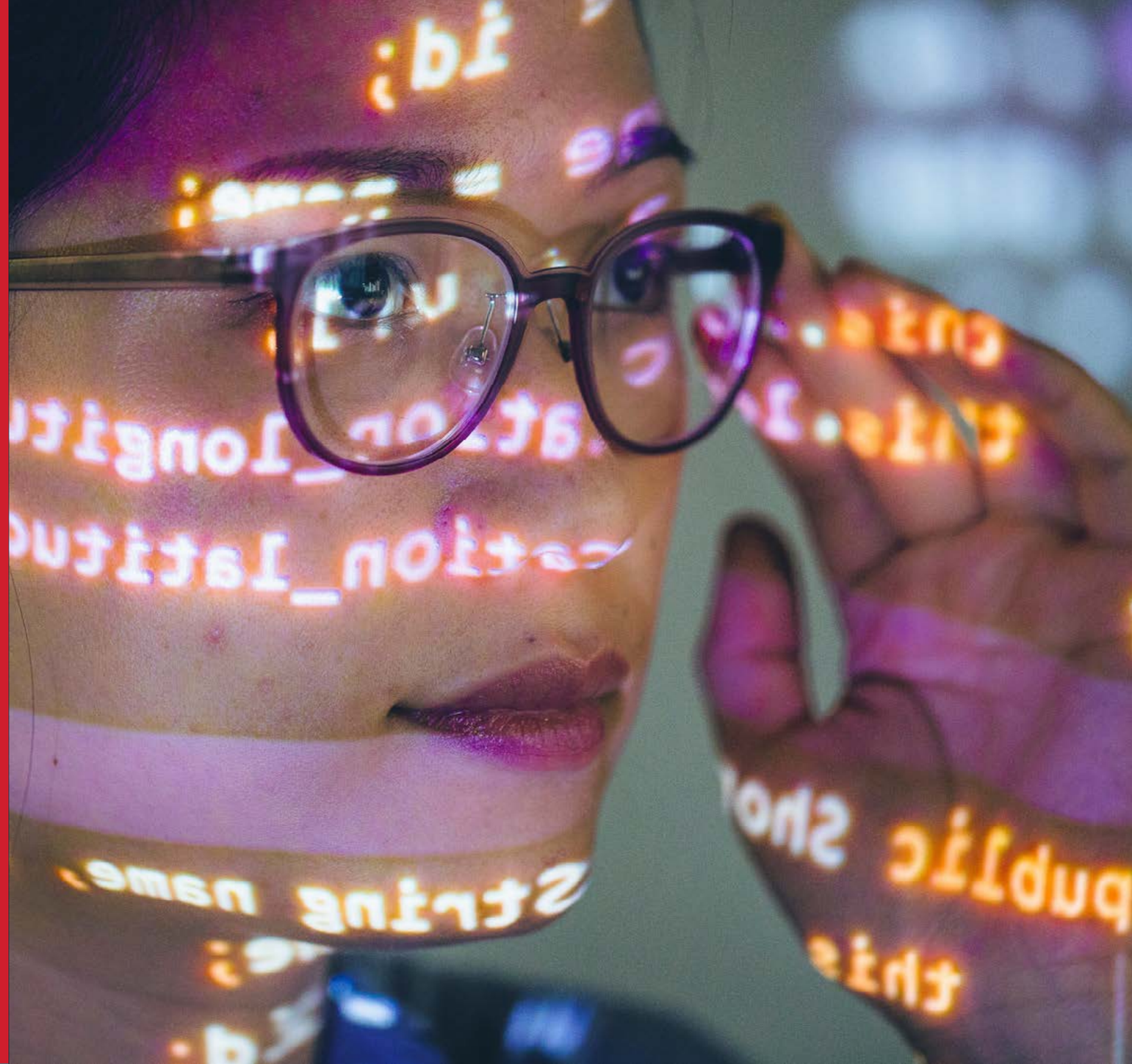
AON

VI Estudio Anual de Aon sobre Ciberseguridad y Gestión del Riesgo Ciber en España

Junio 2025



Entidades Colaboradoras

Allianz

BHSI
BERKSHIRE HATHAWAY SPECIALTY INSURANCE

AIG

TOKIO MARINE HCC

beazley

AXA

QBE

CHUBB

GARRIGUES

ZURICH

HISCOX

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

Arch

resilience

Índice

1. Resumen Ejecutivo 4
2. Respuesta a incidentes y protocolo de siniestros 10
3. Evolución y retos de la siniestralidad en España 16
4. Panorama del riesgo cibernético en España 26
   a. Ciberseguridad en grandes cuentas en 2024 27
   b. Ciberseguridad en mercado medio en 2024 36
5. Principales Novedades Normativas 43
   a. Nuevo mapa de autoridades en materia de ciberseguridad y su interrelación con la autoridad de supervisión de privacidad 44
   b. Marco regulador de la ciberseguridad en 2024/2025: certezas e incertidumbres 53
6. Checklist Normativa NIS2: ámbito de aplicación y cumplimiento 62
7. Nuevos riesgos y amenazas en ciberseguros: escenario emergente en 2025 65
8. Estrategia integral de ciberresiliencia: conexión entre IT y el C-Level 74
9. Análisis comparativo de madurez cibernética: España vs. EMEA 79
10. Metodología 87

1

Resumen Ejecutivo

1

Siguiendo la estructura de los informes anteriores, este informe de la VI edición explora la situación del riesgo cyber desde diferentes perspectivas como por ejemplo los planes de respuesta, la evolución de la siniestralidad, el mercado actual, las normativas, entre otros. Todo ello refleja un entorno de una rápida transformación. Hemos sido testigos de una sofisticación creciente de las amenazas, un aumento sostenido de la siniestralidad, y una consolidación del seguro cyber como herramienta crítica para garantizar la continuidad de las empresas.

Durante los últimos años, hemos visto que los casos de ransomware han puesto a **prueba los planes de respuesta ante incidentes** de muchas organizaciones, los cuales actúan como un factor crítico para poder minimizar el impacto. Activar la póliza en las primeras 24—48 horas, notificar al asegurador y movilizar los proveedores especializados es clave para contener el daño y acelerar la recuperación. De esta manera, los incidentes nos han revelado que no solo el peritaje y la cobertura son clave, sino también la **mejora continua de las medidas** y la necesidad de la **adaptación de las condiciones** de la póliza en futuras renovaciones. Todo ello nos ha mostrado que el protocolo de siniestros y los planes de respuesta no se tratan simplemente de un trámite, sino una pieza muy importante que forma parte de la estrategia cibernética en las organizaciones.

Siniestralidad: El riesgo cibernético se intensifica. La frecuencia de los incidentes cyber sigue aumentando. Al mismo tiempo, las instituciones encargadas de identificar y gestionar incidentes disponen de una capacidad reactiva más afinada, aunque esto no implica una mayor contención.

- Por **frecuencia** de los incidentes, las **brechas de seguridad** están en el primer lugar. También hemos observado que el **fallo de sistemas o ataques al proveedor** que cada vez tiene una mayor frecuencia, son además una de las mayores preocupaciones actuales.
- Por **coste económico** de los incidentes, el ransomware continúa siendo la amenaza más costosa. Y por sectores, industrias como construcción, educación y logística, y **servicios profesionales** están más expuestos a las amenazas.
- En cuanto a la **facturación**, las compañías **de 50 millones** concentran la mayor frecuencia de siniestros. Esto se debe principalmente a la subestimación de su exposición real.

Mercado asegurador: el mercado asegurador ha entrado en una fase de **consolidación.**

- Grandes cuentas: Durante el último año, hemos observado una ampliación de coberturas y capacidades aseguradoras, una reducción generalizada de primas y un aumento de competencia. Adicionalmente, las aseguradoras empiezan a ofrecer servicios de **valor añadido de prevención y gestión de incidentes.** Esto ha facilitado la contratación de mayores límites, especialmente entre empresas con buena postura de seguridad. Además, existen servicios **de análisis de cuantificación,** permitiendo a las empresas comprender la exposición financiera potencial ante incidentes y determinar si el programa actual es adecuado. Para este año, se espera una **continuidad general** de esta tendencia como el mantenimiento de su interés, pero con una **posible moderación en las estrategias comerciales agresivas,** lo que implicaría una mayor selectividad.
- Mercado medio: el mercado medio actual también se caracteriza por un incremento en los límites, una estabilización de precios y una evolución en las condiciones. Además, el proceso de suscripción ha evolucionado hacia **modelos más flexibles,** basados en mayor **compromiso y acompañamiento** integrando prevención, detección, respuesta y recuperación. Las evaluaciones automáticas y los formularios simplificados permiten adaptar condiciones y límites según la evolución del cliente, lo que hace que el seguro se convierta en una herramienta real de resiliencia.

Novedades Normativas:

El entorno normativo se endurece de cara a 2025 con la implementación de la Directiva NIS 2, que sustituye y amplía la anterior NIS. Tiene el objetivo de reforzar el nivel común de ciberseguridad de todos los Estados miembros. Regula las obligaciones de gestión de riesgos y notificación y exigirá a muchas organizaciones adaptar rápidamente sus estructuras de seguridad digital. La directiva también refuerza la supervisión y el régimen sancionador, así mismo, las autoridades nacionales podrán realizar inspecciones y aplicar sanciones económicas. En España, su transposición se concreta en el Centro Nacional de Ciberseguridad (CNC) como Autoridad Nacional Competente y CSIRTs de referencia.

En cuanto al ámbito de aplicación de NIS 2, se amplía para incluir sectores críticos que antes no estaban regulados directamente, como el sector agroalimentario, farmacéutico, manufacturero, gestión de residuos, logística, distribución digital o los proveedores de servicios en la nube, entre otros. Aquellas organizaciones que están clasificadas como “esenciales” o “importantes” deberán implementar medidas de ciberseguridad analizando su riesgo. Dentro del ámbito español, esta normativa se aplica a las entidades que residan en España o desarrollen su actividad en nuestro país.

Además, cabe destacar dentro de la directiva, la exigencia de la gestión estructurada de la cadena de suministro, obligando a las empresas a evaluar los riesgos que puedan derivarse de sus proveedores y subcontratistas. Esto impactará significativamente en el diseño de las pólizas cyber.

Sin embargo, este anteproyecto dependerá en gran medida de la implementación práctica. Existe la necesidad de integrar culturas y competencias dispersas en una única gobernanza.

Amenazas emergentes

El entorno de amenazas se ha vuelto cada vez más volátil y complejo.

- la **Inteligencia Artificial Generativa** ha tenido un gran impacto. Además de servir para la automatización de los sistemas, dar soporte en las tareas, su uso ha sido adoptado por actores maliciosos para crear nuevas vulnerabilidades. Como consecuencia, se ha generado un desafío para el sector asegurador. Algunas pólizas ya incluyen lenguaje afirmativo para cubrir el uso responsable de IA, siempre que se apliquen controles adecuados. En cuanto a la adopción interna de la IA en las organizaciones, es importante implementar un entorno controlado para probar y validar herramientas, asegurar una gobernanza 360°, adoptar los estándares internacionales como NIS AI-RMF; ISO/IEC 42001 o ISO 23894, y por último, actualizar el threat modeling tradicional.
- **Shadow IT:** se refiere al conjunto de aplicaciones, dispositivos y servicios digitales que operan al margen del control de los equipos de tecnología y seguridad. Surge muchas veces cuando los empleados instalan herramientas o plataformas sin aprobación formal. A primera vista parece inofensivo, pero puede convertirse en una grieta crítica de seguridad. Debido al entorno de trabajo híbrido, este fenómeno se ha intensificado. Los riesgos cyber que se pueden producir debido a Shadow IT son pérdida de control sobre los datos, incumplimiento normativo y exposición de información confidencial, entre otros. Además, complica significativamente la respuesta ante incidentes. Por lo tanto, recomendamos impulsar políticas claras sobre el uso de tecnología, integrar las tecnologías de descubrimiento de activos y análisis de tráfico.
- **Ciberataques a la cadena de suministros** (El talón de Alquiles): una de las mayores amenazas actuales para las organizaciones es el riesgo de su cadena de suministro digital. Su sofisticación, alcance y frecuencia han crecido significativamente en los últimos años. Desde los proveedores consolidados hasta los pequeños subcontratistas sin controles mínimos de seguridad pueden ser objetivos de ataques. Para afrontar esta situación, el mercado asegurador ha evolucionado en cuanto a la inclusión de coberturas específicas para interrupciones causadas por terceros, tanto para proveedores IT como non-IT. Y para que las empresas estén mejor preparadas, es importante identificar cuáles son los servicios y datos críticos y revisar bien los contratos con dichos proveedores.

Conclusión:

Después de haber visto las amenazas actuales y emergentes, se puede concluir que el enfoque tradicional de ciberseguridad basado en la noción de un perímetro corporativo confiable ha quedado obsoleto. Para ello, el modelo de Zero Trust se ha convertido en una exigencia técnica, estratégica y aseguradora. “Nunca confíes, verifica siempre” es un estándar de facto para todas las empresas.

Por último, también hemos visto que para definir estrategias de ciberseguridad, el CISO es una figura clave y el interlocutor principal para la alta dirección, influyendo en decisiones críticas. Para fomentar una cultura organizacional orientada a la resiliencia digital, se recomienda que las organizaciones integren al CISO, CRO, CFO y el Consejo para mejorar la respuesta ante incidentes. Deben compartir conciencia del riesgo, asegurar una gobernanza clara y colaborativa, y lograr una inversión sostenida en capacidades.

En este contexto, la gestión integral del riesgo cibernético se consolida como un pilar esencial para la sostenibilidad y competitividad empresarial. No se trata solo de contratar un seguro, sino de construir una estrategia coordinada que combine prevención, análisis, respuesta y transferencia del riesgo. Las organizaciones que adoptan este enfoque holístico no solo protegen sus activos digitales, sino que también fortalecen su capacidad de adaptación, mejoran su reputación y generan confianza en sus clientes, socios e inversores.

La ciberresiliencia ya no es una opción: es una ventaja estratégica.

2

Respuesta a Incidentes y protocolo de siniestros

Ransomware en 2024: amenazas emergentes y estrategias efectivas de gestión de incidentes y siniestros

En el contexto actual de transformación digital acelerada, las organizaciones enfrentan un entorno tecnológico en constante cambio, donde la innovación va acompañada de nuevos riesgos. A medida que las empresas adoptan tecnologías emergentes para mejorar su competitividad y eficiencia, también amplían su superficie de ataque, exponiéndose a actores maliciosos cada vez más sofisticados. El año 2024 no ha sido la excepción: las amenazas cibernéticas continúan evolucionando, integrando técnicas avanzadas y utilizando herramientas como la inteligencia artificial generativa. Esta realidad demanda un cambio de paradigma en la forma en que las organizaciones perciben y gestionan los incidentes de seguridad, pasando de una postura reactiva a una verdaderamente proactiva.

Panorama de Amenazas Cibernéticas en 2024

Durante 2024, se ha evidenciado un incremento considerable en la sofisticación y frecuencia de los ciberataques. Las organizaciones se enfrentan a un ecosistema digital mucho más complejo, donde la automatización de amenazas, el uso de inteligencia artificial y la interconectividad con terceros incrementan la superficie de riesgo. A continuación, se describen las amenazas más relevantes que afectan al tejido empresarial actual y que deben ser consideradas prioritarias en las estrategias de ciberresiliencia.

01 Ransomware

Uno de los vectores de ataque más presentes y destructivos sigue siendo el ransomware. Según datos de Aon, entre el tercer y cuarto trimestre de 2024, el número de "observed ransomware breaches" aumentó un 28% en promedio. Esta amenaza cifra archivos y sistemas, paralizando operaciones críticas hasta que se paga un rescate, normalmente en criptomonedas. Los atacantes utilizan ahora técnicas más dirigidas, aprovechando el reconocimiento previo y la explotación de vulnerabilidades. La sofisticación del ransomware también incluye el uso de estrategias de doble extorsión, donde además del cifrado de datos, se amenaza con la publicación de información confidencial.

02 Vulnerabilidades en IoT

La proliferación de dispositivos del Internet de las Cosas ha ampliado los puntos de entrada para los atacantes. Muchos de estos dispositivos carecen de actualizaciones de seguridad o tienen configuraciones predeterminadas, facilitando accesos no autorizados y ataques DDoS. Este tipo de amenazas han sido especialmente relevantes en entornos industriales y sanitarios, donde la integridad y disponibilidad de los sistemas conectados es crítica para la operación.

03 Phishing e Ingeniería Social

Los ataques de phishing siguen siendo muy efectivos, especialmente en contextos de teletrabajo y sobrecarga informativa. Engañan a los usuarios para que revelen credenciales, instalen malware o ejecuten acciones comprometedoras. La evolución de la inteligencia artificial ha permitido que estos ataques sean cada vez más creíbles, con correos y sitios web falsos difíciles de distinguir de los originales.

04 Ataques a la Cadena de Suministro

El uso de terceros con poca madurez en ciberseguridad ha aumentado la frecuencia de ataques a través de proveedores. Estos incidentes son complejos por la cantidad de partes involucradas y la dificultad de acceder a información clave que sólo está en manos del proveedor comprometido. La dependencia digital entre organizaciones implica que la ciberseguridad de una empresa está íntimamente relacionada con la de sus socios estratégicos.

05 Amenazas Persistentes Avanzadas (APT)

Frecuentemente respaldadas por gobiernos, estas amenazas son sigilosas, persistentes y difíciles de detectar. Están dirigidas principalmente a entidades gubernamentales y empresas con activos críticos. La motivación detrás de estos ataques puede ser tanto política como económica, lo que incrementa su complejidad y duración en el tiempo.

06 IA ofensiva, exploits y entornos en la nube

La inteligencia artificial también está siendo utilizada con fines ofensivos, facilitando la automatización de ataques y la creación de contenido falso. A esto se suman los exploits de día cero y configuraciones erróneas en entornos cloud. Las brechas en la nube están muchas veces relacionadas con errores humanos, como permisos mal configurados o ausencia de autenticación multifactor.

07 Amenazas Internas y Riesgo Sistémico

El personal con acceso privilegiado representa un vector crítico, especialmente sin políticas de seguridad robustas. Los ataques que afectan a servicios de nube pueden generar impactos sistémicos, comprometiendo a miles de clientes. Este tipo de eventos plantea nuevos desafíos para el sector asegurador, que busca delimitar su exposición frente a incidentes que puedan considerarse catastróficos o de “afectación masiva”.

Protocolo de Siniestros: Activación y Coordinación Aseguradora

La correcta gestión de un siniestro cibernético no solo depende de la respuesta técnica. La activación oportuna de la cobertura correspondiente en la póliza de ciber es fundamental para minimizar los impactos y garantizar el acceso a servicios especializados. La colaboración entre los equipos técnicos, legales y aseguradores resulta esencial para garantizar una respuesta integral. En primer lugar, la notificación al asegurador debe realizarse tan pronto como se tenga conocimiento del incidente, idealmente dentro de las primeras 24-48 horas, ya que algunas pólizas establecen plazos máximos estrictos, como 72 horas. Esta notificación permite activar la red de proveedores aprobados por la aseguradora, que puede incluir expertos en forense digital, comunicación de crisis, asesoría legal y negociación con atacantes, si es necesario.

Durante el proceso, es imprescindible recopilar y documentar toda la evidencia relacionada con el incidente: cronología de eventos, decisiones adoptadas, correos internos, logs, reportes técnicos y cualquier comunicación con terceros. Esta documentación no solo será evaluada por el asegurador para determinar la cobertura del siniestro, sino que también facilitará la realización de auditorías internas y externas posteriores. El corredor de seguros juega un rol fundamental como puente entre la empresa y la aseguradora, ayudando a interpretar la póliza, guiar en los trámites de notificación y asegurar que se cumplan los requisitos de cobertura.

Posteriormente, el asegurador realizará una evaluación para determinar qué partidas serán cubiertas, incluyendo los costes de respuesta, pérdidas por interrupción de negocio, asesoría legal, posibles rescates pagados, restauración de sistemas y gastos de comunicación reputacional. Es importante tener en cuenta posibles franquicias, sublímites y exclusiones dentro de la póliza, que pueden influir en el monto final cubierto. Finalmente, como parte del aprendizaje organizacional, se recomienda realizar una revisión crítica del incidente y del tratamiento asegurador recibido, con el objetivo de ajustar límites de cobertura, exclusiones y condiciones para futuras renovaciones del programa de seguros.

Gestión de incidentes por Ransomware: un caso práctico

Fase 1. Infección y Demanda de Rescate

El ransomware se infiltra y compromete activos críticos. Se cifra la información y se exige un rescate. Se interrumpen las operaciones y comienzan a generarse pérdidas económicas. Esta fase inicial es altamente estresante para los equipos internos, ya que la organización pierde visibilidad y control sobre sus recursos digitales.

Fase 2. Detección y Reporte Inicial

Los equipos de IT y los usuarios detectan comportamientos anómalos. Se canalizan los primeros reportes y se activa el plan de respuesta. Es esencial la existencia de procedimientos claros y entrenados. Si hay afectación de datos personales, se activan las obligaciones del RGPD. Además, se inician las comunicaciones internas de crisis, estableciendo canales seguros para coordinar la respuesta sin agravar la situación.

Fase 3. Confirmación del Incidente y Aislamiento

Se delimita el alcance del ataque y se protegen los sistemas no comprometidos. Se activan mecanismos de contención como la desconexión de redes. Se notifica a reguladores, si aplica. Esta fase puede incluir la segregación geográfica o funcional de sistemas para evitar la propagación del malware.

Fase 4. Análisis Forense

Se realiza una investigación detallada del incidente: entrada del malware, exfiltración, estado de los respaldos. Este análisis permite tomar decisiones informadas sobre la recuperación. También ayuda a comprender si el ataque fue oportunista o dirigido, lo que influye directamente en la estrategia de contención futura.

Fase 5. Evaluación y Posible Negociación

Si no existen alternativas técnicas viables, se evalúa la posibilidad de contactar con los atacantes, siempre con asesoramiento legal y bajo medidas estrictas de confidencialidad. En algunos países, el pago del rescate puede estar sujeto a restricciones legales si los atacantes forman parte de entidades sancionadas.

Fase 6. Restauración y Mejora Continua

Se reintegran sistemas, se validan respaldos, se aplican parches y se refuerzan controles. También se revisan y actualizan los planes de respuesta, se realizan auditorías y se comunica a los stakeholders. Esta fase también puede incluir campañas de concienciación y capacitación para reforzar la importancia de una cultura de seguridad.

Conclusión

El panorama de ciberseguridad en 2024 impone retos cada vez más complejos. No solo es indispensable una gestión técnica eficaz ante incidentes como el ransomware, sino también una visión aseguradora que permita activar con agilidad los recursos de la póliza contratada. Adoptar un enfoque multidisciplinar, que combine la respuesta operativa con la gestión formal del siniestro, es la vía más sólida para proteger los activos críticos de las organizaciones y garantizar la continuidad del negocio frente a amenazas cada vez más sofisticadas. El ciberseguro, lejos de ser un simple respaldo financiero, se convierte en una herramienta esencial dentro del ecosistema de resiliencia digital corporativa.

3

Evolución y retos de la siniestralidad en España

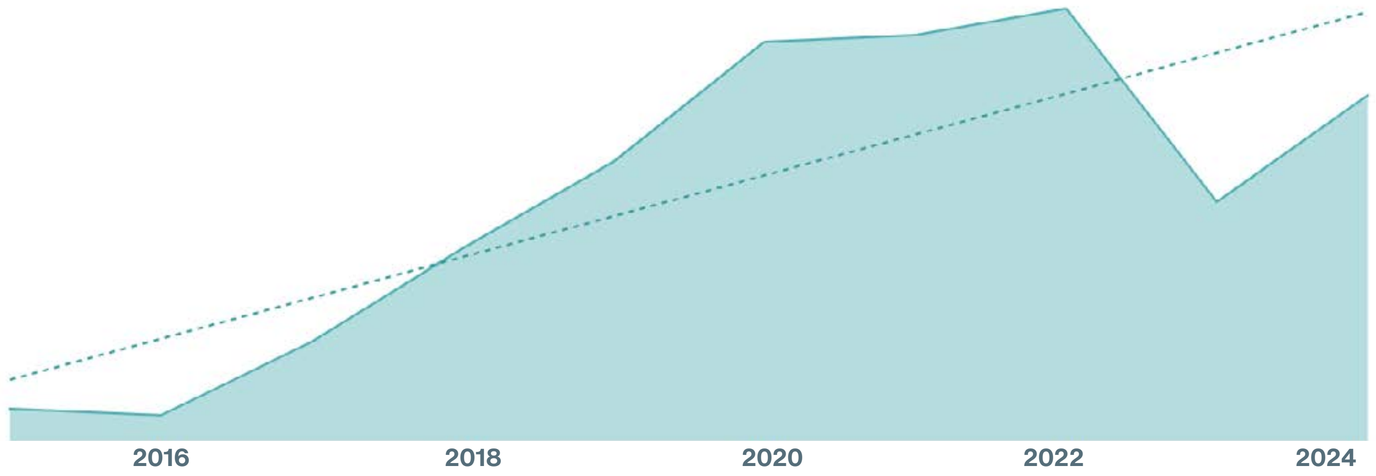
3 Evolución y retos de la siniestralidad en España

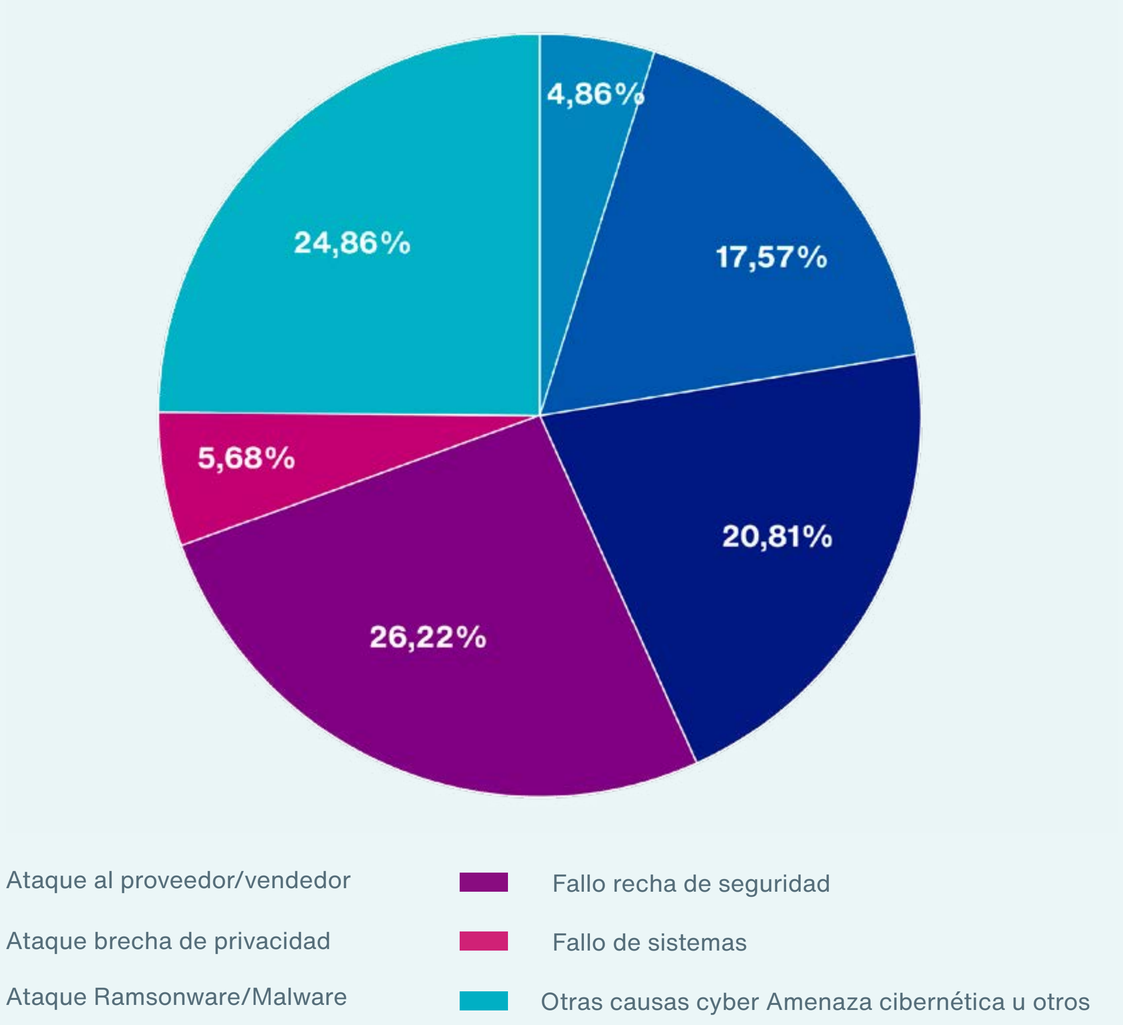
El ecosistema de ciberseguridad en España atraviesa una etapa de clara intensificación. Los datos más recientes del **Balance de Ciberseguridad 2024 del INCIBE** revelan que se gestionaron **97.348 incidentes** a lo largo del año, lo que representa un **aumento del 16,6 % respecto a 2023**, cuando se registraron 83.517 casos. Esta cifra incluye tanto a **ciudadanos como a empresas, operadores críticos y la red académica y de investigación (RedIRIS).** Esta diversificación de las víctimas evidencia que el riesgo no se limita a sectores tradicionalmente expuestos, sino que **se ha democratizado el ciberataque.**

Este crecimiento no solo habla de una mayor superficie de ataque, sino también de una **capacidad reactiva más afinada** por parte de las instituciones encargadas de identificar y gestionar incidentes. Aun así, el ritmo de detección no necesariamente implica una mejor contención. Al contrario: en muchas ocasiones, lo que se detecta **ya ha causado impacto económico o reputacional.**

A esta situación se suma la perspectiva penal. Según los balances del Ministerio del Interior (2T 2024), las estafas informáticas representan el 88,9 % de toda la cibercriminalidad denunciada en España. Es decir, más de 211.000 delitos informáticos fueron registrados, convirtiendo este tipo de fraude en la **infracción penal más común dentro del entorno digital** y en una de las más frecuentes a nivel general, al representar el **17,3 % de todas las infracciones penales denunciadas.**

Frecuencia de siniestralidad por año





Frecuencia no es lo mismo que gravedad: causas más comunes vs causas más costosas

Uno de los aspectos más relevantes en el análisis de siniestralidad cibernética es entender que **los tipos de incidentes más frecuentes no son necesariamente los más dañinos en términos económicos.** Esta diferencia es crucial para orientar tanto los recursos de protección como las decisiones estratégicas en seguros.

Según los datos extraídos del conjunto de siniestros analizados, las tres principales causas por número de incidentes en 2024 han sido:

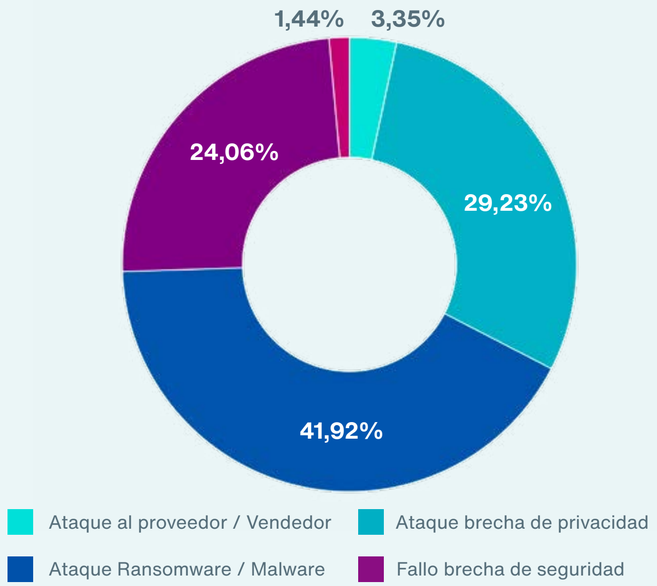
- En primer lugar, los **fallos en la gestión de brechas de seguridad**, con un 26,22 % del total. Este tipo de incidentes incluye errores de configuración, accesos no autorizados debido a mala praxis interna, o controles inadecuados en sistemas expuestos.
- Le siguen los incidentes clasificados como **“otras amenazas cyber”**, que agrupan situaciones como amenazas internas, ataques de denegación de servicio o eventos que no encajan en categorías tradicionales. Este grupo representa el 24,86 %.
- En tercer lugar, se posiciona el **ransomware y otros tipos de malware**, con un 20,81 % de los casos reportados.

Por último, destacar que casi un 10% de los siniestros ya se deben a Fallo de sistemas o Ataques al proveedor, esta última una de las principales preocupaciones del mercado en la actualidad y sobre la que se está poniendo mucho foco en términos de cobertura.

Sin embargo, al observar el **coste económico** de cada tipo de incidente, la jerarquía se invierte de forma significativa. Aunque el ransomware no lidera en frecuencia, **sí es la causa más costosa**, representando **el 41,92 % del coste total** asociado a siniestros. Le siguen las **brechas de privacidad** (29,23 %) y los **fallos en la seguridad** (24,06 %).

Esta divergencia revela una realidad crítica: **el ransomware se comporta como un "cisne negro recurrente"**, con una menor frecuencia, pero con un impacto económico mucho más severo. Además, suele activar coberturas de seguro complejas como gastos de extorsión, recuperación de backups, responsabilidad frente a terceros y sanciones regulatorias.

Coste siniestral por causa



Esta distorsión entre volumen y coste debe ser tenida en cuenta tanto por equipos de ciberseguridad como por gestores de riesgo y suscriptores de pólizas: no basta con reducir la frecuencia; **hay que contener el impacto.**

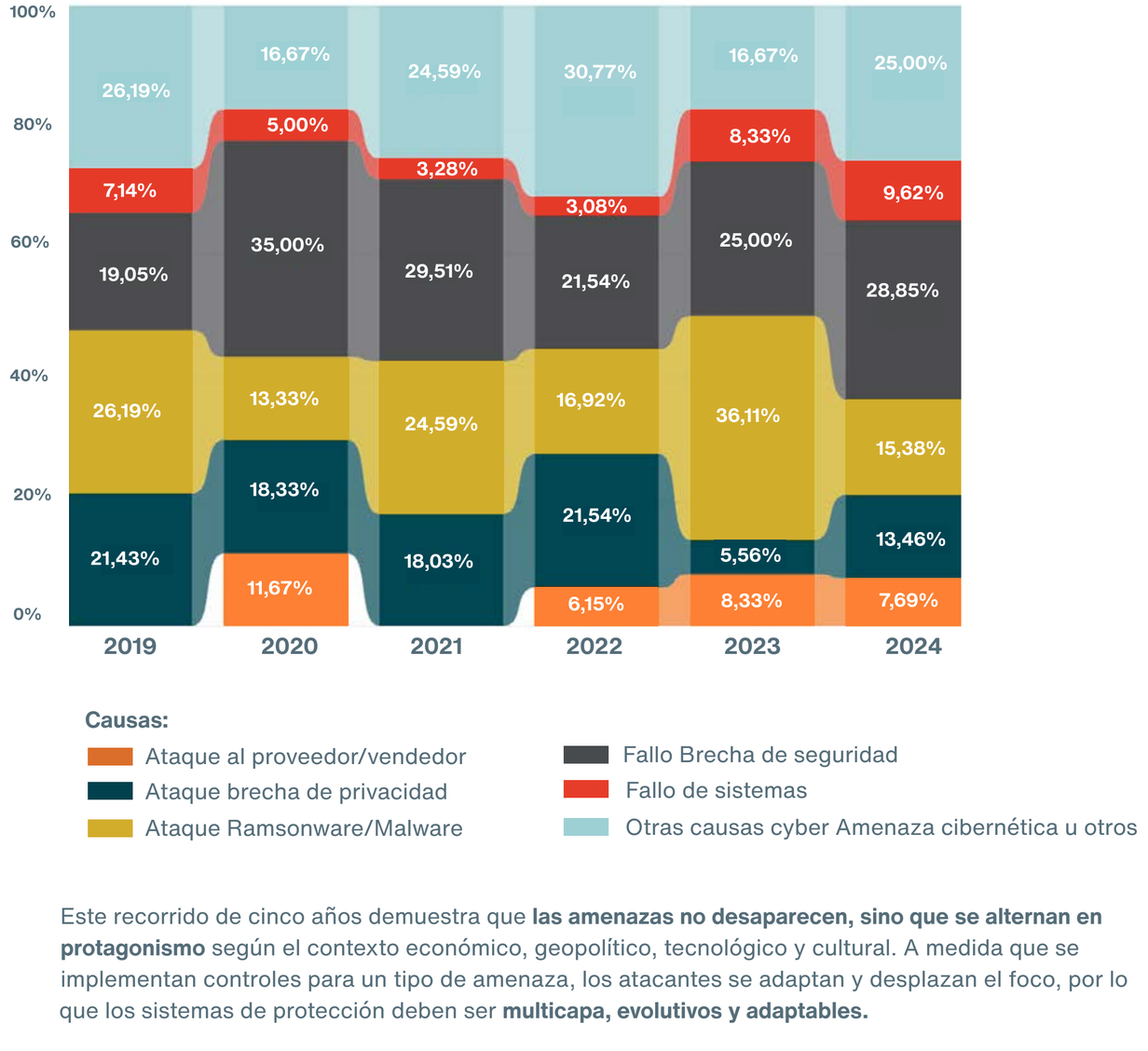
Evolución de las causas de siniestros: 2019–2024, del fallo interno al malware masivo

Comprender cómo han evolucionado las causas de los incidentes cibernéticos a lo largo de los años permite identificar ciclos, anticipar patrones y, sobre todo, ajustar coberturas y controles a las amenazas predominantes en cada momento. Los datos consolidados entre 2019 y 2024 muestran **una dinámica oscilante**, con cambios significativos en la frecuencia relativa de los distintos tipos de siniestros.

Durante el año 2020, el **fallo de seguridad** —por ejemplo, configuraciones incorrectas, contraseñas débiles o errores humanos en entornos cloud— se posicionó como la causa dominante, representando un 35 % del total de incidentes. Este pico puede explicarse por el **efecto pandemia**, cuando la digitalización acelerada obligó a muchas organizaciones a desplegar servicios sin el debido blindaje técnico.

Posteriormente, en 2023, se produjo un giro importante: el **ransomware** se convirtió en el tipo de ataque más frecuente, alcanzando un 36,11 %. Esta tendencia respondió al crecimiento de grupos criminales organizados, la profesionalización del malware como servicio (RaaS) y la alta efectividad de campañas dirigidas a sectores críticos y medianas empresas mal protegidas.

En 2024, sin embargo, se observa una cierta “redistribución” en las causas. El ransomware baja al 15,38 %, aunque como se ha analizado anteriormente, su **coste sigue siendo el más alto.** En paralelo, resurgen los **fallos de seguridad** (28,85 %) y se mantiene un nivel elevado de siniestros clasificados como **otras amenazas cibernéticas** (25 %), que reflejan lo difícil que resulta tipificar algunos incidentes con claridad.

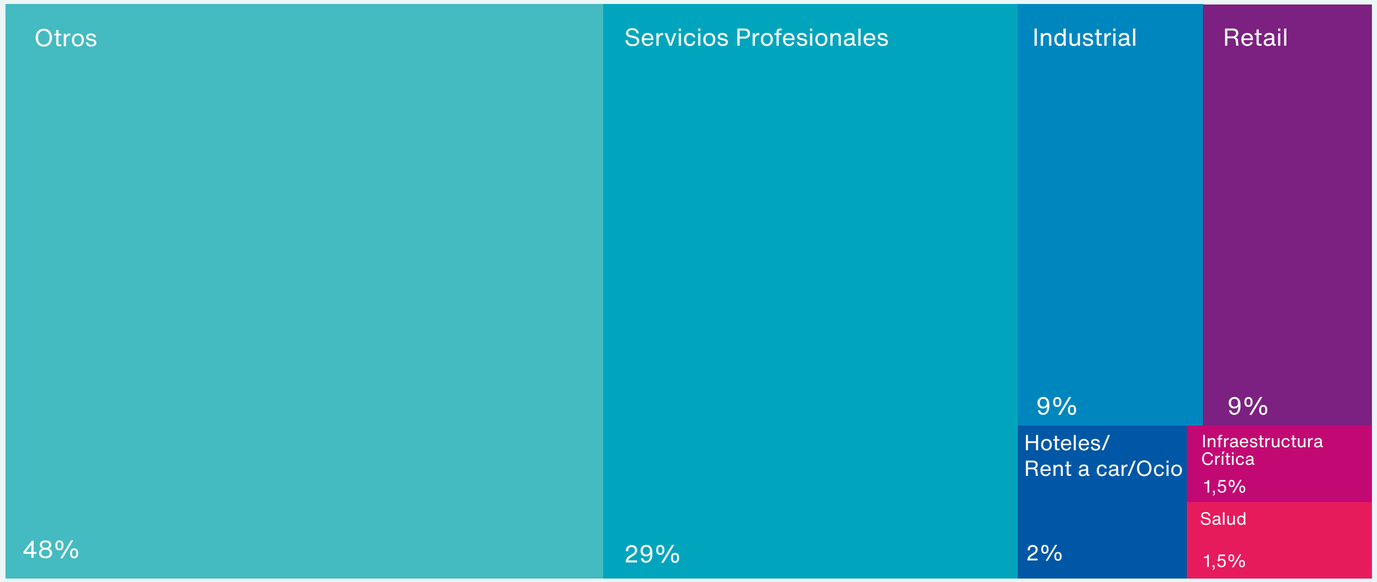


Este recorrido de cinco años demuestra que **las amenazas no desaparecen, sino que se alternan en protagonismo** según el contexto económico, geopolítico, tecnológico y cultural. A medida que se implementan controles para un tipo de amenaza, los atacantes se adaptan y desplazan el foco, por lo que los sistemas de protección deben ser **multicapa, evolutivos y adaptables.**

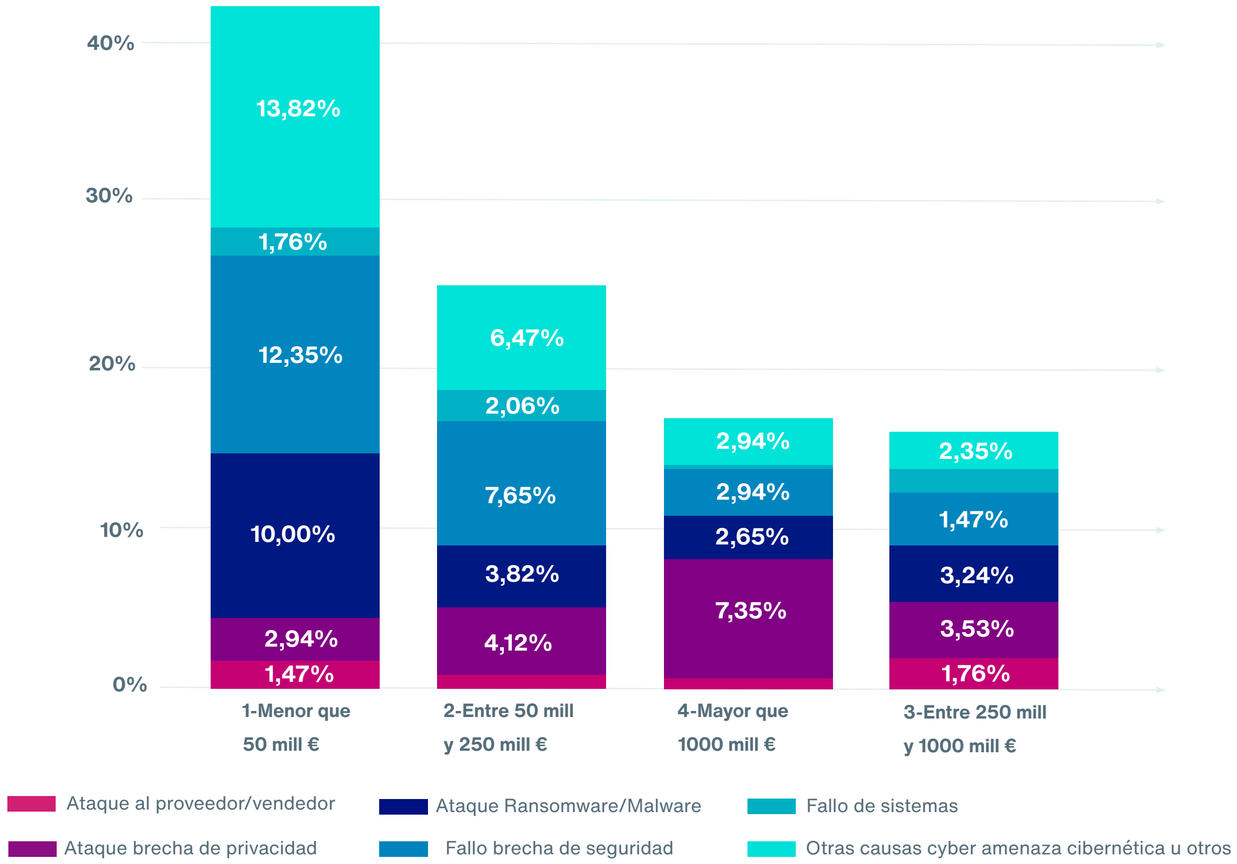
Sectores más afectados y el peso de la facturación: ¿quiénes están más expuestos?

Cuando se analiza la siniestralidad desde la perspectiva del **sector económico**, queda claro que algunas industrias concentran un volumen mayor de incidentes. Sin embargo, más allá del número, lo verdaderamente relevante es entender **por qué ciertas actividades son más vulnerables** y cómo influye su capacidad de respuesta ante un ataque.

Según datos analizados, el mayor número de siniestros se registra en el sector de **Servicios Profesionales**, seguido por actividades agrupadas bajo la categoría **“Otros”**, que engloba sectores como construcción, educación o logística. Este dato no es casual: muchas de estas empresas manejan información sensible, datos de clientes, propiedad intelectual o información contractual crítica, lo que las convierte en objetivos atractivos y simultáneamente frágiles.

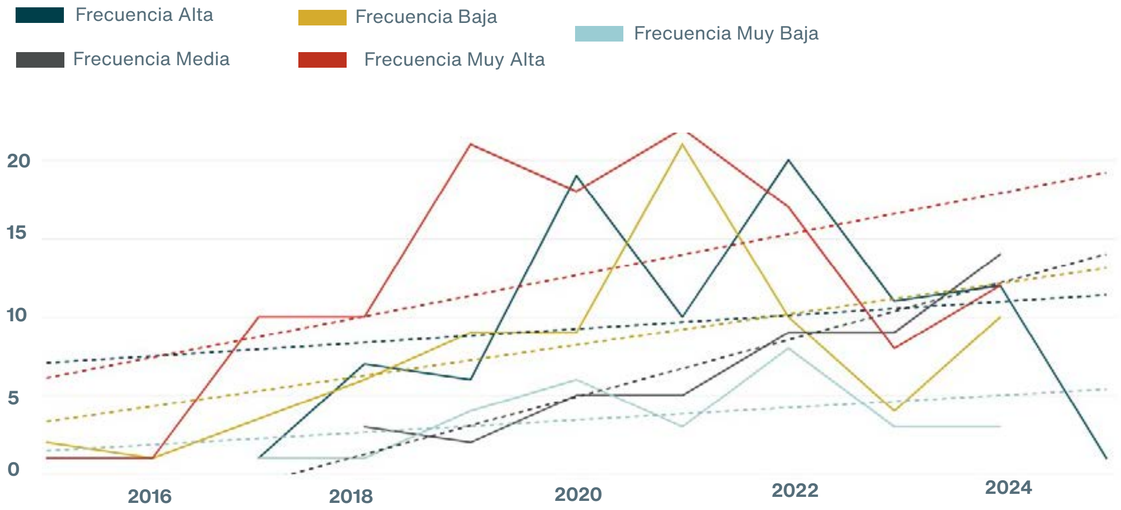


Ahora bien, no todos los sectores con alta exposición tienen la misma capacidad de defensa. Al analizar los siniestros según la **facturación de las empresas**, encontramos una correlación muy significativa: **las compañías de menor tamaño (<50 millones de euros de facturación)** concentran **el mayor número de incidentes reportados.**

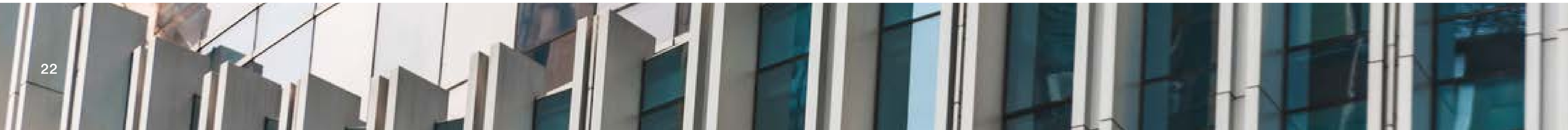


Esta situación se agrava al observar el nivel de **frecuencia de siniestralidad.** Un número importante de clientes se encuentra en la categoría de **frecuencia alta o muy alta**, y no necesariamente por el volumen de negocio o por la criticidad de su actividad, sino por la **persistencia de vulnerabilidades sin resolver.**

Frecuencia de Siniestralidad



Este patrón confirma lo que ya se intuía: la **madurez en ciberseguridad no está necesariamente asociada al tamaño de la empresa**, sino a su cultura de prevención, su nivel de inversión en controles técnicos y su capacidad de respuesta ante incidentes. En muchos casos, las empresas pequeñas subestiman su exposición real, lo que las deja más expuestas y peor aseguradas.



España vs EMEA: amenazas comunes, respuestas desiguales

Comparar la situación de siniestralidad en España con la del resto de Europa no solo permite dimensionar la gravedad de los incidentes locales, sino también detectar **brechas de madurez, diferencias en prioridades de protección y enfoques regulatorios divergentes.** Los datos del informe **ENISA Threat Landscape 2024** y el análisis de **CyQu** (Plataforma interna de Aon) en el ámbito asegurador aportan una visión completa del marco europeo.

A nivel general, las **principales amenazas identificadas en el entorno europeo** coinciden en gran medida con las que afectan a las organizaciones españolas. En el top se encuentran el **ransomware**, los **ataques a la disponibilidad de servicios** (como los DDoS) y las **brechas de datos personales o confidenciales.** Estos tres vectores concentran el mayor volumen de incidentes, tanto en frecuencia como en severidad económica, según ENISA.

Ahora bien, **la intensidad y la gestión de estas amenazas sí presentan diferencias claras entre regiones.** En España, por ejemplo, se observa una mayor proporción de incidentes provocados por **errores internos no maliciosos**, como fallos de configuración o malas prácticas operativas. Esto sugiere una menor madurez en controles básicos, como la autenticación multifactor (MFA), las políticas de backup o la segmentación de red.

Además, según el informe del **CCN-CERT**, en España se han incrementado los **ataques a la cadena de suministro**, tanto en el sector público como en entidades privadas estratégicas. Esta amenaza —también reconocida como prioritaria en ENISA— toma forma especialmente en contextos donde los proveedores no están sometidos al mismo nivel de exigencia en seguridad digital.

Por otro lado, **el entorno regulatorio europeo está presionando para cerrar esa brecha**, con normativas como NIS2 y DORA, que obligarán a muchas empresas a revisar no solo su propio sistema de ciberseguridad, sino también el de terceros con los que operan. Esto afectará especialmente a empresas españolas con menor madurez, ya que deberán adecuarse rápidamente a exigencias que hasta ahora eran optativas o poco fiscalizadas.

En resumen, **España comparte el diagnóstico europeo, pero sufre de una ejecución más lenta y con más disparidades entre sectores y tamaños empresariales.** Esa descompensación es crítica cuando hablamos de seguros: mientras algunas empresas cumplen con requisitos de underwriting, otras operan en la sombra del riesgo no gestionado.

Conclusiones

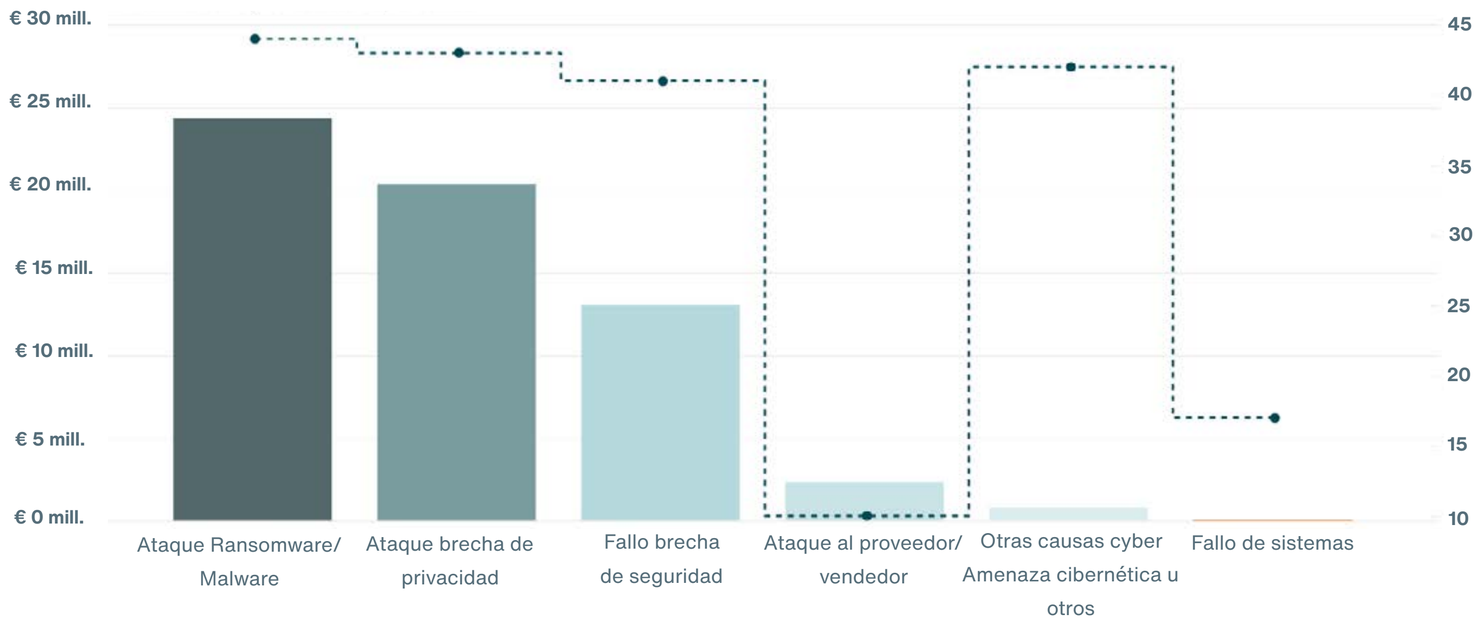
Velocidad sin preparación es vulnerabilidad

La fotografía actual de la siniestralidad cibernética en España muestra **una tormenta perfecta:** más incidentes, más coste por siniestro, y una clara desigualdad en la capacidad de respuesta entre sectores y tamaños empresariales. Aunque las amenazas evolucionan, lo que más preocupa no es la variedad, sino **la recurrencia y el daño económico acumulado.**

La proliferación de incidentes ligados al uso inadecuado de tecnologías emergentes (como la IA generativa), la persistencia de fallos humanos básicos y la fragilidad de las cadenas de suministro dibujan un escenario complejo, donde **la velocidad de adopción tecnológica supera ampliamente a la capacidad de defensa.**

Este desequilibrio se refleja con contundencia al observar la relación entre el número de siniestros y su coste total: **muchos incidentes en empresas pequeñas o mal preparadas generan tanto gasto como los ataques más sofisticados a grandes compañías.**

Coste siniestralidad en € y N° siniestros por causa



En este contexto, **los ciberseguros deben dejar de ser un instrumento meramente reactivo y convertirse en un catalizador de madurez.** Las aseguradoras ya no solo valoran controles técnicos al momento de suscribir, sino que también penalizan la inacción. Un cliente que no documenta sus backups, que no implementa MFA o que no segmenta su red probablemente no podrá renovar su póliza en condiciones aceptables.

Por eso, más allá del análisis, este artículo culmina con una hoja de ruta:

- Asegurar una **base mínima de controles** técnicos: autenticación multifactor, copias de seguridad periódicas, cifrado en tránsito y en reposo.
- Evaluar periódicamente la **exposición a terceros**: no solo proveedores IT, sino también despachos legales, contables, logísticos o de RR. HH.
- Proteger el uso de IA: establecer políticas de seguridad, entornos controlados y validación previa de herramientas generativas.
- Simular escenarios de crisis: preparar al comité de crisis para brechas reales y comunicados regulatorios.
- Revisar la póliza actual y proyectar el futuro: ¿cubre posibles sanciones regulatorias? ¿incluye cobertura para incidentes sufridos por proveedores? ¿responde ante errores humanos?

En definitiva, la siniestralidad no es solo un dato del pasado, sino **una señal del futuro inmediato.** Ignorarla no es una opción.

4

Panorama del riesgo cibernético en España

a. Ciberseguridad en grandes cuentas en 2024

Un seguro que vuelve a inspirar confianza y pasos para avanzar hacia una estrategia de ciberresiliencia completa

Después de un ciclo de incertidumbre y un 2023 marcado por la recuperación del seguro de ciberriesgos, el ejercicio 2024 ha supuesto una consolidación significativa para esta línea de negocio. En particular, la situación del mercado asegurador para el riesgo ciber en grandes cuentas (empresas con facturaciones superiores a 250 millones de euros) está caracterizada no solo por un entorno más estable, sino por una oportunidad concreta para reforzar su estrategia de transferencia de riesgos.

Este nuevo equilibrio ha sido posible gracias a varios factores convergentes: un incremento de la competencia entre aseguradoras, una mayor disponibilidad de capacidad técnica y financiera, y una mejora palpable en la madurez digital de los propios asegurados. El resultado: una oferta más robusta, condiciones de contratación más atractivas y una recuperación de la confianza en el seguro como herramienta de resiliencia empresarial.

Mismo mercado, nuevas reglas del juego

El mercado del seguro cyber ha entrado en una etapa de madurez que, lejos de traducirse en estancamiento, ha potenciado su dinamismo. A finales de 2024 y comienzos de 2025, el entorno es favorable para que las grandes corporaciones revisen y optimicen sus programas de seguros cibernéticos, ya sea ampliando coberturas o adaptando estructuras de colocación.

A pesar de que los ciberataques siguen representando una amenaza significativa para las grandes empresas españolas y los siniestros continúan presentes, algunos con impacto sobre colocaciones complejas, y con consecuencias económicas, operativas y reputacionales de gran envergadura, el mercado ha demostrado flexibilidad. Las tasas han tendido a la baja, y existe un claro apetito por premiar a aquellas organizaciones que han avanzado en su madurez digital. En consecuencia, las aseguradoras han intensificado sus esfuerzos por posicionarse como aliados estratégicos, buscando establecer relaciones de largo plazo con sus clientes clave.

Tendencias que ya no son tendencia: precios, capacidad y exigencia técnica

Durante el segundo semestre de 2024 se confirmó una tendencia que ya se vislumbraba a finales del año anterior: la presión competitiva entre entidades aseguradoras ha contribuido a una reducción progresiva de los precios, incluso en capas primarias, lo cual representa un giro relevante respecto a ejercicios anteriores.

Este escenario ha sido posible por la combinación de varios elementos. Por un lado, se ha producido la reincorporación de capacidades previamente retiradas del mercado, y por otros, siguen entrando nuevos actores a operar en el ámbito español. El número de aseguradoras que ofrecen pólizas de ciber en España se ha incrementado de manera muy significativa, lo que ha intensificado la competencia y ha ejercitado presión a la baja sobre las primas. Esta expansión del mercado ha convertido a España en un entorno favorable para la contratación de ciberseguros en mercado medio en especial, y en los grandes riesgos, ha llevado a las empresas a incrementar sus límites contratados.

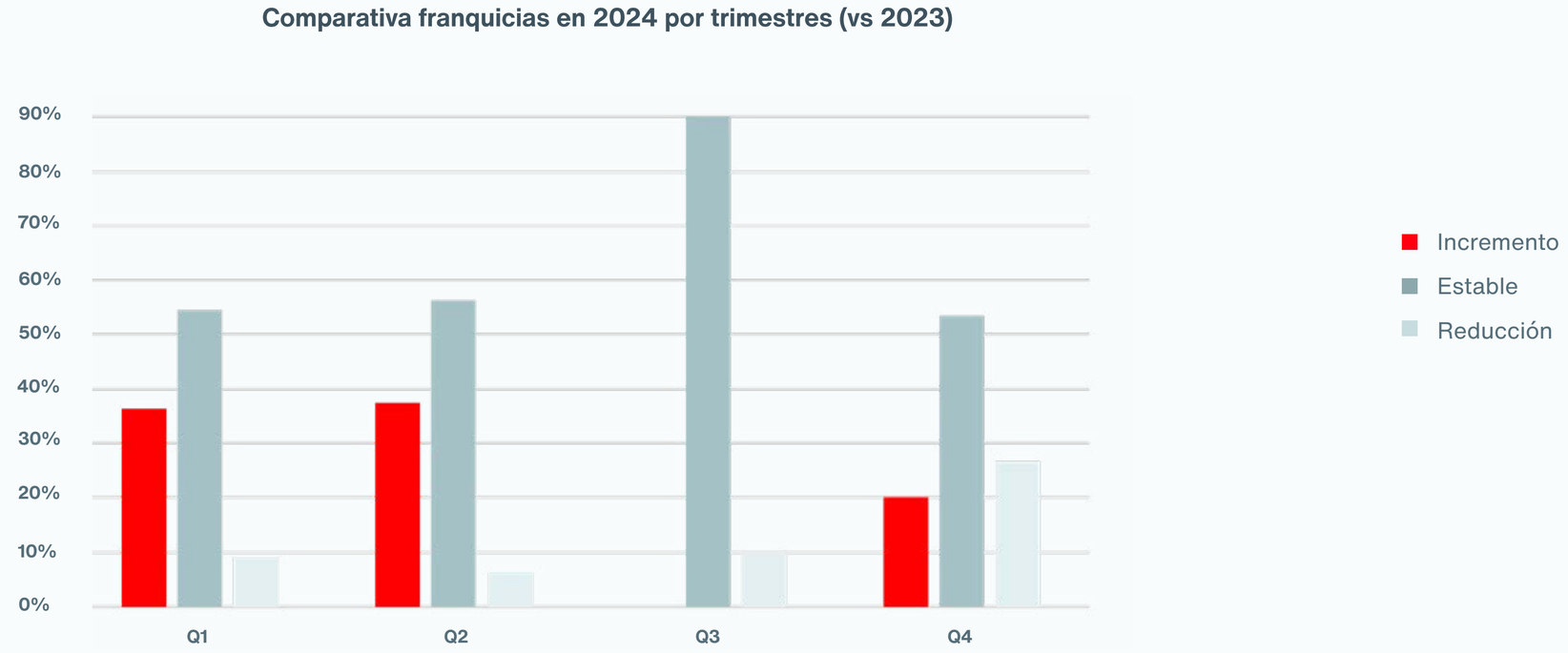
Adicionalmente, las grandes cuentas que han demostrado un compromiso sostenido con la mejora de su postura en ciberseguridad han accedido a condiciones preferenciales, como reducciones de franquicias, descuentos en capas inferiores y acceso a servicios de valor añadido en materia de prevención y gestión de incidentes.

Condiciones en movimiento: ¿más flexibilidad o más presión?

Según la base de datos de Aon y la información facilitada por los principales mercados, los datos analizados durante el último año reflejan una evolución dispar, pero en general positiva, en las principales condiciones de contratación.

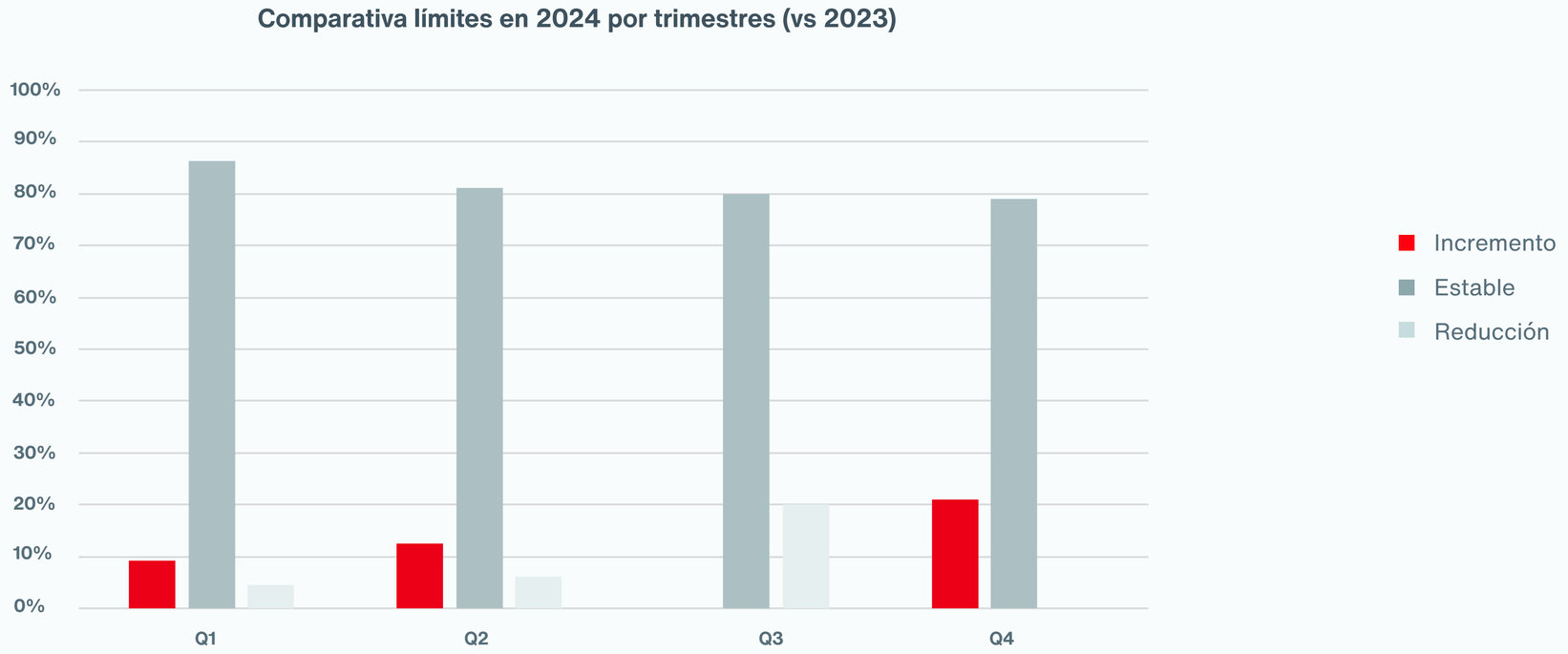
Franquicias

El gráfico adjunto, muestras las variaciones en franquicias del ejercicio 2024 por trimestres, en comparación con el mismo periodo del año anterior. En el primer trimestre de 2024, un 36% de las cuentas experimentaron un aumento en sus franquicias, mientras que un 45% mantuvieron condiciones. No obstante, en el tercer trimestre, el 90% de las cuentas mantuvieron sus niveles sin modificaciones, y en el cuarto trimestre se observó incluso una reducción en el 26,7% de los casos. Esta evolución apunta hacia una mayor flexibilidad en la retención de riesgo, especialmente en perfiles de riesgo más maduros.



Límites asegurados

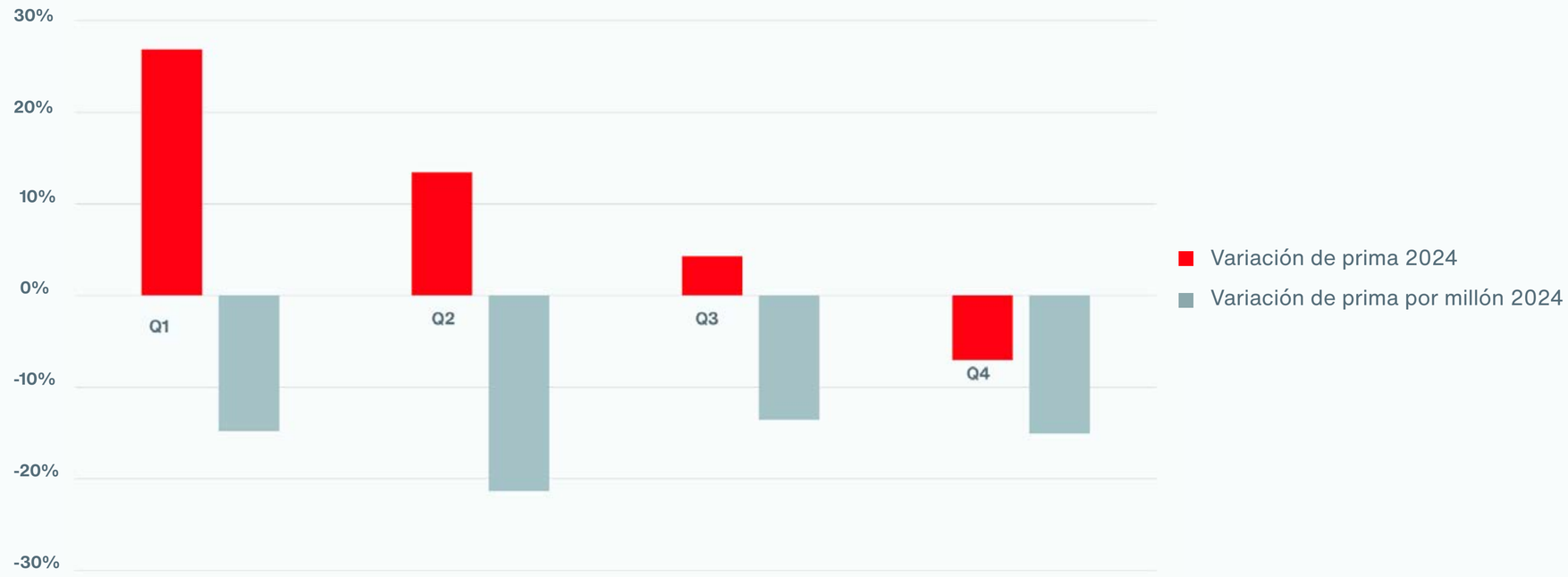
La evolución ha sido, en este punto, bastante estable. En el último trimestre del año, el 80% de las cuentas mantuvieron sus límites asegurados, y solo un 20% los incrementaron. Este dato sugiere que muchas organizaciones han alcanzado un nivel de cobertura que consideran adecuado, aunque sigue existiendo margen para ajustes estratégicos según la evolución de su exposición al riesgo.



Primas

Tal y como muestra el gráfico adjunto, en 2024, el volumen total de primas de las grandes empresas ha mostrado un comportamiento desigual respecto a 2023, con un crecimiento en el primer trimestre (+27%) que se fue desacelerando progresivamente hasta cerrar el año con una caída del -5% en el cuarto trimestre. Esto se debe principalmente a que gracias a la disminución de primas por millón para mismos limites, las grandes corporaciones han aprovechado los ahorros generados para contratar mayores limites en sus pólizas. En concreto, la variación de prima por millón fue negativa en todos los trimestres, destacando especialmente el segundo (-21%) y cuarto (-15%).

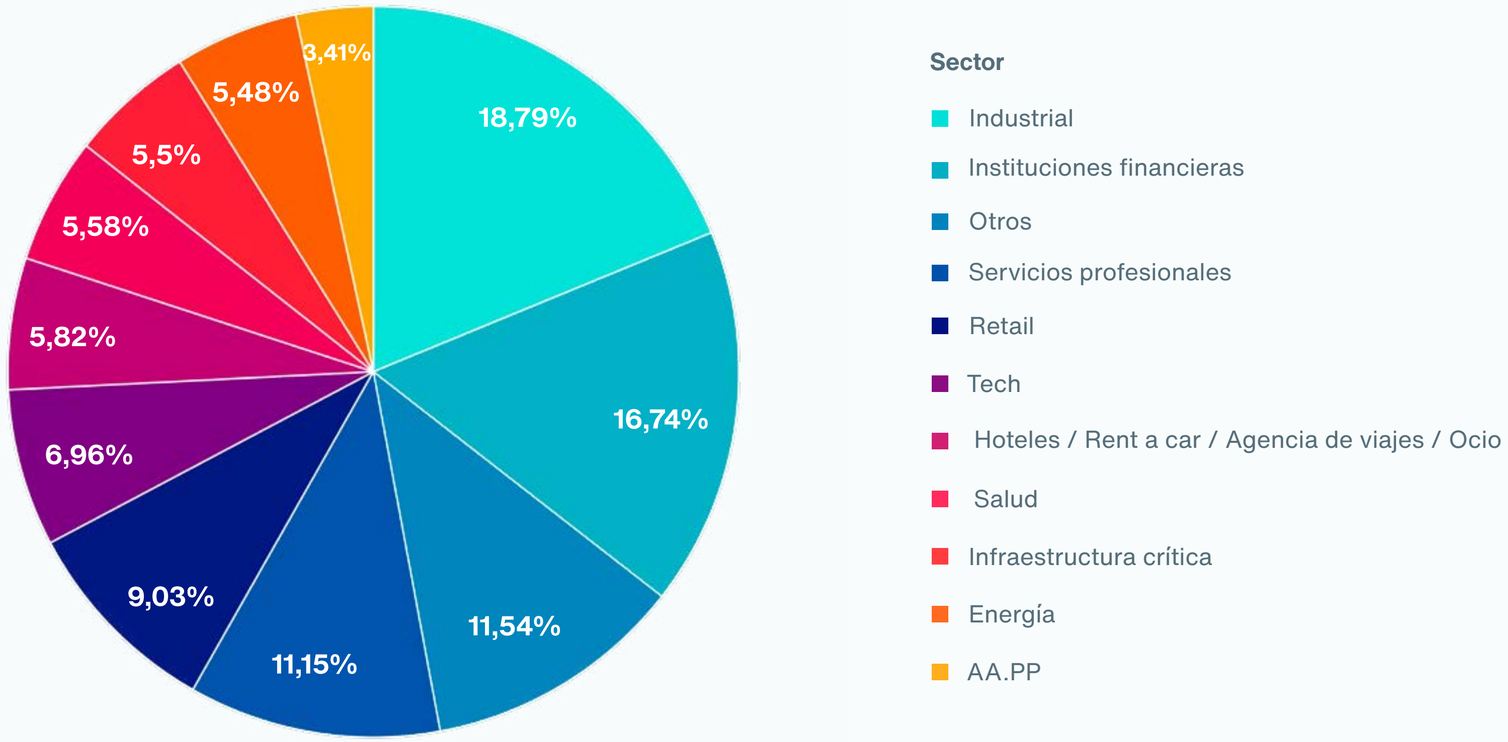
Comparativa primas netas en 2024 por trimestres (vs 2023)



¿Dónde está el riesgo? Claves sectoriales del ciberseguro

El análisis por sectores permite identificar claramente las áreas con mayor concentración de riesgo asegurado, lo cual responde tanto a factores regulatorios como a la sensibilidad de los datos que manejan o a su exposición operativa.

Penetración por sector / Industria

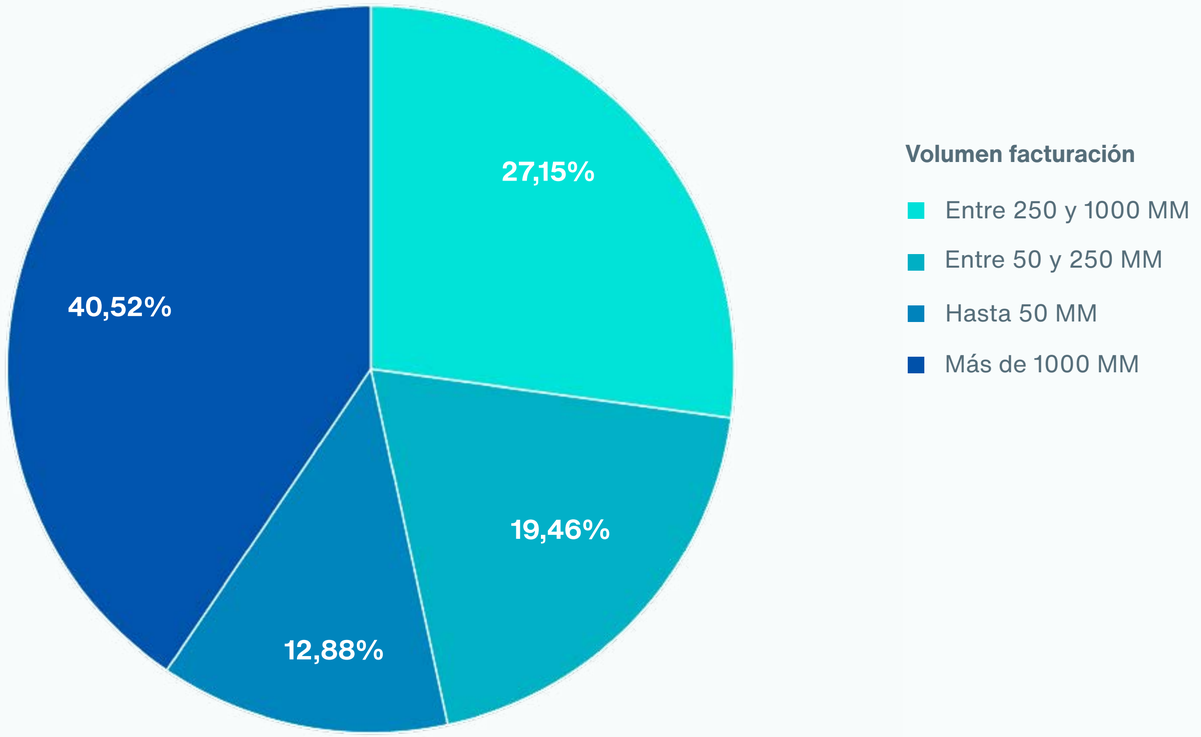


Tal y como se aprecia en el gráfico, y siguiendo la tendencia de los años anteriores, siguen encabezando el ranking sectores como el industrial y el financiero, seguido de empresas de servicios profesionales y el sector retail. Estos sectores lideran claramente la contratación de pólizas de ciberseguro, impulsados por una regulación exigente y una exposición significativa a brechas de datos y ataques tipo ransomware.

En comparación con años anteriores, se aprecia una leve reducción en la representación del sector turístico mientras que el financiero y el industrial han incrementado su participación, reflejando una respuesta activa ante la presión normativa y la materialización de incidentes relevantes.

No obstante, destaca también el aumento del peso de la categoría “Otros”, que agrupa sectores emergentes y compañías con estructuras digitales complejas que empiezan a tomar conciencia del riesgo tecnológico.

Penetración por volumen facturación de empresa



Atendiendo al tamaño de empresa por volumen de facturación, el gráfico anterior muestra que la mayoría de las pólizas ciber contratadas corresponden a empresas de gran tamaño, especialmente aquellas con una facturación superior a los 1.000 millones, que representan el 40,52% del total. Esto sugiere que las grandes corporaciones son más conscientes del riesgo cibernético y tienen mayor capacidad para invertir en seguros especializados. Las empresas con facturación entre 250 y 1.000 millones también tienen una presencia significativa (27,15%), lo que refuerza la tendencia de que, a mayor tamaño empresarial, mayor es la adopción de este tipo de cobertura.

En contraste, las pequeñas y medianas empresas (pymes), especialmente las que facturan hasta 50 millones, solo representan el 12,88% del volumen de pólizas contratadas. Esta baja penetración puede deberse a una menor percepción del riesgo, limitaciones presupuestarias o desconocimiento sobre las ventajas de contar con una póliza ciber. Este segmento representa una oportunidad clara para el sector asegurador, tanto en términos de crecimiento como de concienciación sobre la importancia de protegerse frente a amenazas digitales.

La importancia de la toma de decisiones informadas

Los Brókeres y gestores de riesgos, han intensificados estos últimos años sus servicios en ayudar a sus clientes realizar análisis de cuantificación al objeto de poder determinar límites y franquicias adecuadas para los programas de seguros de las grandes empresas.

El avance en la conciencia del riesgo y el entorno favorable de primas ha permitido a muchas empresas destinar parte de su presupuesto de ciberseguridad en realizar este tipo de análisis porque les ayuda a comprender mejor la exposición financiera potencial antes incidentes cibernéticos. Es decir, ayuda a determinar si la cobertura de seguros actual es adecuada o si se requiere ajustar y a tomar decisiones informadas sobre gestión de riesgos y transferencia.

En este tipo de ejercicios, se definen posibles escenarios de eventos cibernéticos que podrían impactar en el negocio y se estima su impacto económico, identificando tanto pérdidas directas (rescates, recuperación de datos, gastos legales, notificación a clientes, etc.) como indirectas (daño reputacional, pérdida de clientes, interrupción del negocio, sanciones regulatorias, etc.) y se analiza a la vez, la frecuencia estimada de estos eventos considerando datos de la industria, estadísticas, historial de la empresa y exposiciones específicas.

Con la ayuda del bróker especializado, las grandes empresas pueden identificar las pérdidas estimadas frente a la cobertura de seguro, adecuar límites y sublímites, y establecer franquicias adecuadas, así como identificar posibles gaps de cobertura y adaptar la póliza en consecuencia.

Con la ayuda del bróker especializado, las grandes empresas pueden identificar las pérdidas estimadas frente a la cobertura de seguro, adecuar límites y sublímites, y establecer franquicias adecuadas, así como identificar posibles gaps de cobertura y adaptar la póliza en consecuencia. Ello ha dado lugar a una sofisticación de las pólizas.

Otro aspecto que marca este 2024-2025 es la clara evolución del producto asegurador. Dada la entrada de nuevos actores, flexibilidad en el mercado y fruto de las conclusiones de estudios de gap análisis, los Brókeres han intensificado sus esfuerzos en sofisticar las pólizas, incluyendo nuevas coberturas adaptadas al entorno digital cada vez más complejo y a las exigencias normativas. En concreto, los Brókeres están estableciendo alianzas con aseguradoras para ofrecer un producto mejorado respecto a los estándares, en especial para mercado medio. Se han incorporado coberturas como extensión para la pérdida de beneficios por interrupción de negocio derivada de un posible incidente en proveedores, tanto tecnológicos como no tecnológicos, ampliación de cobertura de multas y sanciones garantizadas para dar cobertura a cualquier sanción derivada de las nuevas directivas y legislaciones, etc.

Adicionalmente, para las grandes cuentas se negocian condicionados “tailor made” al objeto de poder adaptar cada póliza a los riesgos específicos que más les preocupen y adaptarse así a las necesidades de cada cliente.

2025: sin sobresaltos, pero con lupa

Las previsiones para 2025 apuntan a una continuidad general de la tendencia observada, aunque con ciertos matices. Se espera que las aseguradoras mantengan su interés por captar las mejores cuentas, aquellas con controles sólidos y una siniestralidad contenida, pero ya se anticipa una posible moderación en las estrategias comerciales más agresivas vistas en el último trimestre de 2024.

Esto no implica necesariamente un retorno a un mercado duro, pero sí una mayor selectividad. Las cuentas con exposiciones especialmente críticas, o con escasa evolución en sus controles, podrían enfrentarse a condiciones más estables o menos ventajosas. En contraposición, aquellas organizaciones que impulsen una gestión activa del riesgo y trabajen de forma colaborativa con sus aseguradoras seguirán accediendo a condiciones competitivas y soluciones personalizadas.

Gestión integral del riesgo cyber

El seguro de ciberriesgos se encuentra, a día de hoy, en una posición privilegiada dentro del mercado asegurador. Las condiciones de contratación son favorables, la capacidad está disponible y las aseguradoras están firmemente decididas a desempeñar un papel activo en la evolución de sus clientes, por lo que es el momento idóneo para que todas aquellas empresas que no cuenten con un seguro cyber puedan hacerlo aprovechando unas condiciones especialmente favorables y aquellas que ya cuenta con el mismo, puedan mejorar considerablemente sus términos y condiciones.

Además de la importancia de contar con un seguro de cyber, se observa que las grandes empresas españolas están adoptando un enfoque integral de ciberseguridad que abarca desde la modernización tecnológica y la integración de inteligencia artificial hasta la gestión de riesgos de la cadena de suministro y el cumplimiento normativo. Estas medidas reflejan un compromiso creciente para proteger sus activos digitales en un entorno cada vez más desafiante.

En este contexto, la gestión integral del riesgo cibernético se consolida como un pilar esencial para la sostenibilidad y competitividad empresarial. No se trata solo de contratar un seguro, sino de construir una estrategia coordinada que combine prevención, análisis, respuesta y transferencia del riesgo. Las organizaciones que adoptan este enfoque holístico no solo protegen sus activos digitales, sino que también fortalecen su capacidad de adaptación, mejoran su reputación y generan confianza en sus clientes, socios e inversores. La ciberresiliencia ya no es una opción: es una ventaja estratégica.

b.Ciberseguridad en mercado medio en 2024

Anatomía de un mercado en mutación: guía estratégica del medio mercado

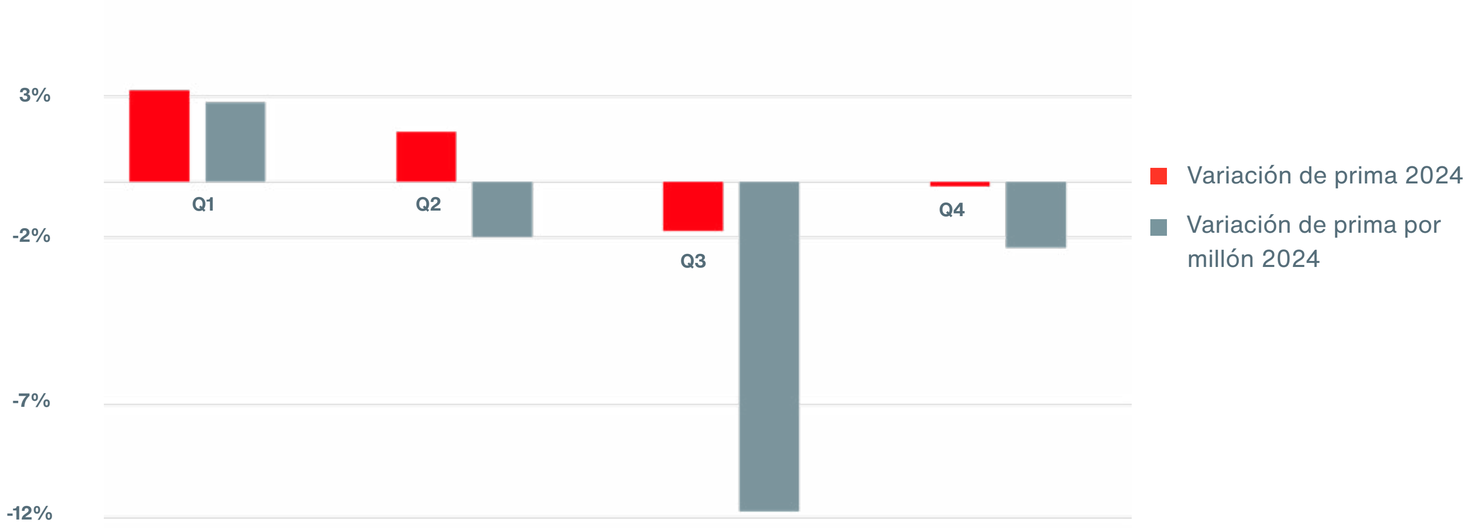
El periodo 2023–2024 ha marcado un punto de inflexión en la evolución del seguro cibernético para el mercado medio en España. Lo que inicialmente era una apertura tímida, impulsada por las primeras señales de madurez tras la pandemia, se ha transformado en una consolidación real del producto dentro de las estrategias de gestión de riesgo de las empresas con facturación inferior a 250 millones de euros.

Durante este tiempo, hemos observado un incremento notable en los límites asegurados, una estabilización de precios a pesar de las coberturas más robustas y una evolución en las condiciones de suscripción. Las aseguradoras han pasado de una postura rígida y selectiva a una visión más dinámica y proactiva, donde el acompañamiento, la personalización y la inclusión de servicios de valor añadido han sido claves para conquistar este segmento.

Uno de los indicadores más reveladores de este proceso es la relación entre los límites contratados y la variación de primas. Según los datos compartidos, los límites medios contratados crecieron de manera interanual entre 2022 y 2024 en todos los trimestres. Esta escalada no fue acompañada de una subida proporcional en las primas, lo que sugiere una mayor eficiencia en el pricing, una mejor segmentación del riesgo y una competencia más intensa entre aseguradoras.

Al mismo tiempo, la variación media de primas, mostrada en el siguiente gráfico, refleja una estabilización en la mayoría de los trimestres, con una media por debajo del 20 %, salvo un pico en Q3 (55 %) que se asocia a contrataciones más sofisticadas y límites más ambiciosos. Esta contención en las subidas indica un mercado que ha sabido ajustarse a las necesidades del mid-market sin penalizar su acceso.

Evolución de primas mercado medio



Este equilibrio ha sido posible por la transformación de la suscripción en una herramienta más estratégica, basada en evaluaciones objetivas y simplificadas.

En definitiva, el periodo 2023–2024 ha dejado claro que el ciberseguro ha pasado de ser una solución emergente para convertirse en una palanca estructural en la continuidad operativa de las empresas medianas. Y lo ha hecho adaptando su producto, su discurso y su tecnología al ritmo y las posibilidades del mid-market.

Condiciones de suscripción y capacidad disponible: de la exigencia al acompañamiento

Uno de los cambios más relevantes en el mercado del ciberseguro para el mid-market ha sido la evolución del proceso de suscripción. Si en años anteriores este constituía una barrera de entrada, en 2024 ha pasado a ser una herramienta de diagnóstico y acompañamiento. Hoy en día, contratar una póliza ya no implica demostrar perfección técnica, sino disposición a mejorar y madurar digitalmente de forma progresiva.

Esta transformación ha sido posible gracias a la combinación de dos factores clave: la incorporación de tecnología en los procesos de underwriting y un cambio de mentalidad en las aseguradoras. En lugar de exigir un cumplimiento estricto desde el inicio, las compañías han comenzado a aplicar modelos de evaluación más flexibles, que valoran tanto el estado actual del cliente como su compromiso de mejora. Se han vuelto comunes las cláusulas de suscripción condicionada, donde el asegurado accede a la cobertura con base en un plan de acciones que debe implementar en los primeros 90 días de vigencia.

Los formularios extensos han sido reemplazados por cuestionarios breves pero estratégicos (entre 10 y 15 preguntas clave), y los escáneres automáticos de exposición digital permiten obtener una puntuación objetiva del riesgo en tiempo real. Esta puntuación sirve como base para definir franquicias, límites, primas y servicios adicionales incluidos. Por ejemplo, una empresa con una puntuación elevada puede beneficiarse de franquicias reducidas o incluso del acceso gratuito a herramientas de prevención.

Esta lógica no solo agiliza la contratación, sino que también democratiza el acceso al seguro. Empresas sin departamentos IT propios, pero con buenas prácticas básicas de ciberseguridad, hoy pueden acceder a coberturas robustas sin necesidad de cumplir con exigencias inalcanzables.

En paralelo, la capacidad disponible ha aumentado de forma considerable. Donde antes el mercado ofrecía coberturas estándar de entre 500.000 € y 1.500.000 €, ahora es habitual encontrar productos automáticos de 2 millones, e incluso pólizas con 3 o 5 millones en empresas con facturaciones entre 10 y 50 millones de euros. Este salto ha sido posible por un mayor apetito de riesgo por parte de las aseguradoras, una mejor disponibilidad de reaseguro y una mejora general en el perfil de riesgo de los clientes.

El proceso de suscripción en el ciberseguro ya no es un examen excluyente, sino una oportunidad de mejora conjunta entre aseguradora y cliente. Las condiciones de acceso se han flexibilizado sin comprometer el rigor técnico, lo que ha permitido una expansión real del seguro en el mid-market, basada en el principio de que protegerse no es una cuestión de perfección, sino de compromiso y acompañamiento.

Límites contratados y evolución de franquicias: cuatro años de expansión progresiva

La evolución de los límites contratados y de las franquicias en el mercado del ciberseguro para empresas del mid-market refleja con claridad la profesionalización tanto de la oferta como de la demanda. Entre 2020 y 2024, el crecimiento no ha sido únicamente cuantitativo, sino también cualitativo, ya que la forma en la que se diseñan las coberturas y se gestiona el riesgo ha cambiado sustancialmente.

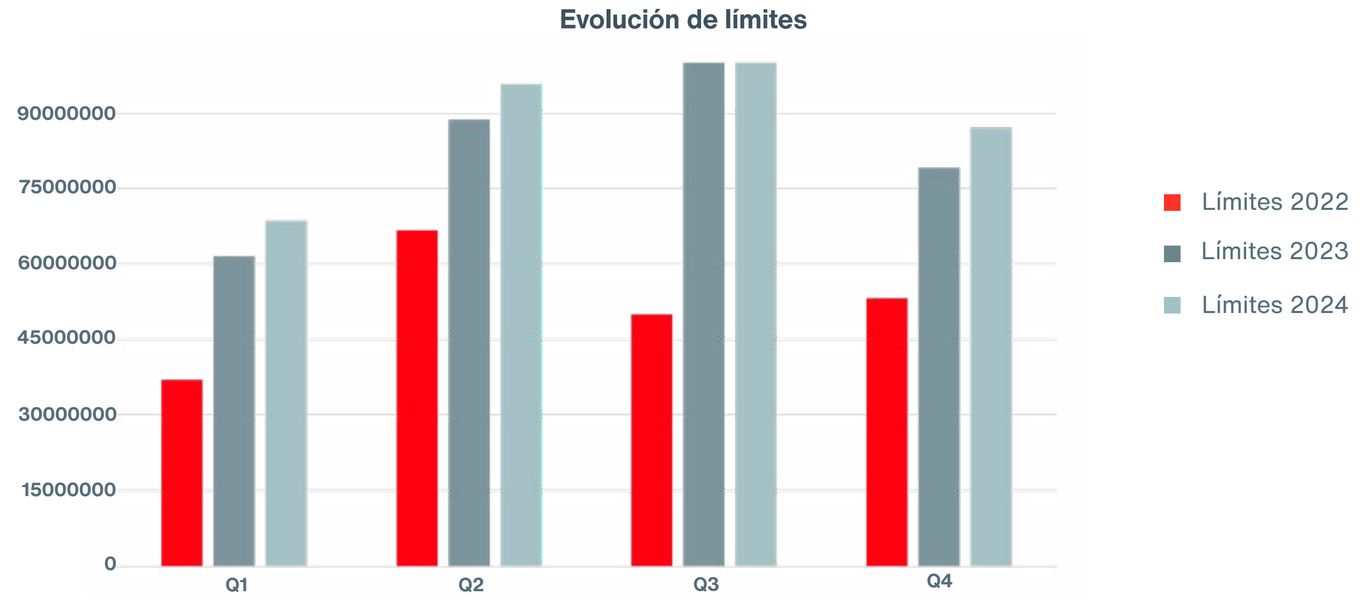
Límites contratados: de la prudencia a la protección real

En los primeros años del análisis (2020–2021), era común que los límites contratados no superaran los 1,5 millones de euros. Muchas empresas consideraban el seguro cibernético como una herramienta auxiliar y no como un componente central de su estrategia de continuidad operativa. La cobertura promedio se limitaba a escenarios catastróficos, y la mayoría de las pólizas se centraban en indemnizar daños directos sin demasiadas capas adicionales de protección.

En 2022 se comenzó a observar una apertura progresiva. Empresas más expuestas digitalmente empezaron a solicitar coberturas más amplias. Esta evolución se tradujo en un aumento del límite medio contratado, que pasó a situarse entre los 2 y 2,6 millones de euros, aunque la mayoría de las pólizas seguían sin superar los 2 millones.

A partir de 2023, con la estabilización del mercado y la entrada de nuevos productos más competitivos, se vivió un verdadero punto de inflexión. La combinación de primas más accesibles, procesos de suscripción más ágiles y mayor comprensión del riesgo digital llevó a muchas empresas a revisar al alza sus coberturas. Esta tendencia se consolidó aún más en 2024, donde los datos muestran un crecimiento significativo de los límites medios contratados, especialmente en el Q3.

El Q3 de 2024 presentó un pico superior a los 110 millones de euros en límites acumulados contratados, más del doble que el mismo trimestre en 2022. Esta progresión responde no solo a una mayor conciencia de los riesgos, sino también a una adecuación de los productos disponibles: hoy es habitual encontrar pólizas para empresas con facturación de entre 10 y 50 millones que incluyen coberturas de hasta 5 millones, ya sea en pólizas consolidadas o estructuradas por capas (primario + exceso).

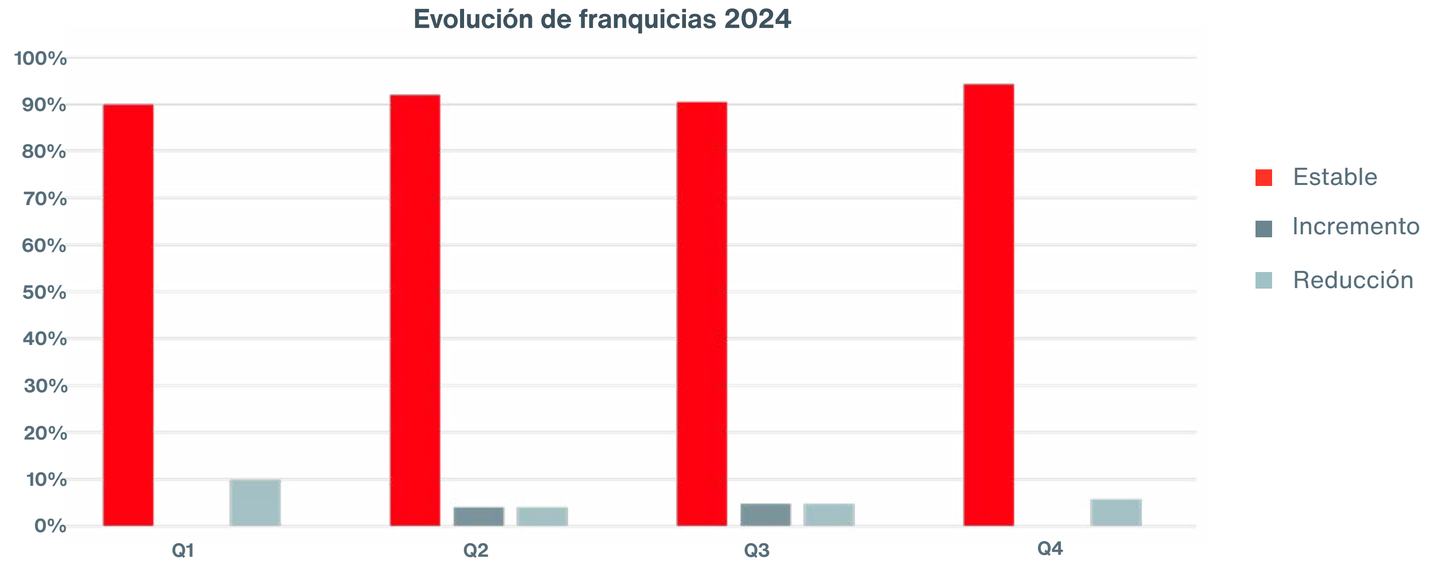


Franquicias: del estándar rígido a la herramienta estratégica

En paralelo al crecimiento de los límites, las franquicias han experimentado una evolución igualmente reveladora. En 2020, el estándar se situaba en torno a los 25.000 €, y rara vez se negociaban condiciones particulares. Las aseguradoras ofrecían paquetes cerrados donde el asegurado no tenía margen de maniobra, y la franquicia se asumía de manera irremediable, no como una variable estratégica.

Con el tiempo, esa rigidez ha dado paso a un enfoque más flexible y adaptado. En 2022, ya se observaba una media entre los 30.000 € y 35.000 €, y en 2023, más del 50 % de los clientes mantuvieron sus franquicias estables, mientras un 40 % optó por incrementarlas voluntariamente para obtener mayores límites o reducir primas. Esto refleja una madurez en la gestión del riesgo: las empresas dejaron de ver la franquicia como un coste oculto, y comenzaron a utilizarla como palanca para optimizar su póliza.

En 2024, esta tendencia alcanza un nuevo nivel. El Q3 muestra un salto significativo, con franquicias que en algunos casos superan los 150.000 €, especialmente en pólizas que buscan cubrir límites de 4 o 5 millones. Esto no implica un endurecimiento del mercado, sino una decisión consciente del asegurado: asumir más riesgo inicial para poder acceder a mejores condiciones globales.



Además, hoy muchas pólizas permiten ajustar la franquicia durante la vigencia del contrato. Si la empresa mejora su puntuación en escaneos de seguridad, implementa políticas de backup, forma a sus empleados o adopta MFA, puede renegociar la franquicia en la renovación, e incluso en mitad de contrato si así lo permite el asegurador. Este dinamismo ha transformado la franquicia en un elemento activo de la estrategia de ciberseguridad corporativa.

Un nuevo equilibrio entre cobertura y retención

La relación entre límites y franquicias ya no se mide en términos absolutos, sino en su coherencia con el perfil de riesgo y la estrategia de negocio de cada cliente. Lo que buscan hoy las empresas del mid-market no es simplemente “asegurar más”, sino estructurar una protección equilibrada, con coberturas realistas, franquicia negociada y servicios añadidos que permitan actuar antes, durante y después de un incidente.

En resumen, entre 2020 y 2024 hemos pasado de un modelo básico y estandarizado a un ecosistema sofisticado y personalizado. La cobertura ya no es una cifra arbitraria, sino una decisión estratégica basada en datos, contexto operativo y evolución digital. Esta evolución es un claro reflejo de la consolidación del seguro cibernético como una herramienta crítica para la continuidad del negocio en el mercado medio español.

Servicios de valor añadido y prevención integrada: el seguro como plataforma de resiliencia

Una de las transformaciones más profundas del ciberseguro en el mid-market entre 2020 y 2024 no ha sido en las coberturas ni en los precios, sino en el propósito mismo del producto. Tradicionalmente concebido como una herramienta de indemnización post-incidente, el seguro cibernético ha evolucionado hacia un modelo de acompañamiento continuo que integra prevención, detección, respuesta y recuperación. En otras palabras: ha dejado de ser solo una póliza para convertirse en una plataforma de resiliencia.

De la indemnización a la intervención temprana

En 2020, los seguros cibernéticos estaban centrados casi exclusivamente en cubrir las consecuencias de un incidente: restauración de datos, responsabilidad legal, costes de comunicación o defensa jurídica. El asegurador solo intervenía una vez declarado el siniestro, y los servicios asociados eran escasos o inexistentes.

Esta lógica ha cambiado radicalmente. Hoy en día, las aseguradoras del mid-market no solo cubren el impacto, sino que actúan como socios activos en la anticipación y gestión del riesgo. Esto se refleja en la inclusión de servicios preventivos dentro del paquete asegurador, sin coste adicional. Algunos de los más comunes en 2024 son:

- Simulacros de crisis (table-top exercises): sesiones prácticas donde se entrenan roles clave en la respuesta a un incidente.
- Monitorización de credenciales en dark web: para detectar filtraciones y anticipar posibles accesos no autorizados.
- Escaneos de vulnerabilidades externas: que permiten identificar y corregir puntos débiles en la infraestructura digital.
- Informes periódicos de exposición digital: con análisis de medidas de ciberseguridad y recomendaciones técnicas.

Estos servicios no solo ayudan a contener incidentes cuando ocurren, sino que también mejoran activamente la situación de seguridad de la empresa asegurada, reduciendo la probabilidad de que un ataque tenga éxito. Además, en muchas pólizas, el uso proactivo de estos recursos puede tener beneficios tangibles, como reducción de primas, mejora de franquicias o acceso a límites más altos.

El asegurador como partner técnico y operativo

Este nuevo modelo también ha redefinido el rol del asegurador. Ya no es solo un financiador del riesgo, sino un facilitador de capacidades. Las compañías de seguros que operan en el mid-market se han dotado de equipos técnicos especializados, alianzas con proveedores de ciberseguridad y plataformas digitales que permiten gestionar incidentes en tiempo real.

Por ejemplo, algunas pólizas incluyen acceso a plataformas de gestión de incidentes, donde el asegurado puede encontrar guías de actuación legal, mediática y técnica ante distintos tipos de ataques.

Esta evolución ha generado una nueva relación entre asegurador y asegurado: más cercana, más dinámica y basada en la confianza. Las empresas sienten que el seguro no es solo un respaldo financiero, sino un recurso tangible que pueden activar cuando más lo necesitan.

Resiliencia como nuevo valor asegurado

En este nuevo paradigma, el concepto de “valor asegurado” se amplía. Ya no se trata solo de cubrir una pérdida económica, sino de garantizar la continuidad operativa, la reputación corporativa y el cumplimiento regulatorio. El seguro cibernético se alinea, por tanto, con los pilares esenciales del negocio moderno:

- Continuidad: al incluir asistencia inmediata y herramientas de prevención, las empresas minimizan los tiempos de inactividad tras un ataque.
- Cumplimiento: muchas pólizas ayudan a cumplir requisitos normativos como NIS2 o RGPD, al documentar procedimientos y ofrecer soporte legal.
- Reputación: la gestión rápida y profesional de un incidente evita crisis mediáticas y pérdidas de confianza con clientes o partners.

Esta lógica responde también a una realidad ineludible: los ciberataques son cada vez más frecuentes, más complejos y destructivos. En este contexto, el seguro ya no puede ser solo reactivo. Debe formar parte activa de la estrategia de ciberseguridad, integrándose con los equipos técnicos, los procesos de gestión de crisis y los planes de continuidad del negocio.

5

Principales novedades normativas

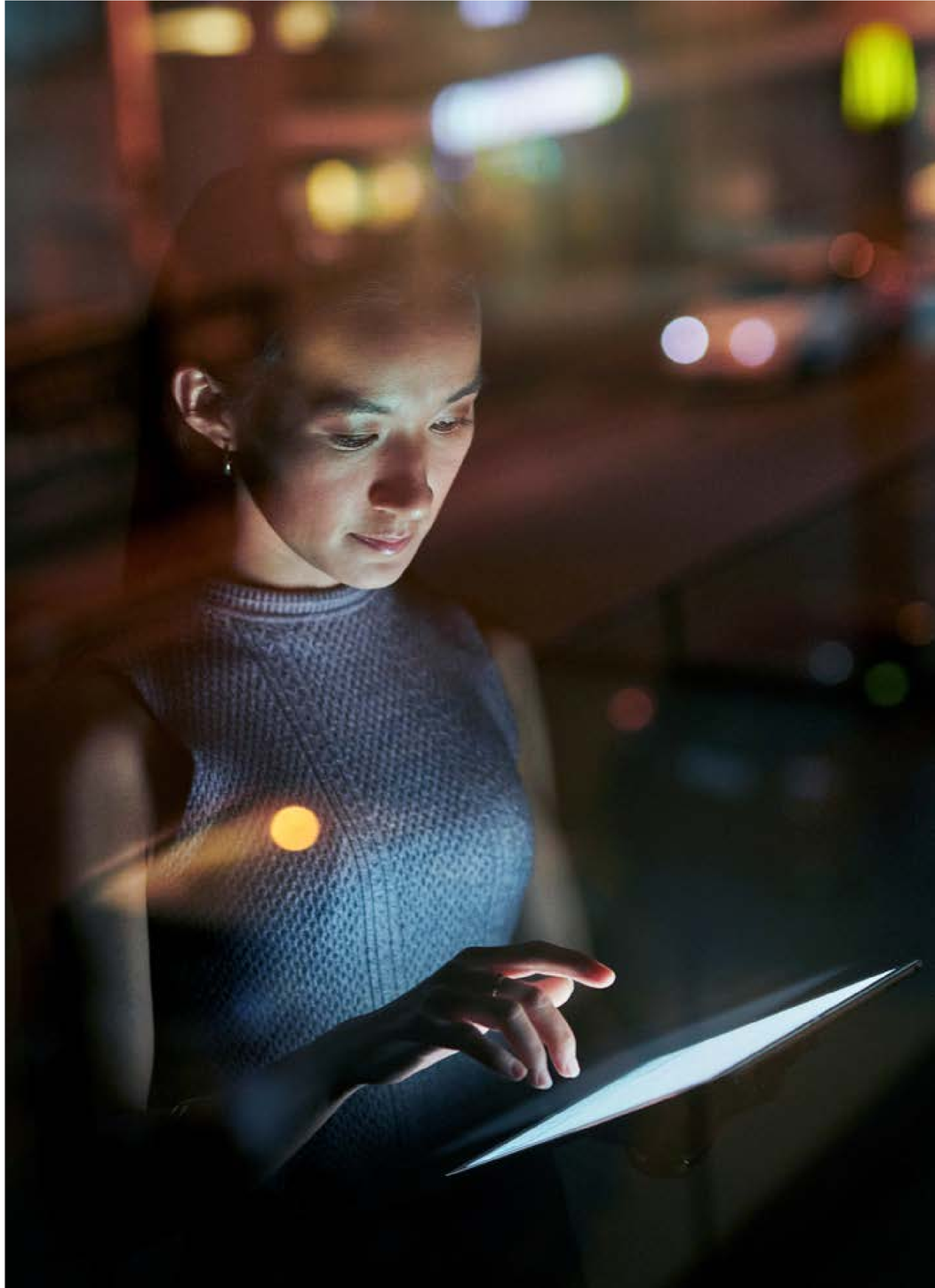
a. Nuevo mapa de autoridades en materia de ciberseguridad y su interrelación con la autoridad de supervisión de privacidad

Alejandro Padín Vidal, *Socio Responsable del Área de Privacidad, Tecnología y Ciberseguridad de Garrigues.*

1. Introducción

En enero de 2025, el Gobierno de España presentó el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, con el objetivo de transponer la Directiva (UE) 2022/2555 sobre seguridad de las redes y sistemas de información, conocida como Directiva NIS 2. Esta futura ley pretende reforzar la protección frente a las crecientes ciberamenazas, estableciendo un marco institucional claro y mejor coordinado. Entre otras medidas, el anteproyecto crea por primera vez un organismo único como Autoridad Nacional Competente en ciberseguridad – el Centro Nacional de Ciberseguridad – y define la estructura de autoridades sectoriales, CSIRTs y centros operativos para gestionar riesgos e incidentes. Asimismo, regula las obligaciones de gestión de riesgos y notificación de ciberincidentes para entidades esenciales y importantes, y prevé un régimen sancionador por incumplimientos.

En este artículo tratamos de presentar cómo se estructura y organiza la administración pública para supervisar y coordinar la recepción y gestión de los incidentes de ciberseguridad en las empresas afectadas por la normativa NIS 2 y cómo esta nueva estructura se interrelaciona, a su vez, con otras autoridades de supervisión que también pueden tener potestades y facultades de actuación cuando se produce un ciberincidente. Todo ello, pendiente de la versión final de este anteproyecto, que puede sufrir todavía alguna modificación tanto en el documento que el Gobierno presente al Parlamento en forma de Proyecto de Ley, como en el texto definitivo que salga de las Cortes Generales y se publique finalmente como Ley de obligado cumplimiento.



2. Arquitectura institucional prevista en el anteproyecto

El anteproyecto configura un nuevo esquema institucional para la ciberseguridad en España, articulado en varios niveles jerárquicos y funcionales. En el centro se sitúa el Centro Nacional de Ciberseguridad (CNC), concebido como la autoridad nacional competente única en la materia. Alrededor de este organismo pivota una red de autoridades de control sectoriales, encargadas de la supervisión en distintos ámbitos, y una serie de CSIRTs nacionales de referencia que actúan como equipos de respuesta técnica a incidentes. También se contempla la existencia de un Centro de Operaciones de Ciberseguridad para la vigilancia activa de redes e identificación de amenazas, integrando capacidades operativas.

2.1. Centro Nacional de Ciberseguridad (CNC)

El CNC se crea ex novo y se erige como la Autoridad Nacional Competente única en materia de ciberseguridad. Estará adscrito al Gabinete de la Presidencia del Gobierno, dada la naturaleza transversal de sus funciones. El anteproyecto le asigna la dirección, impulso y coordinación de todas las actividades necesarias para garantizar un elevado nivel de ciberseguridad en España. Asimismo, el CNC ejercerá como Autoridad Nacional de Gestión de Crisis frente a ciberincidentes graves y como punto de contacto único nacional para la cooperación con otros países de la UE. En la práctica, esto significa que el CNC tendrá capacidad de mando sobre el resto de actores públicos en ciberseguridad (que mantendrán sus funciones ejecutivas) para evitar duplicidades y racionalizar recursos.

2.2.Autoridades de control sectoriales

El anteproyecto define varias autoridades competentes encargadas de las funciones de supervisión y ejecución de la ley en distintos sectores. Cada una se adscribe a un ministerio diferente, reflejando las actuales divisiones competenciales:

- **Ministerio de Defensa (a través del Centro Criptológico Nacional, CCN):** supervisará a las entidades esenciales e importantes del sector público que no sean consideradas infraestructuras críticas.
- **Ministerio de Asuntos Económicos y Transformación Digital:** supervisará a las entidades esenciales e importantes de los sectores de infraestructura digital y proveedores de servicios digitales, así como a las entidades importantes de otros sectores que no hayan sido designadas como críticas.
- **Ministerio del Interior (a través de la Oficina de Coordinación de Ciberseguridad, OCC):** será la autoridad de control para las entidades críticas y para las entidades esenciales de sectores no cubiertos por Defensa o Digital, incluyendo todas las entidades del sector de la seguridad privada.

Estas autoridades de control sectoriales mantendrán sus funciones ejecutivas en el día a día, pero bajo la coordinación estratégica del CNC para asegurar un enfoque coherente.

2.3.CSIRTs nacionales de referencia

Los CSIRTs (Computer Security Incident Response Team) son los equipos de respuesta técnica a incidentes que servirán de referencia nacional. El anteproyecto designa expresamente tres CSIRTs de referencia:

- **CCN-CERT (del Centro Criptológico Nacional)**: será el CSIRT de referencia para las entidades esenciales o importantes del sector público.
- **INCIBE-CERT (del Instituto Nacional de Ciberseguridad)**: será el CSIRT de referencia para las entidades esenciales o importantes de carácter privado.
- **ESPDEF-CERT (del Mando Conjunto del Ciberespacio)**: actuará en coordinación con CCN-CERT e INCIBE-CERT cuando sea requerido, especialmente en incidentes que afecten a entidades con implicaciones para la Defensa Nacional.

Adicionalmente, el anteproyecto menciona un CSIRT del Ministerio del Interior (CSIRT-MIR) integrado en la OCC, que entrará en acción en ciertos supuestos especiales.

2.4.Centro de Operaciones de Ciberseguridad (COCS)

Aunque el texto legal no emplea literalmente este nombre para un órgano concreto, en la práctica la Administración General del Estado ya cuenta con un Centro de Operaciones de Ciberseguridad. Este centro opera en estrecha colaboración con los CSIRTs mencionados.

3. Distribución de competencias y mecanismos de coordinación

La distribución de competencias entre los organismos mencionados está diseñada para aprovechar sus ámbitos de especialización pero asegurando la coordinación bajo la dirección común del Centro Nacional de Ciberseguridad. En términos generales, el CNC tiene competencias estratégicas y de enlace nacional/internacional, las autoridades de control sectoriales tienen competencias ejecutivas de supervisión en sus respectivos dominios, y los CSIRTs ejercen competencias técnicas de respuesta a incidentes.

3.1. Coordinación nacional a cargo del CNC

El Centro Nacional de Ciberseguridad asume la coordinación superior en prácticamente todos los procesos clave. Por ejemplo, será el encargado de coordinar la respuesta a incidentes significativos, emitiendo instrucciones al CCN-CERT (que lidera técnicamente esa respuesta). También coordinará la cooperación entre los CSIRTs nacionales de referencia y su participación en redes europeas.

3.2.Puntos de contacto sectoriales

Además de las autoridades de control principales, el anteproyecto prevé que por cada sector NIS2 se designe un punto de contacto especializado en el ministerio u organismo público competente en ese sector. Estos puntos de contacto sectoriales actuarán como correa de transmisión entre el CNC/autoridades de control y las propias entidades del sector.

3.3.Gestión de incidentes y notificaciones

La ley crea una Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes como herramienta común para canalizar los reportes de incidentes. Las entidades obligadas notificarán incidentes significativos a través de esta plataforma, la cual estará integrada con los CSIRTs de referencia.

3.4.Cooperación en gestión de crisis

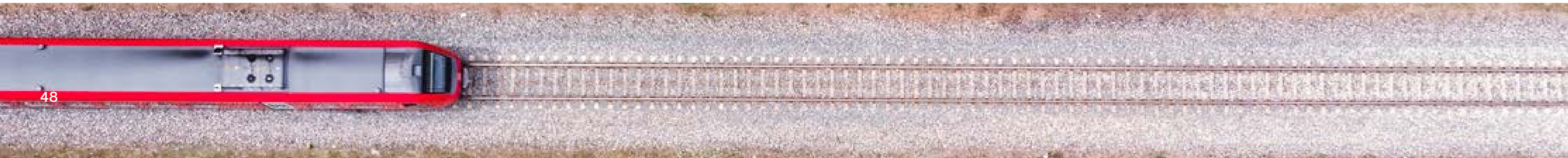
Ante incidentes de gran escala o impacto nacional, el CNC liderará la coordinación de la gestión de crisis de ciberseguridad. Reglamentariamente se definirán los procedimientos y recursos a desplegar en caso de crisis grave.

4. Solapamientos y coordinación con otras autoridades (AEPD y otros)

Una cuestión importante es cómo este nuevo esquema de ciberseguridad se **encaja con autoridades existentes** que también tienen competencias sobre incidentes o seguridad, para evitar solapamientos. Dos casos destacados son la Agencia Española de Protección de Datos (AEPD), dado que muchos ciberincidentes implican violaciones de datos personales, y los supervisores financieros (Banco de España, CNMV), puesto que las entidades financieras estarán sujetas asimismo al Reglamento DORA. El anteproyecto contempla explícitamente la **cooperación con la AEPD** y otros órganos, alineándose con lo que exige la Directiva NIS2 en cuanto a coordinación inter-autoridades.

4.1. Coordinación con la Agencia Española de Protección de Datos (AEPD):

La AEPD es la autoridad encargada de velar por el cumplimiento de la normativa de protección de datos personales (LOPDGDD y RGPD) en España, lo que incluye recibir notificaciones de brechas de seguridad que afecten a datos personales. Es común que un incidente de ciberseguridad (por ejemplo, un ataque informático) conlleve una brecha de datos personales, activando obligaciones de notificación tanto bajo la ley de ciberseguridad (NIS2) como bajo la normativa de datos (RGPD). Para evitar duplicidades y contradicciones, el anteproyecto establece un **mecanismo de cooperación estrecha con la AEPD.** En concreto, el artículo 24 dispone que *"las autoridades de control cooperarán estrechamente con la Agencia Española de Protección de Datos (y con las autonómicas competentes) para hacer frente a los incidentes que produzcan violaciones de la seguridad de datos personales, informándolas sobre aquellos incidentes que deban ser notificados y su evolución"*, todo ello **sin perjuicio de las obligaciones de notificación de brechas que corresponden a los responsables del tratamiento conforme a la normativa de protección de datos.** Esto significa que, si una entidad esencial sufre un ciberincidente que compromete datos personales, la autoridad de control en ciberseguridad (p. ej. Interior si es una entidad crítica) informará de dicho incidente a la AEPD y coordinará la respuesta con ella. La empresa seguirá teniendo que notificar formalmente la brecha a la AEPD según el RGPD, pero las dos autoridades públicas (ciberseguridad y datos) se comunicarán entre sí sobre el caso, compartiendo información de evolución del incidente. Además, la ley asegura que la información sobre incidentes de ciberseguridad relevantes para protección de datos estará a disposición de las autoridades de protección de datos. En resumen, se busca una **respuesta coordinada:** la AEPD aportará su enfoque de protección de derechos de las personas, mientras la autoridad de ciberseguridad gestionará la vertiente técnica y de servicio esencial. De este modo, se evitan lagunas (incidentes notificados solo en un foro) y se garantiza que las investigaciones o sanciones puedan realizarse sin entorpecerse mutuamente.



4.2. Relación con la supervisión financiera (Reglamento DORA)

El sector financiero es considerado sector esencial en NIS2 pero, a la vez, es un sector directamente afectado por el Reglamento (UE) 2022/2554, conocido como Reglamento DORA, que es plenamente obligatorio desde enero de 2025. Para conciliar ambos marcos, la Directiva NIS2 reconoce a DORA como lex specialis en aspectos sectoriales financieros; es decir, las normas de DORA prevalecen en caso de solapamiento, aunque las entidades financieras también están sujetas a obligaciones NIS2 no cubiertas por DORA. El anteproyecto español aborda esta cuestión de varias formas:

- En la **Disposición adicional segunda**, se garantiza el respeto a las competencias del Banco de España y BCE. Esto implica que el nuevo Centro Nacional de Ciberseguridad no sustituirá ni interferirá con el papel del Banco de España como supervisor de la resiliencia operativa de bancos, sino que actuarán de forma complementaria.
- La **Disposición adicional tercera** establece un cauce formal de información: las autoridades de control de ciberseguridad (y los CSIRT) deberán informar al Secretario de Estado de Economía (vía Secretaría General del Tesoro) de aquellos ciberincidentes que puedan tener efectos significativos en los **servicios esenciales del sistema financiero**. Se define que se considerará "efecto significativo" cuando el nivel de impacto del incidente sea alto, muy alto o crítico según los criterios de notificación existentes (Instrucción Nacional de Notificación y Gestión de Ciberincidentes). En la práctica, esto significa que si, por ejemplo, ocurre un ciberataque grave que afecte a la operativa de pagos o al funcionamiento de bancos, el Ministerio de Economía (responsable de la estabilidad financiera) será notificado rápidamente por la estructura de ciberseguridad, facilitando una respuesta coordinada. Además, al Banco de España le seguirán llegando las notificaciones de incidentes de las propias entidades financieras conforme a DORA. Por tanto, habrá un **doble flujo:** la entidad financiera notifica a su supervisor (Banco de España, etc.) según DORA, y en paralelo el CNC/autoridad NIS2 informará a Economía para visión país. Esta interconexión debe evitar que un incidente financiero crítico quede aislado solo en el ámbito financiero sin conocimiento del resto del ecosistema de ciberseguridad, o viceversa.
- Cabe destacar que la Directiva NIS2 explícitamente pide asegurar cooperación adecuada con las **autoridades competentes según el Reglamento DORA** dentro de cada Estado. España está cumpliendo esto al articular dicha cooperación entre el CNC/autoridades NIS2 y el Banco de España/Economía. En adelante, será importante desarrollar memorandos o protocolos operativos entre el Centro Nacional de Ciberseguridad y el Banco de España, CNMV y otros reguladores financieros para clarificar cómo se compartirán alertas, cómo se evitan duplicidades de informes de las entidades, etc. Un posible "gris" competencial podría ser definir quién sanciona a una entidad financiera por incumplir medidas de ciberseguridad: ¿la autoridad NIS2 o la financiera bajo DORA? Lo previsible es que DORA sea la vía principal para sanciones en bancos, y la ley NIS2 se aplique subsidiariamente si hay aspectos fuera de DORA, pero esto requerirá fina coordinación.

4.3. Otras autoridades sectoriales:

La ley también alude a la cooperación con otras autoridades especializadas según el sector afectado. Por ejemplo, indica la necesidad de colaborar con las “autoridades nacionales en el ámbito de aviación civil y seguridad aérea”, lo cual apunta a coordinar con la Agencia Estatal de Seguridad Aérea (AESA) en incidentes que afecten a la aviación. Igualmente, menciona cooperación con los “organismos de supervisión conforme al Reglamento (UE) 910/2014” (supervisores eIDAS de servicios de confianza digitales), que en España es SEDIA para los Prestadores de Servicios de Confianza. Esto tiene sentido ya que los Trust Service Providers ahora son entidades esenciales bajo NIS2, pero SEDIA ya los supervisa por eIDAS, así que las dos funciones deben coordinarse. También la cooperación con autoridades de telecomunicaciones (art. 40 CE / Dir. 2018/1972) está prevista, lo que en la práctica involucra a la CNMC o la propia Secretaría de Estado de Telecomunicaciones para aspectos de redes públicas. Y muy importante, se exige coordinación regular entre la autoridad NIS2 (CNC) y la autoridad de la futura **Directiva CER (Critical Entities Resilience)**, que en España probablemente será también el Ministerio del Interior u otro órgano de seguridad física. De hecho, el anteproyecto de ciberseguridad se ha elaborado en paralelo al de transposición de la Directiva CER, “excluyendo del ámbito CER las materias reguladas en el anteproyecto [NIS2] y garantizando un marco de coordinación entre las autoridades de ambos ámbitos”. Esto para evitar que una infraestructura crítica tenga que lidiar por separado con exigencias de seguridad física y ciber sin coherencia. La OCC del Interior seguramente actuará como puente entre el CNC (ciber) y la autoridad CER (física) para las entidades críticas, dado su doble papel en ambas normativas.

4.4. Importancia de la coordinación

En conclusión, el anteproyecto muestra conciencia de los solapamientos potenciales con otras jurisdicciones regulatorias y establece puentes de cooperación para abordarlos. Se enfatiza que la nueva autoridad de ciberseguridad no actúa aislada, sino en conexión con Protección de Datos (para proteger la privacidad en incidentes), con Supervisores Financieros (en pro de la resiliencia financiera), con reguladores sectoriales específicos (aviación, telecomunicaciones, etc.) y con el esquema de infraestructuras críticas físicas. Esta cooperación multidireccional es un mandato de la Directiva NIS2 y será crucial para que la gobernanza de la ciberseguridad no choque con otros marcos legales, sino que los complemente.

5. Retos de gobernanza y posibles zonas grises competenciales

Implementar esta nueva arquitectura de coordinación y gobernanza en ciberseguridad supondrá afrontar diversos retos de gobernanza y cooperación interinstitucional. Algunos de los principales desafíos y “zonas grises” potenciales son:

Integración efectiva de múltiples actores: Conseguir que todos ellos funcionen coordinadamente, sin fricciones burocráticas ni conflictos de autoridad, será un reto de primer orden.

Evitar duplicidades en la supervisión: Con varias autoridades de control sectoriales más el CNC, existe la posibilidad de solapamiento en funciones de supervisión si no se coordinan bien.

Intercambio de información y confidencialidad: La cooperación intensa implica intercambio de datos sensibles entre organismos.

Áreas grises en sectores específicos: Algunos sectores regulados podrían quedar en una situación intermedia hasta que se ajusten normativas sectoriales.

Carga para las entidades obligadas: Desde la perspectiva de las empresas y entidades sujetas, el ideal es que este nuevo marco les simplifique el cumplimiento.

6. Conclusión

El anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad representa un paso decisivo para modernizar y reforzar la estructura institucional de la ciberseguridad en España. En su versión actual y pendiente de posibles modificaciones que resulten del período de consultas y de otras modificaciones que introduzca el Gobierno y, posteriormente, el Parlamento antes de su promulgación como Ley, su arquitectura prevé un modelo coordinado, con un Centro Nacional de Ciberseguridad como autoridad única dirigiendo un entramado de autoridades sectoriales y CSIRTs de referencia. La distribución de competencias se ha diseñado para aprovechar las fortalezas de los actores existentes bajo una directriz común.

El anteproyecto demuestra sensibilidad hacia los posibles solapamientos con otros marcos legales, incorporando cláusulas de coordinación con la Agencia de Protección de Datos y con los supervisores financieros. La comparación con la Directiva NIS2 revela que el modelo español alinea sus principios fundamentales con los europeos.

No obstante, el éxito de este nuevo esquema dependerá en gran medida de la implementación práctica. Entre los retos identificados figuran la necesidad de integrar culturas y competencias dispersas en una única gobernanza.

En suma, la nueva ley de ciberseguridad busca establecer un modelo de gobernanza equilibrado. Al hacerlo, sitúa a España en línea con las directrices europeas más avanzadas en la materia.

b. Marco regulador de la ciberseguridad en 2024/2025: certezas e incertidumbres

Carlos López Blanco, *Presidente de la Fundación ESYS*

1. Contexto geopolítico europeo y global.

2024 y el comienzo de 2025 han supuesto un momento significativo en materia de seguridad en un contexto general de gran incertidumbre.

En Europa comienza la nueva legislatura, la Comisión Von den Leyen II, que en el ámbito regulatorio digital abre una nueva fase tras haber realizado la UE el mayor cambio regulatorio que se recuerda y que afecta a todos los aspectos del mundo digital: la regulación de los servicios digitales (DSA), los mercados digitales (DMA), la Resiliencia de Entidades Críticas (DREC), los datos (Data Act), y la Inteligencia Artificial, y, como es obvio, la nueva regulación de Ciberseguridad, NIS2 y de las Entidades Financieras, el Reglamento DORA que configuran un marco regulatorio homogéneo y omnicomprensivo que afecta al mundo digital y sus regulaciones.

En este contexto y agotado el ámbito de la Regulación Digital, el desafío de los años venideros se va a centrar en la implementación de estas normativas, la mayoría de los cuales tienen carácter de Reglamento y, no es casualidad, cuenta con una excepción notable la ciberseguridad, regulada hasta ahora por Directivas por que en principio el Tratado de la UE no deja mayor margen de maniobra.

Por ello en España y la mayoría de los países e europeos, todavía morosos en el cumplimiento de su obligación de adaptación de la Directiva NIS2 desde octubre de 2024, van a abordar este año 2025 la adaptación de sus derechos nacionales, tal y como está haciendo España con la aprobación del anteproyecto de ley de Ciberseguridad. Esta situación no afecta a las entidades financieras y demás empresas sujetas a DORA dado su carácter de Reglamento, entró directamente en vigor en toda Europa el pasado 17 de enero de 2025.

En el contexto político europeo debe destacarse la publicación de los informes Draghi y Letta que van a constituir, especialmente el primero, la columna vertebral de la estrategia europea en los próximos años, estrategia acelerada por la necesidad de construir, en el nuevo ámbito geopolítico que dibuja la segunda Administración Trump, la Autonomía estratégica y de Defensa (y también de Ciberseguridad) Europea.

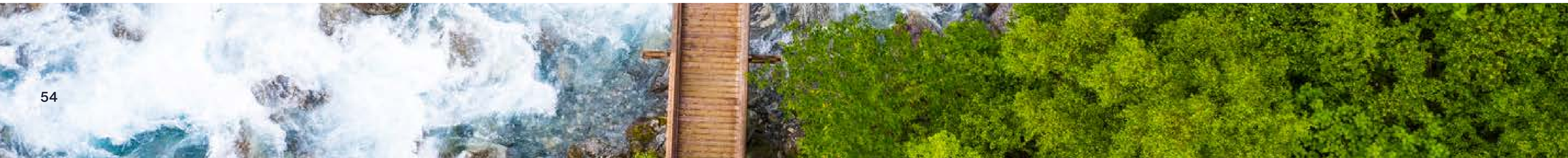
En este contexto se ha acelerado en España la discusión sobre la necesidad de aumentar nuestra contribución a los presupuestos de defensa, y en este debate, la necesidad de entender la Ciberseguridad dentro del marco de la Defensa y Seguridad de España se ha mostrado poco polémica incluso por los más reticentes al aumento de los gastos de Defensa. La Ciberseguridad y la necesidad de su fortalecimiento en el ámbito público y privado está hoy, afortunadamente, fuera del debate político.

Por tanto podemos esperar en nuestro país y en Europa este año y los años próximos un mayor relieve de la política de seguridad y su reflejo presupuestario. Esta política se refleja en el citado informe Draghi que dedica un capítulo entero, el cuarto, a la necesidad europea de incrementar sus políticas de seguridad y reducir dependencias externas. Igualmente en lo que se refiere a las propuestas concretas en materia de política de Telecomunicaciones y Tecnológica, las necesidades de garantizar la no vulnerabilidad de las redes y los sistemas de información se destaca de manera notable.

Es necesario también hacer mención al que ha sido calificado como el informe Draghi de la Defensa, el informe Niinistö, elaborado a petición de la Comisión Europea por el ex Presidente de Finlandia Sauli Niinistö, y titulado Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness, y que dedica tres de sus capítulos a temas relacionados con la Ciberseguridad: El capítulo 4 (Empowering citizens as the backbone of societal resilience and preparedness), el capítulo 5 (Leveraging the full potential of public-private cooperation), y el capítulo 6 (Outsmarting malicious actors to deter hybrid attacks).

No puede obviarse en este contexto geopolítico el cambio de la Administración Americana con el nuevo mandato de Trump que supondrá no solo un realineamiento del papel que EEUU quiere jugar a nivel global y en Europa, sino un mayor distanciamiento en materia de economía digital e intercambio comercial.

Sin embargo, y aunque se produzca un mayor fortalecimiento de las capacidades europeas de defensa y su autonomía estratégica respecto a EEUU, no es previsible que se produzca un distanciamiento en la cooperación trasatlántica en materia de ciberseguridad que creemos que va a mantenerse al margen de otros desajustes en política de Defensa o exterior, tales como la guerra de Ucrania, y continuará siendo una de las prioridades principales de la OTAN.



2. Novedades regulatorias

2.1 España

Actualización legislativa 2024 y 2025

Publicación en enero de 2025 del anteproyecto de la Ley de Coordinación y Gobernanza de la Ciberseguridad, que transpone la Directiva NIS2 de la UE.

Las novedades principales del futuro texto legislativo son:

1. Creación del Centro Nacional de Ciberseguridad, órgano de contacto único con la UE, dependiente de Presidencia del Gobierno para dirigir, impulsar, coordinar y ser autoridad de gestión de las crisis de ciberseguridad.

Incrementar el nivel de coordinación de las competencias en materia de ciberseguridad era una necesidad largamente compartida, y así lo pusimos de manifiesto en el informe de la Fundación ESYS sobre la Gobernanza de la Ciberseguridad en España.

Este paso adelante se ve sin embargo limitado al establecerse en el Anteproyecto la pervivencia de otras autoridades de control como la Oficina de Coordinación de Ciberseguridad de la Secretaría de Estado de Seguridad, el Centro Criptológico Nacional del Centro Nacional de Inteligencia y las Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y de Digitalización e Inteligencia Artificial. Hubiera sido preferible un mayor grado de centralización de las competencias en materia de Ciberseguridad a imagen y semejanza de otros países europeos.

2. Las entidades afectadas por esta norma son aquellas que residan en España o desarrollen su actividad en nuestro país.

Establece un criterio uniforme para clasificar entidades como esenciales o importantes, basado en su criticidad y tamaño y a las que se refieren detalladamente los anexos I y II de la Ley:

Las entidades críticas identificadas por la Directiva (UE) 2022/2557 sobre Resiliencia de las Entidades Críticas se consideran automáticamente entidades esenciales y están encuadradas en sectores considerados de alta criticidad, como la energía, el transporte, banca y mercados financieros, sector sanitario, agua, infraestructuras digitales y servicios tecnológicos, entidades de la administración pública e industria nuclear.

Otros sectores de menor criticidad, bajo la rúbrica de entidades importantes, recogidos en el anteproyecto son los servicios postales y de mensajería; la gestión de residuos; la fabricación, producción y distribución de sustancias y mezclas químicas; la producción, transformación y distribución de alimentos; los proveedores de servicios digitales; la investigación científica, y la seguridad privada, alguno de los cuales es de inclusión muy cuestionable especialmente ante la ausencia de otros.

3. Establece medidas generales para la gestión de riesgos de ciberseguridad y crea una Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes imponiendo a las entidades afectadas tres obligaciones:

Realizar una evaluación individualizada de su riesgo y poner en marcha actuaciones para garantizar y elevar los niveles de seguridad de sus redes y sistemas y prevenir el riesgo de incidentes.

Notificar los incidentes significativos que se produzcan, tanto si son propios como si pertenecen a proveedores externos.

Comunicar a la mayor brevedad a los destinatarios de sus servicios, cualquier ciberamenaza significativa que les pueda afectar y las medidas que pueden aplicar como respuesta.

4. Se crea y diseña la figura del responsable de seguridad de la información como órgano designado por las entidades, encargado de las funciones de punto de contacto y de coordinación técnica.

Se encargará de elaborar y someter a la aprobación y aplicación de la organización la estrategia y políticas de ciberseguridad; supervisar el cumplimiento de la normativa aplicable en materia de seguridad, y gestionar los incidentes de ciberseguridad.

Otros aspectos importantes son la **coordinación e intercambio de información a nivel nacional e internacional** y un **régimen de supervisión y de sanción** detallado que sin duda será muy importante en su aplicación.

También hay que destacar la obligación del artículo 20 de que los **Órganos de Dirección, incluido el Consejo de Administración, reciban la formación adecuada** en materia de ciberseguridad ya que en ellos recae la responsabilidad legal en esta materia.

En cuanto a su tramitación, el proceso legislativo debería culminar antes de mitad de año. No cabe esperar sobresaltos pese al actual contexto político tanto por su necesidad y contenido, poco discutible, como por ser adaptación obligada y tardía del Derecho europeo.

En resumen, una norma necesaria que mejora sensiblemente la regulación de la Ciberseguridad en España y cuyos elementos más cuestionables deberían ser objeto de mejora en el proceso legislativo.

España con esta ley pasará de tener una regulación dispersa (Ley 11/2002, ENS 2010, Ley de infraestructuras críticas 2011) a una estrategia integral y alineada con Europa.

En cuanto a **DORA**, el 17 de enero de 2025 ha terminado su plazo de aplicación y en consecuencia al menos en teoría todas las entidades afectadas deberían haber finalizado su adaptación. Esta circunstancia puede darse por garantizada en las entidades más importantes, pero dado que su ámbito de aplicación es más amplio algunas empresas de menor tamaño todavía se encuentran en el proceso de adaptación.

2.2 Unión Europea

Directiva NIS2

- Entrada en vigor y obligación de transposición nacional en 2024 aunque la mayoría de los países, todos menos tres, entre ellos España han agotado el plazo sin hacer la adaptación.
- Amplía sectores cubiertos (salud, transporte, energía, servicios digitales, administración pública, etc.) y clasifica entidades como esenciales e importantes
- Exige notificación de incidentes graves en 24 horas.
- Refuerza la cooperación y coordinación entre Estados miembros y crea centros de supervisión y respuesta coordinada.
- Sanciones severas por incumplimiento.

Reglamento Europeo de Ciberresiliencia (Cyber Resilience Act, CRA)

- En vigor desde diciembre de 2024
- Establece requisitos de ciberseguridad para productos con elementos digitales durante todo su ciclo de vida (diseño, desarrollo, comercialización y soporte).
- Obligación de notificar vulnerabilidades en 24 horas y soporte de actualizaciones durante al menos 5 años.
- Transparencia para consumidores y apoyo específico a pymes.
- Introducción del marcado CE para productos conformes.

Reglamento de Cibersolidaridad

- Refuerza la resiliencia y capacidad de respuesta ante ciberamenazas a nivel UE, con mecanismos de alerta, preparación y gestión de crisis a gran escala.

Reglamento de Ciberseguridad

- Sistema único de certificación de ciberseguridad para productos, servicios y procesos TIC en la UE, revisado en 2024 para incluir servicios de seguridad gestionados.

2.3. Otros países del mundo

Acuerdos Internacionales

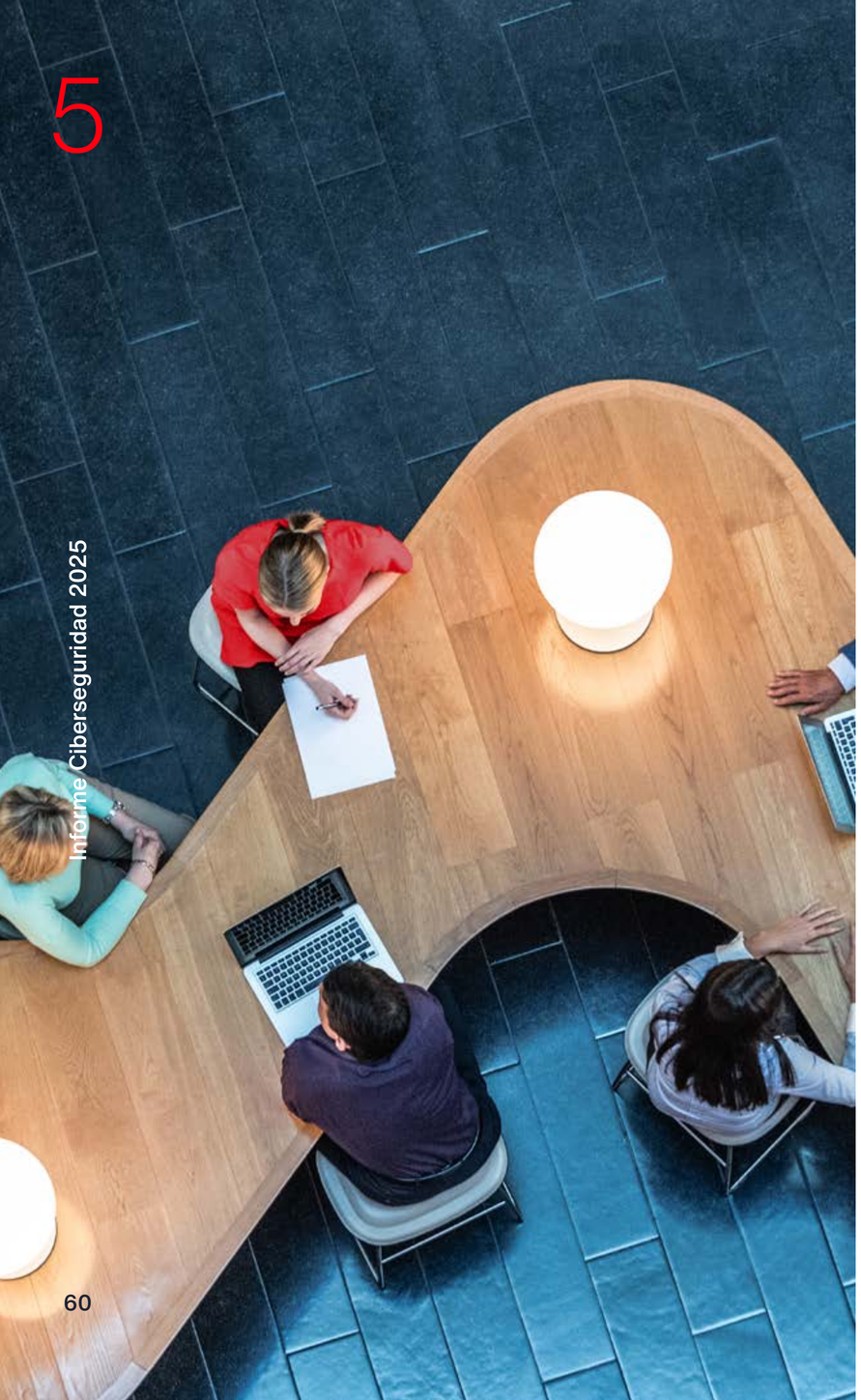
La Cumbre sobre Inteligencia Artificial de 2025 dio continuidad a la Cumbre de Seguridad de la IA de 2023 celebrada en Bletchley Park en el Reino Unido, y a la Cumbre de Seúl de 2024 en Corea del Sur.

Mientras que a la Cumbre de Seguridad de la Inteligencia Artificial de 2023 asistieron representantes de 29 gobiernos y ejecutivos de solo un puñado de empresas, más de 1.000 participantes de más de 100 países asistieron a la Cumbre de París 2025, representando a líderes gubernamentales, organizaciones internacionales, la comunidad académica y de investigación, el sector privado y la sociedad civil.

El Primer Informe Internacional de Seguridad de la IA se publicó el 29 de enero de 2025. Comisionado después de la Cumbre de Seguridad de la IA de Bletchley Park, el informe se centró en los riesgos y amenazas que plantea la IA de propósito general, y estaba programado para ser discutido en la Cumbre de París como parte del pilar de “Confianza en la IA”.

Mientras que la primera Cumbre se centró en los riesgos catastróficos de la IA y su mitigación, la reunión de París se reeditó como una “Cumbre de Acción sobre la IA” enfatizando la innovación, la implementación práctica y las posibles oportunidades económicas de la IA, al tiempo que exploró una gama más amplia de riesgos, incluido su impacto ambiental y las interrupciones en el mercado laboral.

País	Novedades regulatorias clave en 2024
Estados Unidos	Avances en la Estrategia Nacional de Ciberseguridad: traslada la responsabilidad de la ciberseguridad hacia grandes organizaciones y refuerza la colaboración público-privada. Orden ejecutiva para fortalecer la ciberseguridad en puertos, obligando al DHS a evaluar amenazas y reforzar sistemas marítimos. Impulso a estándares de “seguridad por diseño” en compras gubernamentales de IoT. Creación de la Oficina de Política Cibernética y Digital para fomentar alianzas internacionales.
Reino Unido	Entrada en vigor de la Ley PSTI (Product Security and Telecommunications Infrastructure Act) el 29 de abril de 2024. - Exige requisitos mínimos de ciberseguridad para todos los dispositivos conectados de consumo (IoT) vendidos en el país. - Obliga a fabricantes y la cadena de suministro a certificar la seguridad de sus productos antes de su comercialización. - Basada en estándares internacionales como ETSI EN 303 645.
China	- Refuerzo de la vigilancia y control estatal sobre infraestructuras críticas y datos personales. - Endurecimiento de requisitos para empresas tecnológicas y transferencia internacional de datos. - Incremento de la actividad de ciberespionaje y ataques impulsados por IA generativa, lo que ha llevado a mayores exigencias regulatorias y de cumplimiento para empresas extranjeras y nacionales.
Japón	- Presentación de la Ley de Defensa Cibernética Activa, que permite al gobierno y fuerzas de defensa tomar medidas proactivas contra ciberataques (penetrar y neutralizar servidores atacantes, bajo supervisión judicial). - Refuerzo de la cooperación público-privada y obligación de reporte de incidentes para infraestructuras críticas. - Reforma de la Ley de Protección de Información Personal (abril 2024): amplía las obligaciones de notificación y reporte en caso de fuga de datos, incluyendo ahora también “información personal” además de “datos personales”. - Reorganización del Centro Nacional de Estrategia y Preparación ante Incidentes Cibernéticos (NISC).



3. Visión cualitativa de la evolución normativa (2024 vs. años anteriores)

Tendencias comunes:

- Paso de marcos sectoriales a regulaciones integrales, con mayor armonización internacional y enfoque en la protección de toda la cadena de suministro digital.
- Expansión del ámbito de aplicación: más sectores y empresas obligadas, incluyendo pymes y proveedores de servicios críticos.
- Endurecimiento de las obligaciones: notificación rápida de incidentes, auditorías, requisitos técnicos avanzados y sanciones más severas.
- Mayor foco en la resiliencia, la protección de la cadena de suministro y la ciberseguridad “by design”.
- Refuerzo de la cooperación internacional y la respuesta coordinada ante incidentes transfronterizos.
- Mayor atención a la protección de los consumidores y la transparencia, así como apoyo específico para pymes.
- Influencia de tecnologías emergentes (IA, IoT, 5G) en la evolución normativa y en la ampliación de la superficie de ataque.
- Creciente convergencia hacia modelos inspirados en el RGPD europeo, incluso fuera de Europa.

Respecto a años anteriores:

- Se observa una aceleración regulatoria: de marcos mínimos o sectoriales a leyes exhaustivas y armonizadas, con mayor exigencia y supervisión.
- La ciberseguridad pasa de ser un asunto técnico a una prioridad estratégica nacional y europea, con implicaciones económicas, sociales y geopolíticas.
- Las empresas y organismos deben adaptarse a un entorno regulatorio más exigente y dinámico, donde la resiliencia y la gestión proactiva del riesgo son fundamentales.
- La regulación ha evolucionado desde la protección de datos y la defensa de infraestructuras físicas hacia la protección integral del ecosistema digital, incluyendo servicios, productos, procesos y usuarios finales.
- Se observa una clara convergencia internacional, con la UE marcando tendencia y países como EE.UU. y otros adaptando sus marcos para alinearse a estándares globales.

4. Resumen:

En 2024, el marco regulador de la ciberseguridad en España, Europa y las principales economías mundiales ha experimentado una transformación profunda, con normas más estrictas, con mayor alcance sectorial y con la exigencia de notificación obligatoria de incidentes, así como de sanciones más elevadas.

Esta evolución responde a la creciente sofisticación de las amenazas y a la digitalización acelerada, fomentando la cooperación internacional y la protección integral del ecosistema digital, con una clara tendencia hacia la armonización internacional, el refuerzo de la resiliencia y la protección proactiva de los activos digitales y los ciudadanos.

En 2025 el desafío principal de las empresas españolas será adaptarse a la nueva regulación derivada de la Ley de Ciberseguridad, una vez que esta norma entre en vigor.

Sin embargo, existen ya elementos suficientes que permiten que las empresas vayan preparando este ejercicio desde la formación en los Consejos hasta la revisión de todos los planes en materia de Ciberseguridad. El hecho de que la nueva Ley sea implementación de una directiva, hace esta tarea más fácil, puesto que puede anticiparse buena parte de su contenido al estar incluido en una directiva que tiene una técnica muy cercana a la del Reglamento. Es por tanto muy aconsejable que por parte de las empresas no se espere a la entrada en vigor de la Ley para adaptarse a sus contenidos.

En el entorno geopolítico, el debate de la Seguridad y la Ciberseguridad han ocupado un papel central tanto en lo relativo a la Defensa como al papel que la ciberseguridad mantiene en el ámbito de la Defensa y la Seguridad Pública. Todo ello en un entorno de recomposición de las relaciones entre Estados Unidos y Europa en un contexto caracterizado por el fortalecimiento de la autonomía estratégica de Europa mediante el aumento de los presupuestos de defensa, y que tendrá como efecto inducido un fortalecimiento de la Ciberseguridad en el sector público y privado.

Es de esperar que por parte de los gobiernos europeos, y especialmente el español, se lancen en los meses próximos iniciativas y estrategias públicas y líneas de financiación para reforzar la Seguridad de la empresas y ciudadanos en el ámbito de la Ciberseguridad.

6

Checklist Normativa NIS2: ámbito de aplicación y cumplimiento

Checklist NIS2: ¿Es su empresa sujeto obligado y cumple con los requisitos de la normativa?

La Directiva NIS2 marca un punto de inflexión en la gestión del riesgo digital en Europa. Su enfoque no se limita al cumplimiento formal, sino que impulsa una transformación estructural en las organizaciones esenciales e importantes, exigiendo capacidades técnicas, organizativas y de gobernanza avanzadas. Desde la designación de responsables y la trazabilidad de incidentes, hasta la supervisión de la cadena de suministro, el marco NIS2 redefine los estándares mínimos de ciberresiliencia.

Más allá de los requisitos técnicos, NIS2 incorpora un régimen sancionador estricto, plazos de notificación exigentes y una supervisión más directa por parte de las autoridades competentes. En este contexto, el cumplimiento no es solo una obligación legal, sino una palanca para reforzar la confianza de clientes, reguladores e inversores.

Este artículo presenta una checklist práctica que permite a cualquier empresa evaluar su situación frente a la Directiva NIS2 (*) y conocer los principales requerimientos que debe implementar para fortalecer su resiliencia digital.

(*) Incluye el Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, aprobado en España el 14 de enero de 2025.

1. ¿Está su organización dentro del ámbito de aplicación de la normativa NIS2?

Seleccione con una cruz si la respuesta es afirmativa:

- ☐ ¿Es su organización mediana o grande? Es decir, ¿cuenta con 50 o más trabajadores, y el volumen de negocios anual o el balance general anual supera los 10 millones de euros?
- ☐ ¿Opera en la Unión Europea?
- ☐ ¿Pertenece a alguno de los siguientes sectores?
    - **Alta criticidad:** energía, transporte, banca, Infraestructuras de los mercados financieros, sanitario, agua potable, aguas residuales infraestructura digital, Gestión de servicios de TIC, Entidades de la Administración pública, espacio y/o nuclear.
    - **Otros sectores críticos:** Servicios postales y de mensajería, Gestión de residuos, químico, alimentario, fabricación, proveedores de servicios digitales, investigación y/o seguridad privada.
- ☐ ¿Su organización forma parte de la cadena de suministro de alguno de los sectores anteriores?
- ☐ ¿Es su organización una entidad pública con funciones esenciales?
- ☐ ¿Su organización presta servicios digitales esenciales (como servicios en la nube, DNS, centros de datos)?

Si ha respondido afirmativamente a alguna de las preguntas anteriores es probable que su organización sea sujeto obligado de la Directiva NIS2 y clasificada como una **entidad esencial** o **entidad importante** bajo dicha normativa.

2. Checklist de cumplimiento

Antes de implementar cualquier estrategia de adaptación a la Directiva NIS2, es fundamental realizar una evaluación de riesgo de los niveles de seguridad de las redes y sistemas de información de su organización y determinar las medidas técnicas, operativas y organizativas adecuadas y proporcionadas a su exposición.

La siguiente checklist le ayudará a tener una visión clara del grado de cumplimiento frente a los requerimientos mínimos regulatorios y operativos que impone NIS2, y servirá como punto de partida para fortalecer la resiliencia cibernética de la organización.

01. ¿Ha designado un responsable de ciberseguridad?

02. ¿Tiene una política formal de gestión de riesgos y/o política de seguridad de las redes y sistemas de información?

03. ¿Ha realizado su organización una evaluación de riesgos cibernéticos? ¿Realiza auditorías de seguridad anuales?

04. ¿Dispone su organización de un plan de continuidad de negocio, plan de respuesta ante incidentes o similar?

05. ¿Existe un procedimiento para la notificación de incidentes? ¿se documentan y analizan los incidentes para evitar recurrencias?

06. ¿Cuenta su organización con soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto y sistemas seguros de comunicaciones de emergencia?

07. ¿Se forma a la alta dirección y al personal en materia de ciberseguridad?

08. ¿Evalúa su organización los riesgos de sus proveedores y aplica medidas de seguridad con cada uno de ellos? ¿Se incluyen requisitos de ciberseguridad en los contratos con proveedores?

09. ¿Cumple su organización con ENS, ISO 27001 u otra normativa?

10. ¿Tiene su organización visibilidad sobre vulnerabilidades críticas?

11. ¿Cuenta su organización con políticas y procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad?

La implementación de la Directiva NIS2 representa una oportunidad estratégica para que las organizaciones refuercen su nivel de ciberseguridad y aumenten su resiliencia frente a amenazas digitales cada vez más sofisticadas. Esta checklist no solo permite identificar el grado de cumplimiento actual, sino también sirve como hoja de ruta para avanzar hacia una gestión más robusta y proactiva de los riesgos tecnológicos. Adoptar estas medidas no es solo una obligación legal, sino una inversión en la continuidad, reputación y competitividad de la organización en el entorno digital tanto nacional como europeo.

7

Nuevos riesgos y amenazas en ciberseguros: escenario emergente en 2025

Nuevos riesgos y amenazas en ciberseguros: escenario emergente en 2025

Introducción

La transformación digital, la automatización masiva y la integración tecnológica de las últimas décadas han redefinido por completo el panorama del riesgo cibernético. En este nuevo entorno, la aparición de amenazas emergentes ha obligado a las organizaciones —y al mercado asegurador— a evolucionar con rapidez, repensando sus estrategias de prevención, respuesta y transferencia de riesgo. El presente artículo analiza, desde la perspectiva del corredor de seguros especializado, los principales vectores de riesgo que están marcando la agenda de 2025: la inteligencia artificial como amenaza y defensa, la computación cuántica y su potencial disruptivo, los ataques a la cadena de suministro, el Shadow IT como vulnerabilidad interna, y el modelo Zero Trust como nuevo estándar técnico. Cada uno de estos fenómenos plantea desafíos únicos y exige una aproximación aseguradora distinta, más dinámica, adaptativa y estratégica.

Inteligencia Artificial Generativa: riesgo de doble filo

La irrupción de la inteligencia artificial generativa (GenAI) ha transformado el panorama tecnológico y empresarial. Herramientas como ChatGPT, Gemini o Copilot han democratizado capacidades antes exclusivas, mejorando la productividad, pero también facilitando el acceso a técnicas de ciberataque cada vez más sofisticadas.

Más del 70 % de las empresas ya utiliza o planea implementar GenAI en tareas como redacción, soporte y desarrollo. Sin embargo, su uso también ha sido adoptado por actores maliciosos, capaces de crear phishing avanzado, deepfakes, malware personalizado y análisis automatizado de defensas.

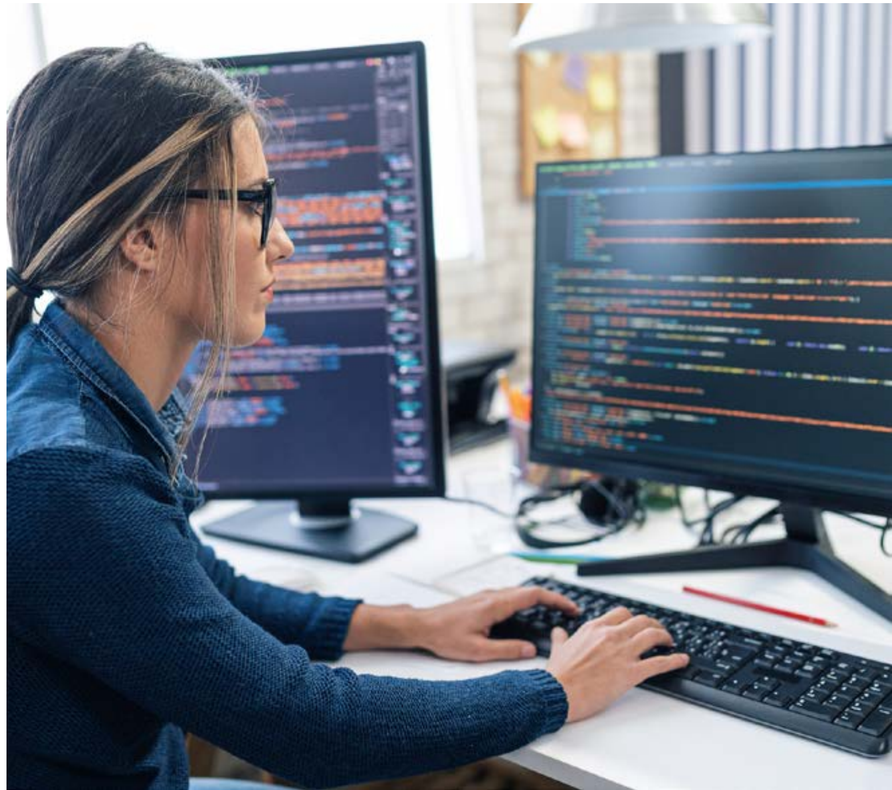
Esto representa un desafío para el sector asegurador. La automatización y autonomía de estos sistemas dificultan la atribución de responsabilidades, lo que complica la gestión de reclamaciones. Las aseguradoras están ajustando sus procesos de suscripción e incorporando cláusulas sobre errores algorítmicos, propiedad intelectual o decisiones automatizadas con sesgos involuntarios. Algunas pólizas incluso incluyen lenguaje afirmativo para cubrir el uso responsable de IA, siempre que se apliquen controles adecuados.

Al mismo tiempo, la IA se está consolidando como una herramienta clave en defensa: sistemas SIEM, EDR y SOAR integran algoritmos que detectan anomalías y responden en tiempo real ante incidentes, con capacidades que superan los métodos tradicionales. Las compañías que adoptan IA defensiva ya están siendo recompensadas con mejores condiciones.

La IA ha dejado de ser una simple innovación tecnológica para convertirse en un factor transversal del riesgo cibernético. Las organizaciones deben adaptarse con políticas sólidas, prácticas responsables y mecanismos eficaces de transferencia de riesgo.

Informe para el CISO: gobernar la GenAI desde la ciberseguridad

La llegada de la inteligencia artificial generativa ha colocado al CISO en el centro de una transformación profunda. Ya no basta con proteger perímetros o monitorizar accesos; ahora, los modelos de lenguaje generan códigos, crean contenido, automatizan procesos... y pueden filtrar información sensible con un solo prompt mal planteado. En este nuevo contexto, la responsabilidad del CISO pasa de ser reactiva a ser estratégica: se convierte en arquitecto de confianza digital.



Principales impactos en la ciberseguridad corporativa

01 Adopción sin control

Las áreas de negocio están impulsando el uso de asistentes de IA sin involucrar al equipo de seguridad. Esto genera un entorno donde los datos críticos pueden terminar en plataformas públicas, sin supervisión, y se crean algoritmos sin trazabilidad ni validación de riesgos.

02 Superficie de ataque ampliada

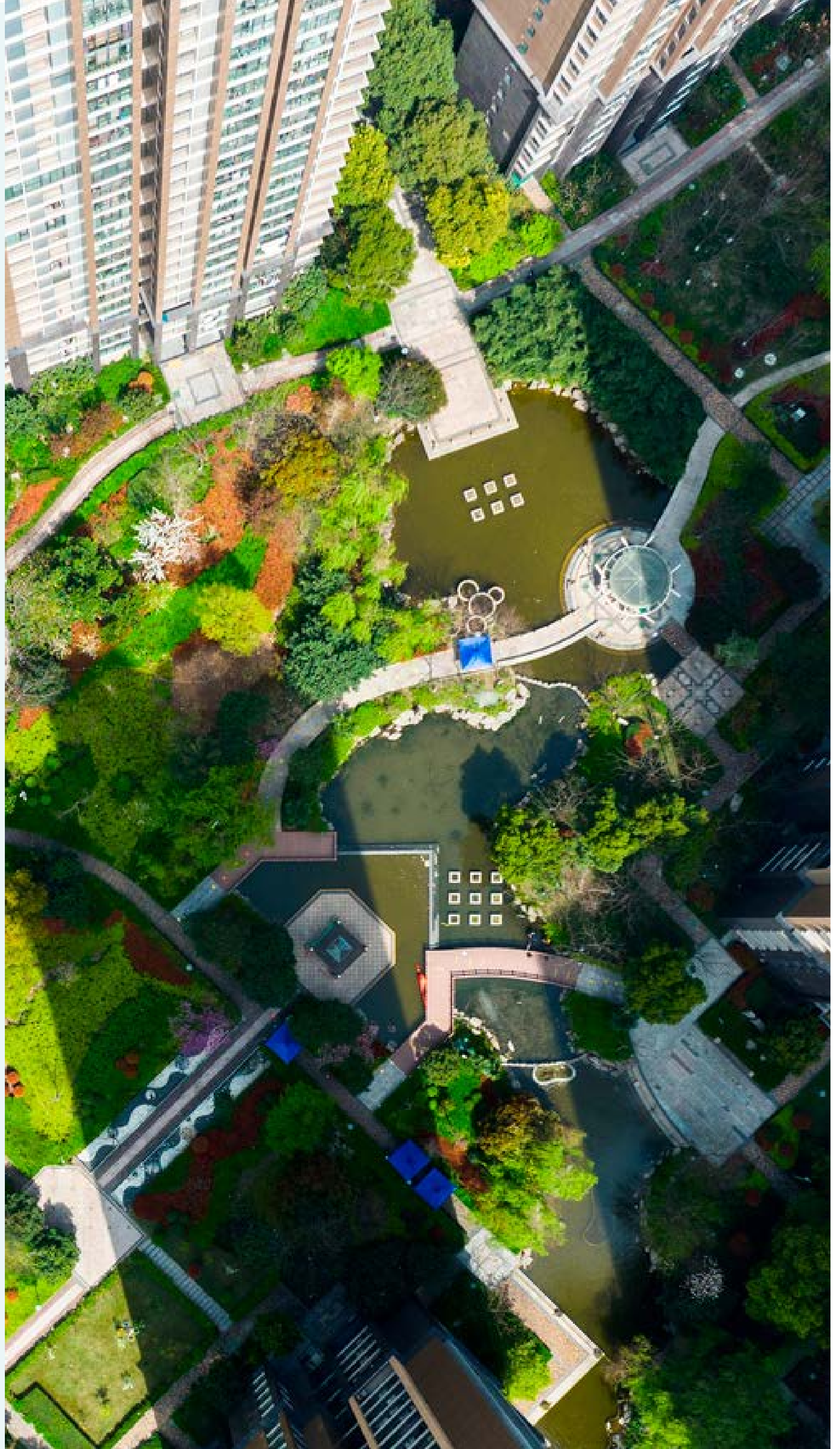
Cada interacción con un modelo puede ser un vector de ataque. Amenazas como la inyección de prompts, la inversión de modelos o el envenenamiento de datos están emergiendo como técnicas frecuentes. Además, el marco legal, como el AI Act, prevé sanciones severas en caso de uso indebido o filtración de datos personales.

03 Modelos propios, mayores desafíos

Entrenar modelos internos con datos confidenciales expone a la organización a riesgos de uso indebido de licencias, uso de fuentes contaminadas, y pérdida de control sobre la cadena de suministro algorítmica. Esto exige aplicar marcos de gobernanza como AI TRiSM (transparencia, trazabilidad y planes de retirada).

04 Amenazas potenciadas por IA

Los ciberdelincuentes ya usan GenAI para diseñar ataques más realistas y automatizados: phishing hiperléxico, malware polimórfico, campañas de reconocimiento o suplantación de identidad. El umbral técnico para atacar ha bajado drásticamente, por lo que es urgente reforzar la inteligencia de amenazas con foco específico en IA.



Hoja de ruta práctica para el CISO

1. Cree un laboratorio interno de ciber-GenAI

Antes de adoptar soluciones de IA generativa a gran escala, implemente un entorno controlado donde pueda probar y validar herramientas. Utilice estos modelos para redactar informes, generar playbooks de respuesta, automatizar análisis de logs o simular ataques de phishing ético y ejercicios de red teaming.

2. Implante una gobernanza 360°

Coordine esfuerzos entre los departamentos de Legal, Tecnología y RR. HH. para garantizar el uso seguro y conforme a la normativa:

- **Legal y Compliance:** asegure cláusulas de protección de datos, gestión de la propiedad intelectual y evaluación de impacto conforme al AI Act.
- **Tecnología:** refuerce medidas como cifrado de extremo a extremo, autenticación robusta, control de peticiones y auditoría de actividad.
- **RR. HH:** promueva una cultura de uso responsable de IA con formación continua en ética digital y buenas prácticas.

3. Adopte estándares internacionales de gestión de IA

Integre marcos como **NIST AI-RMF, ISO/IEC 42001** o **ISO 23894** para establecer un ciclo de vida seguro del uso de GenAI:

- Antes del despliegue: cree fichas técnicas (“model cards”) y realice evaluaciones de impacto.
- Durante el uso: monitorice sesgos, desviaciones y evolución del modelo (drift).
- Después del uso: diseñe un plan de retirada seguro, con “kill switch” y documentación detallada.

4. Actualice el threat modeling tradicional

Amplíe metodologías como STRIDE para incluir los riesgos propios de IA generativa: desde el entrenamiento y fine-tuning hasta la interacción en producción. Incorpore métricas como fiabilidad, explicabilidad y robustez de los modelos en el registro de riesgos.

Resiliencia, innovación y ética desde el primer prompt

La GenAI ya redacta contratos, compila código, atiende clientes y, en manos equivocadas, puede vulnerar sistemas enteros. El nuevo KPI del CISO no es “cero incidentes”, sino lograr un equilibrio entre innovación y resiliencia. Integrar seguridad y ética desde el diseño de estas herramientas es la única forma de construir confianza digital sostenible. No se trata solo de mitigar el riesgo, sino de anticiparlo y convertirlo en una ventaja competitiva.

Computación Cuántica: un riesgo futuro que exige acción presente

La computación cuántica representa uno de los desarrollos tecnológicos más disruptivos del presente siglo. Aunque su adopción práctica aún se encuentra en etapas iniciales, su potencial transformador es tan grande que el sector asegurador ya ha comenzado a prepararse para sus efectos, incluso antes de que estos se manifiesten de forma masiva. La principal preocupación radica en su capacidad de quebrar los sistemas criptográficos tradicionales, lo cual tendría implicaciones devastadoras para la seguridad digital y, en consecuencia, para la cobertura y la siniestralidad en ciberseguros.

En la actualidad, la mayoría de los sistemas de seguridad de la información en empresas y gobiernos están basados en criptografía asimétrica, con algoritmos como RSA, ECC o DSA. Estos sistemas son seguros frente a los ordenadores clásicos porque descifrar la clave privada a partir de la pública llevaría siglos de cómputo. Sin embargo, un ordenador cuántico con suficiente capacidad operativa, gracias a algoritmos como el de Shor, podría reducir esa tarea a cuestión de minutos. Esta posibilidad no es una especulación insignificante: centros de investigación como Google, IBM y la Universidad de Ciencia y Tecnología de China han demostrado avances significativos en los últimos años, acortando la brecha hacia lo que se conoce como “supremacía cuántica”.

El impacto de esta tecnología en ciberseguridad sería estructural. Todas las transacciones cifradas, los contratos digitales firmados electrónicamente, las comunicaciones confidenciales y la identidad digital perderían su integridad si los esquemas criptográficos actuales quedaran obsoletos de la noche a la mañana. Pero el riesgo no se limita al futuro. Ya existen actores que están llevando a cabo lo que se conoce como ataques tipo “store now, decrypt later”, es decir, la interceptación y almacenamiento de comunicaciones cifradas para descifrarlas más adelante cuando la tecnología lo permita. Esto convierte a los datos actuales en posibles fuentes de fuga futura.

Desde el punto de vista del ciberseguro, el reto radica en cómo valorar y suscribir un riesgo que todavía no se ha materializado plenamente. Algunas aseguradoras van a comenzar a introducir exclusiones específicas relacionadas con fallos criptográficos derivados de tecnologías emergentes, mientras otras optan por mantener coberturas, pero exigen que las empresas adopten medidas de transición hacia la criptografía post-cuántica. Estas medidas incluyen la evaluación del inventario de datos cifrados, la implementación de algoritmos híbridos y la planificación de migraciones a estándares resistentes al cómputo cuántico, tal como recomienda el NIST (National Institute of Standards and Technology).

En este contexto, no basta con transferir el riesgo, es necesario educar al cliente sobre la relevancia de un fenómeno que aún no causa pérdidas, pero que puede comprometer toda la arquitectura de confianza digital sobre la que operan sus procesos. Ayudar a los asegurados a comprender el valor de sus activos cifrados, revisar la vigencia tecnológica de sus controles criptográficos, y acompañarlos en la integración de soluciones post-cuánticas se convierte en una tarea tan importante como la negociación de los términos de póliza.

Por otra parte, también emerge la necesidad de repensar la temporalidad del riesgo. Tradicionalmente, las coberturas se centran en eventos ocurridos dentro del periodo de vigencia. Sin embargo, un ataque de “almacenar ahora y descifrar luego” puede tardar años en materializarse. Las compañías podrían no tener claro qué póliza será responsable del daño cuando ocurra el descifrado, si no existía tecnología cuántica funcional al momento de la brecha. Esta ambigüedad genera un vacío legal que será necesario abordar mediante cláusulas específicas de continuidad o de imputabilidad tecnológica en los contratos de seguro.

La computación cuántica aún no ha desatado su potencial destructivo, pero su sola posibilidad ha empezado a alterar los fundamentos técnicos, legales y financieros del ecosistema asegurador. Ignorar este escenario sería, cuando menos, imprudente. A medida que se consoliden los avances, será indispensable anticiparse con políticas que promuevan la resiliencia criptográfica, fomenten la transparencia tecnológica y definan claramente los escenarios de cobertura ante amenazas que, aunque aún invisibles, son cada vez más inevitables.

Shadow IT: la amenaza silenciosa que pone en riesgo la ciberseguridad empresarial

Uno de los desafíos más subestimados en la gestión moderna del riesgo cibernético es el Shadow IT: el conjunto de aplicaciones, dispositivos y servicios digitales que operan al margen del control de los equipos de tecnología y seguridad. Esta práctica, muchas veces bien intencionada, surge cuando empleados, departamentos o unidades externas instalan herramientas o plataformas sin aprobación formal, motivados por la búsqueda de agilidad, autonomía o productividad. Pero lo que a primera vista parece inofensivo, puede convertirse en una grieta crítica dentro del perímetro de seguridad.

En entornos de trabajo híbrido o descentralizado, el fenómeno se ha intensificado. La facilidad con la que cualquier empleado puede descargar softwares, conectar dispositivos personales o contratar servicios SaaS con una tarjeta de crédito corporativa ha multiplicado la cantidad de activos digitales invisibles para los equipos de seguridad. Esta proliferación de soluciones sin supervisión conlleva riesgos sustanciales: pérdida de control sobre los datos, incumplimiento normativo, exposición accidental de información confidencial y creación de superficies de ataque no protegidas.

Lo más preocupante es que el Shadow IT no solo aumenta el riesgo de sufrir un ciberataque, sino que complica significativamente la respuesta ante incidentes. Cuando ocurre una intrusión, la falta de visibilidad impide detectar rápidamente el punto de entrada, contener el daño o incluso identificar si el sistema comprometido forma parte de la red oficial. Además, muchas de estas herramientas no cumplen con estándares básicos de cifrado, autenticación o protección de datos personales, lo cual expone a las organizaciones a sanciones regulatorias severas, especialmente en sectores altamente vigilados como salud, finanzas o servicios públicos.

Desde la óptica del ciberseguro, el Shadow IT representa una variable de difícil cuantificación, pero con gran impacto en la evaluación del riesgo. Las aseguradoras ya han comenzado a realizar preguntas específicas sobre cómo las empresas gestionan sus activos digitales no registrados, qué procesos tienen para descubrir entornos no autorizados y si emplean soluciones como CASB (Cloud Access Security Broker) para monitorear el uso real de servicios cloud. La falta de medidas de control puede afectar negativamente a las condiciones de póliza, derivar en exclusiones, o incluso en la reducción del pago ante un siniestro, si se demuestra que el incidente se originó en un entorno no autorizado ni cubierto.

Es fundamental impulsar políticas claras sobre el uso de tecnología, fomentar la cultura de reporte voluntario, y facilitar canales para que los usuarios puedan proponer nuevas herramientas sin recurrir a soluciones no autorizadas. Además, la integración de tecnologías de descubrimiento de activos y análisis de tráfico es cada vez más recomendable para mapear en tiempo real la infraestructura digital real de la empresa.

El Shadow IT también representa un punto ciego para muchas estrategias de resiliencia. Si la continuidad operativa depende de herramientas no reconocidas formalmente, cualquier interrupción o incidente puede tener efectos no previstos en los planes de contingencia. Asimismo, la desconexión entre el uso real y la infraestructura declarada puede dificultar la renovación o mejora de coberturas aseguradoras, ya que las condiciones contratadas no reflejan fielmente el verdadero nivel de exposición.

El Shadow IT encarna una paradoja de la era digital: cuanto más se intenta innovar y agilizar los procesos, más se multiplican los puntos de vulnerabilidad invisibles. Las organizaciones que no implementen mecanismos de visibilidad y control en tiempo real estarán condenadas a navegar en la oscuridad, asumiendo riesgos ocultos que tarde o temprano se materializarán. Para el corredor, esta es una oportunidad estratégica de aportar valor, ayudando a los clientes a descubrir su perímetro real, cerrar las brechas invisibles y garantizar que sus coberturas evolucionen al ritmo del entorno tecnológico que ellos mismos están impulsando, consciente o inconscientemente.

Ciberataques a la cadena de suministro: el talón de Aquiles

En el ecosistema digital contemporáneo, la dependencia de terceros para el funcionamiento de servicios, operaciones y datos se ha vuelto tan extendida que la cadena de suministro digital se ha convertido, sin exagerar, en uno de los eslabones más frágiles y peligrosos para las organizaciones. El concepto de “supply chain attacks” ya no se limita al ámbito logístico tradicional, sino que abarca cualquier punto de integración externa que forme parte del entorno tecnológico de una empresa: proveedores de software, servicios cloud, desarrolladores de APIs, empresas de mantenimiento, plataformas de terceros y, en muchos casos, hasta pequeños subcontratistas sin controles mínimos de seguridad. Esta interconexión ha generado una superficie de riesgo distribuida que, al ser comprometida, puede derivar en impactos masivos y difíciles de contener.

Los ataques a la cadena de suministro no son nuevos, pero su sofisticación, alcance y frecuencia han crecido exponencialmente en los últimos años. Casos como SolarWinds, Kaseya o más recientemente MOVEit, han demostrado que un solo vector vulnerable puede comprometer a cientos o miles de organizaciones simultáneamente. A estos casos se suma el incidente de 2024 con CrowdStrike, que evidenció que incluso los proveedores más consolidados pueden convertirse en puntos únicos de fallo sistémico.

Estos eventos han provocado una transformación profunda en la manera en que se analiza el riesgo. Las aseguradoras han dejado de mirar exclusivamente al perímetro técnico de la empresa asegurada para enfocarse en su mapa de dependencias críticas. Hoy se evalúa, por ejemplo, si la organización conoce y controla a sus proveedores clave, si tiene cláusulas contractuales de ciberseguridad, si dispone de procesos de due diligence digital antes de incorporar nuevos servicios, y si sus herramientas de monitorización incluyen visibilidad sobre los entornos de terceros. En este contexto, la falta de trazabilidad en la cadena digital no solo incrementa el riesgo operativo, sino que puede derivar en condiciones más restrictivas en la póliza, sublímites o incluso exclusiones para determinados proveedores.

Una evolución destacada en el mercado ha sido la inclusión de coberturas específicas para interrupciones causadas por terceros, conocidos como Dependent Business Interruption (DBI), tanto para proveedores IT como non-IT. Esta ampliación refleja una realidad contundente: la afectación económica que puede sufrir una empresa por la caída de un proveedor de nube, un proveedor logístico o un procesador de datos externo puede ser igual o mayor que la de un ataque directo.

Además, existe una creciente preocupación sobre los contratos con dichos proveedores. Muchos de ellos incluyen cláusulas de limitación de responsabilidad, plazos muy cortos para interponer reclamaciones, o exclusiones contractuales por fuerza mayor que, en la práctica, dificultan cualquier intento de recuperar pérdidas. Desde el punto de vista asegurador, esto obliga a los corredores a trabajar de forma proactiva con sus clientes para revisar estos acuerdos, asesorarlos sobre el impacto que podrían tener en una reclamación futura, e incluso renegociar cláusulas para alinear la cobertura con las condiciones contractuales. A esto se suma la necesidad de contemplar escenarios de riesgo que se materializan de forma indirecta.

No se trata únicamente de conocer los sistemas internos del asegurado, sino de comprender en profundidad su ecosistema digital extendido. Esto incluye identificar qué servicios son críticos, qué datos fluyen entre actores externos, cuáles son las medidas de seguridad impuestas a los terceros, y cómo se gestionan los incidentes compartidos. A medida que los ataques a la cadena de suministro sigan creciendo —y todo indica que lo harán—, las empresas que no integren una visión extendida del riesgo estarán no solo más expuestas, sino también en desventaja frente al mercado asegurador.

La cadena de suministro digital es, sin lugar a dudas, una de las fronteras más complejas del ciberseguro moderno. Su análisis, gestión y cobertura exigen un enfoque integral que combine conocimientos técnicos, jurídicos, contractuales y estratégicos. En este nuevo entorno de riesgos interdependientes, ningún actor está verdaderamente aislado, y la resiliencia no puede entenderse sin una gestión activa de las relaciones externas que sostienen las operaciones críticas de la empresa.

5. Zero Trust: del eslogan al estándar de asegurabilidad

Durante años, el enfoque tradicional de ciberseguridad se basó en la noción de un perímetro corporativo confiable: una red interna protegida tras firewalls, donde los usuarios y dispositivos autorizados podían operar libremente una vez dentro. Sin embargo, esta concepción ha quedado obsoleta frente a un entorno digital fragmentado, híbrido y expuesto a amenazas cada vez más sofisticadas. En este contexto, el modelo de seguridad Zero Trust ha pasado de ser una tendencia conceptual a convertirse en una exigencia técnica, estratégica y, más recientemente, aseguradora.

Zero Trust parte de un principio simple pero poderoso: “nunca confíes, verifica siempre”. Bajo esta lógica, ningún usuario, dispositivo, aplicación o red es considerado confiable por defecto, aunque esté dentro del perímetro organizacional. Cada solicitud de acceso debe ser autenticada, autorizada y monitorizada en tiempo real, basándose en múltiples factores de verificación y en políticas dinámicas ajustadas al contexto. Este enfoque no solo reduce las oportunidades de movimiento lateral en caso de intrusión, sino que limita el alcance de los ataques internos o derivados de credenciales comprometidas, que representan una proporción creciente de los incidentes registrados globalmente.

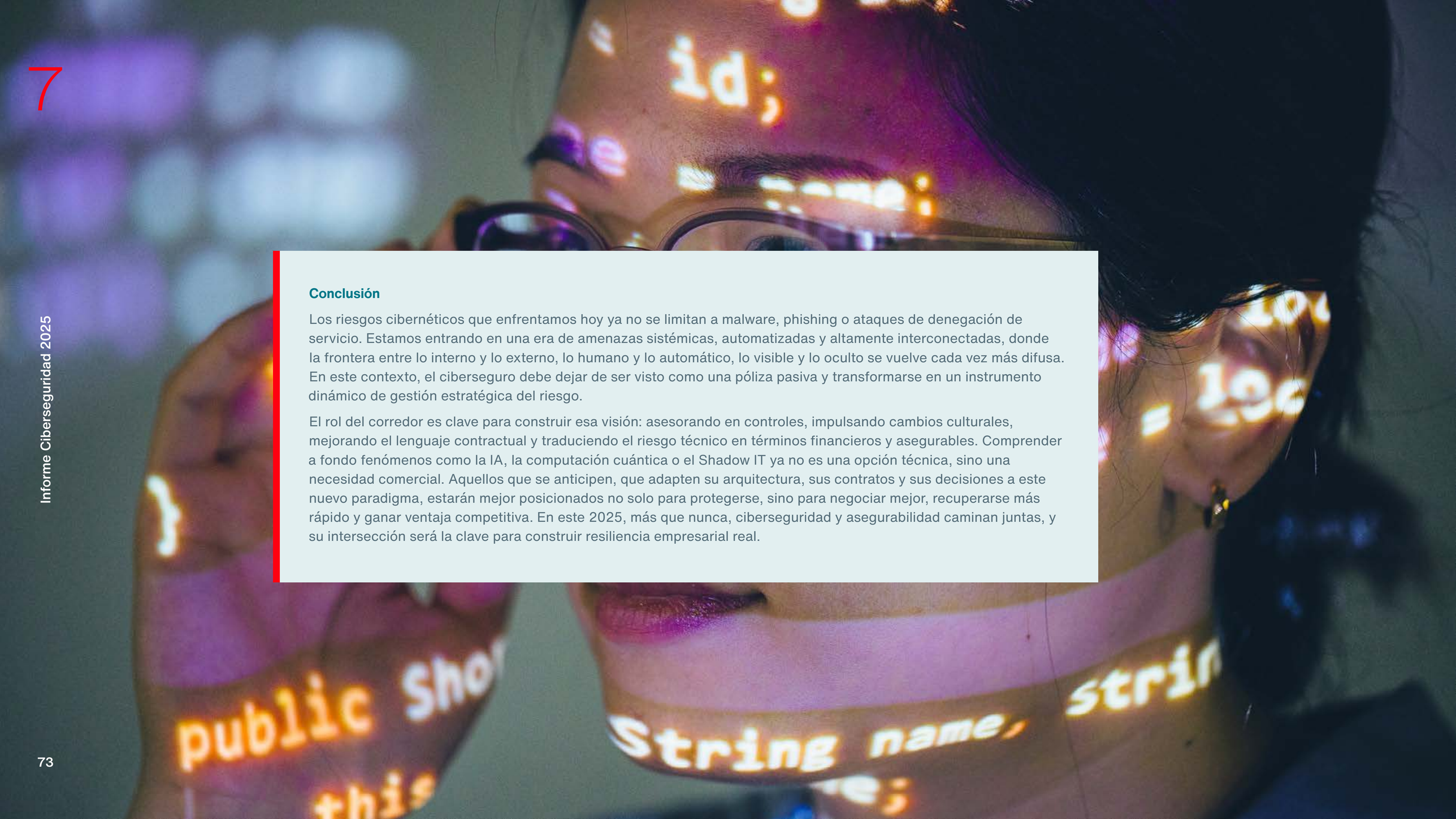
El verdadero valor de Zero Trust no radica únicamente en su filosofía, sino en su capacidad de traducirse en prácticas concretas: la implementación de autenticación multifactor obligatoria, la segmentación granular de redes, el uso de gestión de identidades privilegiadas (PAM), el control de dispositivos personales (BYOD), la validación continua de acceso basada en comportamiento y la integración con motores de inteligencia que evalúan el nivel de riesgo en cada interacción. Estas medidas permiten a las organizaciones tener un control más preciso y adaptativo sobre su infraestructura, incluso en entornos altamente distribuidos como los actuales.

Desde el punto de vista del ciberseguro, la adopción de un enfoque Zero Trust se ha convertido en uno de los principales factores de diferenciación en la evaluación del riesgo. A medida que el mercado asegurador se vuelve más técnico, las aseguradoras ya no se limitan a verificar si existe un firewall o un antivirus, sino que valoran la arquitectura general de seguridad. Empresas que implementan formalmente un modelo Zero Trust, documentan sus políticas, y demuestran madurez en su ejecución, están recibiendo condiciones de cobertura más favorables, reducciones de prima, franquicias más bajas e incluso acceso a coberturas extendidas para escenarios complejos como ransomware persistente o ataques desde entornos no gestionados.

En este sentido, herramientas como CyQu permiten al corredor visibilizar el grado de madurez del cliente en cada dominio crítico del modelo Zero Trust. No se trata de marcar casillas, sino de demostrar una postura de seguridad resiliente, basada en principios sólidos y sustentada en controles activos. La ausencia de un modelo claro puede ser interpretada por el asegurador como una señal de riesgo elevado, especialmente en sectores con alta exposición como salud, energía o servicios financieros.

Sin embargo, implementar Zero Trust no es una tarea menor. Requiere una transformación profunda de la arquitectura tecnológica, de la cultura organizacional y de la relación entre seguridad y operaciones. Muchos clientes aún perciben este modelo como costoso, restrictivo o innecesariamente complejo, lo cual representa una barrera para su adopción. Es ahí donde el rol del corredor se vuelve clave: no solo como asesor de seguros, sino como traductor entre el lenguaje técnico de los equipos IT y el lenguaje financiero del negocio. Identificar los beneficios aseguradores concretos de implementar ciertas capas de Zero Trust puede ser el incentivo definitivo para que la organización dé el paso.

En definitiva, Zero Trust ya no es una moda ni una utopía tecnológica. Es, en 2025, un estándar de facto que separa a las organizaciones resilientes de las vulnerables. La seguridad no puede basarse en la confianza implícita, y el aseguramiento del riesgo tampoco. Las empresas que abracen este modelo estarán mejor posicionadas para enfrentar el entorno de amenazas actual, negociar condiciones más competitivas con sus aseguradoras y reducir el impacto financiero de los incidentes que, inevitablemente, seguirán ocurriendo. Como corredores, debemos fomentar esta evolución no solo como una tendencia técnica, sino como una estrategia integral de mitigación del riesgo, alineada con los intereses del negocio, de los reguladores y del propio mercado asegurador.



Conclusión

Los riesgos cibernéticos que enfrentamos hoy ya no se limitan a malware, phishing o ataques de denegación de servicio. Estamos entrando en una era de amenazas sistémicas, automatizadas y altamente interconectadas, donde la frontera entre lo interno y lo externo, lo humano y lo automático, lo visible y lo oculto se vuelve cada vez más difusa. En este contexto, el ciberseguro debe dejar de ser visto como una póliza pasiva y transformarse en un instrumento dinámico de gestión estratégica del riesgo.

El rol del corredor es clave para construir esa visión: asesorando en controles, impulsando cambios culturales, mejorando el lenguaje contractual y traduciendo el riesgo técnico en términos financieros y asegurables. Comprender a fondo fenómenos como la IA, la computación cuántica o el Shadow IT ya no es una opción técnica, sino una necesidad comercial. Aquellos que se anticipen, que adapten su arquitectura, sus contratos y sus decisiones a este nuevo paradigma, estarán mejor posicionados no solo para protegerse, sino para negociar mejor, recuperarse más rápido y ganar ventaja competitiva. En este 2025, más que nunca, ciberseguridad y asegurabilidad caminan juntas, y su intersección será la clave para construir resiliencia empresarial real.

8

Estrategia integral de ciberresiliencia: conexión entre IT y el C-Level

Estrategia integral de ciberresiliencia: conexión entre IT y el C-Level

En los últimos años, el rol del CISO ha dejado de ser una figura técnica para convertirse en un actor estratégico de primer nivel. El CISO ya no solo vela por el cumplimiento de las políticas de seguridad de la información, sino que se ha convertido en un interlocutor clave para la alta dirección, con capacidad de influir en decisiones críticas del negocio.

Este cambio no ha sido casual. En un entorno regulado, hiperconectado y expuesto a amenazas constantes, las organizaciones han comprendido que la ciberseguridad no puede gestionarse como un aspecto técnico más. La ciberresiliencia exige una visión transversal, donde el CISO actúe como catalizador de una estrategia compartida entre Tecnología, Riesgos, Finanzas y Gobierno Corporativo.

Algunos directivos visionarios han dado un paso adelante, otorgando al CISO una posición elevada en el organigrama, incluso con acceso directo al CEO o al Presidente. Esta decisión no responde a una moda, sino a una necesidad: el CISO es hoy una figura clave en la optimización operativa, el cumplimiento normativo y la conquista de la dimensión digital. Es decir, se le reconoce como una pieza maestra en la continuidad del negocio.

Sin embargo, no todas las organizaciones han recorrido aun este camino. En muchas, el CISO sigue dependiendo del CIO, lo que puede limitar su autonomía y visibilidad estratégica. Aunque en ciertos casos esta dependencia está justificada —especialmente cuando el CIO lidera la innovación y entiende el riesgo digital—, lo ideal es que el CISO tenga una voz propia, complementaria pero no subordinada.

La confusión entre el CISO y el responsable de seguridad TIC (CTSO) es otro error común. Mientras que el CTSO debe garantizar que la infraestructura tecnológica soporte la política de seguridad, el CISO tiene una misión más amplia: gestionar el riesgo digital en todas sus dimensiones, desde la protección de datos personales hasta la prevención del ciberfraude, pasando por la gestión de incidentes, proveedores y cumplimiento legal.

En este contexto, la colaboración con el CRO es fundamental. Ambos comparten la responsabilidad de identificar, evaluar y mitigar riesgos que pueden comprometer la viabilidad del negocio. El CISO aporta la visión técnica y operativa; el CRO, el marco metodológico y la conexión con el apetito de riesgo corporativo. Juntos, deben construir una narrativa común que permita al Consejo entender el riesgo cibernético en términos financieros, reputacionales y estratégicos.

El CFO, por su parte, debe dejar de ver la ciberseguridad como un gasto y empezar a considerarla una inversión en resiliencia. Su rol es clave para asignar recursos, evaluar el retorno de las iniciativas de seguridad y garantizar que la organización esté preparada para absorber el impacto de un incidente sin comprometer su estabilidad financiera.

El Consejo Directivo, finalmente, debe asumir su responsabilidad en la gobernanza del riesgo digital. No basta con recibir informes periódicos; es necesario que los consejeros comprendan la naturaleza cambiante de las amenazas, exijan métricas claras y participen activamente en la definición de la estrategia de ciberresiliencia.

La futura transposición de la Directiva NIS2 y la posible creación de un esquema de certificación profesional para CISOs en Europa abren una oportunidad única para consolidar este nuevo modelo. Un modelo donde el CISO no es un técnico aislado, sino un líder transversal, con visión de negocio, capacidad de influencia y legitimidad para actuar y garantizar la seguridad digital de la organización.

Hacia una cultura organizacional de ciberresiliencia

La integración efectiva entre CISO, CRO, CFO y el Consejo no solo mejora la respuesta ante incidentes, sino que impulsa una cultura organizacional orientada a la resiliencia digital. Esta cultura se basa en tres pilares fundamentales:

01 Conciencia compartida del riesgo:

Todos los niveles de la organización, desde los equipos técnicos hasta la alta dirección, deben comprender que el riesgo cibernético no es un problema exclusivo del área de TI. Es un riesgo empresarial que puede afectar la continuidad operativa, la reputación y la confianza del mercado.

02 Gobernanza clara y colaborativa:

La definición de roles, responsabilidades y flujos de información entre CISO, CRO, CFO y el Consejo debe estar formalizada. Esto permite una toma de decisiones ágil y basada en datos, especialmente en momentos de crisis.

03 Inversión sostenida en capacidades:

La ciberresiliencia no se logra con soluciones puntuales, sino con una inversión continua en talento, tecnología, procesos y simulacros. El CFO juega un papel clave en garantizar que estas inversiones estén alineadas con los objetivos estratégicos y el apetito de riesgo de la organización.

Aunque el CISO lidera la estrategia de seguridad, el CEO es quien debe impulsar el cambio cultural. Su compromiso es esencial para priorizar la ciberresiliencia en la agenda corporativa y fomentar la colaboración entre áreas. Las organizaciones más avanzadas han creado comités ejecutivos de ciberseguridad, donde participan regularmente el CEO, el CISO, el CRO, el CFO y otros líderes clave.

Son innumerables los casos de éxito de mejora de la gestión del riesgo ciber gracias a la colaboración entre CISO y el C-Level. Según la Encuesta Global de Confianza Digital 2025 de PwC, las empresas que integran de forma habitual a toda la C-suite (incluyendo CISO, CFO, CRO y CEO) en la toma de decisiones sobre ciberseguridad tienen menos probabilidades de sufrir filtraciones de datos. Estas organizaciones han institucionalizado la ciberresiliencia como parte del gobierno corporativo, con métricas claras y participación activa del Consejo.

La póliza de cyber: un instrumento clave en la gestión del riesgo digital

En el marco de una estrategia integral de ciberresiliencia, la póliza de ciberseguridad se ha convertido en un componente esencial para transferir parte del riesgo residual que no puede ser mitigado en su totalidad mediante controles tecnológicos u organizativos. Lejos de ser una solución aislada, esta póliza debe entenderse como una herramienta complementaria dentro del ecosistema de gestión del riesgo digital.

En los últimos años, en Aon Cyber Solutions, como unidad líder global en la gestión del riesgo cyber, hemos podido comprobar que las organizaciones más avanzadas en adoptar este enfoque proactivo, donde el CISO, el CRO y el CFO colaboran estrechamente para definir el alcance de la cobertura, evaluar los escenarios de impacto y garantizar que la póliza esté alineada con los activos críticos del negocio, están obteniendo los mejores términos respecto a sus pólizas de seguro. Además esta colaboración tiene otros beneficios como:

- **Traducir el riesgo técnico en términos financieros**, facilitando la toma de decisiones por parte del Consejo.
- **Optimizar la inversión en ciberseguridad**, al identificar brechas que pueden ser cubiertas por el seguro o que requieren refuerzo interno.
- **Aumentar la madurez organizacional**, ya que muchas aseguradoras exigen controles mínimos, evaluaciones periódicas y planes de respuesta ante incidentes como condición para ofrecer cobertura.

Además, la póliza cyber puede cubrir aspectos clave como la interrupción del negocio, los costes de recuperación, la gestión reputacional, la respuesta legal y las sanciones regulatorias, entre otros. En este sentido, el CFO desempeña un papel fundamental al evaluar el retorno de esta inversión y garantizar que la organización esté financieramente preparada para absorber el impacto de un ciberincidente.

En conclusión, la ciberresiliencia ya no es una opción, sino una condición indispensable para la sostenibilidad empresarial. Construirla requiere mucho más que tecnología: exige liderazgo, visión compartida y una gobernanza sólida del riesgo. La colaboración entre el CISO, el CRO, el CFO, el CIO y el Consejo Directivo no solo fortalece la capacidad de respuesta ante amenazas, sino que transforma la seguridad en una ventaja competitiva. Las organizaciones que entiendan esta dinámica y actúen con decisión estarán mejor preparadas para afrontar el futuro con confianza, agilidad y resiliencia.

Marco colaborativo en el entorno empresarial

Visión técnica del riesgo

Visión del marco metodológico

Visión económica centrada en evaluar el retorno de iniciativas de seguridad

Responsabilidad de la gobernanza del riesgo digital

Pilares de la cultura de la ciberresiliencia:

- Conciencia compartida del riesgo
- Gobernanza clara y colaborativa
- Inversión sostenida en capacidades

9

Análisis comparativo de madurez cibernética: España vs. EMEA

Análisis comparativo de madurez cibernética: España vs. EMEA

1.1. Introducción

En la era digital actual, la madurez cibernética es un aspecto crítico de la resiliencia y seguridad organizacional. La plataforma de evaluación de riesgos cibernéticos CyQu, proporciona conocimientos sobre la madurez cibernética de diversas industrias en España y la región EMEA (Europa, Medio Oriente y África). CyQu puntúa del 1 al 4 los diferentes ámbitos cibernéticos de las organizaciones, basándose en los siguientes niveles:

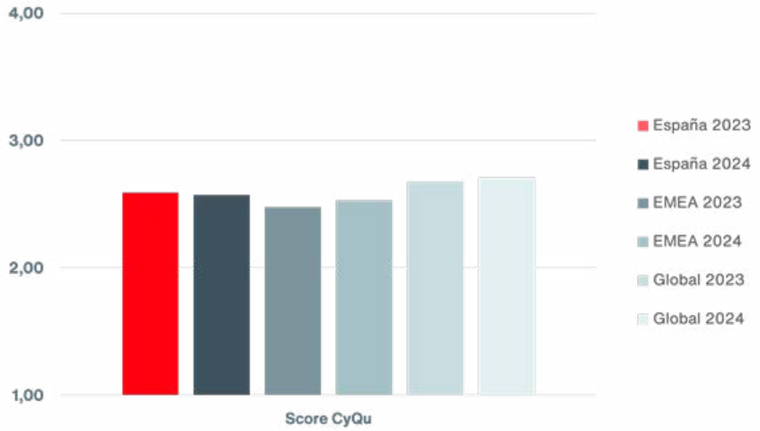
01. Inicial: las prácticas de ciberseguridad son mínimas o inexistentes.

02. Básico: se han implementado algunas medidas de seguridad básicas.

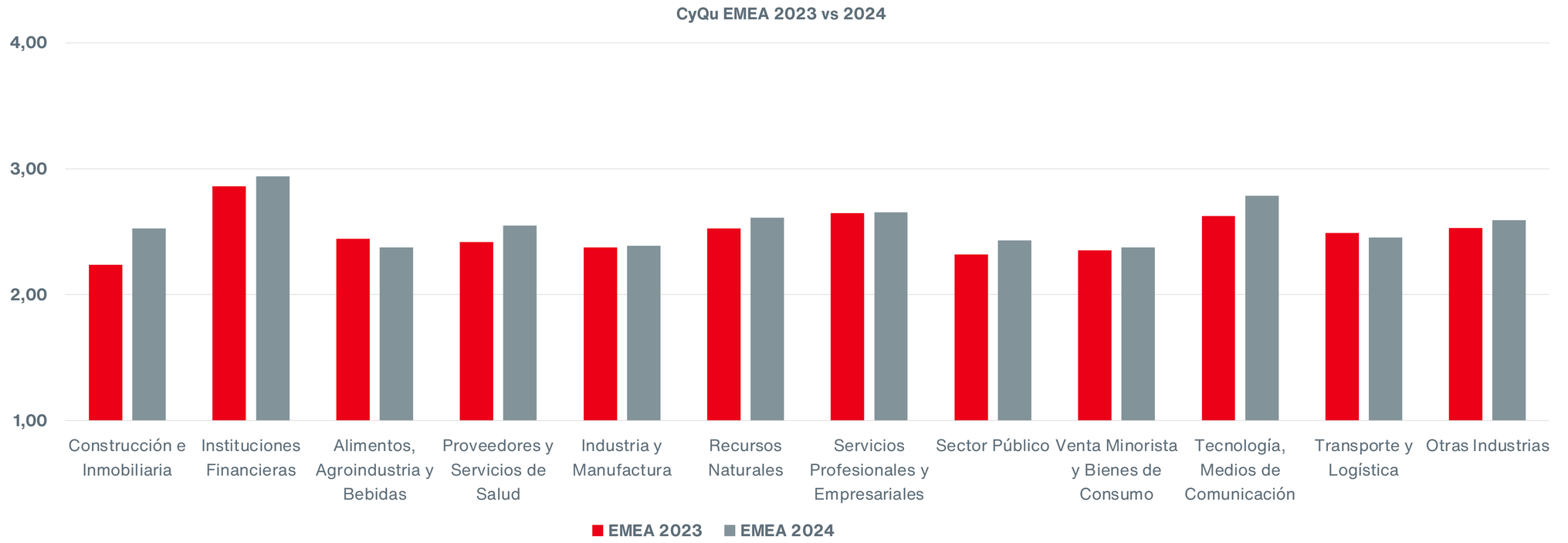
03. Gestionado: las prácticas de ciberseguridad están bien definidas y gestionadas de manera consistente.

04. Avanzado: las prácticas de ciberseguridad son sofisticadas y están integradas en toda la organización.

Conocer la puntuación permite a las organizaciones identificar su nivel actual de madurez cibernética y planificar futuras mejoras que ayuden al crecimiento de la organización. Los próximos gráficos detallados ofrecen una visión detallada de las puntuaciones de madurez cibernética de diferentes industrias de España y EMEA de 2023 y 2024, reflejando diferentes factores cruciales a la hora de valorar la seguridad de las organizaciones, incluyendo políticas de ciberseguridad, prácticas de gestión de riesgos y resiliencia cibernética general.



1.2. CyQu EMEA industrias, 2023 vs 2024



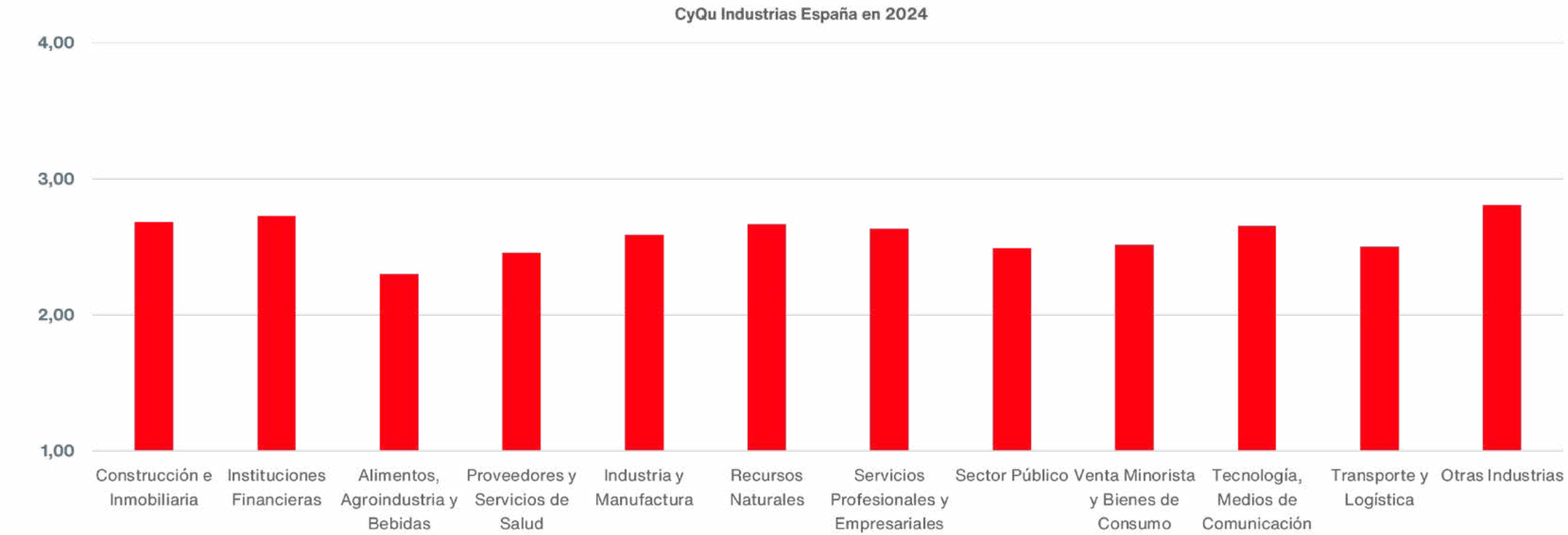
España partía en 2022 con una ventaja holgada: 2,54 frente a 2,41 en EMEA. En 2023 amplió la distancia (2,59 vs 2,48). Pero en 2024 la brecha se estrecha: España sube a 2,57 y EMEA a 2,53. Esto significa que, aunque España renueva su liderazgo por tercer año, EMEA está mejorando significativamente.

Velocidad de mejora: EMEA crece 0,05 puntos anuales; España apenas 0,02.

Proyección lineal: si nada cambia, EMEA alcanzaría la marca española en el primer semestre de 2026.

La convergencia no es homogénea. Países como Francia y Dinamarca tiran de la media al alza, mientras que algunos mercados emergentes frenan la subida. España, por su parte, se apoya en cuatro sectores avanzados que compensan los rezagados

Radiografía sectorial española (2024)



Sector	2022	2023	2024	Tendencia	Catalizadores clave
Instituciones Financieras	2,61	2,70	2,73	▲ Constante	DORA, fraude BEC, auditorías regulatorias
Recursos Naturales	2,48	2,58	2,67	▲ Acelerada	ENS ampliado, OT-IT convergence
Tecnología & Medios	2,55	2,61	2,65	▲	Multicloud, dev-sec-ops
Construcción & Inmobiliaria	2,31	2,47	2,68	▲▲	BIM, cláusulas de ciber en licitaciones
Servicios Profesionales	2,57	2,61	2,63	▲	Subcontratación TI, seguros ciber obligatorios
Manufactura	2,41	2,54	2,59	▲	Ransomware OT, incentivos «Industria 4.0»
Retail & Consumo	2,34	2,37	2,52	▲	E-commerce, PCI-DSS 4.0
Transporte & Logística	2,46	2,56	2,50	▼	Final de ayudas COVID, foco en electrificación
Sector Público	2,37	2,45	2,49	▲	Refuerzo CCN-CERT, ENS alta categoría
Agro-Alimentario	2,19	2,24	2,30	▲ lenta	Fragmentación, baja presión regulatoria

Los datos confirman que el impacto de la regulación es inmediato: DORA en banca y NIS2 en infraestructuras críticas explican buena parte del avance en los dos sectores líderes. Al otro extremo, Agro Alimentario mejora sólo 0,06 puntos en dos años: la falta de presión legal y el peso de micro pymes complican la captación de talento y la inversión en ciberseguridad.

Zoom regional: las comunidades autónomas

Como novedad este año, hemos incluido datos medios por comunidades. Cataluña y Madrid dominan con 2,66 y 2,64, impulsadas por Servicios Financieros, TIC y servicios profesionales. Andalucía y Valencia rondan la media nacional gracias al empuje de industria ligera y logística. Galicia y Castilla La Mancha cierran la tabla con 2,41 y 2,38 respectivamente, penalizadas por la concentración en agro alimentario y manufactura tradicional.

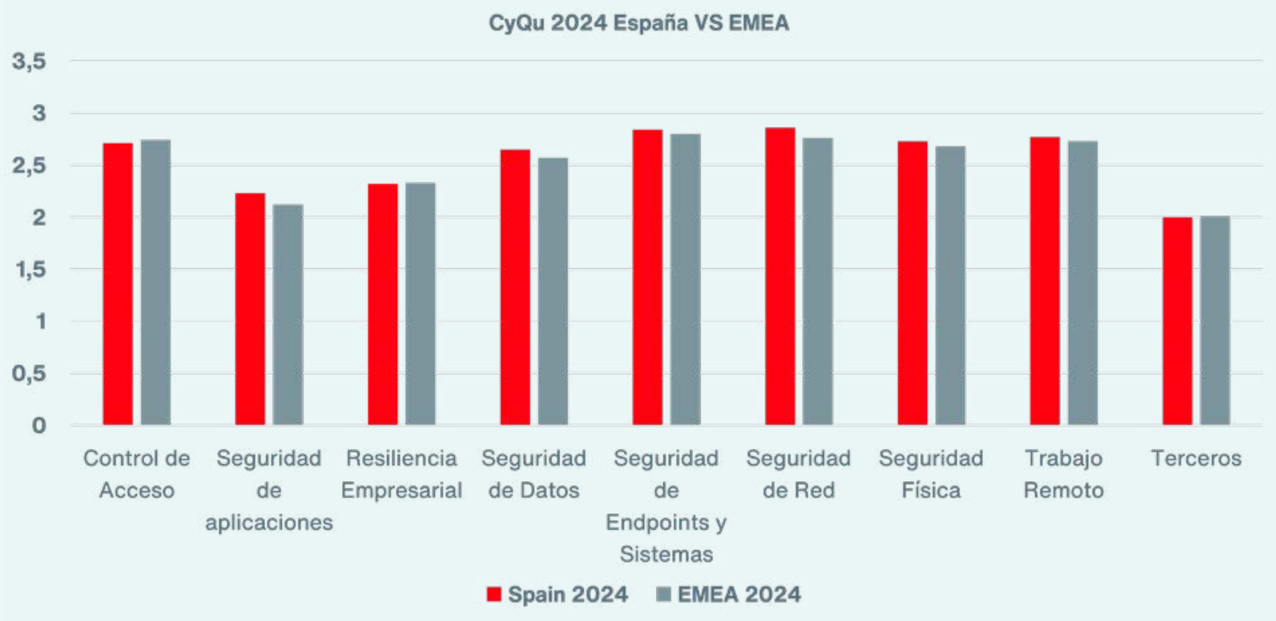
España supera a EMEA en siete de los nueve controles. Las mayores distancias se dan en **seguridad de red (0,10 puntos arriba) y protección de endpoints (0,04).** En cambio, la paridad total en **gestión de terceros** y la ventaja mínima en **resiliencia empresarial** sugieren un techo de cristal. Datos internos de Aon muestran que sólo el 45 % de las empresas españolas exige MFA a sus proveedores críticos y apenas el 32 % ejecuta simulacros de continuidad al menos una vez al año.

Coste de oportunidad: mover estos dos dominios de un 2,0 a un 2,3 equivale a reducir en un 18 % el volumen esperado de pérdidas por incidente grave, según el modelo PRISM de Aon; un retorno superior al de seguir incrementando capas de protección en red.

Casuística 2024: incidentes que marcan tendencia

- **Fabricante de automoción (norte de España):** ataque de ransomware vía proveedor de climatización conectado a la red OT; impacto de 9,2 M € y 11 días de parada.
- **Hospital privado (zona Levante):** doble extorsión ransomware; 380 GB de datos filtrados. Tras el incidente, el CISO obtuvo autorización para duplicar el presupuesto EDR.
- **Operador logístico (Madrid):** fraude BEC con deepfake de voz; los atacantes suplantan al CFO y desvían 2,4 M €. El incidente acelera la adopción de MFA y la segregación de funciones en pagos.

Comparación Europea



El análisis no puede obviar a dos vecinos relevantes:

- **Francia:** media 2,61 y un descenso del 18 % en ataques de ransomware tras la iniciativa de ejercicios obligatorios. El regulador (ANSSI) ya impone certificaciones periódicas a proveedores cloud.
- **Italia:** media 2,48 pero crecimiento de 0,09 puntos en 2024; la Agencia Nacional de Ciberseguridad exige planes de mejora trianuales y subvenciona hasta el 30 % de proyectos OT security.

Acción: si España no acelera en terceros y resiliencia, Italia podría superar su nota promedio en 2026.

Palancas de acción para 2025

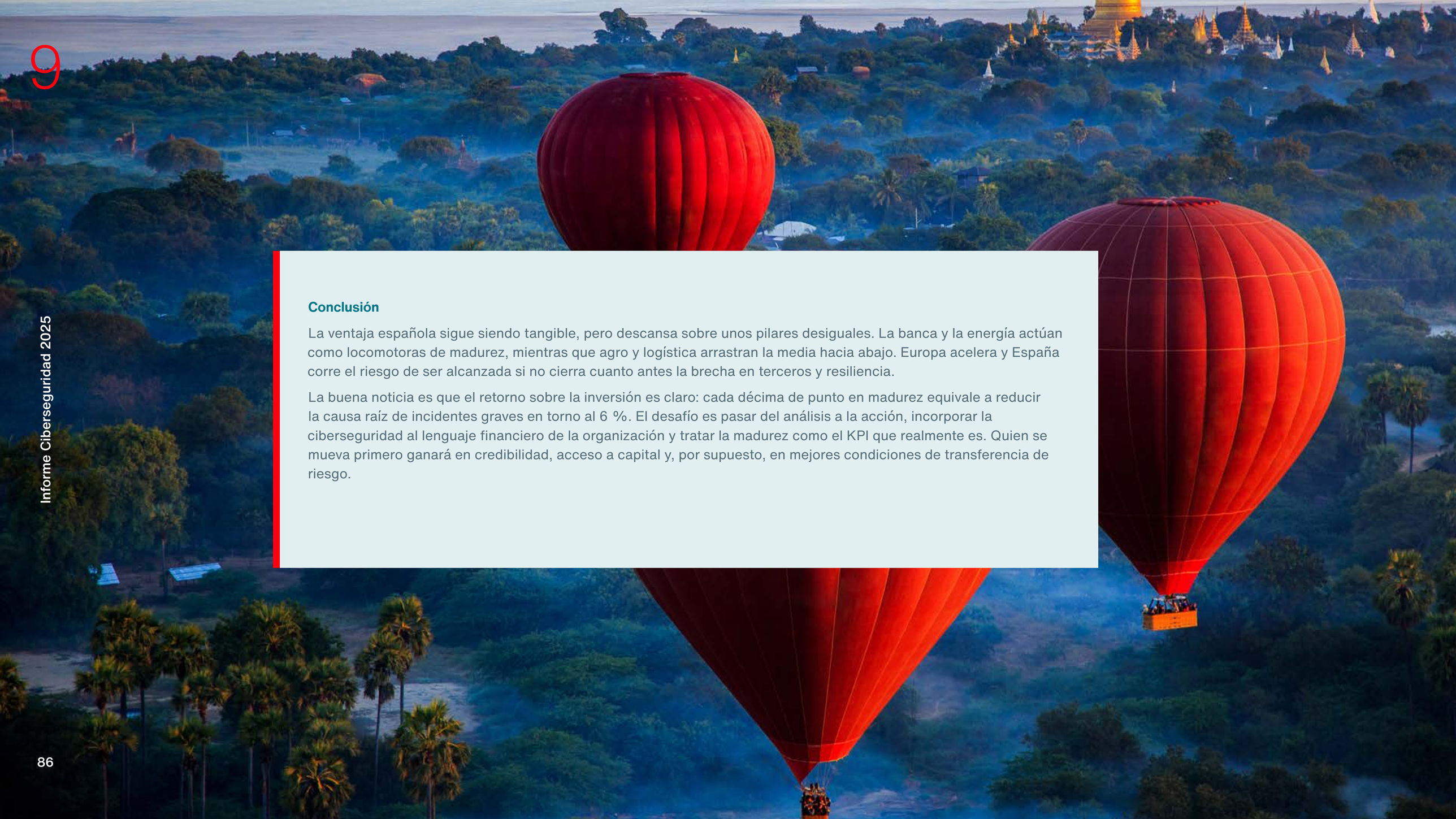
01. Inventario dinámico de proveedores: mantener un listado vivo de terceros críticos, con clasificación por impacto y evidencia documental.

02. Simulacros de crisis: dos por año, uno técnico (ransomware) y otro de continuidad (caída proveedor cloud).

03. Cláusulas contractuales NIS2/DORA: incorporar requisitos de ciber SLAs y derecho de auditoría a contratos renovados a partir de Q3 2024.

04. Modelización financiera: usar PRISM o similar para justificar límites de póliza; correlacionar sublímites de BI y sanciones regulatorias.

05. Comités de cadena de suministro: crear foros sectoriales para compartir inteligencia de amenazas y ratings de proveedores.



Conclusión

La ventaja española sigue siendo tangible, pero descansa sobre unos pilares desiguales. La banca y la energía actúan como locomotoras de madurez, mientras que agro y logística arrastran la media hacia abajo. Europa acelera y España corre el riesgo de ser alcanzada si no cierra cuanto antes la brecha en terceros y resiliencia.

La buena noticia es que el retorno sobre la inversión es claro: cada décima de punto en madurez equivale a reducir la causa raíz de incidentes graves en torno al 6 %. El desafío es pasar del análisis a la acción, incorporar la ciberseguridad al lenguaje financiero de la organización y tratar la madurez como el KPI que realmente es. Quien se mueva primero ganará en credibilidad, acceso a capital y, por supuesto, en mejores condiciones de transferencia de riesgo.

10

Metodología

10 Metodología

Este Estudio ha sido elaborado con información propia y datos del mercado asegurador obtenidos mediante cuestionarios confidenciales, así como mediante entrevistas directas con las aseguradoras que han participado, y con proyección de algunos de los resultados.

El objetivo es seguir publicando anualmente el Estudio, cuya primera edición tuvo lugar hace cinco años, lo que nos permitirá comparar la evolución de esta modalidad aseguradora en términos de tendencia de contratación y evolución de siniestralidad.

Todos los datos de primas, pólizas y siniestralidad están cerrados a 31 de diciembre de 2024.

Los datos y gráficos procedentes de terceros se han citado debidamente.

Tras la investigación y el análisis realizado, los datos respecto a primas y pólizas representan, aproximadamente, el 80% de la cuota de mercado, lo que constituye una radiografía prácticamente completa del mercado asegurador en España en cuanto a Ciber.

En relación con el volumen de primas, la cifra resultante comprende las cantidades que corresponden a las principales aseguradoras del mercado, utilizando los siguientes criterios:

- Se han incluido tanto primas de cartera como de nuevo negocio suscrito en 2024, con independencia del tamaño y sector de actividad, distinguiendo como novedad en este año, volumen de mercado medio y grandes cuentas.
- Las primas reflejan tanto los costes que corresponden a negocio suscrito al 100% por cada asegurador que ha participado, como el suscrito en coaseguro o en tramos de exceso.
- La cifra de primas permite conocer el volumen que corresponde a riesgos españoles de Ciber, con independencia de su tamaño, sector de actividad, ubicación geográfica o nacionalidad del asegurador.

Por tanto, este Estudio ofrece una radiografía nítida y precisa, a 31 de diciembre 2024, del seguro Ciber en España.

Para la elaboración de este informe, se ha utilizado tecnología de inteligencia artificial como herramienta de apoyo en el análisis de datos, redacción de contenidos y generación de visualizaciones. Todas las conclusiones han sido revisadas y validadas por el equipo responsable, garantizando la coherencia y la calidad del contenido final.

About Aon

Aon plc Aon plc (NYSE: AON) existe para dar forma a las mejores decisiones, para proteger y enriquecer la vida de las personas en todo el mundo. Nuestros profesionales ofrecen a nuestros clientes en más de 120 países y soberanías asesoría y soluciones que les aportan la claridad y la confianza para tomar las mejores decisiones con el fin de proteger y hacer crecer su negocio.

La información contenida en este documento ha sido recopilada y elaborada de buena fe y de fuentes que se consideran fiables. La responsabilidad del Grupo de Empresas Aon Iberia Correduría de Seguros y Reaseguros S.A.U. (“Aon”), en el sentido contemplado en el artículo 42 del Código de Comercio, alcanza la legalmente exigible derivada de su actuación profesional, pero no se extiende a obligaciones o compromisos ajenos al objeto, competencia o ámbito de su organización empresarial. El presente documento no supone ni asesoramiento legal ni opinión jurídica.

Aon Iberia Correduría de Seguros y Reaseguros S.A.U. (“Aon”). C/ Velázquez 86D, C.P. 28006, Madrid. Inscrita en el R° Mercantil de Madrid, Hoja M-19857, Tomo 15321, Folio 133, N.I.F. A-28109247

aon.com

© Grupo de Empresas Aon Iberia Correduría de Seguros S.A.U. (“Aon”). Quedan reservados todos los derechos. Se prohíbe la explotación, reproducción, distribución, comunicación pública y transformación, total o parcial, de este documento sin autorización expresa del Grupo de Empresas Aon Iberia, Correduría de Seguros S.A.U.

La información contenida en este documento tiene por objeto ayudar a los lectores y sólo sirve de orientación general.

Este documento no pretende abordar los aspectos específicos de su situación ni proporcionar asesoramiento, incluido, entre otros, asesoramiento médico, jurídico, normativo, financiero o sobre riesgos específicos. Usted debe revisar la información en el contexto de sus propias circunstancias y desarrollar una respuesta apropiada.

Aunque se ha tenido cuidado en la elaboración de este documento, Aon no garantiza, representa ni asegura la exactitud, adecuación, integridad o idoneidad para cualquier propósito del documento o de cualquier parte del mismo y no puede aceptar ninguna responsabilidad por cualquier pérdida incurrida de cualquier manera por cualquier persona que pueda confiar en él. Todo destinatario será responsable del uso que haga de este documento. El presente documento ha sido elaborado con la información de que disponíamos hasta la fecha de su publicación y está sujeto a las salvedades que hayan podido surgir con la información no analizada.

Contact Us

Verónica Jiménez Romero
Director Cyber Solutions
+34 648 450 317
veronica.jimenez@aon.es

Jean-Baptiste Aireau
Manager Cyber Consulting
+34 663 970 179
jean-baptiste.aireau@aon.co.uk

Patricia Sáez Borreguero
Cyber Broker Specialist
+34 636 230 890
patricia.saez.borreguero15@aon.es