3,5	24/25

Fuentes: Balance INCIBE 2025, ENISA Threat Landscape 2025 e ISACA Pulse Poll

Del ranking a la agenda: cómo aplicar las prioridades según el punto de partida

El orden de prioridad global ordena la agenda del conjunto de la mediana empresa española, pero cada organización parte de una posición distinta. Tres lecturas prácticas ayudan a traducir el ranking en decisiones.

La empresa que aún no ha estructurado nada. Para una organización sin políticas, sin responsable de seguridad y con controles básicos, la secuencia arranca por las fichas 06, 07 y 11: asumir la exposición, cerrar la puerta de entrada dominante (correo y credenciales) y dimensionar el riesgo financiero. En la práctica, esto se traduce en cuatro medidas de ejecución inmediata —autenticación multifactor en todos los accesos, copias de seguridad automáticas con restauración probada, actualización sistemática del software y un primer ciclo de formación con simulación de phishing—, seguidas de un diagnóstico formal: inventario de activos, evaluación de riesgos y revisión del mapa normativo aplicable. Ninguna de estas medidas exige una inversión transformadora; todas exigen decisión.

La empresa proveedora de sectores regulados o de la administración. Aquí la jerarquía cambia: las fichas 16, 17, 18 y 09 pasan al primer plano porque la exposición principal no es el ataque sino la descalificación. Determinar el encaje en el perímetro de NIS2 —directo o por la cadena de clientes—, certificar ENS si se licita con el sector público, documentar la supervisión directiva del riesgo y ordenar la evaluación de terceros son las decisiones que condicionan los ingresos de los próximos tres ejercicios. La inversión técnica sin esa capa de gobierno deja la empresa técnicamente protegida y comercialmente descartada.

La empresa con bases resueltas que mira a 2030. Con identidad, copias, formación y detección gestionada ya en marcha, la atención se desplaza a las fichas del bloque V: consolidar la vigilancia 24/7 como servicio, avanzar en la arquitectura de confianza cero por capas, incorporar la gestión continua de la superficie de ataque y gobernar el uso de la inteligencia artificial. En este nivel, el diferencial deja de ser el catálogo de controles —homogéneo entre competidores— y pasa a ser la velocidad de detección y recuperación y la calidad de la evidencia de madurez que la empresa puede presentar a clientes, aseguradoras y reguladores.

Ocho hipótesis de trabajo hacia 2030

Deducciones analíticas del equipo — nunca hechos acreditados

Las siguientes proposiciones son **inferencias del Equipo de Análisis de Smart Team**, construidas sobre la evidencia anterior pero no atribuibles a ninguna fuente. Se presentan como hipótesis a contrastar, no como hechos.

H1 · La transposición española de NIS2 activará una ola de adecuación concentrada en 2027–2028.

Cuando la ley nacional entre en vigor, miles de empresas medianas descubrirán simultáneamente que están en el perímetro o en la cadena de quien lo está, y la capacidad de auditoría y consultoría del país se saturará. Quien se adecue antes evitará la subasta de servicios.

H2 · El primer incidente grave atribuido a un agente autónomo ofensivo se producirá antes de 2028 y cambiará el debate público.

La trayectoria del phishing industrializado y de los modelos maliciosos documentada por ENISA sugiere que la automatización completa de la cadena de ataque es cuestión de iteraciones, no de décadas.

H3 · El ciberseguro se convertirá en auditor encubierto de la mediana empresa.

Las aseguradoras, con primas condicionadas a controles verificables, ejercerán de facto la supervisión que el regulador no puede escalar, y sus cuestionarios se convertirán en el estándar mínimo práctico de seguridad de la pyme.

H4 · La certificación ENS saltará del mercado público al privado.

Las grandes corporaciones empezarán a aceptarla —o exigirla— como atajo de homologación de proveedores, igual que hicieron antes con ISO 27001, reduciendo el coste de los cuestionarios ad hoc.

Ocho hipótesis de trabajo hacia 2030

Deducciones analíticas del equipo — nunca hechos acreditados

H5 · La brecha de talento no se cerrará: se sorteará.

La combinación de servicios gestionados, automatización y formación interna absorberá la mayor parte del déficit de 40.000 profesionales antes de que el sistema educativo llegue a cubrirlo. La escasez dejará de ser noticia sin dejar de ser realidad.

H6 · El correo electrónico dejará de ser el canal dominante del fraude antes de 2030.

A medida que MFA resistente y filtros con IA encarezcan el phishing clásico, la ingeniería social migrará a videollamada sintética y mensajería corporativa, y la verificación de voz e imagen se incorporará a los procedimientos financieros estándar.

H7 · La mediana empresa española convergerá hacia un "núcleo de seguridad" homogéneo.

Identidad fuerte, copias inmutables, EDR gestionado, SOC como servicio y formación continua formarán un paquete de facto —impulsado por aseguradoras, pliegos y proveedores— comparable a lo que la contabilidad normalizada es hoy: nadie lo celebrará, pero todos lo exigirán.

H8 · El diferencial competitivo no será tecnológico sino de gobierno.

Dos empresas con idénticas herramientas obtendrán resultados distintos según la calidad de su supervisión directiva; NIS2 convertirá esa diferencia en responsabilidad jurídica y el mercado la convertirá en precio.

Síntesis ejecutiva

La ciberseguridad de la empresa española mediana se decide en tres frentes simultáneos. El primero es **estadístico**: con 122.223 incidentes gestionados por INCIBE en 2025, una media de casi 2.000 ataques semanales por organización y solo un 1% de pymes que sale indemne, la planificación debe asumir el incidente como escenario base. El segundo es **regulatorio**: NIS2 —aplicable como estándar aunque la transposición española llegue tarde—, el ENS como llave del mercado público y el AI Act como nuevo perímetro convierten la seguridad en condición legal y comercial, con responsabilidad personal para la dirección. El tercero es **económico**: un incidente medio cuesta en torno a 75.000 euros y puede comprometer la supervivencia, mientras la protección gestionada cuesta una fracción marginal de esa cifra.

La agenda que se desprende de las 25 tendencias es menos exótica de lo que sugiere el ruido tecnológico. Las medidas de mayor efecto —autenticación multifactor, copias probadas, formación continua, detección gestionada, gobierno del riesgo desde la dirección— son conocidas, asequibles y verificables. Lo que ha cambiado hasta 2026 es el coste de no ejecutarlas: la amenaza se ha industrializado con IA, el regulador ha personalizado la responsabilidad y el mercado ha empezado a premiar a quien puede demostrar madurez. Hacia 2030, la ciberseguridad no distinguirá a las empresas por su tamaño, sino por su diligencia.

Fuentes principales

- INCIBE y CONETIC – Estudio sobre la industria de la ciberseguridad en España 2025
- INCIBE – Balance de Ciberseguridad 2025 (vía España Digital)
- INCIBE – Protege tu empresa
- ENISA – Threat Landscape 2025
- Hiscox – Informe de Ciberpreparación 2025
- ISACA – Tech Trends and Priorities Pulse Poll
- Fortinet – Global Cybersecurity Skills Gap Report
- EUR-Lex – Directiva (UE) 2022/2555 (NIS2)
- Comisión Europea – Política NIS2
- BOE – Real Decreto 311/2022, Esquema Nacional de Seguridad
- CCN-CERT – Portal del Esquema Nacional de Seguridad
- EUR-Lex – Reglamento (UE) 2024/1689 (AI Act)
- NIST – SP 800-207, Zero Trust Architecture
- Check Point – Security Report 2026
- Context / Channel Partner – Ventas de ciberseguridad en España 2025
- Gartner – Encuesta CIO: iniciativas digitales y objetivos de negocio
- SlashNext / Infosecurity Magazine – Auge del phishing con IA generativa
- ONTSI – Observatorio Nacional de Tecnología y Sociedad
- Observatorio Sectorial DBK – Informa
- Ministerio del Interior – Anuarios y estadísticas (Informe de Cibercriminalidad)

smart-team.tech