AON

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

Junio 2024

Entidades Colaboradoras

ANDERSEN

AIG

Allianz

TOKIO MARINE HCC

beazley

CHUBB

AXA

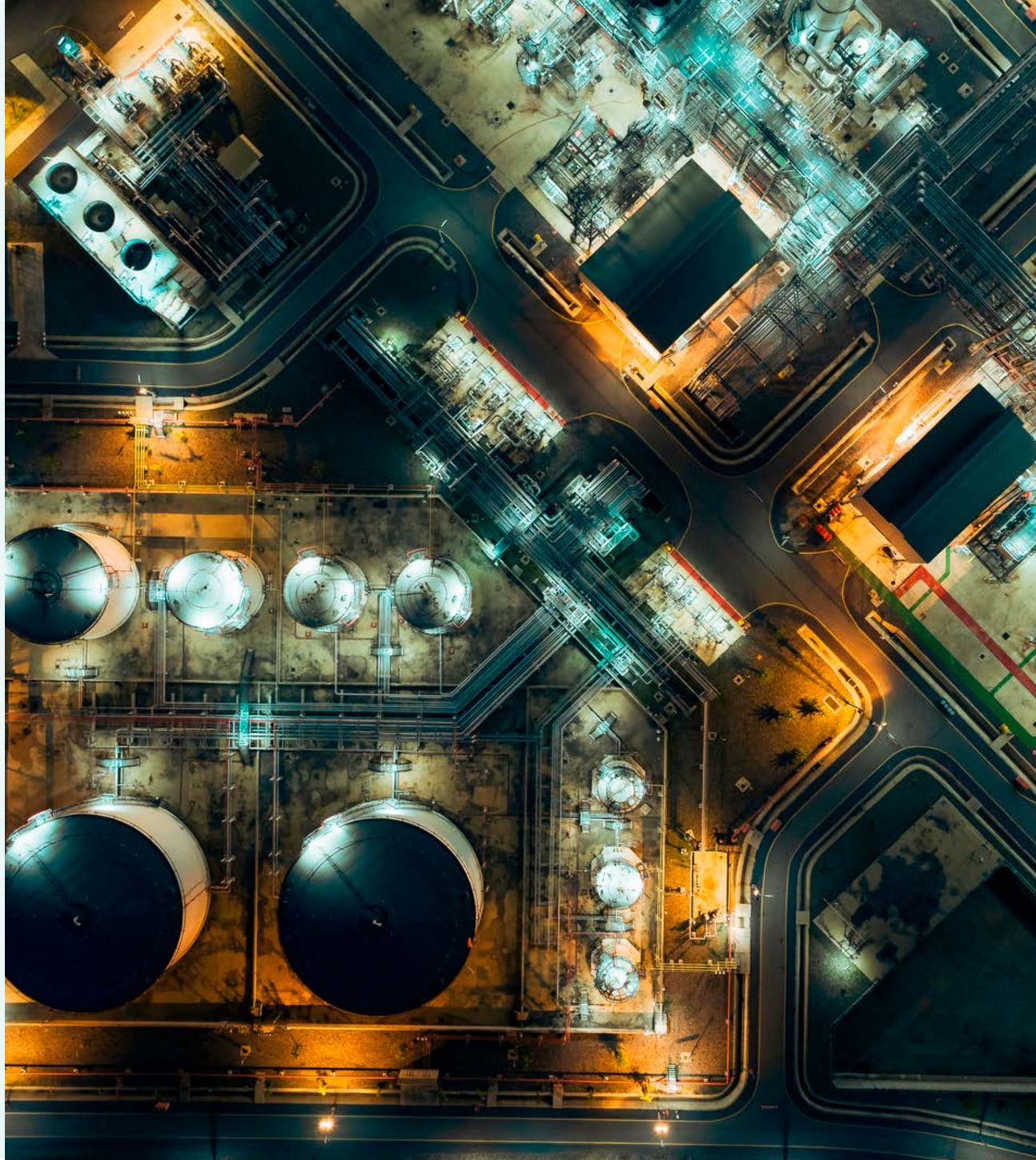
QBE

GARRIGUES

ZURICH

HISCOX

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL



Índice

1

Resumen Ejecutivo

1 Introducción y principales conclusiones del informe

Como venimos haciendo en las ediciones anteriores en esta quinta edición del informe de Ciberseguridad analizaremos la evolución y la gestión del riesgo en España desde diferentes prismas: cambios normativos, inversión en ciberseguridad, la evolución de la siniestralidad, que no cesa, y el futuro inmediato que se pronostica.

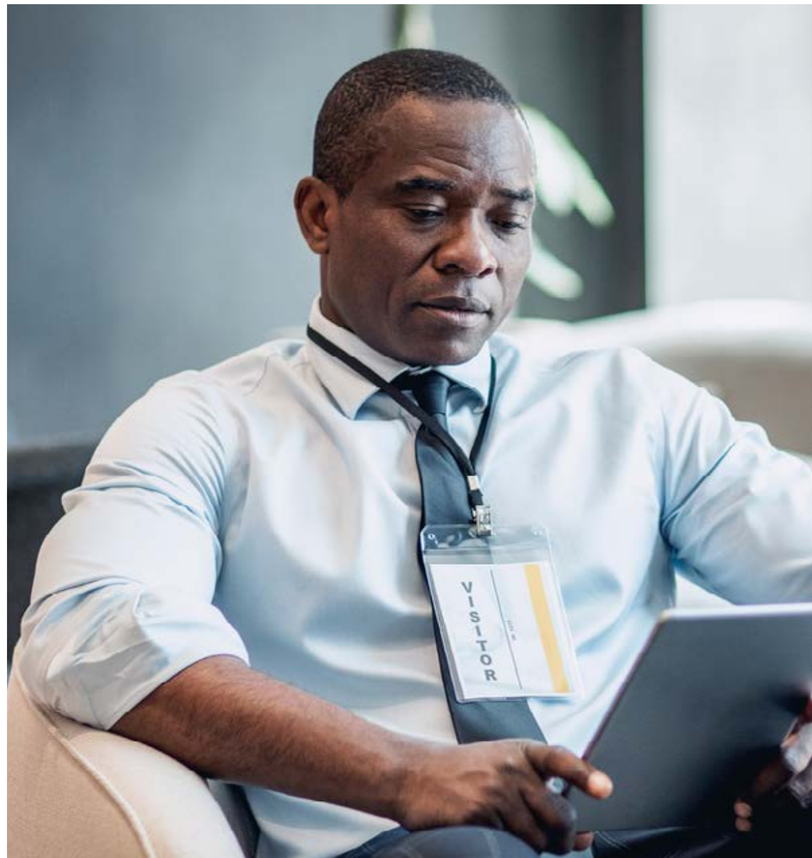
Después del panorama descrito en las ediciones anteriores, y el pronóstico que ya anunciamos en la última edición, somos conscientes que estamos ya ante un mercado que madura muy rápidamente a pesar de la incertidumbre, donde la siniestralidad persiste y se sofistica, la conciencia del riesgo está ya arraigada, la inversión en su preservación es continua y la adecuada transferencia de éste se considera ya esencial para garantizar la continuidad de las empresas.

Veremos, que tras la severidad vivida en el 2021 - 2022, cuando muchos vaticinaban que la transferencia del riesgo ciber al mercado asegurador mediante la póliza de seguro, desaparecería, ha llegado la estabilización del 2023 y la entrada de nuevos mercados que han aterrizado en España con muchas fuerza, apostando por el riesgo Ciber, queriendo crecer en cuota de mercado y en garantías de coberturas, lo que ha provocado que este 2024 las capacidades hayan aumentado y la ley de la oferta y la demanda esté provocando una reducción de las primas de seguro.

El volumen de primas del mercado asegurador sigue aumentando y en España desde el año pasado ya supera los **170 M EUR,** habiendo crecido este año un 25% con respecto a la anualidad anterior. El reto al que nos enfrentamos en este 2024 es mantener este equilibrio, y que las nuevas aseguradoras que han llegado lo hayan hecho para quedarse, porque está claro que la siniestralidad no cesa y en el momento que estos nuevos mercados empiecen a asumir siniestros, veremos si apuestan por la continuidad.

+170M€

En volumen de primas del mercado asegurador



1

Algunos de los puntos sobre los que vamos a incidir a lo largo del informe y que nos han permitido concluir, son los siguientes:

Entorno normativo: Éste sigue tornándose complejo. Haremos un repaso de las últimas novedades regulatorias, y normativas, relacionadas con la ciberseguridad, la tecnología y la privacidad, y futuras regulaciones.

- El 2023 ha estado marcado por el despliegue de la **Directiva NIS 2,** destinada a garantizar un elevado nivel común de ciberseguridad en toda la Unión. Cobran especial relevancia aquellos sectores que hasta ahora no estaban sujetos a obligaciones específicas en materia de ciberseguridad como el sector farmacéutico, agroalimentario o salud entre otros.
- **Reglamento DORA,** sobre la resiliencia operativa digital del sector financiero que será aplicable a partir de Enero 2025
- Durante el 2023 se ha avanzado en los procesos de aprobación de varias normas que van a tener un alto impacto en el marco regulador de la ciberseguridad en el ámbito de la UE, como la **Cyber Resilience Act,** (reforzar la seguridad de los dispositivos digitales mediante una series de obligaciones en toda la cadena de suministro: fabricante, importadores y distribuidores. Y **la Cyber Solidarity Act,** (coordinación de esfuerzos nacionales entre instituciones públicas y privadas).
- No obstante, la gran novedad que se gestó en 2023 y que va a ver la luz en breve con la publicación oficial es el relevante **Reglamento de la Inteligencia Artificial.** Tras años de espera, podemos afirmar que la gran apuesta de la UE es regular esta tecnología destinada a cambiar muchos aspectos y a pesar de las múltiples modificaciones que han sufrido los textos, conservan una de las premisas fundamentales: la ciberseguridad de los sistemas de la IA es crucial frente a los riesgos implicados en el uso de estos sistemas, especialmente si los responsables del despliegue están implantando sistemas de IA calificados como de alto riesgo.
- Destacamos también la reciente aprobación del **Reglamento eIDAS 2** diseñado para actualizar y mejorar la forma en que se gestiona la identificación electrónica dentro de la UE, permitirá a los ciudadanos identificarse de forma electrónica.
- Otra regulación con mucho impacto fue las normas aprobadas el **26 de Julio de 2023 por la US Securities and Exchange Commision (Sec)**, que regirán las divulgaciones y la gobernanza de la ciberseguridad de las empresas cotizadas. Destaca la obligación de informar sobre los incidentes de ciberseguridad materialmente significativos en el deber de comunicar de manera anual información sobre la gestión de riesgos corporativos, estrategia y gobernanza de la ciberseguridad.

Mercado Asegurador: Tras los últimos 3 años de aumentos generalizados de primas con una imprudencia previa de la preservación del riesgo y falta de inversión, donde la siniestralidad no ha dejado de crecer, hemos evolucionado a un mercado más maduro, y en el que, aunque falta mucho camino por recorrer, se tiene una mayor conciencia del riesgo, se invierte más en medidas de mitigación y por tanto las empresas se han tornado más resilientes.

No obstante, la siniestralidad no cesa, cada vez más compleja y con alta sofisticación, donde la responsabilidad civil derivada de los ciberataques está empezando a tomar un protagonismo importante, junto con el ransomware que continúa siendo la forma de ataque más rentable para los ciberdelincuentes.

Aun así, el 2023 y el inicio de este 2024 vienen marcados por nuevos mercados que apuestan por asumir el riesgo ciber, quieren crecer en cuota de mercado y marcado por la oferta y la demanda están presionando los precios de las primas a la baja. Actualmente, la capacidad que se puede obtener en el mercado es mucho mayor para riesgos bien protegidos. Las empresas han empezado a cuantificar sus riesgos, se han dado cuenta que deben trasferir mayor riesgo al mercado que impulsado por la reducción de los costes hace que se esté comprando mayor capacidad. Sin duda nos encontramos en un año de oportunidad para la revisión del riesgo y su transferencia al mercado asegurador.

Por sector de actividad, el de infraestructuras críticas continúa siendo líder en términos de concienciación sobre ciberseguridad y en la generación de contrataciones anuales. En segundo lugar, se ha observado un notable aumento en el sector de servicios profesionales, debido a los servicios de consultoría IT. Sin embargo, el sector industrial ha experimentado una disminución gradual en los últimos años.

1

A lo largo de este 2024, estamos observado una evolución en la gestión de riesgos de las empresas marcadas por los siguientes aspectos:

01 Importancia de la gestión integral del riesgo

La concienciación en la inversión está ya en ADN de las empresas, sin embargo, hay un cambio en la manera de invertir y en la toma de decisiones. Más ordenada, mayor coordinación con todas las áreas: CFO, Gerencia de riesgos y aprobación/supervisión por el Board.

02 Más información, mejores decisiones

Las empresas están analizando sus riesgos y cuantificando los impactos económicos que un incidente les puede suponer. Informes soportados por Data, les lleva a tomar mejores decisiones. El papel del bróker es una pieza importante que puede aportar información de la industria para una óptima transferencia del riesgo.

03 Nuevo capital – mayor competencia

Aunque la capacidad sigue siendo limitada, la entrada de nuevo capital con agresivos presupuestos de crecimiento y con inversión en los equipos de suscripción ha llevado a una mayor competencia provocando una desaceleración de las tasas. Ello está haciendo que las organizaciones estén transfiriendo mayor riesgo a las aseguradoras, mediante el incremento de límites contratados.

En contrapartida, **las aseguradoras mantienen el rigor en la suscripción de sus riesgos,** y siguen apostando por los riesgos mejor protegidos. Además, aquellas empresas con una continua inversión en la seguridad de sus sistemas de información y redes, son las que mejores términos y condiciones pueden conseguir.

No obstante, el informe de este año viene marcado sin duda por **la Inteligencia Artificial, y su debate entre la oportunidad y la amenaza.**

Por un lado, no cabe duda de que el uso de la IA es un aspecto clave para las empresas para ganar en eficiencia y el sector asegurador no es menos y, por tanto, desde este prisma es una oportunidad. Sin embargo, entraña unos riesgos que hay que identificar y analizar para poder contener.

Si lo vemos desde el punto de vista de control del riesgo y la mitigación, y en especial desde el punto de vista de la ciberseguridad, dónde los métodos de ingeniería social son cada vez más complejos, debido justamente a esta IA, entonces, está claro que se puede convertir en una amenaza para la gestión de los riesgos futuros, que se pueden hacer incontrolables a efectos de mitigación y prevención de estos propios riesgos.

Si tomamos como referencia otros ramos de seguro, no estamos acostumbrados a cambios tan drásticos y rápidos de tendencia, pero el mercado de seguros ciber evoluciona tan rápido y es tan cambiante como los riesgos y la normativa a los que protege, así que, debemos aprovechar la oportunidad que nos ofrece este 2024.

2

Novedades legislativas en materia de ciberseguridad

Vicente Moret Millás

Secretario del Patronato de la Fundación ESYS

Cristina Durante del Barrio

Vicesecretaria del Patronato de la Fundación ESYS

2

Novedades legislativas en materia de ciberseguridad

Podemos afirmar que, en el ámbito de la UE, 2023 ha estado marcado por el despliegue de la Directiva NIS 2 (Directiva (UE) 2022/2555, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión), y el Reglamento DORA (Reglamento (UE) 2022/2554, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero). Estas normas fueron publicadas a finales de 2022. Así mismo, durante el año 2023 se ha avanzado en los procesos de aprobación de varias normas que van a tener un alto impacto en el marco regulador de la ciberseguridad en el ámbito de la UE, tales como la Cyber Resilience Act, la Cyber Solidarity Act, la AI Act, y el Reglamento eIDAS 2.

Directiva NIS 2

Respecto a la Directiva NIS 2, las entidades ya han empezado a estudiar y en algunos casos a alinear sus modelos de gobernanza y políticas internas para cumplir con los requisitos establecidos en la **Directiva NIS 2**. Ello es especialmente relevante para aquellas entidades pertenecientes a sectores que hasta ahora no estaban sujetas a obligaciones específicas en materia de ciberseguridad (sector farmacéutico, agroalimentario o salud, entre otros). Sin embargo, salvo excepciones, estos procesos se han iniciado de forma aún paulatina y gradual, a la espera de la transposición en España de la Directiva, la cual, se estima, podría retrasarse hasta el primer o segundo trimestre del año 2025. Así mismo, aún están pendientes de aprobación los distintos actos delegados y de ejecución de la Comisión Europea, y normas técnicas por ENISA que complementarán la plena implementación de la Directiva NIS 2.

Reglamento DORA

Por su parte, el **Reglamento DORA,** entrará en vigor el próximo mes de enero de 2025 y está aún pendiente de ser completado por más de 30 normas técnicas y actos de ejecución (por sus siglas en inglés, “RTS”) que especificarán cómo abordar e implementar ciertas obligaciones fijadas por la norma. Aunque a fecha del presente informe ya conocemos el contenido de varios de estos RTS, su aprobación podría extenderse hasta el tercer o último trimestre de 2024 lo que no deja mucho margen de maniobra temporal a las entidades financieras comprendidas en su ámbito de aplicación. A este respecto y en relación con el ámbito de aplicación de DORA, cabe mencionar la urgente ampliación por parte del legislador español de la aplicabilidad de DORA a los operadores de sistemas y esquemas de pago mediante el Real Decreto-ley 8/2023, dirigido a la adopción de medidas para afrontar las consecuencias económicas y sociales derivadas de los conflictos en Ucrania y Oriente Próximo.

No obstante, la gran novedad que se gestó durante 2023, y que va a ver la luz en breve con la publicación oficial es el relevante **Reglamento de Inteligencia Artificial (AI Act).** Tras años de espera, podemos afirmar que es la gran apuesta de la UE por regular esta tecnología destinada a cambiar muchas cosas. A pesar de las múltiples modificaciones que ha sufrido el texto, conserva una de sus premisas fundamentales: la ciberseguridad de los sistemas de IA es crucial frente a los riesgos implicados en el uso de estos sistemas. Ello supone la necesidad de conectar el control de riesgos sobre el despliegue de estos sistemas con el cumplimiento de los marcos generales de ciberseguridad establecidos por NIS 2 y DORA, especialmente si los responsables del despliegue están implantando sistemas de **IA calificados como de alto riesgo.**

El Reglamento de IA previsiblemente será complementado por la **Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual.** Esta Directiva tendrá como objetivo determinar cómo se articulan los mecanismos de defensa judicial de los usuarios frente al mal funcionamiento de la IA, los cuales deben permitir la exigencia de responsabilidad por daños y al mismo tiempo protejan el desarrollo de la IA frente a demandas infundadas.

Para completar el panorama regulatorio tan complejo que se está configurando en la UE, es necesario hacer referencia a dos normas que verán la luz en breve: la **Cyber Resilience Act** y la **Cyber Solidarity Act** por la relevancia que tendrán para generar evidencias del cumplimiento de las obligaciones de ciberseguridad:

Cyber Resilence Act (CRA):

La **Cyber Resilience Act** (Reglamento relativo a los requisitos de ciberseguridad para los productos con elementos digitales), constituye un esfuerzo considerable destinado a aumentar la seguridad de los dispositivos conectados y proteger a los consumidores y empresas europeos. El texto se encuentra a la espera de su adopción formal por parte del Consejo de la Unión Europea en los próximos meses. A través de esta innovadora propuesta, la Comisión pretende **reforzar la ciberseguridad de los dispositivos digitales** mediante la introducción de una serie de obligaciones en toda la cadena de suministro: fabricantes, importadores y distribuidores. En lo que respecta a los dispositivos, se aplicará a los productos con elementos digitales cuyo uso incluye una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red: en definitiva, a cualquier producto de software o hardware y sus soluciones de procesamiento de datos a distancia.

Entre otras medidas, la **responsabilidad del fabricante** sobre la seguridad del producto se extenderá por lo menos, por un período no inferior a 5 años. Adicionalmente, se establece la obligatoriedad de obtener una declaración de conformidad y de exhibir la Etiqueta CE para los productos previa a la comercialización. A través de esta etiqueta, el fabricante indicará que el producto es conforme con los requisitos esenciales establecidos en la CRA. En caso de vulneración de las obligaciones contenidas en la CRA, se prevé un régimen sancionador con multas máximas para las entidades infractoras de 15 millones de euros, o del 2,5% de su volumen de negocios anual total a nivel mundial durante el ejercicio financiero anterior, lo que sea mayor.

Cyber Solidarity Act (CSA):

Por otra parte, la propuesta de **Cyber Solidarity Act (CSA),** supone un paso muy relevante hacia la **coordinación de esfuerzos nacionales en materia de ciberseguridad.** Supone la creación de estructuras de cooperación estables y abarca no solo la colaboración entre los distintos Estados Miembros, sino también entre **instituciones públicas y privadas,** especialmente aquellas que, por su dimensión, desempeñan un papel importante en el mantenimiento de un nivel adecuado de ciberseguridad.

Esta norma pretende desarrollar las **capacidades de detección, respuesta y resiliencia** frente a ciberamenazas e incidentes significativos a nivel de la Unión Europea. Para ello, la propuesta propone el desarrollo de una **infraestructura europea de equipos de detección y respuesta** ante ciberincidentes (SOCs) nacionales e internacionales, además de la creación de un **mecanismo de emergencia común** que facilite apoyo a los Estados Miembros. Esta estructura se denominará European Cyber Shield.

Para valorar la preparación frente a las ciberamenazas, el Capítulo III de la CSA prevé llevar a cabo **Test de penetración** respecto a las entidades que participen en alguno de los sectores de alta criticidad referidos en el Anexo I de la Directiva NIS 2. También se contempla la creación de una **“cybersecurity reserve”**, integrada por instituciones y agencias de los distintos Estados Miembros, y sobre todo por empresas privadas certificadas y de confianza. La cybersecurity reserve intervendrá en momentos de crisis bajo la supervisión de la propia Comisión y de ENISA.

Reglamento eIDAS 2:

Por último, cabe mencionar la reciente aprobación del **Reglamento eIDAS 2** (Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital). El Reglamento está diseñado para actualizar y mejorar la forma en que se gestiona la identificación electrónica dentro de la UE. En concreto, se prevé la creación de los conocidos como “European Digital Identity Wallets” que permitirán a los ciudadanos identificarse de forma electrónica en cualquier Estado miembro, mediante un único soporte común que aglutine información muy diversa como su edad, identidad, nacionalidad, salud, permiso de conducir, etc. en distintos escenarios. Otra de las novedades que trae el Reglamento eIDAS 2 es su voluntad de ampliar el catálogo de servicios de confianza de los categorizados como “cualificados”.

No obstante, también es relevante para tener una visión global de lo que está sucediendo en el mundo en relación con la regulación de la ciberseguridad, atender a las **novedades que se han producido en 2023 en Estados Unidos.**

El 26 de julio de 2023, the U.S Securities and Exchange Commission (“SEC”) aprobó las tan esperadas normas que regirán las divulgaciones y la gobernanza de la ciberseguridad de las **empresas cotizadas y los Foreign Issuers (FPI) de ese país.**

Estas normas se traducen, entre otras, en la obligación de informar sobre incidentes de ciberseguridad materialmente significativos (Formulario 8-K) y en la obligación de comunicar de manera anual información sobre sobre gestión de riesgos corporativos, estrategia y gobernanza de la ciberseguridad (Formulario 10-K).

Según ha manifestado la SEC, el objetivo de dichas obligaciones es ayudar a los inversores a comprender mejor el entorno de riesgo de ciberseguridad de las empresas cotizadas. Al mismo tiempo, advierte que con las nuevas reglas cuenta con suficientes herramientas para iniciar medidas coercitivas en caso de incumplimiento. De hecho, ya ha iniciado acciones contra varias empresas por divulgación inadecuada y por no contar con controles y procedimientos de divulgación inadecuados.

Las conclusiones que podemos extraer de los primeros formularios presentados son:

El proceso de adaptación de los consejos de administración respecto a las nuevas obligaciones en materia de ciberseguridad.

La rápida adopción de mecanismos sofisticados de gestión del riesgo tecnológico, incluyendo profundos cambios en los modelos de gobernanza de la ciberseguridad en las compañías obligadas.

3

Ciberseguridad en la era de la Inteligencia Artificial

Alejandro Padín Vidal

Socio responsable del área de Economía del dato, privacidad y ciberseguridad de Garrigues

3 Ciberseguridad en la era de la Inteligencia Artificial

2.1. Introducción.

La evolución tecnológica sigue avanzando a paso firme, gracias a la investigación y a la inversión que se está llevando a cabo a nivel global, aunque concentrada principalmente en algunos polos concretos. A rebufo de esa evolución, la regulación de las tecnologías más novedosas también avanza en diversas jurisdicciones.

Cabe señalar que los impulsos regulatorios más intensos no siempre coinciden con aquellos polos de inversión principales, divergencia que daría en sí misma para un artículo, pero no es el objeto de este.

A continuación, vamos a analizar el enfoque regulatorio en la Unión Europea y en España, con algunas pinceladas sobre otros instrumentos internacionales de diferente ámbito.

2.2. Entorno normativo.

En el marco del conjunto normativo de la Agenda Digital Europea, durante el año 2023 se le ha dado el impulso final y definitivo a la propuesta de Reglamento que establece normas armonizadas en materia de inteligencia artificial (“Reglamento de IA”). Esta propuesta ha superado ya todos los trámites del proceso de creación legislativa europea y, una vez en vigor, con distintos plazos de aplicabilidad obligatoria según la materia, establecerá obligaciones para los operadores en el mercado relacionados con la inteligencia artificial. Durante su tramitación en las instituciones, la propuesta de Reglamento de IA ha visto reforzado su enfoque a la ciberseguridad, incluyendo numerosas menciones que analizaremos a continuación.

En EEUU existe también una norma vinculante sobre inteligencia artificial: la Orden Ejecutiva sobre el desarrollo y la utilización seguros y fiables de la inteligencia artificial, dictada por la Casa Blanca el 30 de octubre de 2023. En ella se incluyen diversas referencias a la ciberseguridad y su importancia.

A nivel nacional cabe referenciar la Guía de Buenas Prácticas BP-30 del Centro Criptológico Nacional, que contiene una aproximación a la inteligencia artificial y la ciberseguridad no solo desde el punto de vista del riesgo, sino también de la utilidad.

Ámbito Europeo

Reglamento de IA

Establece normas armonizadas en materia de inteligencia artificial

EEUU

Orden Ejecutiva

sobre el desarrollo y la utilización segura y fiable de la IA

Ámbito Nacional

Guía de Buenas Prácticas BP-30

Contiene una aproximación a la IA y la ciberseguridad en cuanto al riesgo y a la utilidad

1. Análisis de la propuesta de Reglamento de Inteligencia Artificial de la UE.

La ciberseguridad es una cuestión de gran importancia en el Reglamento de Inteligencia Artificial. El texto menciona la ciberseguridad hasta en 53 ocasiones en su versión final, a diferencia de las breves 15 menciones en la versión inicial de la Comisión. Destaca la importancia de la ciberseguridad en el desarrollo y uso de sistemas de IA de alto riesgo.

- **Líneas estratégicas de ciberseguridad en el Reglamento de IA.**

Una de las líneas estratégicas en el Reglamento de IA en relación con la ciberseguridad es que libera de algunas obligaciones regulatorias a aquellos elementos de inteligencia artificial que se destinen exclusivamente a la protección frente a amenazas de ciberseguridad, separando este concepto del concepto general de “seguridad”. Así, el Reglamento establece que los sistemas biométricos destinados a ser utilizados exclusivamente a efectos de posibilitar la ciberseguridad y las medidas de protección de los datos personales no deben considerarse sistemas de IA de alto riesgo, excluyendo, por tanto, toda la carga regulatoria que tales sistemas lleva aparejada. Además, los componentes destinados a ser utilizados exclusivamente con fines de ciberseguridad no deben considerarse componentes de seguridad en los términos del Reglamento.

Desde otra de las líneas estratégicas, se pretende que los sistemas de inteligencia artificial de alto riesgo integren de forma esencial elementos de protección frente a amenazas de seguridad. En este sentido, el Reglamento de IA establece que los sistemas de IA de alto riesgo deben cumplir con requisitos referentes a la gestión de riesgos, la calidad y la pertinencia de los conjuntos de datos utilizados, la documentación técnica y la conservación de registros, la transparencia y la comunicación de información a los responsables del despliegue, la supervisión humana, la solidez, la precisión y la ciberseguridad. Los sistemas de IA de alto riesgo deben funcionar de manera uniforme durante todo su ciclo de vida y presentar un nivel adecuado de precisión, solidez y ciberseguridad, a la luz de su finalidad prevista y con arreglo al estado actual de la técnica generalmente reconocido.

- **Identificación de riesgos de ciberseguridad en la IA.**

El Reglamento de IA nace a partir del entendimiento y convencimiento en la Unión Europea de que la ciberseguridad es fundamental para garantizar que los sistemas de IA resistan a las actuaciones de terceros maliciosos que, aprovechando las vulnerabilidades del sistema, traten de alterar su uso, comportamiento o funcionamiento o de poner en peligro sus propiedades de seguridad.

Es fundamental comprender dónde están los puntos débiles de los sistemas de inteligencia artificial con respecto a los riesgos de ciberseguridad. Los ciberataques contra sistemas de IA pueden (i) dirigirse contra activos específicos de la IA, como los conjuntos de datos de entrenamiento (p. ej., envenenamiento de datos) o los modelos entrenados (p. ej., ataques adversarios o inferencia de pertenencia), o (ii) aprovechar las vulnerabilidades de los activos digitales del sistema de IA o la infraestructura de TIC subyacente. Por lo tanto, para garantizar un nivel de ciberseguridad adecuado a los riesgos, los proveedores de sistemas de IA de alto riesgo deben adoptar medidas adecuadas, como los controles de seguridad, teniendo también en cuenta, cuando proceda, la infraestructura de TIC subyacente. Esas medidas deberán estar implementadas desde el diseño y deberán perseguir que los sistemas de IA de alto riesgo sean resistentes a los intentos de terceros no autorizados de alterar su uso, sus resultados de salida o su funcionamiento aprovechando las vulnerabilidades del sistema. Las soluciones técnicas encaminadas a garantizar la ciberseguridad de los sistemas de IA de alto riesgo serán adecuadas a las circunstancias y los riesgos pertinentes.

- **Ciberseguridad en los modelos de IA de uso general.**

Una de las novedades introducidas en la propuesta de Reglamento de IA durante su tramitación en las instituciones europeas, ha sido la inclusión de la regulación de los denominados “modelos de IA de uso general” (“general purpose AI models”). El Reglamento de IA define un modelo de IA como uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado.

Pues bien, los proveedores de modelos de IA de uso general que presenten riesgos sistémicos (definido este como un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor) deben estar sujetos, además de a las obligaciones impuestas a los proveedores de modelos de IA de uso general, a obligaciones encaminadas a detectar y atenuar dichos riesgos y a garantizar un nivel adecuado de protección en materia de ciberseguridad, independientemente de si dichos modelos se ofrecen como modelos independientes o están integrados en sistemas de IA o en productos.

- **Obligaciones específicas.**

En cuanto a obligaciones específicas, el Reglamento de IA exige a la Comisión Europea que implemente medidas de ciberseguridad con relación a la base de datos de la UE en la que se deben inscribir todos los sistemas de IA de alto riesgo, la responsabilidad de cuya gestión recae en la propia Comisión.

Se exige también que las instrucciones de uso de los sistemas de IA de alto riesgo contengan información sobre el nivel de ciberseguridad, así como sobre los riesgos que puedan afectar a esa ciberseguridad, e igualmente en la documentación técnica deberá incluirse una descripción detallada de las medidas de ciberseguridad adoptadas.

- **Gobernanza.**

En lo que respecta a la gobernanza de la IA, todas las instituciones con funciones de supervisión, coordinación y otras, tanto a nivel europeo (Comité Europeo de Inteligencia Artificial, Oficina de IA de la Comisión) como a nivel nacional (autoridad notificante, autoridad de vigilancia del mercado) tienen asignadas potestades relacionadas con la cibersegurdad.

En resumen, el Reglamento de Inteligencia Artificial reconoce la importancia de la ciberseguridad en el desarrollo y uso de sistemas de IA de alto riesgo y establece requisitos y medidas para garantizar un nivel adecuado de ciberseguridad.

2. Orden Ejecutiva de la Casa Blanca sobre Inteligencia Artificial.

Como ya se ha comentado, diversos gobiernos en diferentes jurisdicciones han tomado consciencia de la importancia de la ciberseguridad en relación con la inteligencia artificial. Se trata de un pilar fundamental en la era digital y su relevancia se ha visto reflejada en la Orden Ejecutiva emitida por el Presidente de los Estados Unidos, Joe Biden, el 30 de octubre de 2023.

01

Contexto de la Orden Ejecutiva

02

Evaluaciones Estandarizadas y Ciberseguridad

03

Riesgos de Seguridad y Respuestas Estratégicas

04

Innovación Responsable y Protección de la Propiedad Intelectual

05

Principios de Seguridad para la IA

01 Contexto de la Orden Ejecutiva

La Orden Ejecutiva hace referencia a la importancia de la IA como una tecnología integrada profundamente en las infraestructuras críticas, desde sistemas de energía hasta redes de comunicaciones y defensa. La Orden Ejecutiva reconoce que el nivel en que la sociedad depende de la IA, ha traído consigo riesgos sustanciales que deben ser mitigados para proteger tanto a individuos como a la nación en su conjunto. El enfoque se refiere a la defensa de los ciudadanos de Estados Unidos.

02 Evaluaciones Estandarizadas y Ciberseguridad

Uno de los elementos clave de la Orden es la implementación de evaluaciones estandarizadas para los sistemas de IA. Estas evaluaciones son cruciales para identificar vulnerabilidades que podrían ser explotadas por actores maliciosos. Al establecer políticas e instituciones dedicadas a estas pruebas, se busca comprender y mitigar los riesgos asociados con la IA antes de su despliegue en entornos reales.

La ciberseguridad se destaca dentro de estas evaluaciones, ya que los sistemas de IA están intrínsecamente conectados con la infraestructura de datos. La protección contra ataques cibernéticos es esencial para mantener la integridad y la confidencialidad de la información procesada por la IA.

03 Riesgos de Seguridad y Respuestas Estratégicas

La Orden también aborda los riesgos de seguridad más apremiantes relacionados con la IA. Esto incluye la biotecnología, donde la IA puede jugar un papel en la identificación de amenazas biológicas, y la infraestructura crítica, donde la IA ayuda a monitorear y responder a incidentes de seguridad física y cibernética.

La respuesta estratégica a estos riesgos implica no solo la detección y prevención, sino también la capacidad de respuesta rápida ante incidentes. La ciberseguridad, en este contexto, se convierte en una disciplina dinámica que requiere una actualización constante de conocimientos y herramientas para proteger contra las amenazas emergentes.

04 Innovación Responsable y Protección de la Propiedad Intelectual

La promoción de una innovación responsable es otro aspecto destacado de la Orden. Esto implica un enfoque en la propiedad intelectual y la protección de los derechos de inventores y creadores. En el ámbito de la ciberseguridad, esto significa asegurar que las innovaciones en IA no solo sean efectivas sino también éticamente diseñadas y con respeto a la privacidad y los derechos individuales.

05 Principios de Seguridad para la IA

Finalmente, la Orden establece principios claros para garantizar que la IA sea segura y proteja los intereses de los ciudadanos estadounidenses. Esto incluye la protección contra fraudes, sesgos no intencionados, discriminación, infracciones de privacidad y otros daños potenciales. La ciberseguridad es fundamental en este esfuerzo, ya que asegura que los sistemas de IA operen dentro de los marcos éticos y legales establecidos.

En conclusión:

La Orden Ejecutiva sobre IA establece un marco para el desarrollo seguro de tecnologías que son fundamentales para el futuro, al tiempo que protege los valores y la seguridad de la sociedad. La ciberseguridad no es solo una cuestión técnica, sino también una prioridad estratégica que abarca la protección de la infraestructura, la innovación responsable y la salvaguarda de los derechos civiles.

2.3. Otros instrumentos normativos.

1. Recomendación del Consejo de la OCDE sobre Inteligencia Artificial

La Organización para la Cooperación y el Desarrollo Económico ha publicado una Recomendación sobre Inteligencia Artificial en la que se establecen una serie de principios que deberían formar parte de cualquier normativa o instrumento legislativo relativo a la regulación de la inteligencia artificial. Cabe decir que este documento no habla expresamente de "ciberseguridad", pero si contiene diversas menciones al concepto de "seguridad digital", que tiene un significado equivalente.

2. Tratado del Consejo de Europa sobre Inteligencia Artificial

El Consejo de Europa acaba de aprobar en el mes de mayo de 2024 un Convenio Marco para la Inteligencia Artificial, Derechos Humanos y Estado de Derecho. Este documento, de gran importancia como primer tratado internacional relativo a la IA, cita también el concepto de "seguridad" en relación con los sistemas de inteligencia artificial.

3. Guía de Buenas Prácticas del Centro Criptológico Nacional

El Centro Criptológico Nacional español (CCN) ha publicado una Guía de Buenas Prácticas (BP-30) sobre ciberseguridad e inteligencia artificial. Esta guía contiene información muy útil sobre las relaciones entre la inteligencia artificial y la ciberseguridad, desarrollando no solo cuestiones relativas a los riesgos de ciberseguridad que afectan a la IA, sino analizando los casos en que el uso de la IA puede favorecer y mejorar la ciberseguridad.

2.4. Reflexiones finales y perspectivas para el futuro de la ciberseguridad

Como podemos observar, la inteligencia artificial es una tecnología de moda por su irrupción masiva en todos los ámbitos de la economía y la sociedad, en todas las profesiones y actividades humanas. En relación con esta tecnología, los estados y organizaciones internacionales han visto necesario regular aquellos aspectos que pueden suponer un mayor riesgo para las personas, imponiendo obligaciones de revisión, supervisión y sanciones por incumplimiento. En este contexto, los riesgos de ciberseguridad se presentan como uno de los aspectos más relevantes en el control de la inteligencia artificial, resultando esencial prestar una atención especial y cercana a esta materia para permitir su evolución sin riesgos para los derechos y libertades fundamentales de los ciudadanos, así como para el mercado y la sociedad en general.

4

La Responsabilidad Civil de los ciberriesgos

Antonio Belda Blanco

Executive Director Claims Professional Services Aon

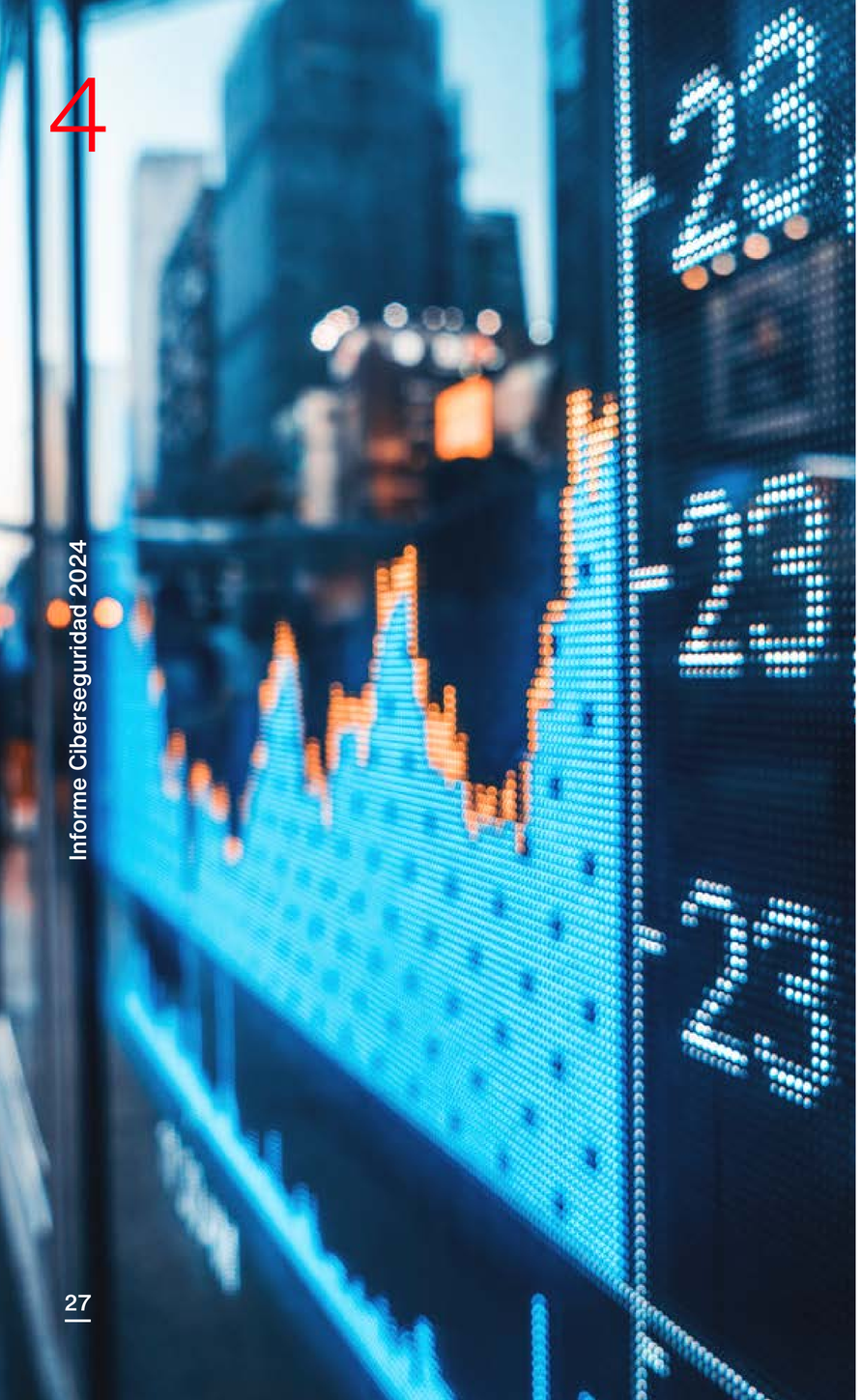
4

La Responsabilidad Civil de los ciberriesgos

Sobre el papel y, en la mente de todos, estamos inicialmente concienciados de los riesgos del uso de la tecnología, así como de las advertencias para no caer en las trampas y hacer un uso seguro.

Cierto es que no dejamos de recibir mensajes en este sentido, tanto de las propias redes sociales que usamos, como de las entidades financieras, los cuerpos y fuerzas de seguridad del Estado, las propias empresas y hasta las noticias de prensa que nos lo recuerdan todos los días. Pero, aun así, el aumento de los delitos cibernéticos, como los medios para su comisión, crecen casi al mismo ritmo que la tecnología.

> Nadie está libre de sufrir un ataque informático, por muy avanzadas que sean los sistemas y herramientas informáticos que usemos.



En cada ocasión que he analizado una reclamación derivada de un ataque cibernético, dejando al margen la capacidad técnica de los ciber delincuentes para vulnerar los sistemas informáticos y quedarse como residentes ocultos en la red, **el desencadenante del desastre casi siempre obedece a los mismos patrones:** un archivo que nunca debió de descargarse; un correo que no debió de contestarse; una información confidencial con prohibición de ser compartida; alguien que no se fijó que el logo de su marca o nombre comercial era algo diferente; o que le faltaba una letra; o que la dirección de correo electrónico después de @ era distinta, y se mandó, compartió o exhibió lo que no debía.

A partir de ese momento, se inicia una crisis cuya contención y efectos en muchas ocasiones es difícil de predecir con certeza, en cuanto que el acto ilícito que la desencadena no siempre produce un daño, pérdida o perjuicio inminente y materializable y, mucho menos restringida al ámbito societario o empresarial de la entidad que ha sufrido el ataque.

La diligencia debida clásica de un ordenado comerciante/empresario ya no es suficiente para evitarlo, con el agravante además de que, siendo otro el causante, la mayoría de las veces el perjuicio o daño ocasionado va más allá de la esfera de control de quien lo sufre, pudiendo afectar a proveedores, clientes o terceros, cuya vía de resarcimiento irá dirigida en la mayoría de los casos frente al que sufrió la vulneración en sus sistemas (aunque sea un perjudicado más) por no haber adoptado las medidas de prevención adecuadas, desencadenando las consecuencias de que dicha vulneración haya permitido entrar en las redes de otros.

La realidad es que una sola vulneración de los sistemas informáticos de una empresa puede ocasionar daños, pérdidas o perjuicios de muy distinta naturaleza y dimensión, y de consecuencias inciertas. No podemos olvidar que la responsabilidad civil, fuera del ámbito del seguro, puede llegar a ser ilimitada, sin perjuicio de la facultad que tienen los Tribunales de Justicia de atemperar o modular la misma en función de las circunstancias del caso, conforme a lo dispuesto en el artículo 1103 de nuestro Código Civil.

Sin ánimo de ser exhaustivos en la casuística de eventos derivados de ataques cibernéticos, uno de los supuestos que más amplitud de perjuicios suele provocar, son las brechas de seguridad que afectan a los datos de carácter personal, de especial protección institucional por su configuración como un derecho fundamental (artículo 18.4 de la Constitución Española). **Toda vulneración de datos personales puede dar lugar a responsabilidad de naturaleza administrativa ante la Agencia Española de Protección de Datos,** tras la tramitación del correspondiente expediente sancionador, lo que conllevará la imposición de una multa cuya cuantía dependerá del tipo de infracción cometida; naturaleza de los derechos personales afectados; grado de intencionalidad del infractor; beneficios obtenidos; medidas de seguridad existentes en los sistemas; o los daños y perjuicios causados.

El simple riesgo latente de sufrir una **brecha de seguridad en el tratamiento de los datos de carácter personal** ha de llevar consigo una continua revisión, actualización e implementación de medidas de seguridad adecuadas para que no haya transmisión de datos fuera del ámbito para el que han sido cedidos, medidas estas que son especialmente analizadas en los procedimientos sancionadores instados por la Agencia Española de Protección de Datos, como órgano supervisor.

Una de las cuestiones novedosas a la hora de valorar la diligencia debida en la implementación de las medidas que garanticen la seguridad de los datos, ha sido la consideración, por parte de nuestro Tribunal Supremo, de que la obligación de adoptar tales medidas no es una obligación de resultado, sino de medios. La diferencia entre una y otra es relevante.

En las obligaciones de resultado existe siempre un compromiso para el cumplimiento de un objetivo concreto, de manera que, la no consecución del mismo (la seguridad de que el dato no sea vulnerado), daría lugar a responsabilidad. Por el contrario, si la obligación es de medios, el compromiso que se asume es de adoptar los medios tecnológicos adecuados, e idóneos, para la protección del dato, garantizando la implementación de las medidas, de manera que permita demostrar un comportamiento diligente.

Si a pesar de ello se sufre una vulneración, la existencia de esta no debería generar de forma automática responsabilidad, sino que para ello será necesario analizar el tipo de medidas implantadas, su finalidad, la tecnología utilizada, pues su suficiencia hay que ponerla en relación con el estado de la técnica existente en cada momento, el nivel de protección del tipo de dato protegido, los costes de aplicación de las medidas, el contexto, o riesgos de probabilidad que ocurra.

Otra cuestión a destacar sobre la protección de datos de carácter personal, es la inclusión de su normativa dentro del ámbito de aplicación de la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020 relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, que permitirá a las entidades habilitadas por cada uno de los Estados miembros, poder defender acciones de cesación o resarcimiento en beneficio del colectivo afectado, de manera que veremos cómo situaciones iniciadas por una persona concreta que ha visto sus datos vulnerados, por ejemplo por una acción comercial genérica de una empresa, se puede transformar en una acción colectiva, lo que obliga claramente a prestar una mayor diligencia de prevención y cuidado en todas aquellas materias referentes a la protección de datos, y a tener siempre presente la necesidad de transferir dicho riesgo al mercado Asegurador.

Pero a su vez, el mismo evento puede ser susceptible de verse inmerso en una reclamación de daños y perjuicios como ocurriría si, con motivo de la prestación de un servicio con un cliente, hubiéramos garantizado la confidencialidad de sus datos y estos se vieran vulnerados (o publicitados) tras la brecha de seguridad sufrida, en cuyo caso se estaría expuesto a una acción de resarcimiento de los daños y perjuicios.

Y lo mismo sucedería en el caso de que con motivo de un fallo de seguridad o de sistemas, se introdujeran terceros en nuestra red, permitiendo con ello que los ciber atacantes cometiesen alguno de los delitos de nuevas tecnologías reconocidos en nuestro derecho penal como: descubrimiento o revelación de secretos (artículo 197); estafas (artículos 248 y 249); o daños informáticos (artículo 264), provocando la paralización, retención, daño, deterioro o destrucción de sistemas y datos informáticos que paralizasen nuestra actividad y la de nuestros clientes.

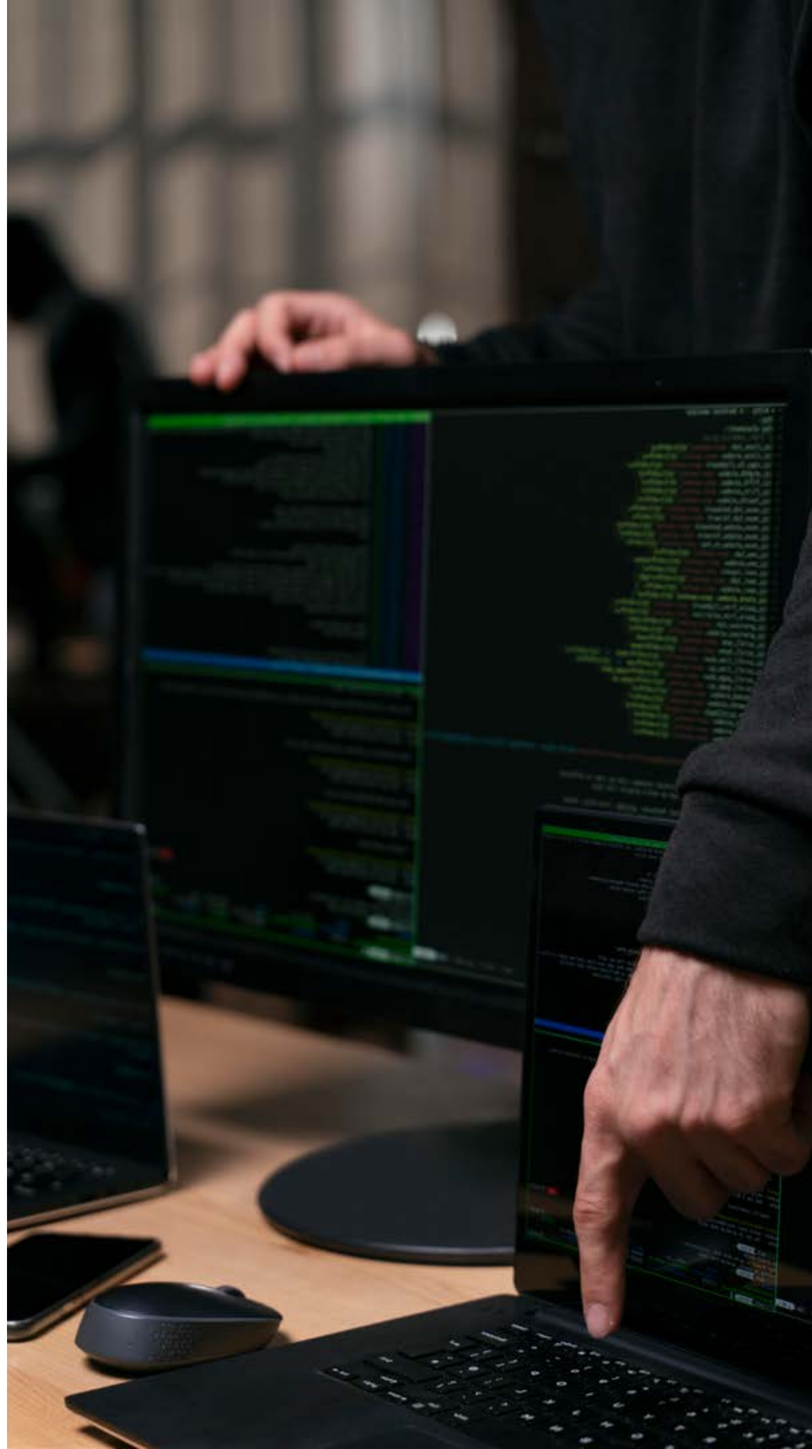
Así pues, nos podemos encontrar con la situación crítica de que un acontecimiento cibernético, no solo ponga en marcha mecanismos de responsabilidad administrativa, contractual o extracontractual, sino que el mismo puede ser generador de daños y perjuicios propios, como la destrucción de sistemas o la paralización de actividad, como asimismo para terceros con los que compartiéramos sistemas o redes.

4

La inmediatez en las transacciones comerciales es básica, y solo el uso de las tecnologías nos lo permite. Compartimos diariamente millones de datos e información relevante sobre nuestras compañías (planes estratégicos, políticas de distribución y precios, acuerdos comerciales, etc.), y todo a través de la red. Pero ¿estamos seguros de que la operación no tiene riesgo?, o, mejor dicho, ¿somos conscientes de que, frente al riesgo comercial de perder una venta concreta, existen otros adicionales? ¿Conocemos a nuestros intermediarios? ¿Confiamos en que nuestros proveedores, e incluso clientes, tengan sus sistemas adecuadamente protegidos?

> El conocimiento de los riesgos del uso de la tecnología; las medidas de prevención; los planes de seguridad y formación interna; la mejora de los estándares de seguridad informática para adaptarlos a su última versión; la vigilancia de los sistemas; las copias de seguridad, y un gran número de medidas de prevención, si bien sirven para tratar de evitar, y también mitigar, los efectos negativos de un ciber ataque, no garantizan la desaparición del riesgo al 100%, ni facilitan una visión anticipada de la responsabilidad civil que se puede llegar a asumir ante tal eventualidad.

Máxime si tenemos en cuenta que una vez localizado el problema, la solución técnica del mismo suele ser posible en un tiempo razonable y con cierta inmediatez, mientras que la localización e identificación de los perjuicios ocasionados, tanto los propios como los de terceros, suelen surgir en un momento posterior (sobre todo los de terceros), con la dificultad adicional de su acreditación cuando ocurren fuera de la órbita y control empresarial de quien ha sufrido el ataque, y con la incertidumbre de su alcance, pues el tercero perjudicado puede reclamar no solo el daño emergente, sino también la ganancia dejada de percibir.



El **mercado Asegurador no ha sido ajeno a esta realidad social**, y a la necesidad de crear productos que den cobertura a la responsabilidad civil derivada de un ciber ataque. Estas pólizas combinan, con acierto, tanto cobertura de daños y pérdidas propias, como de terceros, tratando de abarcar la mayoría de las causas que pueden generar daño, pérdida o perjuicio, dibujando sus coberturas perfectamente los estadios de este tipo de siniestros.

Teniendo en cuenta que **la delincuencia cibernética se incrementará, gracias también al uso de las tecnologías, como el hecho de la globalización y mercado universal y que la conectividad no tiene fronteras,** no cabe duda de que a lo largo de los próximos años veremos como también los Aseguradores harán sus mayores esfuerzos por abarcar nuevos riesgos tecnológicos, y diseñar nuevas coberturas que permitan mitigar los efectos nefastos de este tipo de siniestros.

No será la solución definitiva a este problema, ni única tampoco, pero sí un elemento imprescindible para la supervivencia de nuestras empresas en caso de recibir una intrusión ilegítima en sus sistemas capaz de generar daños, perjuicios o pérdidas, o una inspección en materia de protección de datos.

5

Inteligencia Artificial ¿oportunidad o amenaza?

Pablo Constenla LLM

Head of Cyber Coverage & Claims, Cyber Solutions EMEA

Inteligencia artificial ¿oportunidad o amenaza?

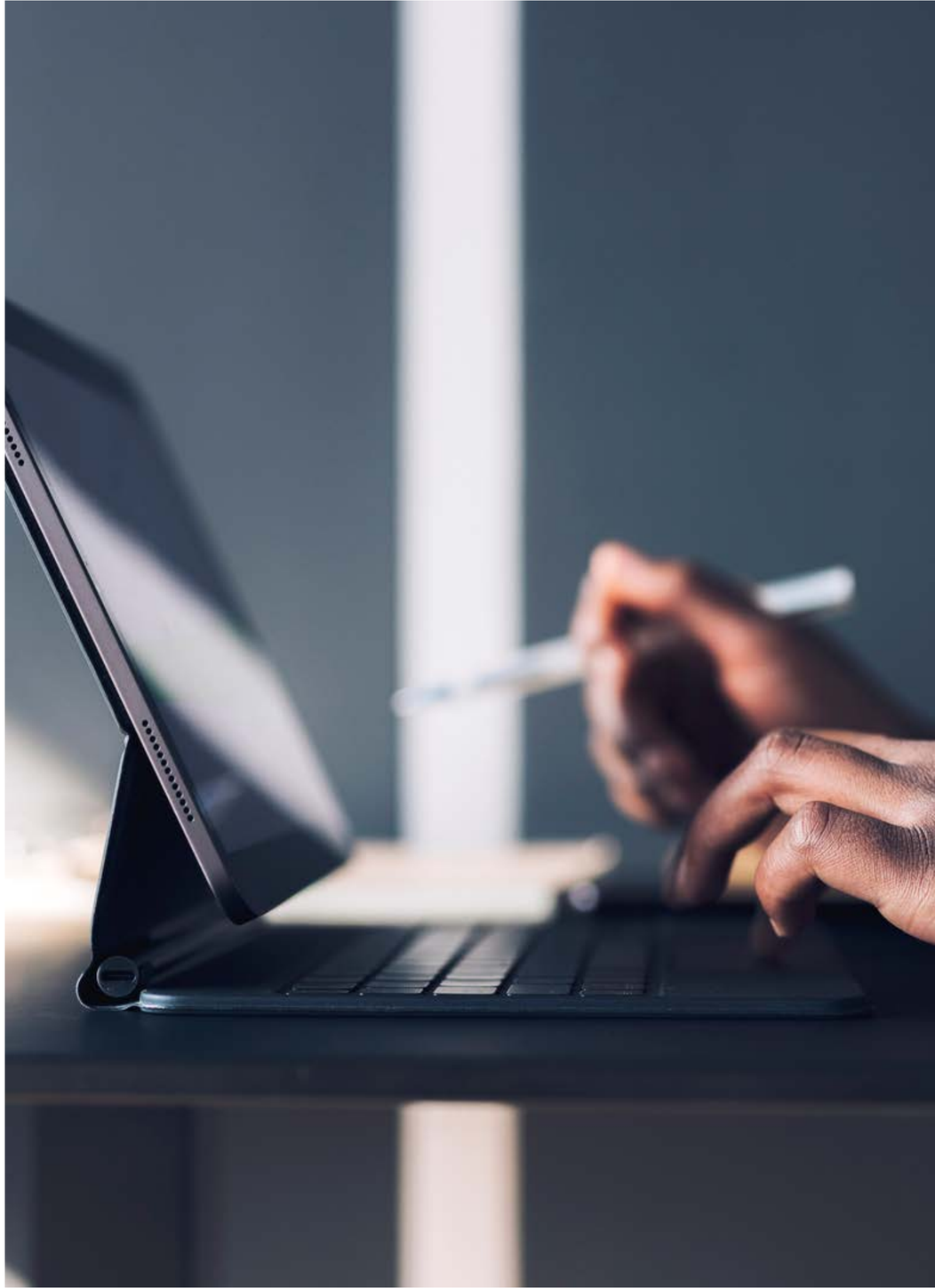
Que estamos ante una revolución digital, unida a una evolución tecnológica sin precedentes, no es ninguna novedad. La clave está en cómo las organizaciones se adaptan a esta revolución, donde entra también en juego la ética y la moral.

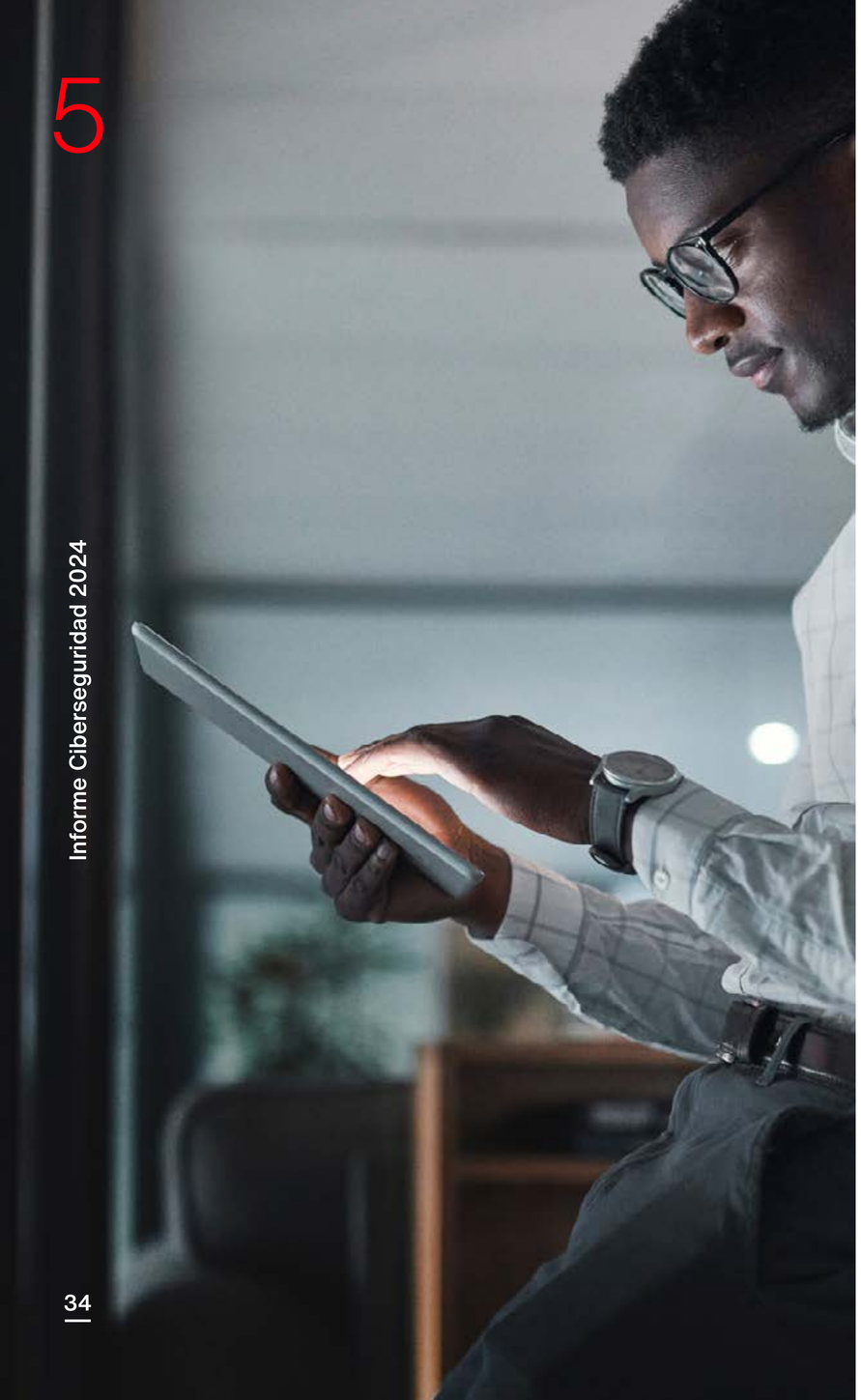
La disrupción de **COVID-19 cambió los plazos para la adopción de la IA al acelerar significativamente la digitalización para todas las empresas.** Prácticamente de la noche a la mañana, las organizaciones tuvieron que adaptarse: trabajo en remoto, ampliar sus capacidades digitales para respaldar la distribución y actualizar sus canales. Si bien es probable que la mayoría de las organizaciones no invirtieron mucho en IA durante la pandemia, la realidad es que las que estén poniendo el mayor énfasis en las tecnologías digitales y una mayor disposición a adaptarse al cambio las colocarán en una mejor posición para incorporar la IA en sus operaciones.

Partimos de la base de que cuando hablamos de inteligencia artificial, hablamos de sistemas inteligentes, es decir máquinas que están programadas para llevar a cabo determinadas tareas de forma automática, que se enfocan en crear sistemas de aprendizaje, razonamiento, percepción y que por tanto mejoran las tareas que requieren de inteligencia humana. Sin embargo, esto se puede convertir en **un arma de doble filo.**

> Por un lado, se gana gran eficiencia para las empresas en términos de innovación, productividad y en definitiva, rentabilidad.

> Por otro, entraña una gran variedad de consecuencias no deseadas. Por tanto, es crucial ser consciente de los riesgos asociados a su adaptación en entornos empresariales y su manera de mitigarlos.





Respecto al sector asegurador, se espera que la IA y sus tecnologías relacionadas tengan un impacto sísmico en todos los aspectos de la industria, desde la suscripción y la fijación de precios, hasta la distribución y la gestión de los siniestros. De hecho, ya se está empezando a observar cómo **este sector está evolucionando de su estado actual de "detectar y reparar"** a **"predecir y prevenir".**

Detectar y reparar

↓

Predecir y prevenir

El **análisis de datos** utilizando Inteligencia Artificial **permite a las aseguradoras y en general a todos los sectores, ser más competitivas.** Pueden evaluar con precisión su rentabilidad actual, así como predecir ventas, productos y precios futuros. Su capacidad para analizar datos de manera eficiente, identificar patrones y predecir riesgos la convierte en un activo invaluable para las aseguradoras.

El objeto último de las compañías de seguros, es garantizar el pago de la reposición de un daño, que nace de un riesgo existente. Para la debida suscripción de todos los riesgos y poder garantizar la rentabilidad de las Aseguradoras, se realizan análisis actuariales que, en base a históricos de siniestralidad, evalúan la probabilidad estadística de diferentes tipos de eventos y cuantifican los posibles impactos financieros de dichos eventos, lo que permite a las aseguradoras seleccionar los riesgos y determinar los precios más competitivos.

En este sentido, la IA se presenta como una herramienta clave para mejorar la eficiencia de determinados procesos dentro de estas empresas y tener un mayor control de los riesgos y por tanto mejorar sus ratios de rentabilidad siniestral.

Además, el sector asegurador ha sido por antonomasia uno de los sectores más tradicionales de la industria de servicios, por lo que la IA cobra más sentido si cabe.

Con esta base, está claro que la Inteligencia Artificial es ya un enorme aliado para esta industria y se abre un mundo de oportunidades infinitas que permiten que el sector asegurador evolucione sin freno.

Pero, ¿y si lo vemos desde el punto de vista del control del riesgo y la mitigación? ¿Y en especial, desde el punto de vista de la ciberseguridad, dónde los métodos de ingeniería social son cada vez más complejos, debido precisamente a esta IA?

Entonces, está claro que **esta tecnología se puede convertir en una amenaza para la gestión de los riesgos futuros,** que se pueden hacer incontrolables a efectos de mitigación y prevención de los mismos.

Pero vamos por partes, porque, por un lado, el reto está para las empresas que deben preservar sus activos ante posibles ataques y hacer una debida transferencia de sus riesgos al mercado asegurador y por otro, el control de la siniestralidad a la que deben hacer frente las aseguradoras ante ingeniería social cada vez más sofisticada.

Ante el reto de las empresas para hacer frente a estas nuevas amenzas, es fundamental que, en primer lugar, tengan identificados los riesgos que la IA les pueda acarrear y, los evalúen, y por otro lado, las responsabilidades derivadas de su uso indebido.

Ambos, tanto riesgos como responsabilidades son numerosas (y hasta incluso, inciertas), pero a grandes rasgos, podemos enumerar desde:

- Responsabilidades por prácticas de empleo indebidas.
- Responsabilidades por sesgos en la elección de ciertos puestos de trabajo.
- Riesgos relacionados con violaciones de las leyes de propiedad intelectual, por ejemplo, por la utilización de materiales protegidos.
- Responsabilidad de administradores y directivos por incumplimiento de sus obligaciones fiduciarias relacionadas, por ejemplo con la presentación de informes financieros inadecuados elaborados con el soporte de IA.
- Responsabilidad cibernética y en especial, la relacionada con la privacidad de los datos.
- Responsabilidad mediática.
- Responsabilidades profesionales por imprecisiones y errores de juicio en los servicios profesionales apoyados en sistemas de IA, con especial atención a los sectores médico-sanitarios y financieros.

Una vez identificados, las empresas deberían preguntarse qué protecciones podrían existir para los riesgos relacionados y hacer así una debida transferencia de estos al mercado asegurador.

Para todos los riesgos enumerados, **la cobertura del seguro debe ser una herramienta clave para la gestión de los mismos.** Tanto con seguros tradicionales de Daños y, Responsabilidad Civil, como con otros que han ido evolucionado, sea el caso de infidelidad de empleados hacia una cobertura de Fraude Informático, o con seguros más emergentes, como pueden ser los de Cyber o Propiedad Intelectual. O los que quedan por venir. Algunas aseguradoras ya están empezando a comercializar seguros a medida para cubrir los riesgos financieros asociados al desarrollo y la venta de nuevos modelos de inteligencia artificial, incluyendo su falta de rendimiento.

Pero **nos detenemos muy especialmente en el riesgo ciber por motivos obvios.** Si un sistema es pirateado o sus datos son comprometidos, las pólizas de riesgos cibernéticos suelen ser las más adecuadas, pero ¿qué ocurre cuando son incidentes derivados de (o ocasionados por) el uso de la inteligencia artificial?

En las pólizas de ciberseguridad de momento, no se suele establecer referencia expresa a un incidente que derive de (o esté ocasionada por) la IA, y se siguen garantizando, a grandes rasgos, ya sea por fallo de seguridad o de sistemas, las pérdidas derivadas del incidente, entre los que destacan los gastos de gestión del propio incidente (gastos de forenses, asesores jurídicos, gastos para contratar firmas profesionales para preservar el daño reputacional), la pérdida de beneficio por interrupción del negocio debido a la pérdida de los activos digitales, los gastos inherentes a la recuperación de estos mismos activos, la responsabilidad civil por vulneración de la ley de protección de datos, etc.

Hasta la fecha, **tampoco se han identificado exclusiones específicas de la Inteligencia Artificial** en el mercado asegurador. No obstante, en caso de que tales exclusiones u otras limitaciones de la cobertura empiecen a aparecer durante la colocación y renovación de pólizas -por ejemplo, exclusiones de reclamaciones, pérdidas o daños que “surjan de” o estén “relacionados con” la IA-, los asegurados deberían resistirse a tales cambios. Además, en los casos en que las definiciones de las pólizas puedan ampliarse para cubrir claramente la IA, debe procurarse negociar esas mejoras. En todos estos aspectos, el bróker de seguros tiene un papel fundamental.

Además, debemos **estar atentos a la hora de cumplimentar las solicitudes de seguro.** Aunque las aseguradoras no han empezado a preguntar de forma rutinaria a las empresas sobre el uso de la IA durante el proceso de suscripción, a medida que el panorama de la IA siga creciendo, esto podría cambiar.

En términos más generales, la inteligencia artificial representa una nueva era de riesgo que las aseguradoras están aprendiendo a gestionar y suscribir adecuadamente. Al igual que ocurrió con la repentina aparición de los ciberataques que transformaron el sector de los ciberseguros, es inevitable que se produzca una curva de aprendizaje, que podría dar lugar a una suscripción, tarificación y oferta variables e inciertas en los próximos años.

> En las pólizas de ciberseguridad de momento, no se suele establecer referencia expresa a un incidente que derive de la IA.

> Hasta la fecha, todavía no se han identificado tampoco exclusiones específicas de la Inteligencia Artificial en el mercado asegurador.

Ante el reto de las aseguradoras para hacer frente a la creciente siniestralidad por una ingeniería social cada vez más compleja, hay que indicar que al igual que los asegurados deben gestionar sus propios riesgos con respecto a la inteligencia artificial, las aseguradoras deben emplear igualmente la inteligencia artificial para ayudarles en sus funciones de predecir y prevenir. Seguir invirtiendo en IA les ayudará además de poder realizar una suscripción más rigurosa y eficiente, tener el riesgo más contenido.

Claramente, el sector asegurador debe tener en cuenta la realidad que veremos en los próximos años, en la que destacará:

01 Conectividad de los datos.

02 Incremento de la robótica.

03 Ampliación de código abierto.

04 Cambio psicológico y neuronal.

Conectividad de los datos:

Se estima que podrá haber hasta un billón de dispositivos conectados para 2025. Dicha conectividad y conocimiento de datos dará como resultado nuevas coberturas con adaptación a las necesidades concretas de cada cliente con una prestación de servicios cada vez más en tiempo real.

Incremento de la rotótica:

Los aseguradores tendrán que entender cómo la creciente presencia de la robótica en la vida cotidiana y en todos los sectores cambiará los grupos de riesgo, y las expectativas de los clientes.

Ampliación de código abierto:

Probablemente surgirán protocolos de código abierto para garantizar que los datos se puedan compartir de forma amplia para múltiples casos de uso bajo un marco regulatorio y de ciberseguridad común.

Cambio psicológico y neuronal:

Las tecnologías cognitivas, que se basan vagamente en la capacidad del cerebro humano para aprender a través de la descomposición y la inferencia, se convertirán en el enfoque estándar para procesar los flujos de datos increíblemente grandes y complejos que generarán los productos de seguros “activos” vinculados al comportamiento y las actividades de un individuo.

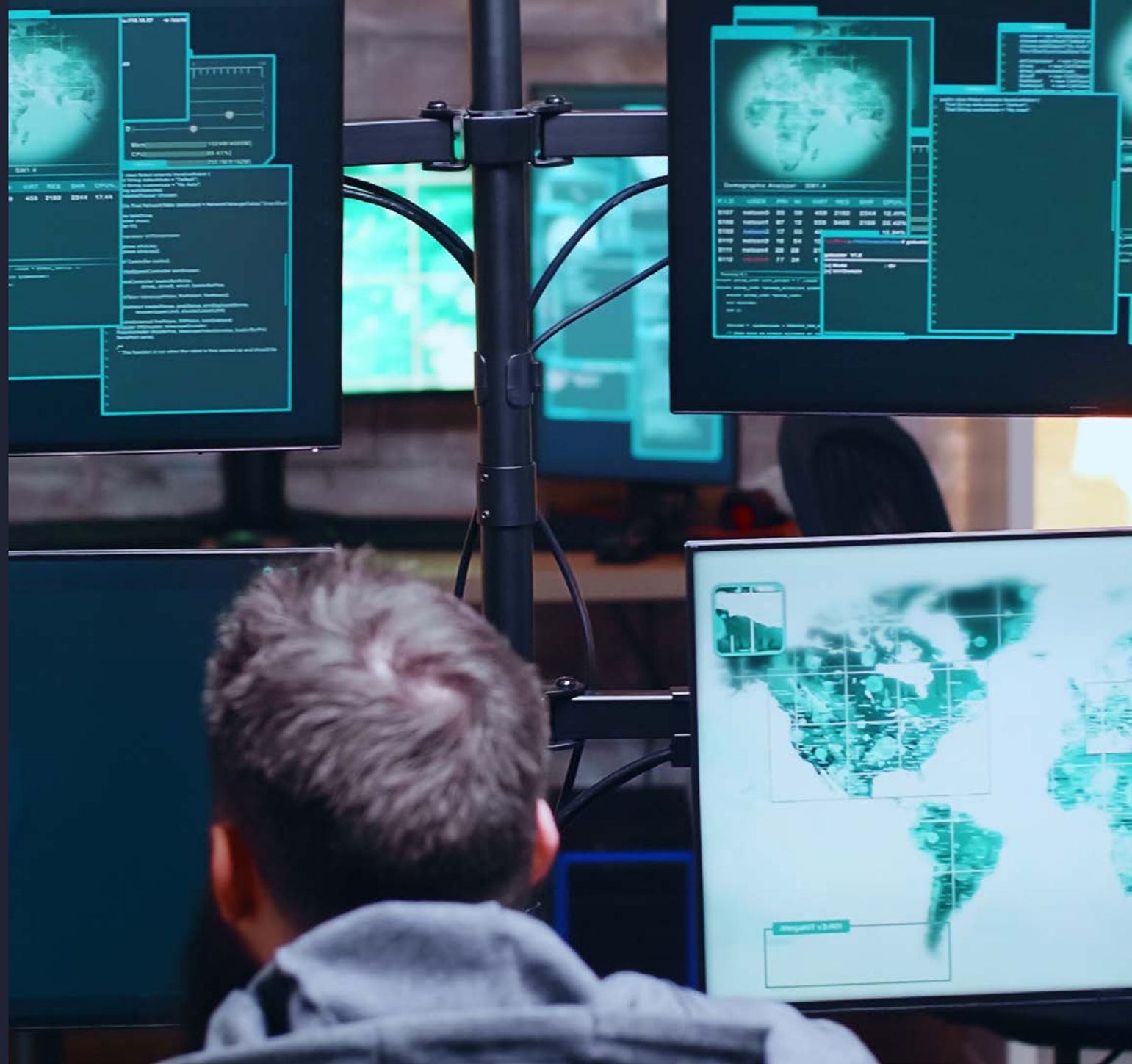
Pero lo que es más importante, las aseguradoras que adopten una mentalidad centrada en crear oportunidades a partir de tecnologías disruptivas, en lugar de verlas como una amenaza para su negocio actual, prosperarán en el sector de los seguros en un corto plazo.

Por tanto, el panorama actual de los riesgos relacionados con la inteligencia artificial es fluido e incierto, y no sólo encierra inmensas promesas, sino también peligros ocultos.

Pero, en cualquier caso, **no hay oportunidad sin riesgo.**

6

Contexto de la ciberseguridad y su nivel de madurez



6 Contexto de la ciberseguridad y su nivel de madurez

La importancia de la Gestión Integral del riesgo ciber.

La gestión del riesgo cibernético mantiene la tendencia alcista de posicionarse como una de las principales prioridades en cualquier organización. Las empresas, independientemente del sector de actividad, continúan incrementando sus esfuerzos para proteger sus sistemas de información, de los ciberataques y otras amenazas digitales. Según la Encuesta Global de Riesgos 2023 de Aon, diseñada para evaluar las actitudes de los líderes empresariales hacia el riesgo y la gestión de riesgos en general, el riesgo (de un total de 60) que más preocupa a las organizaciones es el riesgo de ciberataques.

El uso intensivo (e imparable) de la tecnología de la información en los últimos años incrementa la exposición a los ciberdelincuentes, los errores de los empleados, los desastres naturales y otras amenazas de ciberseguridad. Estas amenazas pueden materializarse de diversas formas causando una paralización total o parcial de los sistemas críticos o cualquier otro daño, lo que puede provocar en definitiva una crisis dentro de la organización con un impacto económico y reputacional significativo.

El crecimiento de estos ataques en términos de probabilidad e impacto está intensificando el entorno normativo, con regulaciones como la Directiva NIS2[1] o el Reglamento Dora[2], que amplían la obligatoriedad de cumplir los requisitos de ciberseguridad a un mayor número de organizaciones de diversos sectores de actividad. Estas normativas, ya en vigor y de obligado cumplimiento a partir de finales de 2024 y principios de 2025[3] (para las empresas incluidas en el ámbito de aplicación) imponen rigurosos requisitos de gestión de riesgos y notificación de incidentes. Por tanto, la capacidad de cualquier organización para anticiparse, mantenerse y recuperarse en caso de incidente, lo que se conoce como ciberresiliencia, se ha convertido en un aspecto fundamental en la gestión de los riesgos empresariales.

La ciberresiliencia implica una gestión integral del riesgo, es decir, identificar, evaluar y responder al riesgo como un proceso continuo y en constante evolución. Parte de esta gestión integral del riesgo ciber implica tener en cuenta las necesidades de toda la organización, por lo que la toma de decisiones y la gestión de riesgos cibernéticos debería incluir a miembros del equipo de IT, el director de seguridad de la información (CISO), pero también directores, consejeros, y responsables de otras unidades de negocio.

Esta coordinación de la seguridad cibernética entre las diferentes unidades de negocios se ha vuelto más importante que nunca para adoptar un enfoque proactivo y minimizar los riesgos cibernéticos, así como una correcta comunicación y gestión el día del incidente.

Top 1 - Riesgo en Ciberataques

El riesgo de ciberataques es el que más preocupa a las organizaciones según la Encuesta Global de Riesgos 2023 de Aon, diseñada para evaluar las actitudes de los líderes empresariales hacia el riesgo y la gestión de riesgos en general.

Se observa cada vez más una colaboración más estrecha entre el director de seguridad de la información (CISO) y al director de riesgos (CRO). Este enfoque unificado, del CRO centrado en mejorar los resultados de los seguros de transferencia de riesgos y el enfoque del CISO en la aprobación del presupuesto para iniciativas de ciberseguridad, resulta estratégica para cualquier organización porque podría mejorar los resultados en términos de cobertura y al mismo tiempo minimizar los riesgos financieros y de reputación.

La incorporación del Director Financiero refuerza esta gestión, dado que esta figura a menudo supervisa las funciones del CRO y el CISO, y una comprensión más profunda sobre cómo invertir en controles cibernéticos adecuados se puede traducir en una mitigación del impacto financiero tras un incidente cibernético o las limitaciones en la cobertura.

Las organizaciones con un nivel de madurez del riesgo cibernético avanzado ya no se limitan exclusivamente a implantar las correspondientes medidas de seguridad, si no que están trabajando en incorporar a su gestión integral del riesgo, la cuantificación de un posible incidente cibernético que permita comprender mejor los riesgos e impacto real al que se enfrentan y la toma de decisiones basada en datos: ¿Cuáles son mis riesgos financieros? ¿Cuáles son nuestros riesgos técnicos? ¿Cuáles son las vulnerabilidades y amenazas a las que se enfrenta nuestra empresa? ¿Cuánto podemos transferir?

1. Directiva NIS2: Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

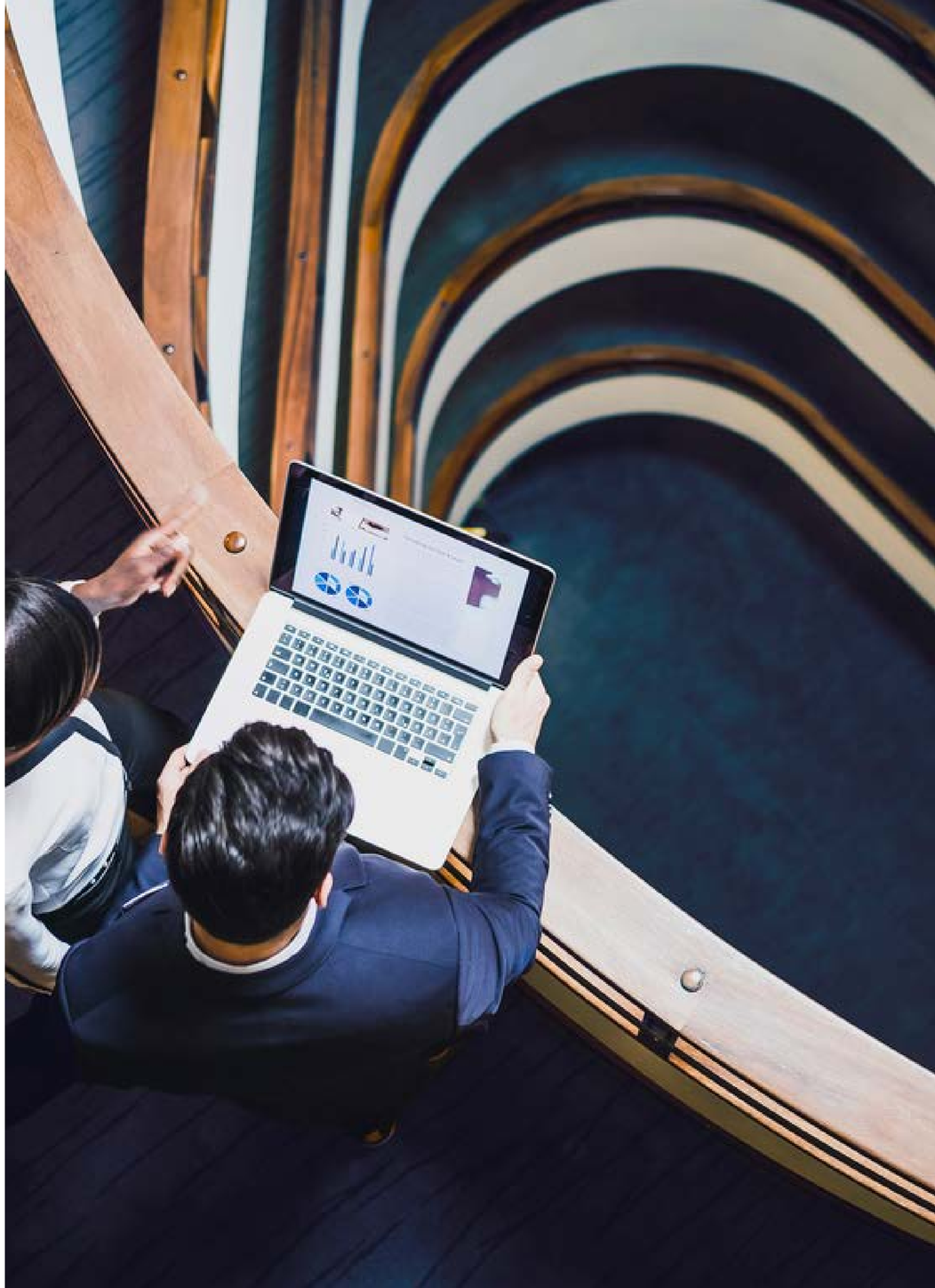
2. Reglamento DORA: Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero.

3. La Directiva NIS2 necesita transposición al ordenamiento jurídico español antes del 17 de octubre de 2024 y será aplicable a partir del 18 de octubre de 2024. El Reglamento DORA será aplicable a partir del 17 de enero de 2025.

Panorama del riesgo cibernético.

En los últimos años, han surgido varios riesgos cibernéticos importantes, incluidos ataques de ransomware dirigidos a grandes empresas, organizaciones gubernamentales y proveedores de servicios críticos.

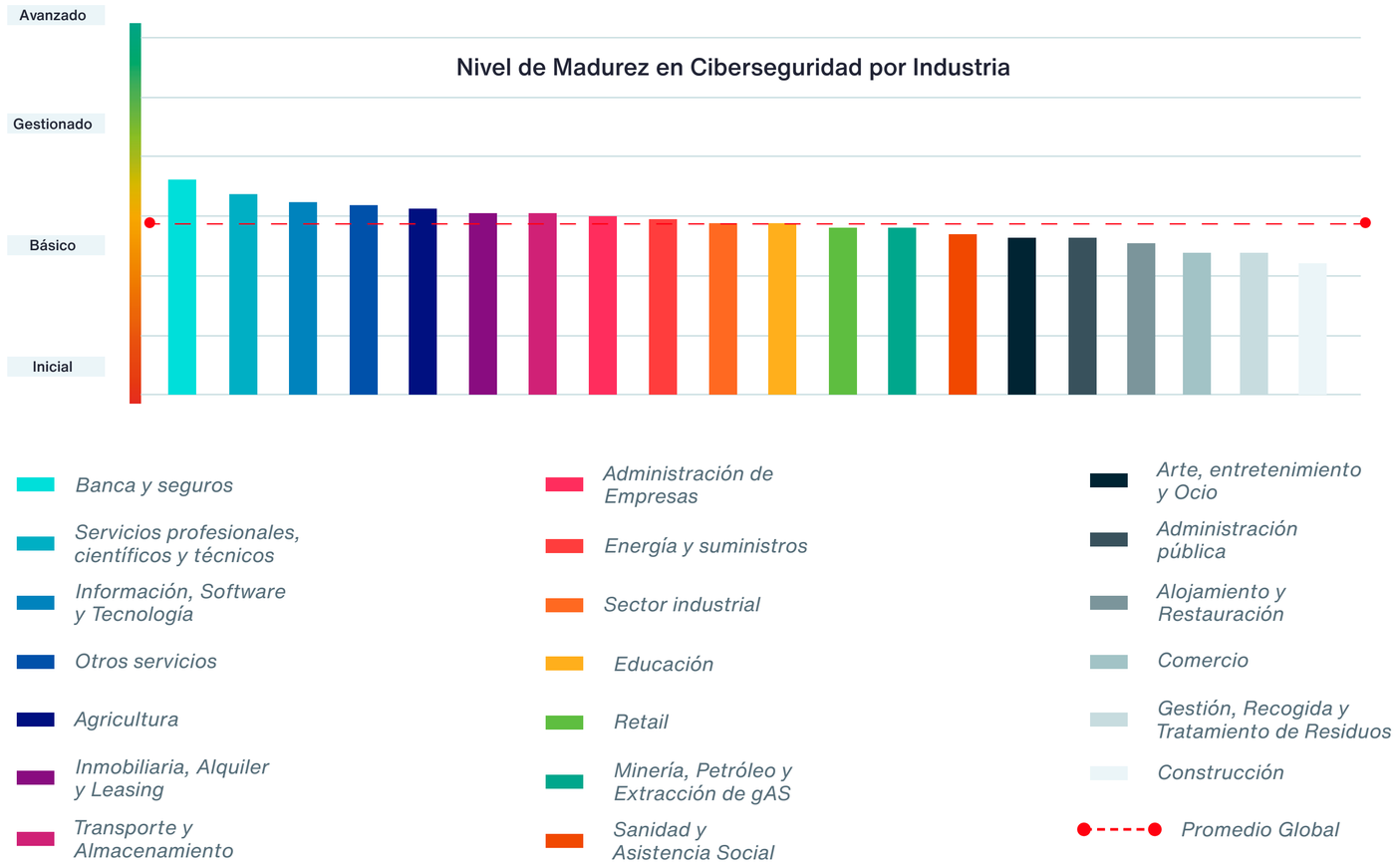
- **Los ataques de ingeniería social** se están volviendo cada vez más sofisticados y ahora utilizan métodos como la Inteligencia Artificial (IA) y la tecnología Deepfake para engañar a los usuarios para que revelen información confidencial o mediante phishing para lograr que descarguen malwares en sus dispositivos conectados.
- **Las vulnerabilidades de IoT (Internet de las Cosas)** también están creciendo, los piratas informáticos han logrado tomar el control de cámaras de seguridad, dispositivos inteligentes conectados como termostatos, sensores y dispositivos médicos. Por otro lado, como resultado de las guerras recientes, ha habido un aumento en la actividad de grupos de hackers patrocinados por gobiernos con el objetivo de obtener información estratégica o llevar a cabo operaciones de desinformación.
- **Los ciber acontecimientos pueden afectar a varias áreas de una organización (riesgo sistémico),** y los organismos reguladores están endureciendo los requisitos de ciberseguridad; en consecuencia, la ciberresiliencia es un tema crítico para cualquier organización.
- **Estados Unidos sigue siendo el país más atacado,** y los países de Europa occidental también figuran en las primeras posiciones por la percepción de riqueza y capacidad para pagar altas demandas de rescate.
- **El sector más afectado por el ransomware en el primer trimestre de 2024 fue el de productos industriales y de consumo** mientras que en acceso a datos fue el sector público, siendo la ruta más común para obtener acceso a la red de la víctima a través de la explotación de una vulnerabilidad tales como CVE-2023-46805 (Ivanti ICS 9.x, 22.x e Ivanti Policy Secure), CVE-2024-21762 (Fortinet FortiOS, múltiples versiones) y CVE-2024-23296 (iOS 17.4 y iPadOS 17.4).



Madurez en ciberseguridad.

- **Nivel de Madurez en ciberseguridad por Industria.**

En el último año, el estudio del **Nivel de Madurez en Ciberseguridad** basado en los datos obtenidos a través de la plataforma CyQu desarrollada por Aon, con información de más de **3.000 empresas** (a nivel EMEA) pertenecientes a 20 sectores industriales y analizadas bajo una serie de dominios y controles de seguridad cibernética, muestra que el sector de **Banca y Seguros** cuenta con el mejor nivel de madurez cibernética, seguido de **Servicios Profesionales, Científicos y Técnicos** y el sector de la **Información, Software y Tecnología** en tercer lugar. Por otro lado, 9 sectores (de un total de 20) se encuentran por debajo de la media de madurez global, ocupando la industria del **Comercio, Gestión, Recogida y Tratamiento de Residuos** y el sector de la **Construcción**, las últimas posiciones.

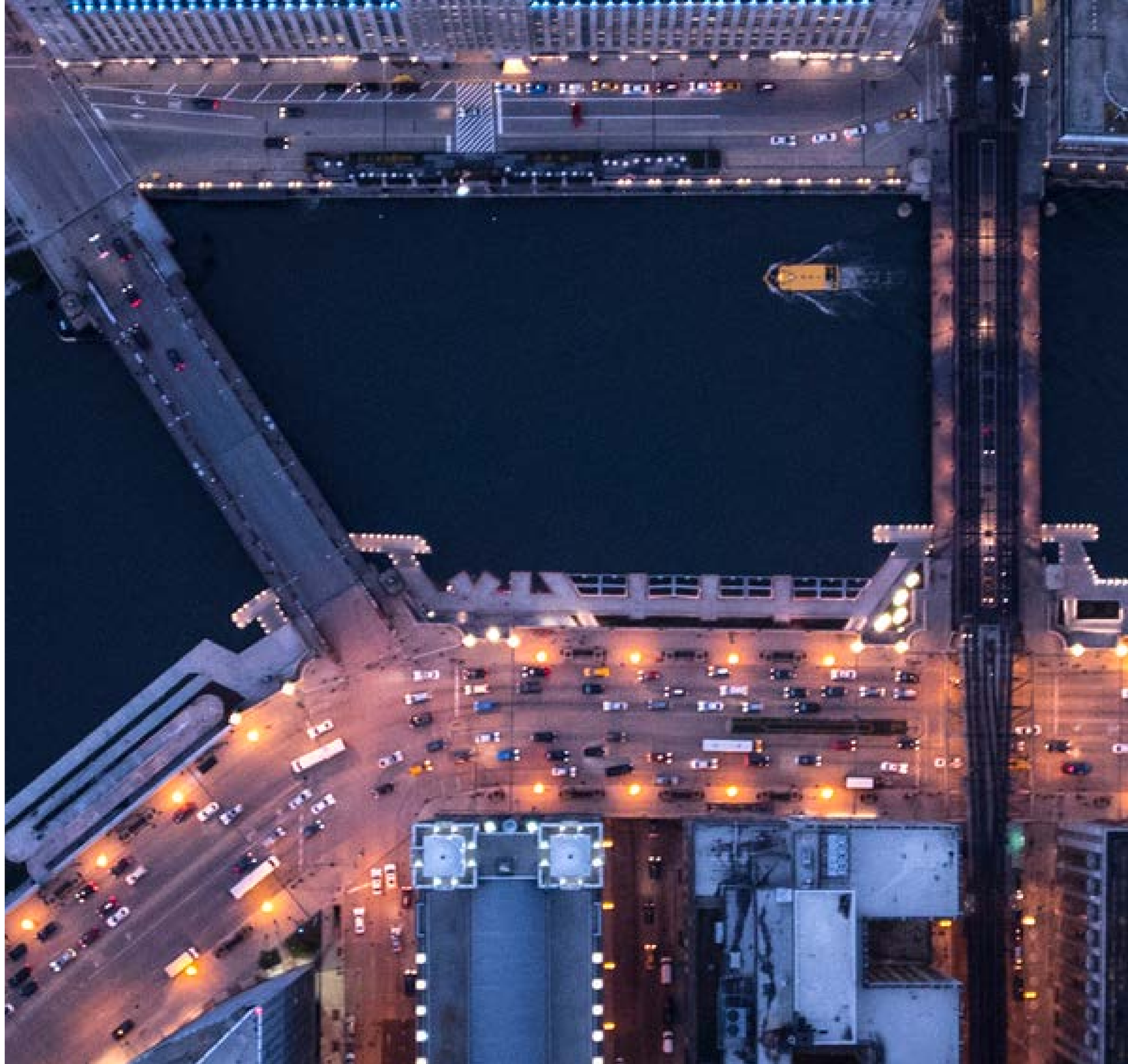


- **Madurez de Ciberseguridad por tamaño de la Empresa EMEA**

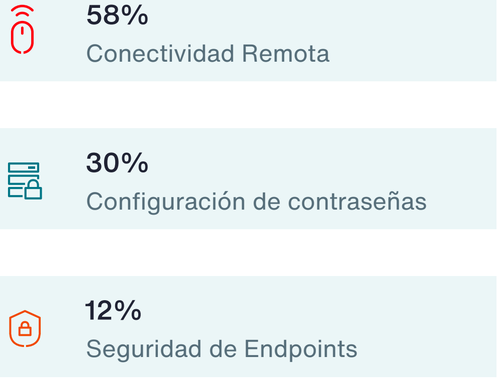
Las empresas multinacionales con una facturación anual **mayor a 5.000 millones** se posicionan en el mayor nivel de madurez. Para el resto de las empresas, Enterprise, Mercado Medio y PYMES, aunque ha habido una evolución positiva, todavía necesitan invertir en materia de ciberseguridad para poder salir de la franja de los controles básicos.

En España vemos el mismo reflejo que los datos que se arrojan desde EMEA, siendo las empresas las empresas de mayor tamaño las que cuentan con un nivel más elevado de madurez. A nivel sectorial destacan:

- Banca
- Servicios profesionales
- Telecomunicaciones
- Infraestructuras críticas.



Mejora en Controles de Seguridad a Nivel EMEA.



01 Conectividad Remota.

La Conectividad Remota ha sido uno de los controles con mejor valoración a nivel EMEA. Un **58%** de las empresas de todos los sectores han mejorado los controles de seguridad relacionados con la conectividad remota en el último año, principalmente debido a los avances tecnológicos y a la demanda creciente de flexibilidad laboral. Las herramientas de colaboración en línea, como videollamadas, plataformas de gestión de proyectos y aplicaciones de mensajería instantánea, han evolucionado significativamente, permitiendo una comunicación más fluida y eficiente entre equipos distribuidos geográficamente. Además, la pandemia de COVID-19 aceleró esta tendencia, obligando a muchas empresas a adaptarse rápidamente al trabajo remoto para garantizar la continuidad de sus operaciones.

Dentro las medidas y herramientas más implementadas para la seguridad de las conexiones en remoto destacan VPN (Red Privada Virtual), Autenticación de doble factor (2FA), Firewalls, Actualizaciones y parches de seguridad, Políticas de seguridad de la información.

02 Configuración de contraseñas.

El segundo control mejor valorado y que a su vez se considera como uno de los pilares fundamentales de la seguridad cibernética es la Configuración de Contraseñas. Un **30%** de las empresas han mejorado los controles de seguridad relacionados con la configuración de contraseñas siendo ya común el uso de herramientas tipo **PAM.**

03 Seguridad de Endpoints.

Un **12%** de las empresas han mejorado sus controles cibernéticos relacionados con la **Seguridad de Endpoints,** con medidas de seguridad como la instalación de **antivirus y antimalware, el monitoreo y la detección de amenazas** y el **control de acceso** a los dispositivos y a los recursos de la red según las necesidades del usuario.

Las herramientas de protección de endpoints se están convirtiendo en una necesidad fundamental en las empresas, como, por ejemplo, un **EDR** que cubra la mayoría de endpoints y que envíe notificaciones sobre alertas y amenazas, un sistema **SIEM** para un control total sobre todos los eventos que sucedan en la empresa y así poder detectar cualquier tendencia o patrón fuera de lo común y actuar de forma inmediata, o un equipo **SOC** que supervise estas fuentes de información, dispositivos, bases de datos, aplicaciones de red, sitios web y otros sistemas para detectar posibles amenazas en tiempo real.

Previsiones sobre ciberamenazas

Las previsiones sobre el riesgo cibernético para el final de 2024 y 2025 indican un panorama complejo y dinámico, con varias tendencias emergentes y persistentes que afectarán tanto a organizaciones como a individuos. Aquí presentamos algunas de las principales:

01 Aumento de los ataques de ransomware:

Los ataques de ransomware continuarán siendo una de las mayores amenazas, con grupos de ciberdelincuentes mejorando sus tácticas y apuntando a infraestructuras críticas y grandes corporaciones. Se espera que sigan prevaleciendo los métodos de doble y triple extorsión, donde los atacantes no solo cifran datos, sino que también amenazan con divulgarlos.

02 Auge de ataques a la cadena de suministro:

Los ataques continuarán enfocándose en las cadenas de suministro de software y hardware, explotando vulnerabilidades en terceros para infiltrarse en las redes corporativas más grandes. Los ataques a la cadena de suministro, como los ocurridos con SolarWinds y MOVEit, seguirán siendo un gran riesgo.

03 Aumento de la inteligencia artificial (IA) en los ciberataques

Tanto atacantes como defensores utilizarán cada vez más la IA y el aprendizaje automático. Los ciberdelincuentes usarán la IA para automatizar y perfeccionar sus ataques, mientras que las empresas emplearán la IA para detectar y responder a amenazas más rápidamente. Los ataques con IA se dividen básicamente en cuatro áreas: ataques a la privacidad de los datos, entradas adversarias, extracción de modelos y envenenamiento de datos de entrenamiento. Estos ataques pueden comprometer la privacidad de los datos, evadir los sistemas de IA, robar el modelo y afectar negativamente al proceso de aprendizaje o salida del sistema.

04 Repetir el ataque a una empresa ya atacada:

Recientemente estamos observando que las empresas que han sufrido un primer ataque sufren otro ataque con una intensidad mucho mayor al poco tiempo del primero. No se trata de una continuidad del primero, sino de un nuevo ataque pero que aprovecha el conocimiento que ya se tiene de la organización.

Conclusiones.

- Los análisis detallados basados en los datos históricos proporcionados por la plataforma CyQu reflejan una realidad dinámica en el campo de la ciberseguridad. En el contexto actual, caracterizado por la volatilidad creciente y los cambios tecnológicos, cabe subrayar la necesidad urgente de todas las organizaciones, independientemente del tamaño o sector de actividad, de intensificar sus esfuerzos en fortalecer sus defensas cibernéticas y asignar recursos adecuados para enfrentar las crecientes y sofisticadas amenazas en línea.
- Es fundamental implementar controles de ciberseguridad para proteger los activos tecnológicos contra las amenazas que cada vez son más sofisticadas. Algunos de los controles mencionados anteriormente ayudan a prevenir accesos remotos no autorizados, suplantación de identidad, asegurar la integridad de los datos, garantizar la disponibilidad de los sistemas y cumplir con las regulaciones y estándares de seguridad. Además, un buen nivel de ciberseguridad fortalece la confianza de los clientes, reduce el riesgo de pérdidas financieras y daños a la reputación de la empresa, y asegura la continuidad y la resiliencia de las operaciones empresariales frente a posibles incidentes de seguridad.
- La gestión de la ciberseguridad debe ser considerada como un tema de suma importancia estratégica. Las empresas necesitan adoptar un enfoque proactivo y holístico en la protección de sus sistemas y datos.
- El riesgo ciber requiere de una gestión integral que tenga en cuenta las necesidades de toda la organización, por lo que la toma de decisiones y la gestión de riesgos cibernéticos debería incluir a miembros del equipo de IT, el director de seguridad de la información (CISO), pero también directores, consejeros, y responsables de otras unidades de negocio.
- La colaboración entre el sector público y privado, junto con la implementación de nuevas regulaciones y políticas sólidas de gestión de riesgos, son fundamentales para mitigar riesgos en un entorno en constante evolución.

7

La Evolución del Seguro Cibernético: Adaptándose al Mercado Medio/Pyme

La evolución del Seguro Cibernético: Adaptándose al Mercado Medio/Pyme

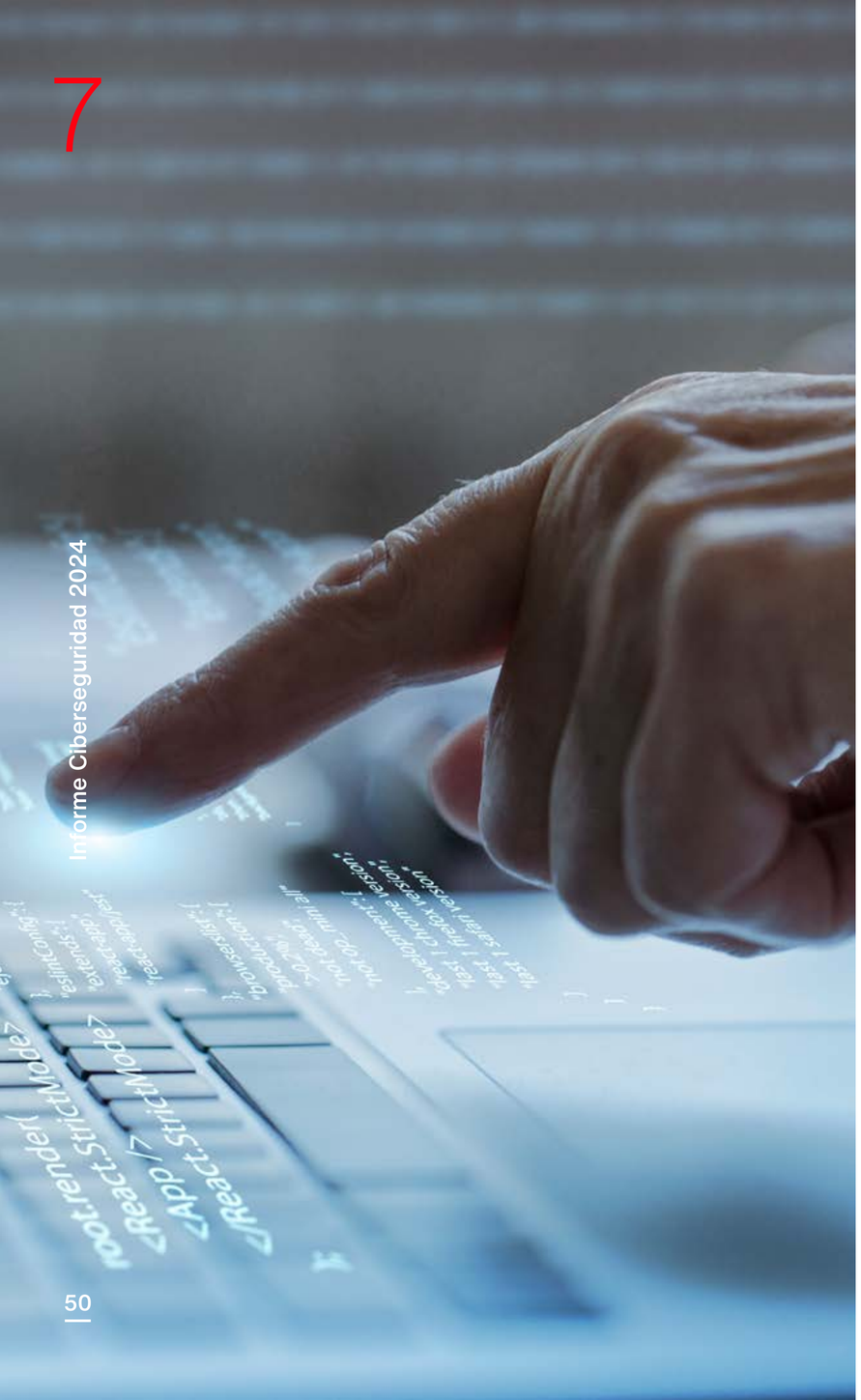
En años anteriores, el riesgo cibernético apenas preocupaba a las empresas de mercado medio. Se pensaba que este tipo de incidentes solo afectaba a grandes corporaciones debido a su supuesto “mayor impacto”. De hecho, en los años previos a la pandemia, el seguro cibernético era considerado un producto novedoso que incluso se ofrecía de forma gratuita al adquirir otros servicios, ya que pocas personas veían la necesidad de protegerse contra estos riesgos.

Sin embargo, la situación ha cambiado drásticamente en la actualidad. Muchas empresas que contrataron este seguro en ese momento se vieron obligadas a prescindir de él cuando comenzó lo que se conoce como “mercado duro”. Inicialmente, estas empresas no veían la necesidad de contar con él, especialmente las pymes, y se encontraron con la rigurosidad de las aseguradoras para asumir el riesgo. Las plataformas de contratación pasaron de ser simples cuestionarios de cinco preguntas o incluso sin requerir información previa, a cuestionarios interminables con requisitos de seguridad casi imposibles de cumplir para muchas empresas, sobre todo por sus limitados presupuestos dedicados a la ciberseguridad.

En la actualidad, todas las empresas son susceptibles de sufrir ataques cibernéticos, siendo un blanco particularmente atractivo para los ciberdelincuentes aquellas que son menos conscientes del riesgo y destinan menos recursos a la ciberseguridad, creyendo que nunca serán víctimas. Además, muchas de estas empresas carecen de un departamento de TI propio y ni siquiera consideran la posibilidad de tenerlo hasta que están en riesgo.

> ⚠
>
> El principal riesgo sigue siendo el ransomware, con un aumento anual de más del 400%. También se ha observado un incremento en los ataques de phishing y las reclamaciones derivadas de la violación de la ley de Protección de Datos.

A mediados de 2023, se produjo un cambio de tendencia y en la actualidad, existen muchas soluciones disponibles para estas empresas a precios más asequibles, e incluso algunas sin aplicación de franquicia.



Esto se debe al aumento en las medidas de seguridad adoptadas por estas compañías y a la creciente concienciación sobre los riesgos cibernéticos, lo que ha llevado a un aumento en la contratación por parte de empresas con una facturación inferior a los 250 millones de euros.

Este cambio de mentalidad y las medidas tomadas han resultado en una mayor protección para las pymes contra los ciberataques, aunque aún queda mucho por hacer para garantizar una seguridad cibernética sólida y efectiva en este segmento empresarial. La inversión en ciberseguridad se ha convertido en una necesidad prioritaria, con muchas empresas reconociendo la importancia de tener un plan de acción claro y efectivo para proteger sus activos digitales y su reputación.

En este sentido, el mercado ha respondido con una mayor oferta de soluciones especializadas y accesibles, lo que ha permitido a las empresas de menor tamaño obtener la protección necesaria sin comprometer su presupuesto. Sin embargo, la educación continua y la concienciación sobre los riesgos cibernéticos siguen siendo fundamentales para prevenir futuros ataques y garantizar la seguridad a largo plazo de estas empresas.

Evolución del mercado asegurador respecto al medio mercado en 2023.

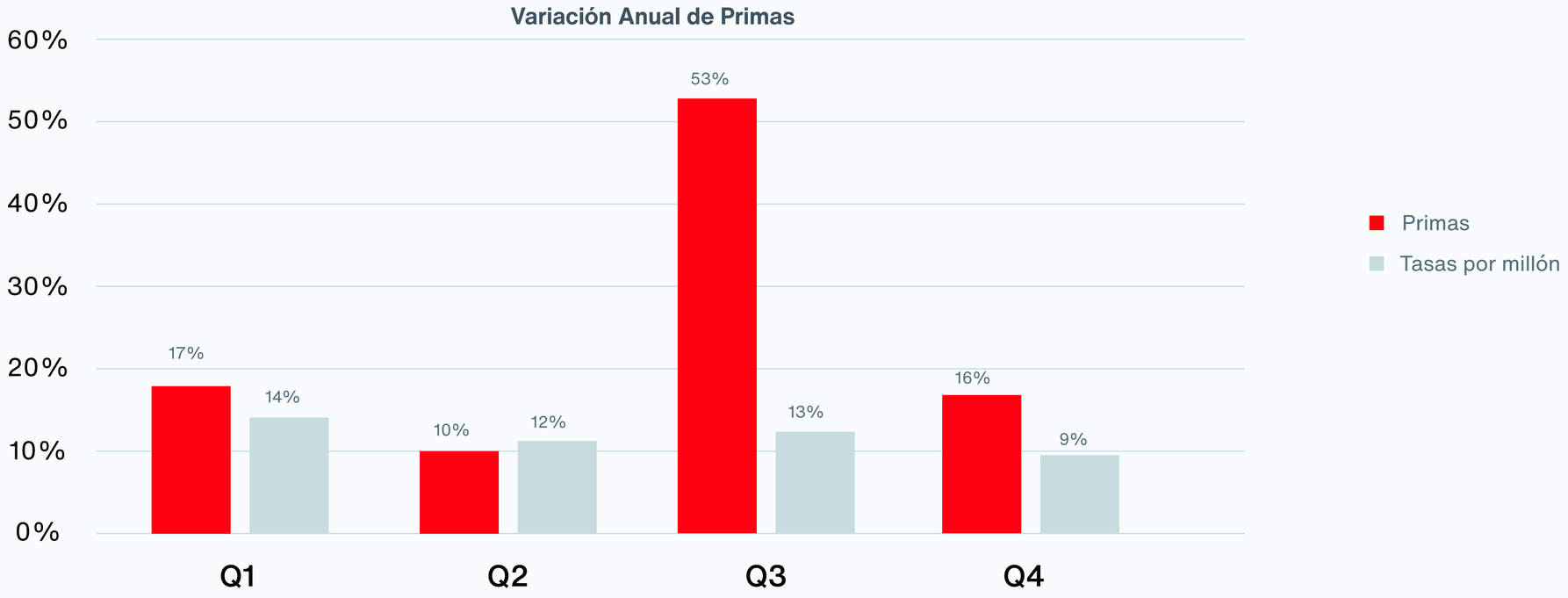
El año pasado marcó un cambio drástico en el mercado asegurador. Durante el primer semestre de 2023, se observaron incrementos moderados en las primas y una estabilización generalizada. Sin embargo, hacia finales de ese mismo año, se registraron notables disminuciones tanto en las primas como en las franquicias. En 2024, esta tendencia se ha mantenido estable, lo que ha llevado a que las compañías decidan incrementar los límites contratados, a veces incluso el doble, por la misma prima que pagaban en 2022.

La competencia entre las aseguradoras ha contribuido a esta tendencia, ya que buscan atraer a más clientes ofreciendo mejores condiciones y precios más competitivos.

Este escenario presenta una gran oportunidad para las pymes, que ahora pueden obtener una cobertura más amplia y efectiva contra los riesgos cibernéticos sin incurrir en costos excesivos. Se espera que esta estabilización y mejora en las condiciones del mercado asegurador continúen en el futuro, lo que beneficiará tanto a las compañías como a los asegurados al garantizar una protección más sólida y accesible contra las amenazas digitales.

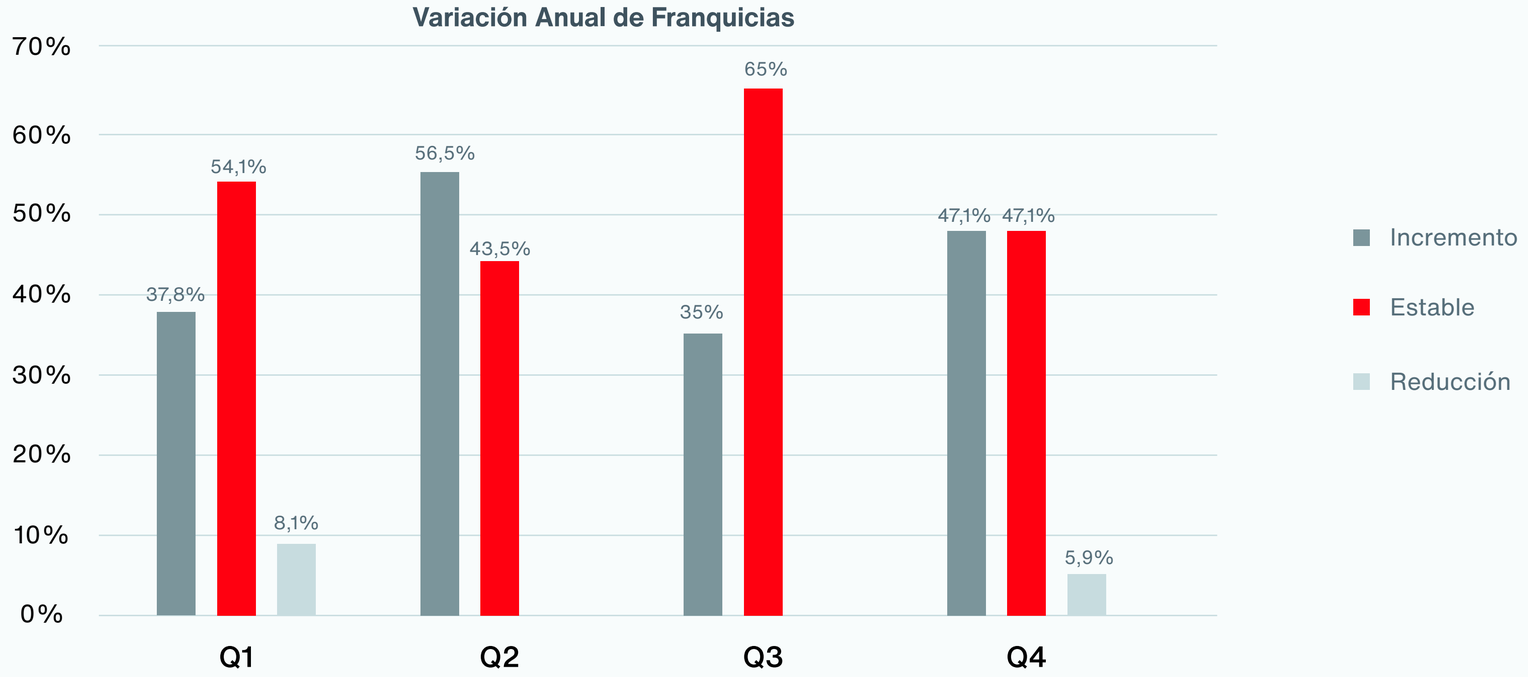
Volumen de primas: El aumento en el volumen de primas ha sido impulsado por la estrategia de las compañías de expandir los límites contratados aprovechando descuentos disponibles. Estas primas, significativamente más bajas que las convencionales, reflejan la estabilización del mercado en este ámbito y la competitividad entre las aseguradoras.

Se prevé que esta tendencia evolucione de manera favorable en el futuro, lo que podría resultar en una reducción aún mayor en las primas. De hecho, se vislumbra la posibilidad de que, en un futuro cercano, cualquier compañía del sector pueda acceder a un seguro de ciberseguridad sin que esto represente una carga financiera excesiva. Este cambio refleja la adaptación del mercado y su respuesta a la creciente demanda y necesidad de protección contra los riesgos cibernéticos.



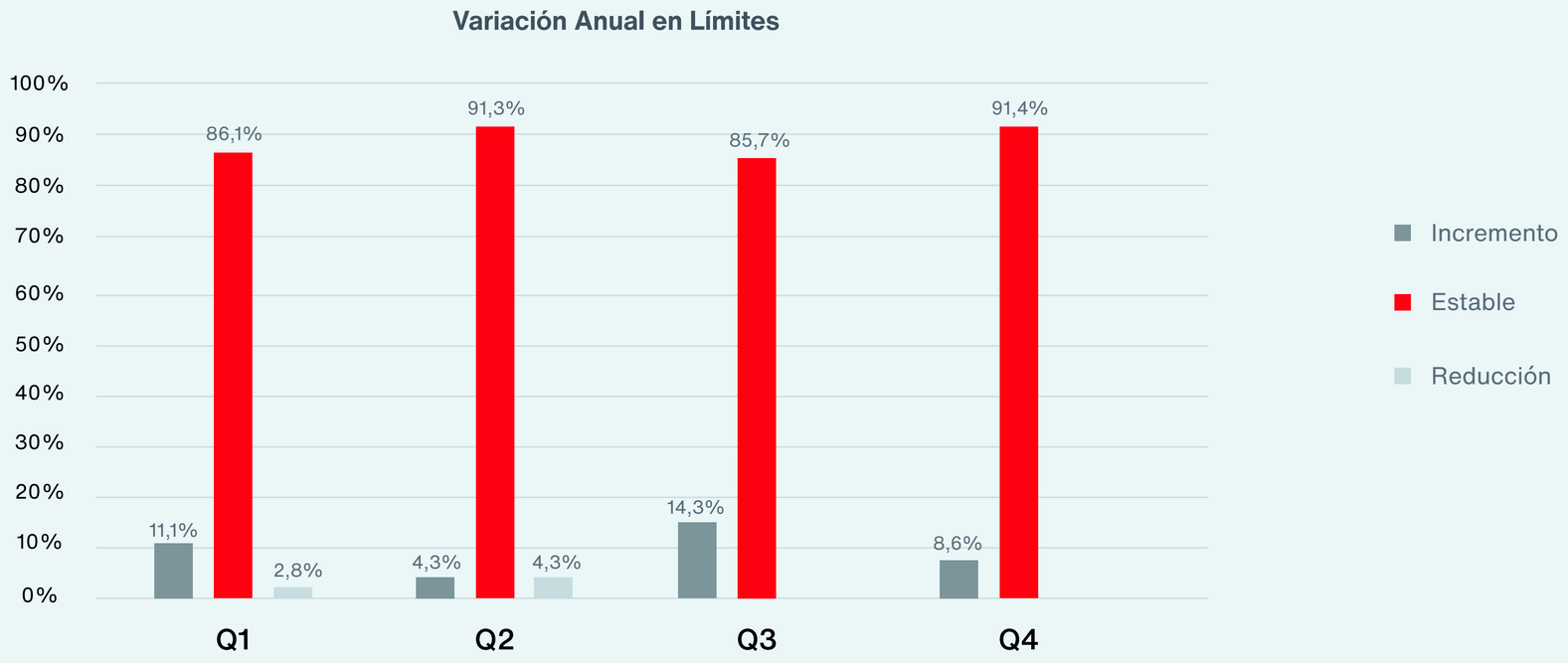
Límites y Retenciones/Franquicias: En este 2023, los clientes han aprovechado la estabilidad del mercado blando. Gracias a la estabilización de las primas, muchos han optado por incrementar los límites contratados o mantener los que tenían anteriormente. Además, las franquicias han experimentado un leve aumento, lo cual se debe al incremento de límites.

Esta tendencia demuestra cómo los clientes están respondiendo positivamente a las condiciones favorables del mercado, ajustando sus coberturas para adaptarse a sus necesidades y al entorno económico actual. El incremento en los límites contratados refleja la confianza de las empresas en la protección ofrecida por los seguros de ciberseguridad, mientras que el leve aumento en las franquicias sugiere una mayor consideración de los riesgos y una estrategia de gestión de riesgos más proactiva por parte de los asegurados.



Durante el proceso de renovación, se observó que aproximadamente el 40% de los clientes experimentaron un aumento en las franquicias. Este incremento se debió tanto al aumento de la siniestralidad como a la acertada decisión de incrementar los límites contratados para una mayor protección. Por otro lado, un 8% de los clientes experimentaron una reducción en sus franquicias, lo que indica una posible mejora en sus perfiles de riesgo o una negociación exitosa con las aseguradoras.

Sin embargo, lo más destacable es que un significativo 52% experimentaron una estabilidad en este aspecto, manteniendo las mismas franquicias que en períodos anteriores. Esta estabilidad es realmente notable, ya que en años anteriores nunca se había presenciado en esta magnitud.



En conclusión, la estabilización de las primas, la introducción de nuevos productos y coberturas específicas, así como una mayor flexibilidad en el proceso de suscripción, han permitido que las empresas de este sector accedan a una protección cibernética más sólida y adaptada a sus necesidades.

Estos cambios han llevado a una mayor conciencia sobre la importancia de la ciberseguridad y a una mejora significativa en la protección ofrecida a las empresas de mercado medio. Sin embargo, aún queda trabajo por hacer en términos de educación y concienciación sobre los riesgos cibernéticos, así como en la adaptación continua de los productos y servicios ofrecidos por las aseguradoras para garantizar una protección efectiva en un entorno digital en constante evolución.

En este sentido, el futuro del mercado de seguros cibernéticos promete seguir ofreciendo soluciones cada vez más accesibles y adaptadas a las necesidades específicas de las empresas, contribuyendo así a mitigar los riesgos y fortalecer la seguridad en línea. La colaboración entre aseguradoras, empresas y organismos reguladores será fundamental para impulsar una cultura de ciberseguridad sólida y sostenible en el mercado medio y más allá.

Inclusión de coberturas de crime: estos productos presentan una particularidad destacada al incluir aspectos relacionados con el ramo de crime, como el fraude de transferencia de fondos y el robo de identidad digital, que para algunas aseguradoras se denominan "Delitos cibernéticos". Esta ampliación de las coberturas muestra una mayor conciencia sobre la importancia de protegerse contra una amplia gama de amenazas cibernéticas, que van más allá de los tradicionales riesgos de ciberseguridad.

Capacidad disponible: Anteriormente, las compañías con una facturación inferior a los 30 millones de euros tenían límites de cobertura bastante discretos. Sin embargo, en la actualidad, estas empresas pueden contratar hasta 5 millones con mayor facilidad. Aunque la mayoría de los productos automáticos en el mercado establecen un límite máximo de 2/3 millones de euros, las aseguradoras muestran una gran flexibilidad para estudiar incrementos adicionales según las necesidades del cliente. Esta mayor capacidad de cobertura refleja una respuesta activa a la creciente demanda de protección contra riesgos cibernéticos por parte de las empresas de mercado medio.

Información de suscripción: aunque la rigurosidad continúa siendo una característica de la suscripción de seguros cibernéticos, se ha observado una mayor flexibilidad en este sentido. Se han creado cuestionarios más sencillos, con aproximadamente 10 preguntas, simplificando así el proceso de suscripción y haciendo que sea más accesible para las empresas de mercado medio. Además, se han introducido cláusulas de compromiso en caso de que el cliente no cumpla con algún requisito, lo que demuestra un enfoque más colaborativo y orientado a soluciones por parte de las aseguradoras. Esta evolución en el proceso de suscripción refleja una mayor comprensión de las necesidades específicas del mercado medio y un esfuerzo por parte de las aseguradoras para adaptarse a ellas. Todo ello contribuye a fortalecer la protección cibernética de las empresas en un entorno cada vez más digitalizado y expuesto a amenazas.

8

Mercado Asegurador: principales cambios y tendencias 2024

Mercado asegurador: principales cambios y tendencias 2024

Durante el último año hubo cierta incertidumbre sobre la continuidad del seguro de Ciber, incluso hubo quien se planteó su desaparición, pero la realidad es que ha sido como el resurgir del Ave Fénix.

Aunque en España hace ya más de una década que se suscriben pólizas de Ciberseguridad, **no fue hasta 2020-2021 cuando realmente la concienciación ante el riesgo ciber en las organizaciones fue real.** A raíz, como principal motivo, del incremento exponencial de la actividad delictiva en la red en entorno de pandemia y la incertidumbre que vivimos, las empresas empezaron a invertir en medidas de seguridad.

Aquellas organizaciones que contrataron póliza de seguro **antes del periodo de pandemia,** cuando todavía las aseguradoras no analizaban las medidas de seguridad de manera tan exigente, se beneficiaron de condiciones competitivas en términos de cobertura y coste de la póliza, y aquellos que además tuvieron que vivir la experiencia de tener que gestionar un incidente de impacto, pudieron comprobar lo rentable de la cobertura comparado con el pago de la prima, ya que, en la mayoría de los casos, el importe de la prima no llegaba ni para hacer frente a los honorarios de los expertos de informática forense.

Las **organizaciones tuvieron que tomar conciencia** a golpe de disgusto y ante la amenaza del riesgo, y empezaron a invertir en ciberseguridad, para preservar sus negocios, al tiempo que pretendían encontrar aseguradoras que les soportaran el riesgo. Las empresas empezaron a preocuparse por analizar sus perfiles de riesgo, cuantificaron el posible impacto que les podía suponer en su cuenta de resultados y tuvieron que diseñar un óptimo programa de seguros para transferir el riesgo al mercado asegurador adecuadamente y de manera más ordenada.

Se produjo un punto álgido en el mercado a finales de 2022, donde los incrementos de prima no cesaban, las coberturas cada vez estaban más restringidas y la exigencia por parte de las aseguradoras en las medidas de seguridad mínimas que tenían establecidas en sus procesos de suscripción, era mayor.

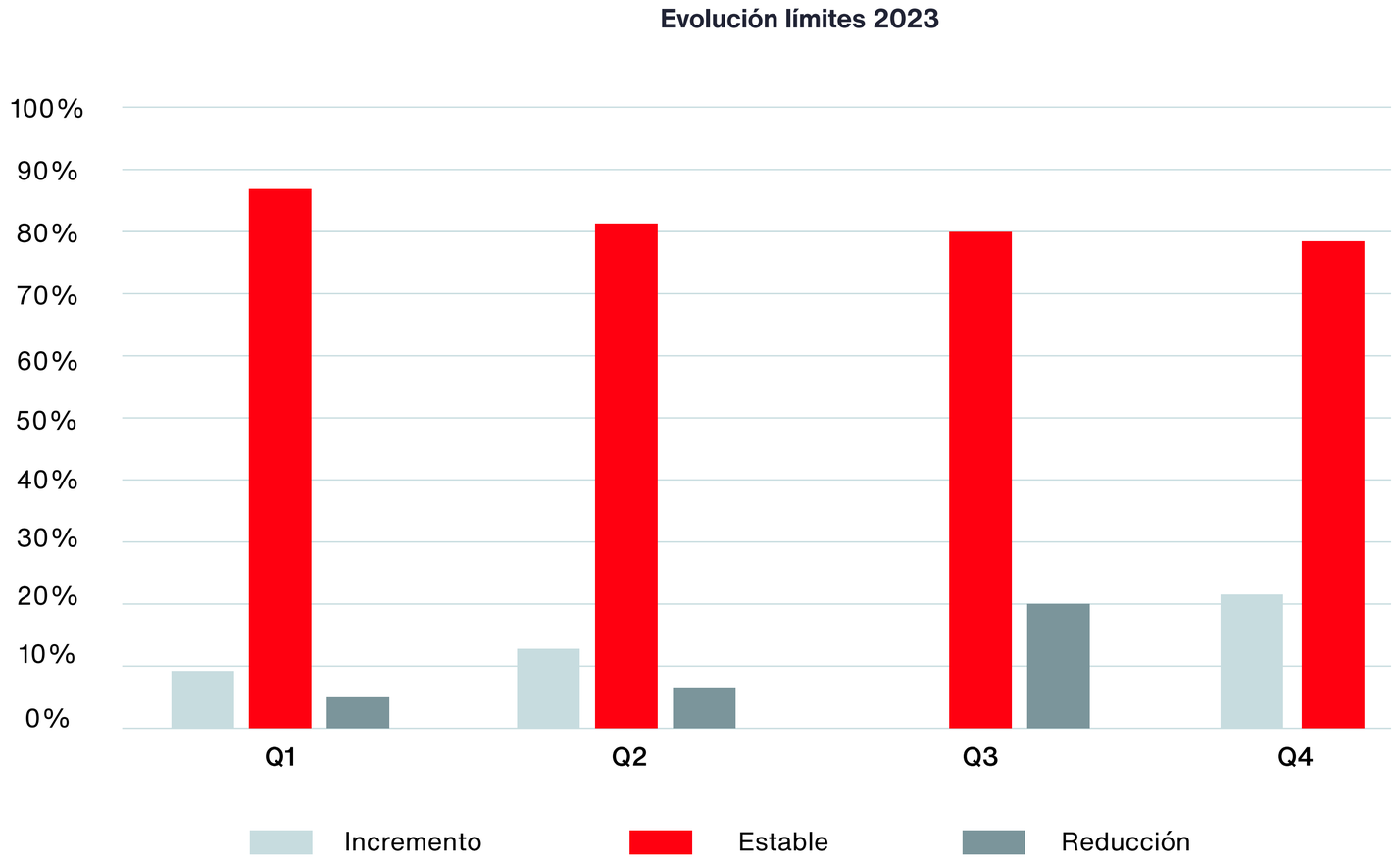
Llegados a este punto se plantea la continuidad de la cobertura. Era tan cara la capacidad que se podía obtener en el mercado asegurador, que hubo organizaciones que optaron por reducir los límites contratados o incluso algunas, dejaron de contratarlos y correr el riesgo con la inconsciencia de asumir la pérdida en caso de ataque, sin tan siquiera saber cuál era su potencial. En ese momento se pensó que, dado que la siniestralidad no frenaba, tampoco había freno con el incremento exponencial de las primas y algunos llegaron a pensar que la cobertura aseguradora dejaría de existir.

Sin embargo, el número de pólizas se sigue incrementando exponencialmente al igual que el volumen de primas que tampoco ha cesado, alcanzando un volumen aproximado de 160-175M EUR en 2023, un crecimiento del 25% sobre el año anterior. Se debe tener en cuenta que una parte de este volumen viene motivado por el incremento de las primas que ha arrastrado el sector en los últimos años, y lo cierto es que todavía es un mercado poco maduro donde hay todavía un alto volumen de empresas que no transfiere el riesgo al mercado asegurador y por tanto con mucho potencial para crecer. **Con esta premisa, muchas aseguradoras que no suscribían el riesgo vieron la oportunidad de hacerlo.**

En España han desembarcado nuevas aseguradoras durante el 2023 e inicio de 2024, suscribiendo el riesgo de Ciber en primario y con condiciones muy agresivas, otras han entrado de manera más moderada participando únicamente en excesos, pero con una alta competitividad de prima. Y aseguradoras que habían dejado de suscribir parcialmente, han revisado nuevamente sus políticas de suscripción. Estamos viendo que, en general, el mercado está apostado por crecer en el ramo de Ciber y lo está haciendo con fuerza.

En el mercado español, hemos pasado de poder contar con los dedos de un mano las aseguradoras que suscribían riesgos en primario en 2022, y considerar todo un éxito contar con una opción de primario, a triplicar el número de aseguradoras que quiere crecer en este ramo. Para ello, se está invirtiendo tanto en equipos de suscripción como en IA para tratar de poder hacer una suscripción más rigurosa y eficiente basadas en datos para convertir su ratio de rentabilidad en cifras positivas.

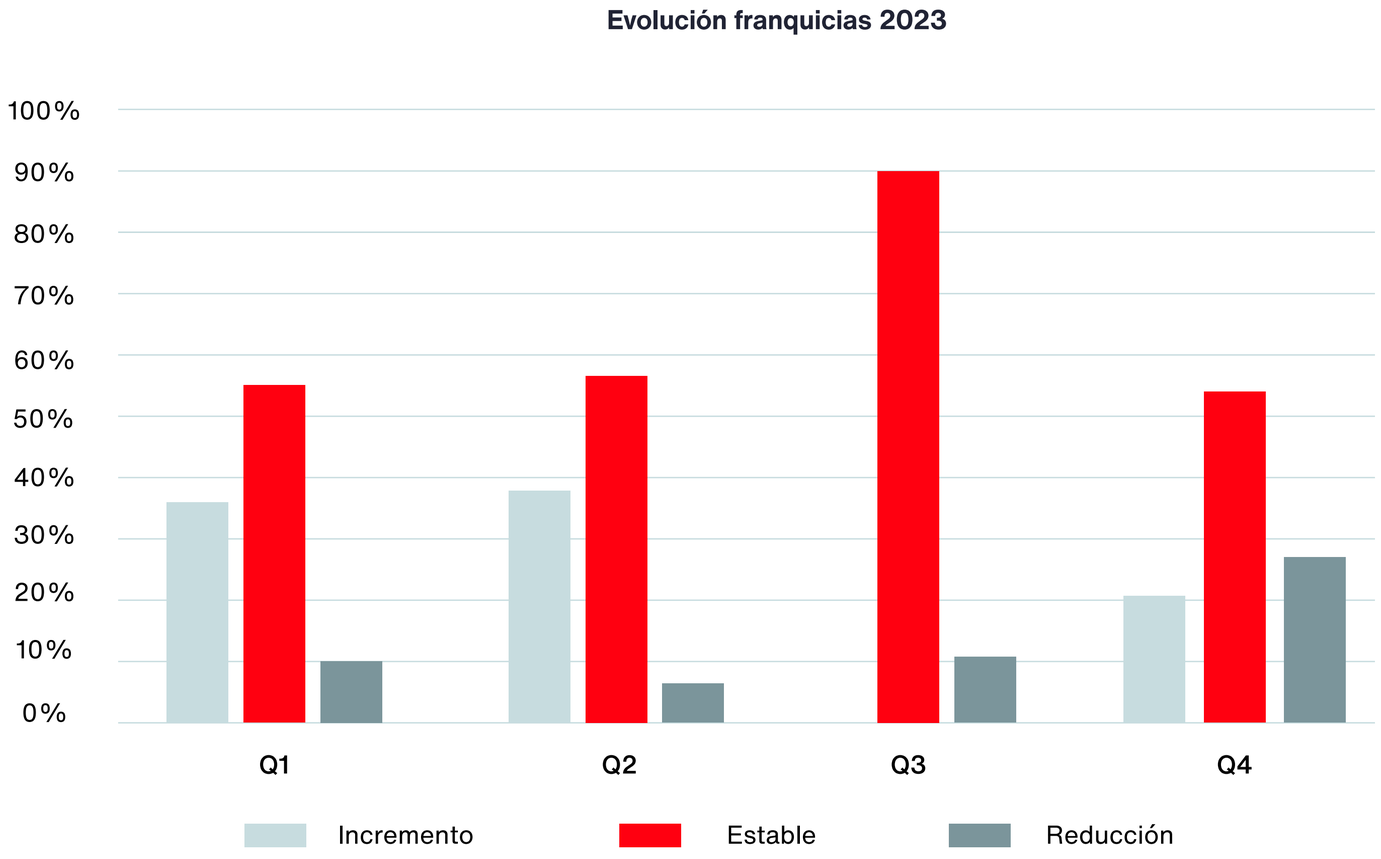
Es la **ley de la oferta y la demanda.** Más aseguradoras, más capacidad que se oferta y todavía muchas empresas sin contratar la cobertura que la están demandando. Todo esto ha propiciado que desde finales de 2023 ya no hablemos de “mercado duro” sino de “oportunidad” para la contratación de una póliza nueva, incrementar un límite o recuperar una cobertura perdida en el pasado.



El mercado asegurador es un entorno dinámico y en constante evolución, donde las innovaciones tecnológicas desempeñan un papel fundamental en la transformación de la industria. Conforme nos adentramos en el año 2024, es crucial comprender las tendencias tecnológicas emergentes que están redefiniendo la manera en que las compañías de seguros operan y cómo interactúan con sus clientes.

La realidad es que, ante el **incremento de la competencia,** las aseguradoras que han sido pioneras en la suscripción del riesgo ciber en el mercado español y que son las que mayor siniestralidad están soportando, o se adaptan a la competencia, y **frenan los incrementos de primas o mueren por la pérdida de competitividad.** No les queda otra que competir además de en precio, en coberturas si quieren seguir creciendo y mantenerse en el mercado. Se habla ya de nuevas coberturas referentes a los riesgos emergentes y cada vez más las aseguradoras ofrecen servicios adicionales para tener monitorizados a sus clientes en aras de detectar los incidentes de una manera temprana y poder mitigar cuanto antes el impacto en caso de incidente.

De momento, todo en beneficio de los asegurados. Se ha generado competencia, se reducen las primas, hay más capacidad, flexibilidad en la negociación de las franquicias y ante algunas coberturas. El ransomware que se venía limitando en los contratos, vuelve a poderse negociar sin sublímite. Y aquellas organizaciones que redujeron los límites en años anteriores, los están volviendo a incrementarlos, dado el entorno favorable.



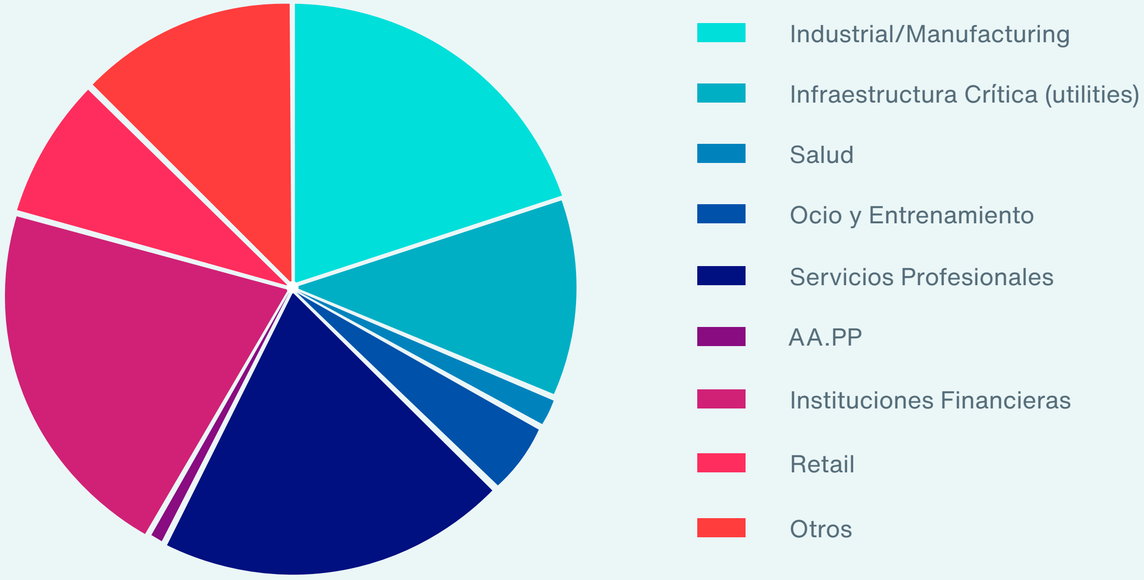
Se están actualizando los contratos de seguros, incluyendo revisiones favorables, nuevas coberturas, mayor amplitud de definiciones. Aunque sigue preocupando y siendo un punto crítico para las aseguradoras, la exclusión de guerra e infraestructuras críticas, para tratar de contener un ataque gubernamental, así como el riesgo sistémico.

La IA también está teniendo mucho que ver. Nuevas tecnologías permiten a las aseguradoras automatizar una amplia variedad de procesos, desde la evaluación de riesgos y la fijación de precios hasta la detección de fraudes. Además, la capacidad de la IA para analizar grandes volúmenes de datos permite una personalización aún mayor de las ofertas de seguros, lo que mejora la experiencia del cliente y aumenta la eficiencia operativa. La IA y el aprendizaje automático han evolucionado de manera significativa en los últimos años y se espera que sigan siendo uno de los pilares fundamentales en el mercado asegurador en 2025.

A todo lo anterior, le sumamos el hecho diferenciador de que hay una mayor conciencia del riesgo y por tanto mayor inversión, con lo que las empresas están mejor protegidas. Además, creen en la importancia de la transferencia del riesgo al mercado asegurador y lo más importante es que el riesgo Ciber es el que más preocupa al Consejo de Administración, por lo que su involucración aumenta exponencialmente.

El número de entidades en las que la función de ciberseguridad depende directamente de la Dirección General ha aumentado un 12%, según muestra el III Termómetro de la ciberseguridad en el Sector Asegurador. Este hecho muestra la relevancia que los asuntos de ciberseguridad cobran dentro de la agenda de la Dirección General de las compañías.

El incremento de riesgos relacionados con seguridad cibernética y compromiso de datos, así como la mayor involucración del C-Suite en la gestión del riesgo asociado a la continuidad del negocio, han llevado al aumento en la compra de pólizas de ciber riesgos.



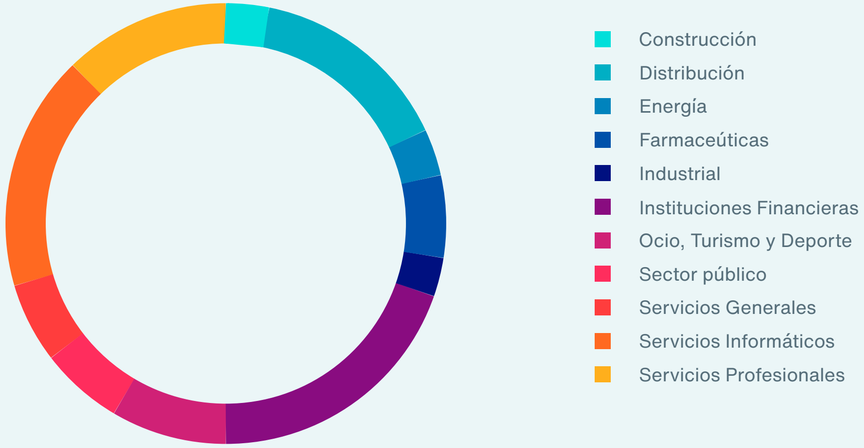
El volumen de primas sigue creciendo.

En el último año se ha incrementado aproximadamente un 25% el volumen de primas en España. En cuanto a los sectores de actividad, las infraestructuras críticas siguen liderando en términos de concienciación sobre ciberseguridad y contratación de seguros cibernéticos. También se ha observado un aumento significativo en el sector de Instituciones Financieras y los servicios profesionales, especialmente en consultoría de tecnologías de la información. Y el sector industrial que había experimentado una disminución gradual en los últimos años, vemos que está repuntando con la llegada de la estabilización del mercado.

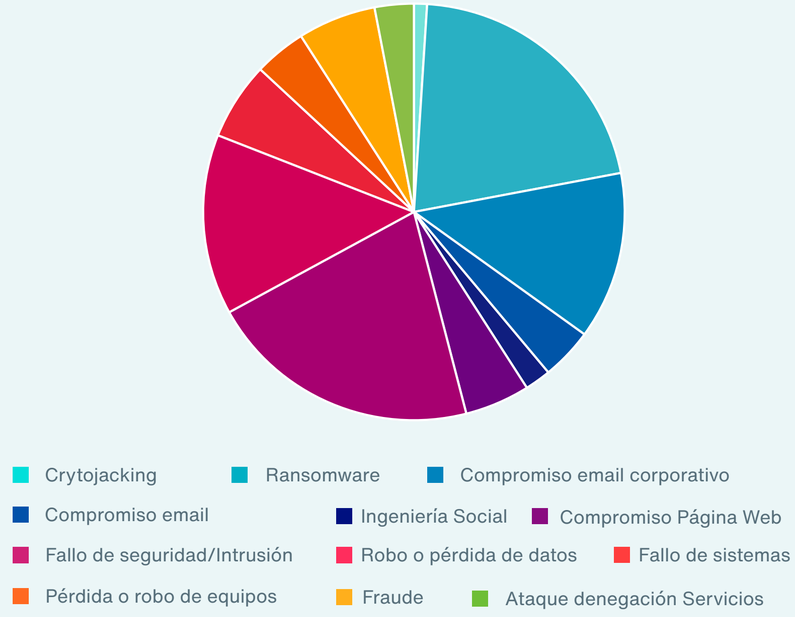
En determinados sectores considerados agravados, como el sector público, la sanidad, la aviación, la educación, las telecomunicaciones y la industria manufacturera, la capacidad disponible puede ser mucho menor debido a la falta de apetito del mercado. Sin embargo, las aseguradoras mantienen el rigor en la suscripción de sus riesgos, mientras siguen de cerca los acontecimientos mundiales que pueden afectar a los siniestros cibernéticos.

No obstante, a pesar de la gran competencia y de la reducción de las primas que estamos viendo en varios sectores de actividad, la realidad es que **los incidentes no cesan y por tanto las aseguradoras siguen haciendo frente al pago de siniestros.**

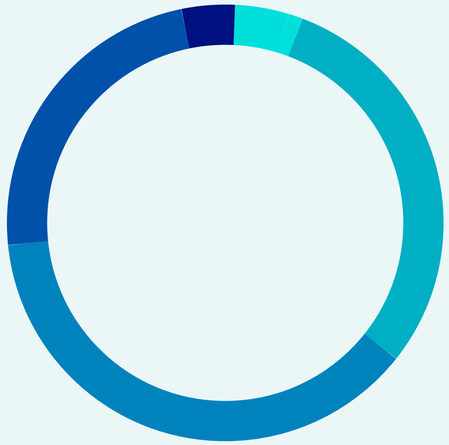
Los sectores más afectados por siniestralidad coinciden con los sectores que más contratan y que son manufacturing, servicios profesionales e Instituciones Financieras. Comparativamente con respecto a 2022, hubo también siniestralidad elevada en el sector de la Construcción.



El volumen de siniestros ha disminuido en 2023 y aunque parece que en ciertos riesgos hay un mayor control y las estadísticas dicen que hay una estabilidad, incidentes de ransomware y brechas de seguridad junto con compromiso de datos a través de técnicas como phishing, smishing y similares siguen aumentando de manera exponencial año tras año como podemos ver en el grafico siguiente.



La siniestralidad en seguros cibernéticos afecta principalmente a clientes con una facturación por encima de 250M€, representando más del 75% de los siniestros, mientras que las pequeñas y medianas empresas (pymes) representan solo el 4%. Esto no nos sorprende dado que más del 50% de las pólizas contratadas corresponden a empresas que facturan más de 1000M€.



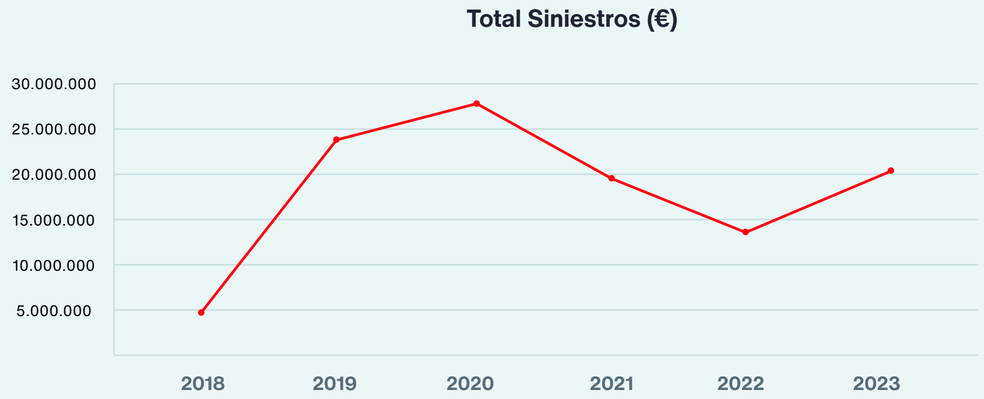
Cliente Multinacionales Globales
Grandes cuentas
Mercado medio
Personales
Pymes

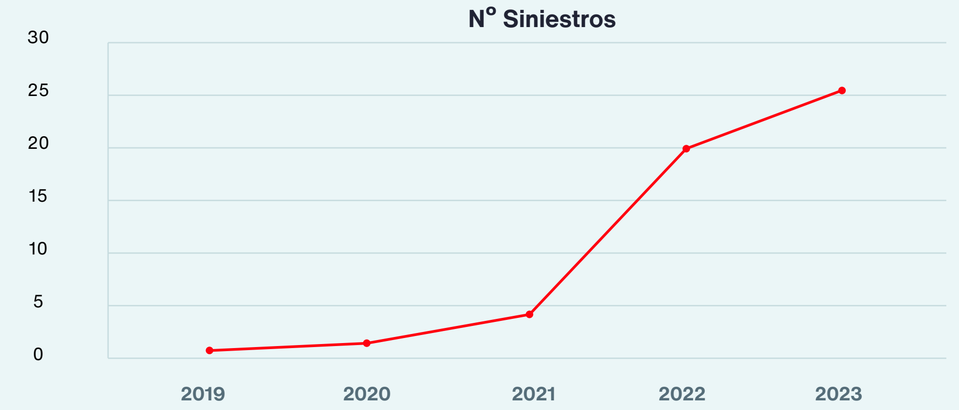
Según muestra la III edición del Termómetro de la ciberseguridad en el sector asegurador español, realizada por ICEA en colaboración con Deloitte, si bien la mayoría de las entidades cuentan con un plan de respuesta ante incidentes, casi el 50% de estas afirman haber sufrido algún tipo de brecha de seguridad.

En la situación actual, los ataques de denegación de servicio y los ataques de malware/ransomware, siguen siendo las principales preocupaciones de los responsables de seguridad dado el alto impacto que pueden llegar a tener estos en los procesos de negocio de las Entidades.

Si analizamos el coste medio de los siniestros en España, observamos que se ha reducido significativamente de los años más duros (2019 y 2020) que fueron los que iniciaron el ciclo de mercado duro.

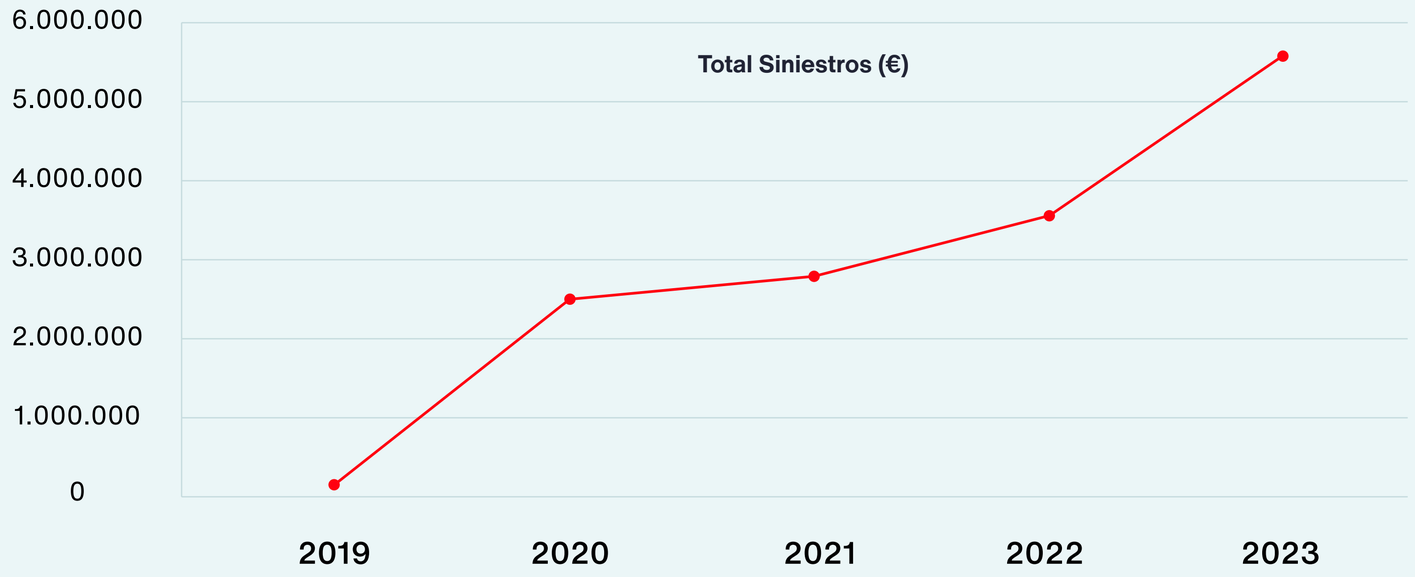
Se observa también un cambio de tendencia y un incremento en la frecuencia de los siniestros de responsabilidad civil a causa de un evento cibernético, así como un incremento significativo en el coste de estos.



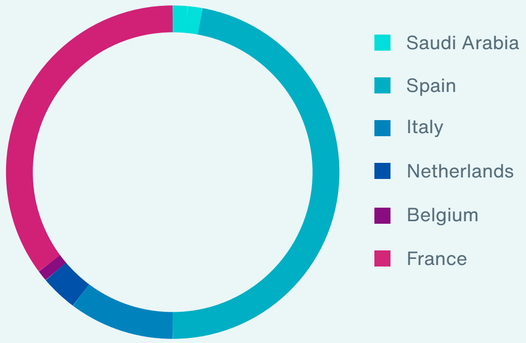


Y aunque el ransomware sigue siendo el siniestro por excelencia, empieza a preocupar el importante incremento de siniestros derivado de un data breach. Las tan temidas class actions ya han llegado a España y se espera un incremento en las mismas en un futuro cercano.

Por otra parte, en 2024 se espera que haya más fugas de datos en las que intervenga el elemento humano. Los ciberdelincuentes saben que su mayor oportunidad de éxito consiste en jugar con las emociones humanas, y por eso utilizan la ingeniería social. Con la profesionalización de la ciberdelincuencia y el auge de la IA, ahora los ciberdelincuentes pueden realizar ataques de ingeniería social muy convincentes y complejos. Así es más difícil distinguir entre mensajes auténticos y maliciosos. Además, cada vez hay más formas de comunicarse, por lo que estas amenazas se propagan más rápido que nunca.



Por último y si comparamos España con otros países de EMEA, se observa que España es uno de los países con siniestralidad más elevada de EMEA.



La **profesionalización de la ciberdelincuencia avanza con paso firme** y va a alcanzar un nuevo nivel de madurez en 2024 gracias a la aparición de la IA y de otras potentes tecnologías recientes.

Las organizaciones no deben cesar en su inversión en seguridad, ya que los avances de los últimos años son solo el principio de un futuro en el que los ciberdelincuentes van a desarrollar métodos cada vez más sofisticados para lograr sus objetivos.

8

A medida que surgen nuevas vulnerabilidades, vectores de ataque y variantes de malware, algunas amenazas pasan a primer plano mientras que otras pasan de moda por un tiempo. En 2024, los actores de las amenazas cibernéticas se inclinan en gran medida hacia ataques sofisticados que han demostrado una buena tasa de éxito y retorno de la inversión (ROI) en el pasado. **Destacamos algunas amenazas en 2024:**

01 Ransomware:

Ha sido una de las principales preocupaciones de seguridad desde hace varios años. Cada vez más, los atacantes están pasando del cifrado de datos a directamente robarlos y exigir un rescate para no revelarlos públicamente.

02 Cadena de suministro:

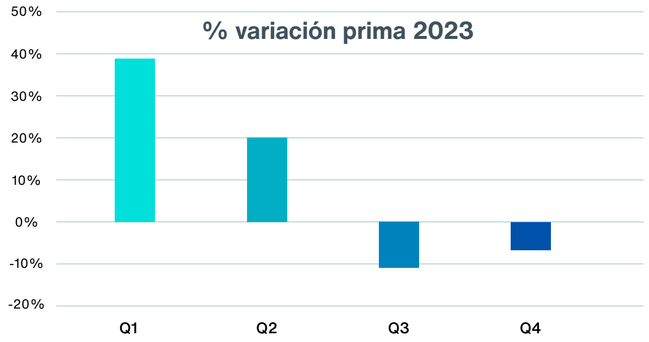
Los ataques importantes como el hackeo de SolarWinds demostraron la eficacia potencial y la escala de un ataque a la cadena de suministro. Las amenazas a la cadena de suministro incluyen explotar las relaciones de confianza entre organizaciones y trabajar para inyectar vulnerabilidades o códigos maliciosos en bibliotecas y dependencias de código abierto comúnmente utilizadas dentro de las aplicaciones corporativas.

03 Ataques multi-vector:

Los ataques multi-vector combinan múltiples técnicas y vectores de ataque dentro de una sola campaña de ciberataque. Los actores de amenazas cibernéticas están usando estas tácticas porque hacen que los ataques sean más difíciles de detectar y contener, lo que aumenta la probabilidad de éxito.

Las brechas de seguridad, la falta de talento, la externalización del servicio, el uso de la IA, la ciberguerra y las aplicaciones móviles, son algunos de los desafíos a superar en 2024.

Sin embargo, la realidad es que en los últimos meses estamos viendo un **descenso de las primas de seguro en el mercado asegurador, debido principalmente al incremento de la competencia, mayor número de players en el mercado, mayor capacidad, la constante**



evolución en ciberseguridad de algunas empresas, que hace que algunas organizaciones estén consiguiendo condiciones de renovación de sus contratos de póliza de ciberseguridad muy competitivas.

¿Mercado blando? Se habla del mercado blando por la enorme competencia y la bajada de las primas, pero los más cautos no se atreven a mencionar el mercado blando cuando la siniestralidad no cesa y la inteligencia artificial, en este caso, se está convirtiendo en amenaza. Si continúa este nueva tendencia del 2024 en incremento en número y complejidad de siniestros, es posible que volvamos a vivir un ciclo de mercado duro. Lo que sí podemos afirmar en la actualidad es que nos encontramos en un momento favorable para la contratación de pólizas, incremento de capacidades, diseño de condicionados, y sobre todo y como gran novedad frente a lo que hemos vivido en años anteriores, algunas aseguradoras empiezan a estar abiertas a ofrecer acuerdos de larga duración a sus asegurados, muestra clara de que el mercado quiere perdurar en el tiempo y apostar por las relaciones a largo plazo entre bróker-asegurador y asegurado.

¿Cuánto tiempo será sostenible esta situación?, es una incógnita. Algunas aseguradoras han llegado para quedarse y otras no correrán la misma suerte.

El desafío para 2025 es mantener este equilibrio y seguir ofreciendo soluciones efectivas a medida que evolucionan las amenazas cibernéticas.

El futuro es incierto y aunque ahora estemos viviendo un momento en el mercado asegurador más estable y con muchos brotes verdes para según que riesgos, la realidad es que no sabemos cuánto tiempo el mercado asegurador será capaz de aguantar esta situación.

¿Quién va a aprovechar mejor el poder de las nuevas tecnologías y la piscología del comportamiento humano: las empresas y el mercado asegurador o los ciberdelincuentes?

9

Metodología

9 Metodología

Este Estudio ha sido elaborado con información propia y datos del mercado asegurador obtenidos mediante cuestionarios confidenciales, así como mediante entrevistas directas con 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 tres 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 2023.

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 2023, 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 2023, del seguro Ciber en España.

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.

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

Contact Us

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

Carlos Bereciartua González
Head of Cyber Consulting
+34 683 299 813
carlos.bereciartua@aon.es