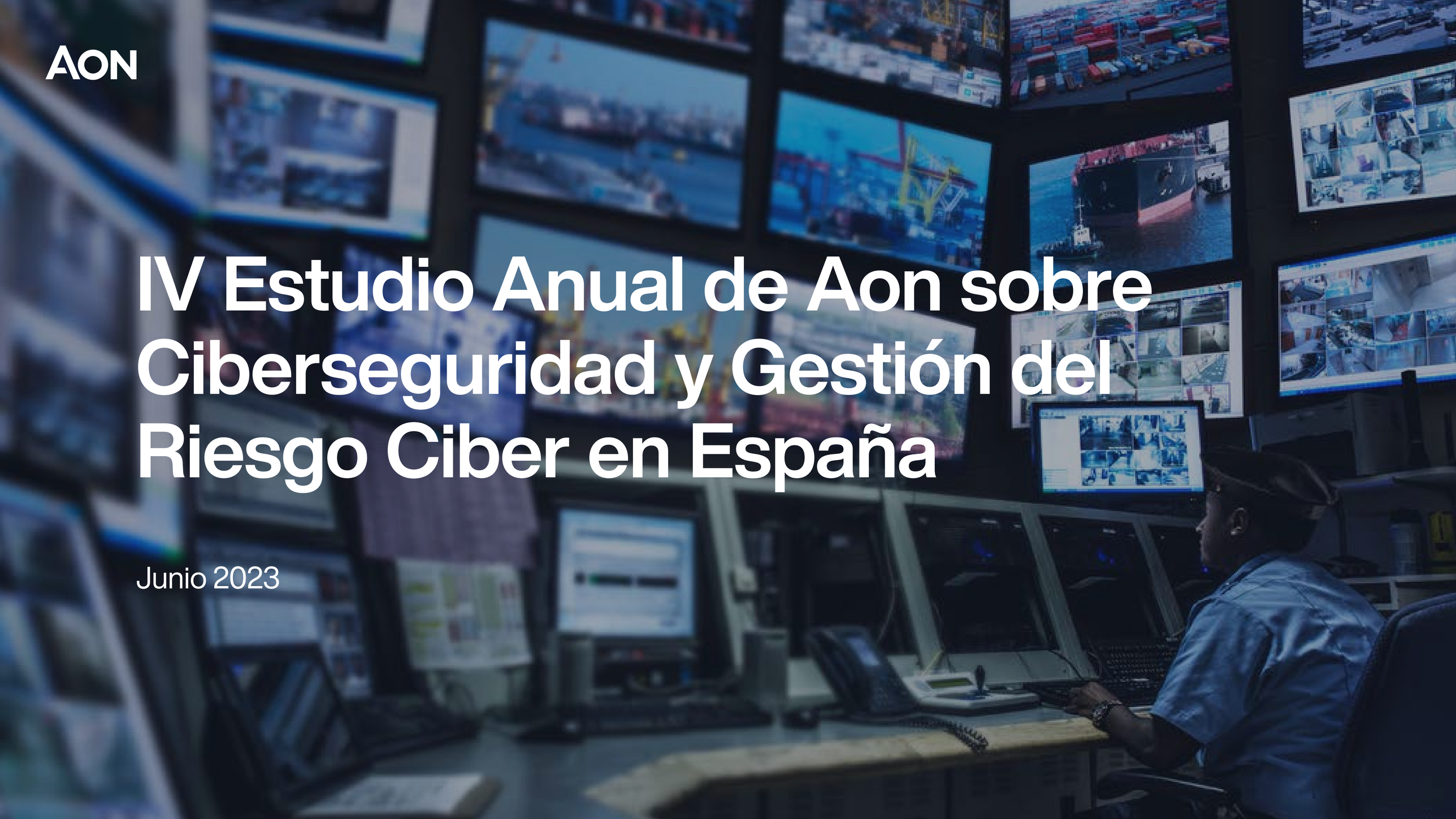


IV Estudio Anual de Aon sobre Ciberseguridad y Gestión del Riesgo Ciber en España

Junio 2023

Entidades colaboradoras

ANDERSEN

TOKIO MARINE HCC

Allianz

AXA

beazley

CHUBB

AIG

QBE

GARRIGUES

ZURICH

Índice

1

Resumen Ejecutivo

1 Resumen Ejecutivo

La ciberseguridad es una prioridad empresarial. En los últimos años hemos visto cómo el tema ha pasado de ser responsabilidad únicamente del departamento de Sistemas, a ser prioridad en los Consejos de Administración. Principalmente, este cambio ha venido motivado por las siguientes cinco palancas o necesidades:

- Reducir la exposición y el impacto de posibles incidentes de ciberseguridad
- Adaptarse a nuevas regulaciones, cada vez más exigentes en materia de ciberseguridad
- Cumplir con los requisitos de los distintos grupos de interés (stakeholders) en la cadena de valor
- Aportar seguridad y confianza, tanto interna como externa, en todo proceso de transformación digital
- Alinearse con las mejores prácticas/estándares en materia de seguridad

En esta esta cuarta edición del Informe de Ciberseguridad, analizaremos la evolución y la gestión del riesgo en España desde diferentes prismas: cambios normativos, inversión en ciberseguridad, tendencias del mercado asegurador y evolución de la siniestralidad, entre otros.

Después del panorama descrito en las ediciones anteriores, afrontamos el año 2023 con un mejor pronóstico, aunque con la cautela de seguir siendo un riesgo que evoluciona muy rápidamente con continuas amenazas e incertidumbres. No obstante, veremos que los aspectos que apuntamos en ediciones anteriores, en cuanto a conciencia del riesgo, inversión en su preservación y la adecuada transferencia de este, se han convertido efectivamente en esenciales.

El volumen de primas del mercado asegurador sigue aumentando y en España desde el año pasado ya supera los 100M EUR, habiendo crecido este año más de un 50% para algunas aseguradoras. La severidad que hemos vivido en el 2021 y 2022 parece haber llegado a un punto de estabilización. El reto al que nos enfrentamos en este 2023 es mantener ese equilibrio, que se puede ver rápidamente truncado por un ciberataque masivo o un evento sistémico.

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 2022, ha sido el año en el que cambió el marco regulador de la ciberseguridad, destacaremos tanto a nivel mundial, como europeo.

- La **Directiva NIS2,** que amplía el ámbito de aplicación respecto a la directiva NIS 1 con una intensificación de las obligaciones en materia de ciberseguridad, donde introduce la responsabilidad directa órganos de administración.
- **Reglamento DORA**, que viene a unificar los criterios relativos a la ciberseguridad que se aplican a las distintas entidades del sector financiero y asegurador, que previamente estaban dispersos entre múltiples normas y Directrices de las autoridades europeas.
- **CIRCIA** donde destacamos la obligatoriedad de. las entidades gestoras de infraestructuras críticas a comunicar.

Desde el punto de vista prospectivo, haremos hincapié en la nueva normativa que se espera sea aprobada en los próximos años:

- Propuesta de **Reglamento de Inteligencia Artificial (AI Act).** A lo largo del 2023 se espera que vea la luz esta norma que va a tener un efecto transversal en el cual también hay implicados elementos relativos a la ciberseguridad de los sistemas de IA.
- Reglamento **eIDAS 2** que pretende fomentar la adopción de un sistema de identidad digital único a nivel europeo.
- Sin embargo, la norma con más impacto y que será aprobada en 2023 será la nueva **regulación en materia de ciberseguridad de las empresas cotizadas impulsada por la SEC.**

Mercado Asegurador: El aumento de las primas en 2022 fue una realidad generalizada en todos los sectores y actividades. Si bien algunas industrias pudieron verse más afectadas que otras, pero la mayoría de los clientes han experimentado subidas considerables, donde se registraron incrementos superiores al 100% en algunos casos.

Se siguieron experimentando cambios en las estructuras de los programas para mantener el riesgo, con reducción significativas de capacidades. Se observó un notable incremento en las retenciones; aproximadamente el 60% de los clientes experimentaron un incremento en sus franquicias.

En función del volumen de facturación, se observa un considerable incremento de contratación de pólizas en el número de empresas que superan los 250 millones de euros en comparación con el periodo anterior.

Por sector de actividad, el de infraestructuras críticas continúa liderando 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.

A lo largo de este 2023 estamos observado un cambio de tendencia hacia un mercado más estable y favorable. Son varios los factores de mercado que contribuyen a este cambio de tendencia.

- **Concienciación del riesgo y fuertes inversiones en medidas de seguridad:** Las empresas han tomado conciencia del riesgo y han invertido en medidas de seguridad.
- **Mejora de rentabilidades:** Si analizamos la evolución de las primas vs la siniestralidad ésta continúa siendo de alto impacto, pero ha frenado la frecuencia.
- **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 que ha llevado a una mayor competencia provocando una desaceleración de las tasas.

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, que sigue provocando limitaciones en las garantías.

Veremos que el entorno geopolítico, el riesgo sistémico y la gestión de los datos biométricos, junto con el evento de ransomware, son aspectos que siguen preocupando a los mercados e influyen a la hora de negociar la transferencia del riesgo.

2

2022, El año en el que cambió el marco regulador de la ciberseguridad en la Unión Europea

Vicente Moret, Letrado de las Cortes Generales of Counsel Andersen, y **Cristina Durante,** Associate en Andersen.

2022, EL AÑO EN EL QUE CAMBIÓ EL MARCO REGULADOR DE LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA.

2.1. Contexto.

2022 ha sido un año especialmente importante en cuanto al ámbito de la regulación de la seguridad digital, y, en general, para la progresiva incorporación de elementos legales al sector de la ciberseguridad. Varias razones explican este cambio impulsado especialmente por la Unión Europea y Estados Unidos. Por un lado, en el nivel **geopolítico**, es evidente que la invasión de Ucrania y el riesgo real de acciones hostiles desde el ciberespacio contra operadores de servicios esenciales, han impulsado una aceleración en la adopción de nuevas regulaciones. Por otra parte, el **ciberdelito** ha aumentado de forma creciente su impacto sobre empresas y ciudadanos, especialmente por la amenaza de la extorsión digital (ransomware).

Por último, y con carácter general, conviene tener en cuenta que la acelerada transformación digital que estamos viviendo hace que el **derecho asuma la obligación de regular el ámbito digital** que ya es decisivo para la economía, las empresas, y en general para nuestra vida como individuos y como ciudadanos, en la medida en que nuestros **derechos fundamentales y libertades públicas** también deben quedar garantizados en el ciberespacio mediante la garantía de la ley. Los Estados y la Unión Europea son conscientes de ello y han acelerado la ordenación general sobre la economía digital, los datos o la inteligencia artificial, y también la regulación específica en materia de ciberseguridad como garantía de todo el sistema.

Esta aceleración en el número, intensidad y relevancia de las normas adoptadas en 2022 es la mejor demostración del cambio de paradigma en cuanto a la regulación del ciberespacio, que establece un nuevo contexto **con más obligaciones y con más garantías de derechos.** En ese nuevo marco regulatorio, el elemento central sobre el que pivota la aproximación legal a las normas aprobadas en 2022 es el de riesgo, y más en concreto el de **riesgo tecnológico.**

Por otra parte, son varias las **tendencias comunes** de esas nuevas regulaciones que se pueden señalar como esenciales. Entre otras, cabe destacar la obligatoriedad de adoptar modelos de **gobernanza** de la ciberseguridad en las empresas, especialmente las que son operadoras de servicios esenciales; el aumento de la exigencia de **responsabilidad** en esta materia al nivel del consejo de administración; o los aspectos referidos a la seguridad de las **cadenas de suministro** y terceros proveedores.

Por último, se puede afirmar que la seguridad digital se entiende, en estas nuevas, normas como un **asunto no exclusivamente tecnológico,** en el cual confluyen aspectos geopolíticos, legales, normativos y conductuales, haciendo de la gobernanza de la ciberseguridad un ámbito de adaptación necesario y complejo por parte de las empresas.

2022

El año en el que cambió el marco regulador de la ciberseguridad en la Unión Europea

2.2. Novedades regulatorias.

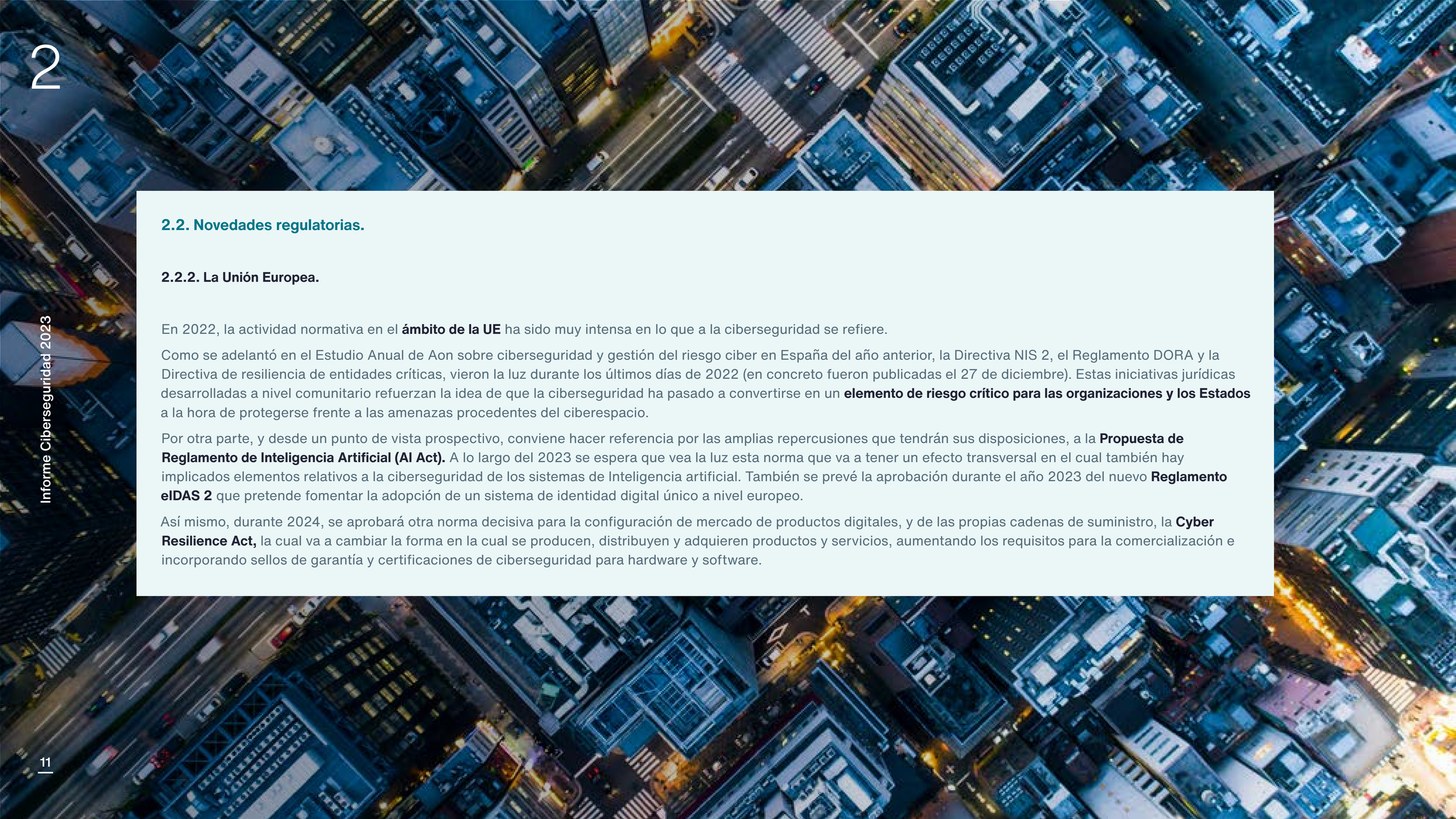
2.2.1. Estados Unidos.

En cuanto a los Estados Unidos, de forma muy breve hay que señalar que las novedades durante 2022 y lo que llevamos de 2023 son numerosas. Cabe destacar por su relevancia la nueva **Estrategia Nacional de Ciberseguridad** de marzo de 2023, por su alto impacto en cuanto al modelo de gobernanza que recoge y porque marca las directrices regulatorias que se plasmarán en normas concretas. En este sentido la Estrategia señala la protección del ciberespacio como una cuestión de seguridad nacional, así como la importancia de la colaboración público-privada y la responsabilidad de las empresas de software por lo fallos en la seguridad de sus productos. También la necesidad de aprobar nuevas normas para impulsar los esfuerzos en materia de ciberseguridad con respecto a las empresas, superando así los esquemas basados en la autorregulación.

Además, en marzo de 2022 se aprobó la ley **“CIRCIA”** (Cyber Incident Reporting for Critical Infrastructure Act). Esta ley obligará a las entidades gestoras de infraestructuras críticas a notificar los ciberincidentes en un plazo de 72 horas.

No obstante, la norma que va a tener más impacto y que será aprobada en 2023 previsiblemente, es la nueva regulación en materia de **ciberseguridad de las empresas cotizadas impulsada por la SEC.** La propuesta tiene dos componentes básicos, la notificación obligatoria de incidentes de ciberseguridad en un formulario 8-K en los cuatro días hábiles siguientes al incidente y la obligación de publicación de información sobre las políticas de la empresa para gestionar los riesgos de ciberseguridad, con el objeto de que sea el mercado el que analice si son las adecuadas o no.

En conclusión, aunque con las peculiaridades propias del marco normativo norteamericano más centrado en normas y recomendaciones de cumplimiento voluntario, lo cierto es que el mapa regulatorio en materia de ciberseguridad ha variado sustancialmente en Estados Unidos, tanto en el nivel federal, como en el estatal.



2.2. Novedades regulatorias.

2.2.2. La Unión Europea.

En 2022, la actividad normativa en el **ámbito de la UE** ha sido muy intensa en lo que a la ciberseguridad se refiere.

Como se adelantó en el Estudio Anual de Aon sobre ciberseguridad y gestión del riesgo ciber en España del año anterior, la Directiva NIS 2, el Reglamento DORA y la Directiva de resiliencia de entidades críticas, vieron la luz durante los últimos días de 2022 (en concreto fueron publicadas el 27 de diciembre). Estas iniciativas jurídicas desarrolladas a nivel comunitario refuerzan la idea de que la ciberseguridad ha pasado a convertirse en un **elemento de riesgo crítico para las organizaciones y los Estados** a la hora de protegerse frente a las amenazas procedentes del ciberespacio.

Por otra parte, y desde un punto de vista prospectivo, conviene hacer referencia por las amplias repercusiones que tendrán sus disposiciones, a la **Propuesta de Reglamento de Inteligencia Artificial (AI Act).** A lo largo del 2023 se espera que vea la luz esta norma que va a tener un efecto transversal en el cual también hay implicados elementos relativos a la ciberseguridad de los sistemas de Inteligencia artificial. También se prevé la aprobación durante el año 2023 del nuevo **Reglamento eIDAS 2** que pretende fomentar la adopción de un sistema de identidad digital único a nivel europeo.

Así mismo, durante 2024, se aprobará otra norma decisiva para la configuración de mercado de productos digitales, y de las propias cadenas de suministro, la **Cyber Resilience Act,** la cual va a cambiar la forma en la cual se producen, distribuyen y adquieren productos y servicios, aumentando los requisitos para la comercialización e incorporando sellos de garantía y certificaciones de ciberseguridad para hardware y software.

2.3. La directiva de la NIS 2: La intensificación de las obligaciones de ciberseguridad para las empresas.

La Comisión ya reconocía en la Estrategia de Seguridad 2020-2025 la necesidad de revisar la Directiva NIS 1 dando un enfoque más coherente, uniforme y coordinado que armonizara los requisitos de ciberseguridad y la implementación de las medidas de seguridad digital en el conjunto de los Estados miembros.

Desde el pasado 16 de enero está en vigor la Directiva 2022/2555 ("NIS 2") que supone un **cambio de paradigma en el marco regulatorio de las obligaciones en materia de ciberseguridad.** NIS 2 tiene como objetivos principales introducir la obligación de asumir el enfoque de riesgo tecnológico por parte de las empresas obligadas, así como aumentar significativamente los requerimientos en materia de gobernanza de la ciberseguridad. Para ello, la Directiva crea un amplio catálogo de obligaciones en cuanto a la forma de gobernar internamente la ciberseguridad, **incluyendo la responsabilidad directa de los órganos directivos,** e introduce medidas de supervisión más rigurosas y requisitos de aplicación más estrictos con sanciones armonizadas en toda la UE.

- NIS 2 **amplía el ámbito de aplicación de la Directiva NIS 1**, obligando a más entidades pertenecientes a nuevos sectores a adoptar medidas, lo que incluye partícipes de sectores tales como el farmacéutico o el de la producción, transformación y distribución de productos alimentarios. Se establece una diferenciación en función de su tamaño e importancia, distinguiendo entre las "entidades esenciales", que operan en sectores críticos (banca, energía, transporte, salud, infraestructuras digitales, agua, administración y espacio); y las "entidades importantes", que operan en sectores no tan críticos (alimentación, químicos, distribución, o servicios digitales, entre otros). Además, se deja abierta la posibilidad de que, en los procesos de transposición en normas nacionales, se amplíe ese conjunto de empresas obligadas al abrir la posibilidad de incluir otras entidades con independencia de su tamaño si son críticas por su relevancia nacional o regional. Del mismo modo, todas las entidades que sean responsables de infraestructuras críticas serán incluidas en su ámbito de aplicación directamente.
- NIS 2 **introduce, además, nuevas responsabilidades para los órganos de dirección:** aprobar las medidas para la gestión de riesgos de ciberseguridad; supervisar su puesta en práctica y responder por los incumplimientos, así como asistir periódicamente a formaciones específicas en materia de ciberseguridad, que también deben ser ofrecidas a sus empleados.

Así mismo, se refuerzan las obligaciones en cuanto a la necesidad de configurar un marco de normativas internas sólido, con una serie de políticas y protocolos que deben configurar el gobierno de la ciberseguridad dentro de las empresas obligadas.

Por último, debe señalarse que la publicación de la Directiva NIS 2 se produjo juntamente con otras dos normas de gran trascendencia en materia de seguridad: la Directiva sobre Resiliencia de Entidades Críticas, que contiene obligaciones tendentes a garantizar la continuidad en la prestación de servicios esenciales, y el Reglamento DORA que, como lex specialis, regula las normas de ciberseguridad que serán de aplicación a las entidades del sector financiero.

2.4. El reglamento DORA: El marco más completo de regulación de la seguridad digital.

En los últimos años, las autoridades europeas encargadas de supervisar el sector financiero y asegurador (AEVM, ABE, EIOPA, etc) habían venido aprobando diversas Directrices que incluían obligaciones en materia de ciberseguridad. No obstante, ello resultó en una situación de relativa **inseguridad jurídica,** ya que las normas relativas a la ciberseguridad se encontraban repartidas entre múltiples textos; y de heterogeneidad, en la medida en que no existía un marco único de obligaciones para la totalidad del sector financiero y asegurador.

El Reglamento DORA surge como respuesta a las limitaciones de la situación anterior. Esta norma viene a **unificar** los criterios relativos a la ciberseguridad que se aplican a las distintas entidades del sector financiero y asegurador, que previamente estaban dispersos entre múltiples normas y Directrices de las autoridades europeas. El Reglamento DORA representa la iniciativa más relevante en la materia al ser **obligatoria en todos sus elementos y directamente aplicable** en todos los Estados miembros sin necesidad de ser transpuesta a las legislaciones nacionales.

DORA, que será de plena aplicación a partir del 17 de enero de 2025, afectará a **un gran número de entidades** (entidades de crédito, entidades de pago, entidades de dinero electrónico, agencias de calificación, gestores de fondos, empresas de seguros y reaseguros, entre otros), además de a sus proveedores de servicios TIC, tales como plataformas de cloud o servicios de análisis de datos.

Con carácter general será aplicable a todas las entidades que **no sean microempresas.** No obstante, el **nivel de obligaciones es muy diverso** atendiendo al tamaño y relevancia de la empresa. A este respecto, DORA incluye entre sus principios el de **proporcionalidad,** de tal forma que las entidades deben aplicar las normas teniendo en cuenta su tamaño y perfil de riesgo general, así como el tipo de operaciones que llevan a cabo.

La aprobación conjunta de **NIS 2 (lex generalis) y DORA (lex specialis)** solo se explica teniendo en cuenta la inmensa carga regulatoria que asumen este tipo de entidades y la necesidad de armonizar dicha carga normativa en materia de ciberseguridad. Las obligaciones de DORA son sensiblemente más exigentes que las de NIS 2, por ello no debe perderse de vista la utilidad del Reglamento como un estándar de “mejores prácticas”, también para aquellas entidades que, sin participar en dicho sector, quieran asegurar su alineamiento con la regulación más exigente a nivel internacional en lo que a la ciberseguridad se refiere.

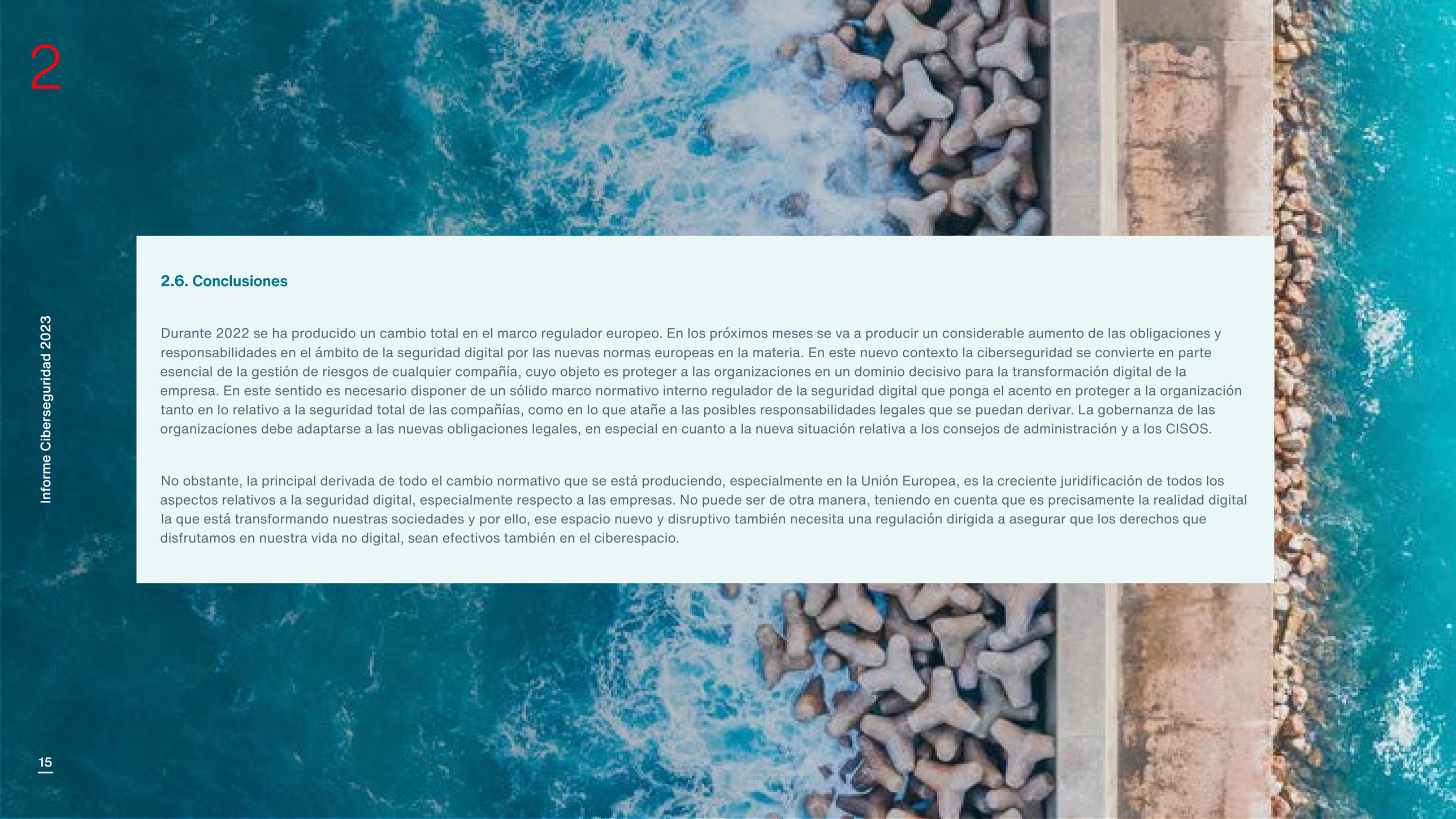
Por último, debe tenerse en cuenta que las instituciones europeas deberán aprobar múltiples normas de desarrollo o actos de ejecución (más de 26), a las que se remite el texto de DORA. Por ello, hay que estar muy pendientes de dicho desarrollo para tener la imagen completa del contenido de DORA.

Las obligaciones de DORA son sensiblemente más exigentes que las de NIS 2.

2.5. La propuesta de reglamento de inteligencia artificial.

La **gran respuesta regulatoria de la Unión Europea** ante los retos planteados por la IA es la Propuesta de Reglamento de IA presentada en abril de 2021 y actualmente en tramitación. Esta norma impondrá una serie de obligaciones para todos los operadores involucrados en la cadena de valor del sistema de IA, a fin de lograr que estas tecnologías se desarrollen de forma ética y responsable. El texto de la Propuesta incluye la prohibición de ciertos tipos de sistemas de IA, tales como las prácticas manipulativas o subliminales, o los sistemas de evaluación social. Otros sistemas de IA no están prohibidos, pero su desarrollo queda sujeto al cumplimiento de una serie de obligaciones en materia de transparencia y de ciberseguridad, entre otros puntos.

Juntamente con el Reglamento de IA, la Comisión hizo públicas **dos propuestas de Directivas** (la Propuesta de modificación de la Directiva 85/374/CEE sobre responsabilidad por los daños causados por productos defectuosos y la Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial) cuyo objetivo es facilitar el resarcimiento de los daños provocados por un sistema de IA. En otras palabras, se establecen normas procesales para facilitar que, cuando un individuo se vea perjudicado por el funcionamiento de una IA, se le puedan indemnizar los daños ocasionados.



2.6. Conclusiones

Durante 2022 se ha producido un cambio total en el marco regulador europeo. En los próximos meses se va a producir un considerable aumento de las obligaciones y responsabilidades en el ámbito de la seguridad digital por las nuevas normas europeas en la materia. En este nuevo contexto la ciberseguridad se convierte en parte esencial de la gestión de riesgos de cualquier compañía, cuyo objeto es proteger a las organizaciones en un dominio decisivo para la transformación digital de la empresa. En este sentido es necesario disponer de un sólido marco normativo interno regulador de la seguridad digital que ponga el acento en proteger a la organización tanto en lo relativo a la seguridad total de las compañías, como en lo que atañe a las posibles responsabilidades legales que se puedan derivar. La gobernanza de las organizaciones debe adaptarse a las nuevas obligaciones legales, en especial en cuanto a la nueva situación relativa a los consejos de administración y a los CISOS.

No obstante, la principal derivada de todo el cambio normativo que se está produciendo, especialmente en la Unión Europea, es la creciente juridificación de todos los aspectos relativos a la seguridad digital, especialmente respecto a las empresas. No puede ser de otra manera, teniendo en cuenta que es precisamente la realidad digital la que está transformando nuestras sociedades y por ello, ese espacio nuevo y disruptivo también necesita una regulación dirigida a asegurar que los derechos que disfrutamos en nuestra vida no digital, sean efectivos también en el ciberespacio.

3

Aspectos jurídicos de la ciberseguridad en el centro del desarrollo de la tecnología

Alejandro Padín Vidal, Socio responsable del área de “data economy”, privacidad y ciberseguridad en Garrigues

3 Aspectos jurídicos de la ciberseguridad en el centro del desarrollo de la tecnología

3.1. Introducción.

Durante el último año se han producido importantes avances regulatorios y tecnológicos que es necesario conocer y analizar jurídicamente En el presente análisis haremos un repaso de las últimas novedades regulatorias y legislativas relacionadas con la ciberseguridad, la tecnología y la privacidad, tres elementos que se interrelacionan de forma inseparable y que avanzan paralelas a la evolución y desarrollo de la economía digital.

Ciberseguridad

Privacidad

Tecnología

3.2. Novedades legislativas y contexto.

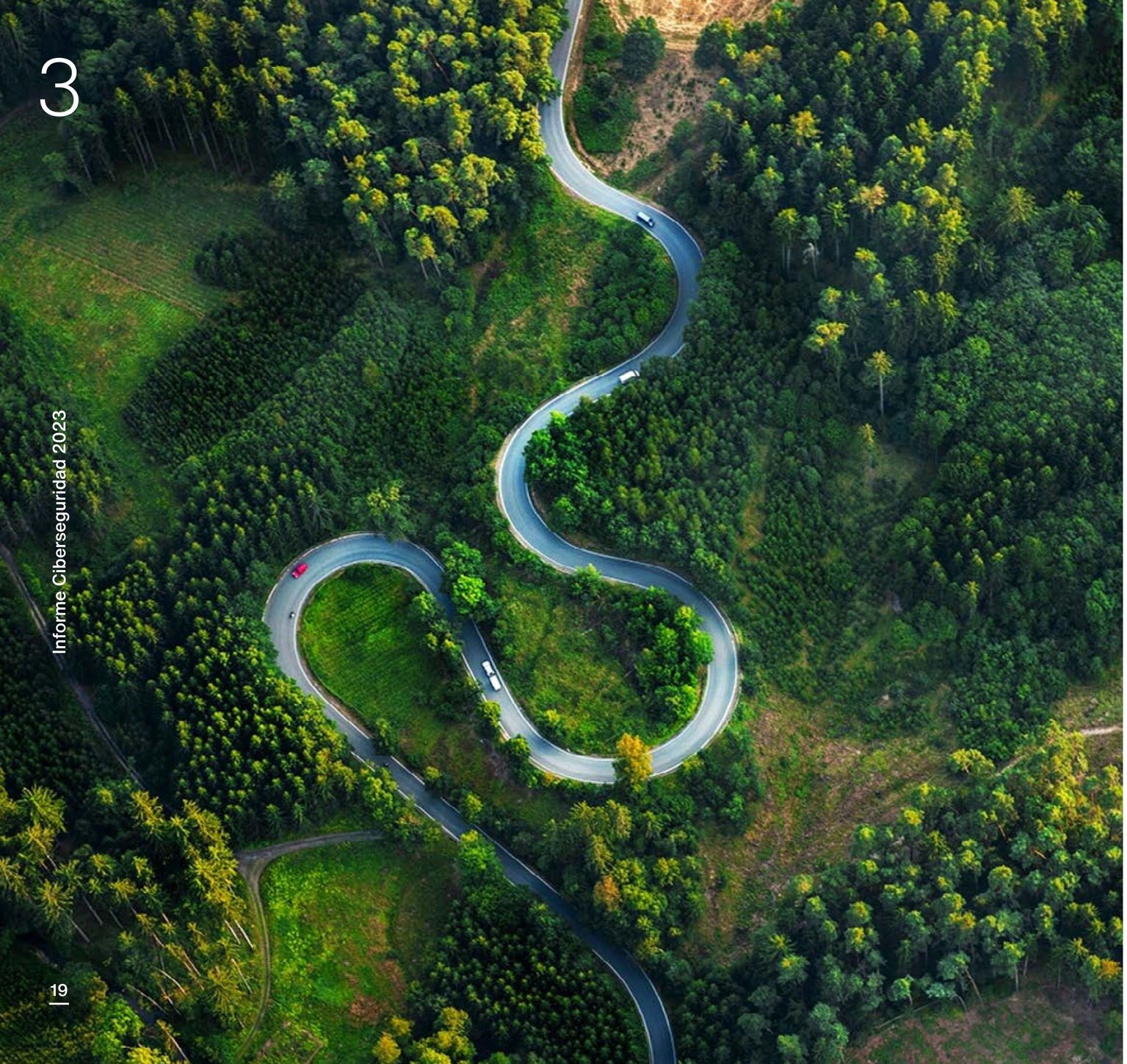
Una primera mención en materia regulatoria de ciberseguridad es la publicación de tres normas de grandísima relevancia: la nueva Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en toda la Unión **(Directiva NIS 2)**, el Reglamento sobre la resiliencia operativa digital del sector financiero **(Reglamento DORA)** y la Directiva relativa a la resiliencia de las entidades críticas.

Todas las normas citadas, enfocadas a ámbitos diferentes, tienen en común la imposición de obligaciones a entidades públicas y privadas con el fin de lograr un alto nivel de resiliencia frente a incidentes de seguridad, con el objetivo final de garantizar la prestación de los servicios afectados en cualquier situación. Vamos a entrar en el detalle de las dos primeras, analizando su impacto e importancia y su relación con el estado actual de la tecnología y la regulación de la privacidad en la Unión Europea.

Directiva NIS 2: Nueva Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en toda la Unión.

Reglamento Dora: Reglamento sobre la resiliencia operativa digital del sector financiero.

Directiva relativa a la resiliencia de las entidades críticas.



3.3. Análisis detallado de la nueva normativa.

3.3.1. Directivas NIS 2[1]:

La Directiva NIS 2 establece medidas que tienen por objeto alcanzar un elevado nivel común de ciberseguridad en toda la Unión con el objetivo de mejorar el funcionamiento del mercado interior. Para ello, esta Directiva se plantea, como objetivos principales, (i) eliminar las divergencias que han surgido entre la regulación nacional de ciberseguridad de los Estados miembros y su aplicación, concretamente mediante la definición de normas mínimas relativas al funcionamiento de un marco regulador coordinado, (ii) el establecimiento de mecanismos para que las autoridades competentes de cada Estado miembro cooperen de manera eficaz, (ii) la actualización de la lista de sectores y actividades sujetos a las obligaciones de ciberseguridad y (iv) la disponibilidad de vías de recurso y medidas de ejecución eficaces para garantizar el cumplimiento efectivo de dichas obligaciones.

Esta norma fue publicada en el Diario Oficial de la Unión Europea el día 27 de diciembre de 2022 y entró en vigor el día 16 de enero de 2023. Al tratarse de una Directiva, es necesario que se incorpore a la legislación interna de cada estado miembro de la Unión Europea mediante la correspondiente ley nacional. Los estados tienen para ello un plazo que finaliza el 17 de octubre de 2024.

1. Su denominación completa es “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, por la que se modifican el Reglamento (UE) N° 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)”.

- *¿A quién le aplica la Directiva NIS 2?*

El alcance objetivo de aplicación de la nueva Directiva amplía considerablemente el número de entidades que se verán obligadas a cumplir este marco normativo. Así, si en la primera Directiva NIS quedaban obligadas las empresas que gestionaban infraestructuras críticas, prestaban servicios esenciales o prestaban servicios digitales, la Directiva NIS 2 se aplica a un número de empresas mucho mayor que se identifican con un criterio mixto de tamaño, sector y actividad, de la siguiente forma:

- Cualquier empresa de tamaño medio[2] que esté incluida en alguno de los sectores denominados como de “Alta Criticidad” en el Anexo 1 o en “Otros Sectores Críticos” según se describen en el Anexo 2. Ambos anexos incluyen un listado de numerosos sectores y subsectores que afectan a un número muchísimo mayor de empresas con respecto a la Directiva NIS 1.
- Cualquier empresa, independientemente de su tamaño, que esté en alguno de los sectores de los anexos 1 y 2, cuando se den determinados requisitos como, por ejemplo, que la entidad sea el único proveedor en un Estado miembro de un servicio esencial, o cuando una perturbación del servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad pública, el orden publico o la salud pública, entre otros casos.

Adicionalmente, se establece un criterio de clasificación de las entidades obligadas según su tamaño y otros criterios de actividad, distinguiendo entre “entidades esenciales” y “entidades importantes”.

Por tanto, el ámbito objetivo de aplicación se amplía de forma considerable, haciendo que gran número de empresas se vean obligadas a cumplir esta normativa.

2. Se establece el criterio de aplicación a empresas que sean consideradas “medianas empresas” con arreglo al artículo 2 del anexo de la Recomendación 2003/361/CE, o que superen los límites máximos para las medianas empresas previstos en el apartado 1 de dicho artículo, y que presten sus servicios o lleven a cabo sus actividades en la Unión. Es decir, empresas que tengan entre 50 y 250 trabajadores y con un volumen de negocios anual de entre 10 y 50 millones de euros o un balance general anual de entre 10 y 43 millones de euros.

- *Principales obligaciones de la Directiva NIS 2.*

1. Responsabilidad del órgano de administración:
Como principal elemento novedoso a tener en cuenta debemos citar que la normativa NIS 2 impone al órgano de administración de las entidades esenciales e importantes la obligación directa de aprobar, supervisar y poner en práctica las medidas para la gestión de los riesgos de ciberseguridad. Además, se establece la responsabilidad directa del órgano de administración sobre el incumplimiento de tales obligaciones.

Esta atribución expresa de responsabilidad al órgano de administración, que se incorpora de forma independiente a la responsabilidad de las entidades, supone un clarísimo paso en la intención de la Unión Europea de elevar el nivel de importancia de la ciberseguridad en el listado de prioridades de gestión de las empresas.

Como complemento a esa responsabilidad, la Directiva establece de forma expresa la obligación de los miembros de los órganos de dirección de las entidades esenciales e importantes de asistir a formaciones en esta materia.

2. Medidas concretas para la gestión de riesgos de ciberseguridad:

- **Adopción de medidas:** Las entidades esenciales e importantes deberán tomar medidas técnicas, operativas y de organización. Estas medidas deberán ser adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de los sistemas de redes y de información que utilizan dichas entidades en sus operaciones o en la prestación de sus servicios. Asimismo, estas medidas deberán prevenir o minimizar las repercusiones de los incidentes en los destinatarios de sus servicios y en otros servicios.

La Directiva NIS 2 establece un catálogo de diez elementos clave que deben incluir las medidas de seguridad, entre los que podemos citar, entre otros, la implantación de políticas de seguridad de los sistemas de información y análisis de riesgos, la gestión de incidentes, la continuidad de las actividades, la seguridad en la cadena de suministro, etc.

- **Obligaciones de notificación:** Las entidades esenciales e importantes deberán notificar, sin demora indebida (alerta temprana en 24 horas, notificación del incidente en 72 horas e informe final 1 mes después de la notificación) a su CSIRT o, en su caso, a su autoridad competente, cualquier incidente que tenga un impacto significativo en la prestación de sus servicios. Cuando proceda, las entidades afectadas notificarán, sin demora indebida, a los destinatarios de sus servicios los incidentes significativos susceptibles de afectar negativamente a la prestación de dichos servicios.

Se define como **“incidente significativo”** aquel incidente de seguridad que:

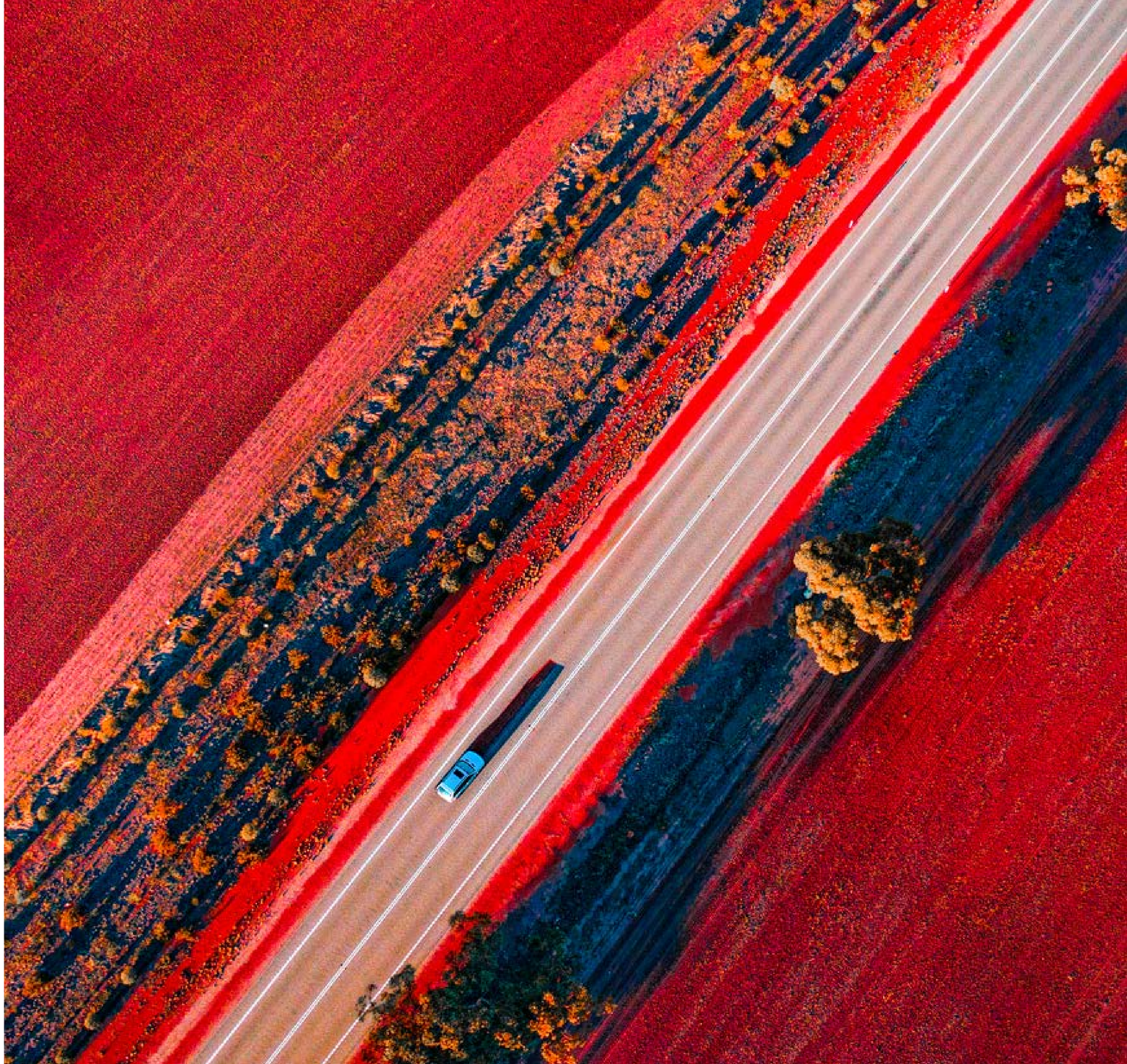
1. ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada.

2. ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables.

- *Régimen sancionador.*

La Directiva NIS 2 establece un amplio listado de facultades de supervisión y control por parte de las administraciones competentes (inspecciones, auditorías, solicitudes de acceso a datos, etc.) y una amplia capacidad sancionadora, tanto en forma de acciones ejecutivas (apercibimientos, instrucciones de actuación o ejecución, suspensión de actividades, publicación de información, etc.) como, además, en forma de sanciones económicas, con multas que pueden llegar a los diez millones de euros o el 2% del volumen de negocios anual total a nivel mundial de la empresa durante el ejercicio financiero anterior.

En la Directiva se establece también una coordinación en materia de sanciones con el Reglamento General de Protección de Datos de la UE (“RGPD”), para aquellos casos en que las infracciones de las obligaciones de la Directiva supongan también una infracción al RGPD, por afectar a la seguridad de los datos personales. Para estos casos, se impone a las autoridades de supervisión de ciberseguridad la obligación de reportar a la autoridad de supervisión de protección de datos (en España, la Agencia Española de protección de Datos) aquellos hechos de los que tenga conocimiento en virtud de sus funciones que puedan afectar a posibles incumplimientos del RGPD.



3.3.2. Reglamento Dora[3].

El Reglamento DORA tiene por objeto lograr un elevado nivel común de resiliencia operativa digital, estableciendo unos requisitos uniformes para la seguridad de las redes y sistemas de información que sustentan los procesos empresariales de las entidades financieras, con el fin de conseguir un nivel elevado de continuidad en el funcionamiento de los sistemas del sector financiero.

El Reglamento gira en torno al concepto de “resiliencia operativa digital”, que es definido en esta norma como “La capacidad de una entidad financiera para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente mediante el uso de servicios prestados por proveedores terceros de servicios de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los sistemas de información que utiliza una entidad financiera y que sustentan la prestación continuada de servicios financieros y su calidad, incluso en caso de perturbaciones”.

3. Su denominación completa es “Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) Nº 1060/2009, (UE) Nº 648/2012, (UE) Nº 600/2014, (UE) Nº 909/2014 y (UE) 2016/1011”.

Esta norma fue publicada en el Diario Oficial de la Unión Europea el día 27 de diciembre de 2022 y entró en vigor el día 16 de enero de 2023. Dada la complejidad de las obligaciones que contiene, el Reglamento concede un plazo amplio de adaptación a las entidades obligadas, de forma que solo será de obligado cumplimiento a partir del 17 de enero de 2025.

- *¿A quién le aplica el Reglamento DORA?*

En términos generales, estarán dentro del perímetro de aplicación del Reglamento DORA todas las entidades del sector financiero en sentido amplio, es decir, tanto entidades bancarias de crédito, pago, depósito e intermediación, como entidades de seguros, reaseguros y otros intermediarios del sector asegurador.

Adicionalmente, como cuestión relevante, también están obligadas de forma directa todas las empresas que sean proveedores terceros de las anteriores entidades, que les presten servicios de tecnologías de la información, comunicaciones y datos (“servicios TIC”).

- *Principales obligaciones del Reglamento DORA.*

1. Responsabilidad del órgano de administración: Al igual que ocurría en la Directiva NIS 2, el Reglamento DORA atribuye al órgano de administración de la entidad obligada la obligación de definir, aprobar y supervisar todas las disposiciones relacionadas con el marco de gestión del riesgo relacionado con las TIC, imponiendo a aquel órgano la responsabilidad directa sobre su aplicación.

De nuevo vemos cómo se eleva el nivel de importancia de esta materia, que cobra especial relevancia a efectos de la responsabilidad directa del órgano de administración.

2. Obligaciones directas: El Reglamento DORA establece una serie de obligaciones directas para las entidades afectadas. Estas obligaciones se refieren a distintos ámbitos que se desarrollan de forma detallada:

- Gestión del riesgo TIC, referido al marco de gobernanza y organización. En este ámbito se establece la responsabilidad directa del órgano de administración en la implementación del marco de gestión. Dentro de la gestión del riesgo TIC se incluye, como aspecto importante, la gestión del riesgo TIC derivado de terceros, estableciendo medidas de evaluación preliminar y regulándose el contenido de los contratos;
- Notificación de incidentes graves TIC, incluyendo el proceso de gestión de los incidentes TIC, su clasificación y las decisiones sobre la notificación obligatoria de incidentes o voluntaria de ciberamenazas;
- Notificación de incidentes graves relacionados con pagos;
- Pruebas de resiliencia operativa digital, que incluye las pruebas de herramientas y sistemas TIC o las pruebas avanzadas basadas en pruebas de penetración (“pen testing”) enfocadas a amenazas;
- Intercambio de información e inteligencia, previéndose la posibilidad de que las entidades financieras intercambien información sobre ciberamenazas;
- Medidas para una buena gestión del riesgo TIC.

3. Requisitos sobre acuerdos contractuales con proveedores TIC: Dado el alcance del Reglamento DORA, esta norma establece cuál debe ser el contenido de los contratos entre las entidades obligadas del sector financiero y sus proveedores terceros de servicios TIC.

Entre las menciones al contenido, cabe destacar que los contratos deberán contener cláusulas específicas en las que se dé una descripción clara y completa de los servicios TIC que prestará el proveedor tercero, indicación a la posibilidad de subcontratación, ubicación de los servicios y funciones y en los que se deberán tratar los datos, disposiciones sobre disponibilidad, autenticidad, integridad y confidencialidad en relación con la protección de los datos, incluidos los datos personales, disposiciones sobre las garantías de la entidad financiera de poder acceder a los datos tratados, etc. etc., hasta un total de quince medidas concretas y otras generales.

- *Régimen sancionador.*

El Reglamento DORA identifica una serie de autoridades competentes según la actividad y les otorga facultades de supervisión e intervención (acceder a documentos o datos, realizar investigaciones o inspecciones, exigir medidas correctoras, etc.), además de crear un régimen sancionador específico para aquellos casos en que las entidades obligadas incumplen alguna de las obligaciones previstas en el Reglamento.

Las sanciones concretas se deberán determinar a nivel de cada uno de los Estados miembro y pueden llegar a tener relevancia penal en los casos de incumplimientos más graves, quedando a discreción de cada Estado miembro el establecimiento de este tipo de sanciones.

Se establece un régimen específico para los denominados “proveedores terceros esenciales de servicios TIC”[4] . Las sanciones a estos proveedores pueden consistir en multas coercitivas de devengo diario hasta que se logre el cumplimiento. El importe de la multa coercitiva podría ser de hasta el 1% del volumen de negocios diario medio a escala mundial del proveedor tercero esencial del servicios TIC en el ejercicio precedente.

Como medida adicional a las sanciones, estas pueden ser objeto de difusión pública mediante la publicación de anuncios indicando la identidad del infractor y la infracción.

4. Las autoridades europeas de supervisión deberán designar a los proveedores terceros de servicios de TIC que sean esenciales para las entidades financieras, tras una evaluación que tenga en cuenta determinados criterios, tales como el impacto sistémico en la estabilidad, la continuidad o la calidad de la prestación de servicios financieros en caso de un posible fallo operativo a gran escala.

3.4. Evolución regulatoria en materia de ciberseguridad y sus consecuencias.

Como se puede apreciar, el marco regulatorio en materia de ciberseguridad se va completando y desarrollando, imponiendo obligaciones más rigurosas y detalladas a cada vez un mayor número de empresas y a las administraciones públicas. Como medida general de refuerzo, se está atribuyendo al órgano de administración de las entidades la responsabilidad directa en la implantación, supervisión y funcionamiento de los esquemas de seguridad de la información.

Todo ello incide directamente en algunas cuestiones fundamentales que es necesario tener en cuenta en cualquier organización:

- La necesidad de que las organizaciones asignen recursos adecuados a la gestión de la ciberseguridad.
- La relación directa que existe entre la ciberseguridad y la protección de datos personales. Esta relación, ya conocida por los profesionales relacionados con ambas materias, es ahora recogida de forma expresa en la nueva normativa. Las áreas de cumplimiento en materia de ciberseguridad y en materia de protección de datos de las organizaciones tienen que estar, necesariamente, coordinados.

El cumplimiento de esta normativa y la concienciación creciente en estas materias aumentará, sin duda alguna, la seguridad de las organizaciones y del tejido económico en su conjunto.

3.5. Protección de datos y ciberseguridad en la Unión Europea: desafíos y avances.

Según datos extraídos de la Memoria Anual 2022 de la Agencia Española de Protección de Datos recientemente publicada[5], durante el año 2022 se han notificado 1751 brechas de seguridad de datos personales a la AEPD. De todas ellas, únicamente 10 han sido objeto de análisis por la Subdirección General de Inspección de Datos. En 31 de los casos totales la AEPD ha requerido al responsable del tratamiento para que cumpliera con la obligación de comunicar la brecha a los interesados.

Como ya avanzábamos en el informe anual anterior, la jurisprudencia se ha inclinado por entender que la obligación de aplicar medidas de seguridad a la información es una obligación de medios y no de resultado. Es decir, que la obligación de una organización está en definir e implementar las medidas de seguridad más adecuadas según el riesgo específico existente, pero no se puede considerar que tal obligación debe impedir de forma absoluta la ocurrencia de un incidente. Así viene establecido por la Sentencia del Tribunal Supremo español número 188/2022, de 15 de febrero de 2022. Dicho lo anterior, el propio Tribunal Supremo en esa misma sentencia ratificaba la insuficiencia de las medidas de seguridad aplicadas por la entidad afectada en el caso concreto enjuiciado. Ello quiere decir que resulta de la máxima importancia realizar los correspondientes análisis de riesgos y definir de forma adecuada las medidas de seguridad que se van a implementar, debiendo la organización ser capaz de demostrar que ha llevado a cabo ese análisis y que las medidas aplicadas son las más razonables para el caso concreto.

Este enfoque se aplica también a la gestión de los prestadores terceros de servicios TIC, con los que deberá tratarse la cuestión de las medidas de seguridad de forma específica y concreta, y no de forma genérica o en un segundo nivel de importancia. Debemos recordar, además, que el RGPD impone, como obligación independiente y autónoma, la correcta gestión de los proveedores de servicios que traten datos personales. El incumplimiento de esa obligación de gestión ha dado lugar ya a varias sanciones de la AEPD.

En definitiva, como decíamos, podemos ver que los ámbitos regulatorios de la ciberseguridad y la protección de datos personales se entrelazan y convergen. Una correcta gestión de las obligaciones de protección de datos puede poner de manifiesto carencias en materia de ciberseguridad y viceversa.

5. Se puede obtener en el siguiente link, consultado por última vez a efectos de este artículo el 21 de mayo de 2023: https://www.aepd.es/es/documento/memoria-aepd-2022.pdf

3.6. Reflexiones finales y perspectivas para el futuro de la ciberseguridad y la privacidad de datos en la Unión Europea.

La tecnología sigue avanzando a paso veloz y, aunque el regulador sigue esos avances de forma bastante ágil, solo las organizaciones pueden tomar las decisiones adecuadas en tiempo real para prevenir y mitigar los riesgos que la tecnología presenta y seguirá presentando. Debemos apostar por la innovación tecnológica, siendo conscientes de sus riesgos y tratando de acotarlos y gestionarlos de la mejor forma posible.

Resulta relevante también mencionar la creciente importancia de los sistemas de inteligencia artificial, con los retos que presentan tanto para la ciberseguridad como para la privacidad. Comienzan a analizarse de forma pormenorizada esos retos pero, desde nuestro punto de vista, no solo se trata de identificar riesgos, sino también ventajas.

Teniendo en cuenta ambos enfoques y asumiendo que los avances de la tecnología no van a detenerse, la posición más práctica desde un punto de vista operativo sería buscar la utilización de sistemas de inteligencia artificial para mejorar la ciberseguridad. Las mismas técnicas de analítica de datos mediante sistemas de inteligencia artificial cuyos riesgos se deben minimizar, pueden ser utilizadas para identificar riesgos ocultos de ciberseguridad. Siempre dentro del cumplimiento del marco regulatorio marcado por la normativa de privacidad y de ciberseguridad, los sistemas de inteligencia artificial podrían ser utilizados para aplicar técnicas de analítica que permitan detectar patrones de comportamiento anómalo, identificar amenazas emergentes o simular ataques cibernéticos, o aflorar patrones irregulares en la gestión de datos que podrían sugerir riesgos de ciberseguridad. Todo ello permitiría mejorar los esquemas de prevención.

En todo caso, y para terminar, no debemos olvidar que, a pesar de a pesar de la evolución de la tecnología y de los avances de la regulación, cada vez más detallada y rigurosa, el factor humano sigue siendo un elemento fundamental en la ciberseguridad. Una recomendación práctica siempre útil es garantizar la formación adecuada y la concienciación de todos los equipos de todas las organizaciones. Solo con la mejora del nivel de formación y concienciación de los equipos humanos ya se puede conseguir mejorar en la capacidad de la organización de evitar violaciones de la protección de datos y amenazas a la ciberseguridad.

4

Evolución de la madurez cibernética en España y el equilibrio en la inversión en ciberseguridad

4 Evolución de la madurez cibernética en España y el equilibrio en la inversión en ciberseguridad

En los últimos años ha habido un cambio de tendencia y ya la mayoría de las empresas consideran el riesgo ciber, y por tanto la ciber seguridad, como una de sus “top priorities”. Cada vez hay más involucración por parte del consejo de administración que ya ven estos riesgos como una responsabilidad empresarial y no una responsabilidad del director de sistemas o CISO.

El estudio realizado en base a los datos obtenidos a través de la plataforma CyQu[6] muestra la evolución de los últimos dos años de la madurez cibernética de las diferentes industrias con respecto a los controles de seguridad implementados.

4.1. Madurez de ciber seguridad por industria.

Para este estudio se han identificado industrias, actividades y sectores de operación con referencia a Europa. Para el año 2022 se han analizado un total de 1.397 empresas y en 2023 un total de 3.936.

1.397 Empresas analizadas en 2022

3.936 Empresas analizadas en 2023

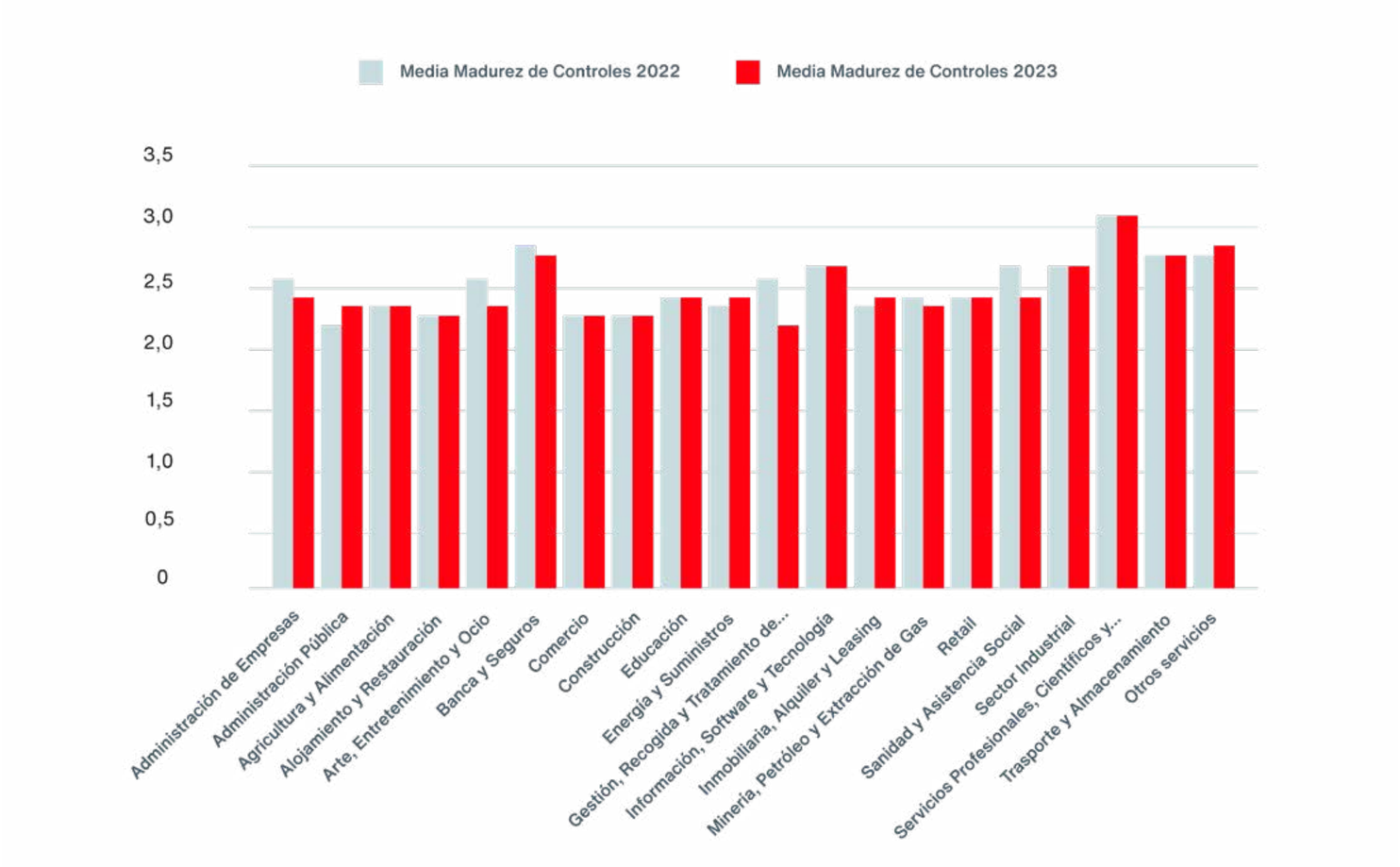
6. CyQu es una plataforma propiedad de Aon para la evaluación de riesgos cibernéticos construida con metodología de análisis de datos y basada en los estándares ISO y el marco NIST.

Los sectores como la Administración Pública, Energía y Suministros, así como Inmobiliaria y Alquiler han mejorado sus niveles de madurez cibernética durante el último año. En el caso de la Administración Pública, una de las posibles razones de mejora puede deberse en gran medida a que la ciberseguridad se ha convertido en uno de los ejes en la estrategia de inversión y progresivamente se busca garantizar la seguridad de sus datos e infraestructuras.

Los sectores de Agricultura y Alimentación, Alojamiento y Restauración, Comercio, Construcción, Educación, Software y Tecnología, Retail, Servicios Profesionales, Científicos y Técnicos, Tratamiento y Almacenamiento mantienen estables sus niveles de madurez en relación con el año anterior. Los sectores de Administración de Empresas, Arte, Entretenimiento y Ocio, Banca y Seguros, Gestión, Recogida y Tratamiento de Residuos, Minería, Petróleo y Extracción de Gas, Sanidad y Asistencia Social, Sector Industrial son los que han reducido sus niveles de gestión y actuación con respecto al año anterior.

Y si pormenorizamos este mismo análisis a España, vemos que el comportamiento es similar y sigue la misma tendencia que en EMEA.

- *Evolución de la Madurez de Controles de Ciberseguridad*

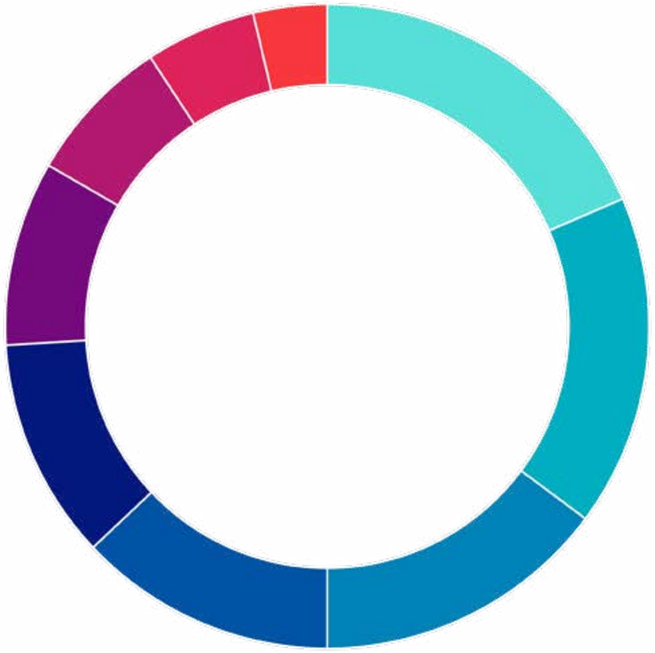


- *Dominios de seguridad*

Poniendo el foco del análisis en los dominios de seguridad permite determinar aquellos sobre los que las empresas están invirtiendo.

Los dominios de seguridad que reciben mayor gestión por parte de las empresas son ‘Seguridad de la Red’, seguido de ‘Seguridad Física’. Las áreas de ‘Control de Acceso’, ‘Endpoints y Seguridad’ y ‘Teletrabajo’ comparten el mismo nivel de atención por parte de las empresas. Por otro lado, nos encontramos con que ‘Seguridad de Datos’, ‘Resiliencia de Negocio’, ‘Proveedores’ y ‘Seguridad de Aplicación’ son los dominios que necesitan más atención o destinar un mayor presupuesto y recursos para mejorar los controles implementados.

Estos nueve dominios están sujetos al constante cambio en el escenario de riesgos y amenazas emergentes. La rápida evolución digital, el surgimiento de nuevas normativas y regulaciones o los riesgos concretos y relativos al ransomware y riesgo de proveedores, confirman la necesidad de abordar rápidamente estos ámbitos.



Ordenado de mayor a menor

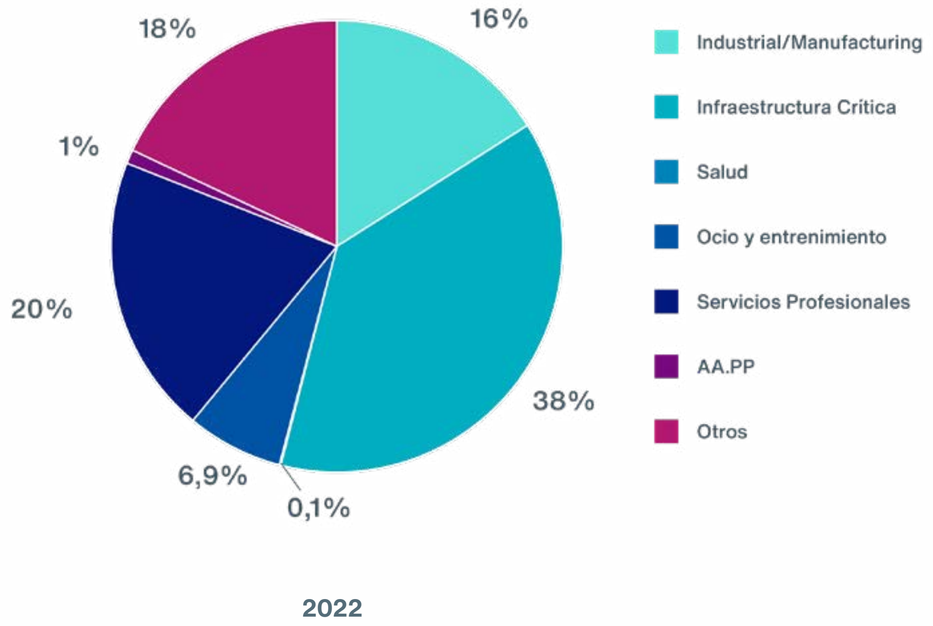
- Seguridad de la Red
- Seguridad Física
- Control de Acceso
- Teletrabajo
- Endpoints y Seguridad
- Seguridad de Datos
- Resiliencia de Negocio
- Proveedores
- Seguridad de Aplicación

4.2. Aseguramiento Riesgo Ciber

Adicionalmente a la inversión de las empresas en materia de ciberseguridad, se ha visto una evolución en el aseguramiento del riesgo ciber.

- *Aseguramiento por sectores de actividad en España*

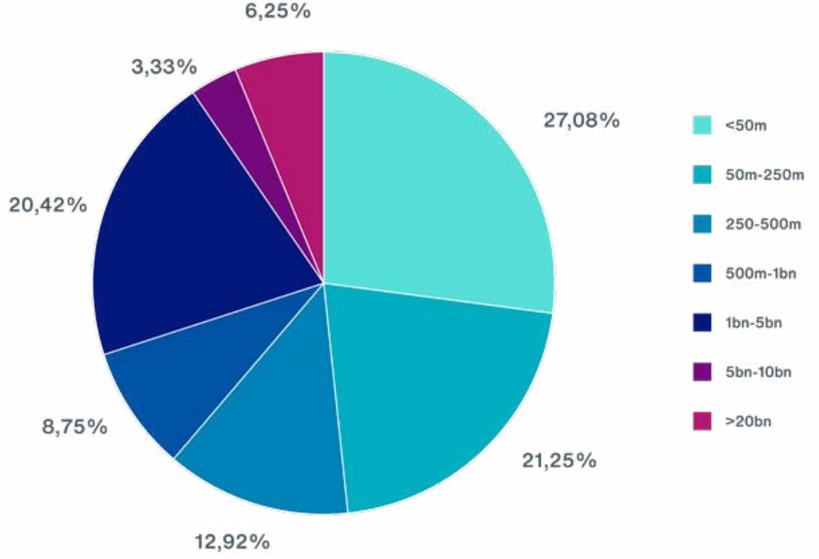
Se ha realizado el análisis agrupando las actividades en 8 sectores:



2022

- *Aseguramiento por volumen (facturación)*

Por volumen de facturación se obtiene un resultado esperado, siendo las empresas con mayores volúmenes las que más contratan un seguro ciber:

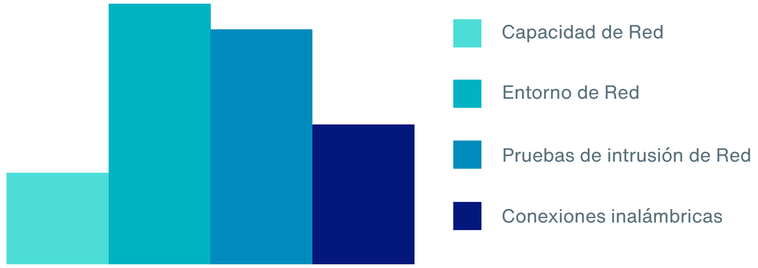


2022

4.3. Situación España.

El estudio realizado nos muestra que España está en línea con EMEA en relación con el dominio que mayor nivel de madurez tiene, siendo este Seguridad de la Red. A su vez, agrupando los controles correspondientes a este dominio, el control más implementado es la seguridad del Entorno de Red.

Seguridad de la Red



En el Entorno de Red se establecen capacidades de control preventivo y de detección basados en la red para detener el tráfico no deseado y ofrecer visibilidad para la investigación y remediación. Por un lado, abarca la correcta configuración de dispositivos de red, utilizando los estándares aprobados internacionalmente, la implementación de herramientas de protección de perímetro de red, como, por ejemplo, firewalls, IPS, filtros web y detección de malware, hasta la inversión en herramientas de mayor alcance para la protección, detección y bloqueo de ataques basados en red.

Otro aspecto destacable de este dominio de seguridad son las Pruebas de Intrusión de Red o Pentesting, el cual ayuda a identificar, calificar e informar sobre las vulnerabilidades de red y recomendar una respuesta adecuada para el tratamiento. Los controles sobre Conexiones Inalámbricas y Capacidad de Red forman parte de este grupo mayor valorado entre las industrias a nivel nacional.

Los datos revelan que existen bloques transversales claves en la gestión de la ciberseguridad por parte de las empresas, independientemente de su industria, en los que se está poniendo foco de actuación:

Formación y concienciación de empleados: una barrera ante cualquier amenaza cibernética son los propios usuarios de los sistemas y, por tanto, los empleados. Es fundamental para cualquier empresa establecer protocolos de actuación alienados con la seguridad y garantizar su actualización y puesta en práctica.

Configuración de Contraseñas: controles implementados para evitar que se pongan en peligro los datos confidenciales al garantizar la configuración correcta de contraseñas. Factores como, longitudes mínimas, complejidades, rotaciones, evitar reutilización, forman parte de las políticas utilizadas para asegurar la robustez al momento de establecer una contraseña.

Gestión de parches y actualizaciones: mantener los sistemas actualizados a su última versión garantiza que las vulnerabilidades identificadas por el proveedor están solucionadas, y en muchos casos, se refuerzan además otras configuraciones de estos. Tener una política que defina revisiones periódicas y que contengan un proceso definido para aplicar los parches identificados como críticos ayuda a mejorar la madurez cibernética de la empresa. Existen herramientas que además de controlar las versiones de parches instaladas en los sistemas de su red, envían notificaciones cuando se detecta un sistema obsoleto y pueden ejecutar la instalación de determinados parches de manera automática.

Copias de seguridad: con políticas para la gestión de las copias tales como frecuencia, de qué datos se hacen copias, tiempo de que se almacenan estas copias; claves para minimizar el impacto de la recuperación de sistemas.

Habilitar autenticación multifactorial: muchas de las soluciones técnicas que requieren de un login cuentan con la posibilidad de activar la autenticación multifactorial. Tener esta capa de protección extra habilitada puede evitarnos accesos no autorizados a los sistemas críticos de la empresa.

Definición de normas de acceso a información sensible y sistemas críticos: con diferentes niveles de privilegio ajustados a las necesidades de cada rol.

Respuesta ante incidentes: finalmente, cuando el riesgo se ha materializado, es crítica la rapidez de actuación ante el incidente. Por tanto, disponer de un protocolo de respuesta ante incidentes ayudará a minimizar su impacto.

4.4. Conclusiones

En general el nivel de protección y concienciación es mayor cuanto mayor es la empresa y su exposición externa (la actividad es fundamental tanto en la percepción del ciber riesgo como en la concienciación para su gestión). No quiere decir que las empresas pequeñas tengan menor protección, pero su capacidad y presupuesto de inversión en seguridad es menor.

Cada vez más el enfoque es más proactivo porque venimos de una tendencia de reacción, donde se venían tomando acciones como consecuencia de un ciber ataque en la propia empresa o en una de su entorno.

En cualquier caso, creemos que el nivel de importancia y por tanto de presupuesto y compromiso de la dirección sigue siendo reducido en relación con la amenaza que suponen estos riesgos.

Por tanto, la gestión de la ciberseguridad no es común ni por sector ni por tamaño de empresa. Hay más variables que intervienen en la decisión de invertir en seguridad (concienciación, apetito al riesgo, incidentes acontecidos propios o en terceros, etc.).

Ante esta situación, unido a la variedad de medidas de seguridad, la complejidad de su implementación, las empresas y en concreto los CISOs se enfrentan al reto de decidir como invertir un presupuesto siempre limitado que tenga un mayor impacto en su ciber seguridad.

Antes de comenzar a implementar medidas de seguridad, es fundamental establecer y priorizar cuales pueden ser las amenazas que pueden impactar en la empresa. Aunque nadie está libre de un potencial ciber riesgo, según la actividad y situación, las amenazas podrán tener diferente probabilidad de ocurrencia e impacto. Posteriormente, realizar un análisis de situación sobre la gestión de la ciber seguridad permitirá definir un plan de acción para mitigar las amenazas más críticas y priorizar las medidas a implementar.

5

Ciber ataque a sistemas de producción

El compromiso tras el compromiso

5

Ciber ataque a sistemas de producción

Una empresa manufacturera vio la práctica totalidad de sus sistemas de producción comprometidos en un ciberataque de ransomware en 2021.

La compañía se negó al pago del rescate y consiguió superar la crisis gracias al enorme compromiso de empleados y proveedores.

- Los atacantes accedieron a través de la VPN
- Dos semanas de duro impacto en la actividad, seis de impacto más reducido
- La recuperación de todos los sistemas afectados llevó un año
- Los empleados prácticamente acamparon en las oficinas durante los momentos iniciales

5.1. El ataque.

Los atacantes tuvieron acceso a los sistemas de la empresa. El software malicioso que utilizaron es ejecutado de forma manual por el grupo cibercriminal, por lo que tuvieron acceso a los sistemas de la víctima de forma remota. Instalaron, además, otros componentes maliciosos para conseguir persistencia accediendo a la red desde el exterior.

Los atacantes accedieron a través del VPN. Se desconoce como consiguieron el acceso al usuario y cuál fue el vector de entrada inicial. Como dato relevante hay que destacar que en aquel momento la empresa no utilizaba doble factor de autenticación.

Se da la circunstancia de que el usuario a través del que accedieron a la red tenía privilegios, con lo que los ciber atacantes no tuvieron que escalar privilegios y pudieron moverse directamente por el entorno.

Realizaron el cifrado de datos. Se detectaron herramientas para la exfiltración de datos, si bien finalmente no la llevaron a cabo.

El entorno corporativo se vio afectado de forma leve, si bien **la práctica totalidad del entorno productivo** (gestión de stocks, producción, embalaje y logística) **se vio comprometida.**

En el entorno industrial se cuenta habitualmente con muchos equipos asociados a máquinas y procesos en concreto, que están interconectados entre sí y con los servidores.

En estos equipos, la funcionalidad es el principal objetivo. Se trata de que contribuyan a hacer el proceso productivo lo más preciso, coordinado y eficiente posible. No suelen actualizarse, y su seguridad ante intrusiones no suele ser una característica a la que se preste atención. En situaciones de ciberataque son especialmente vulnerables.

La empresa afectada no utilizaba un doble factor de autentificación

5.2. La respuesta y la recuperación.

Tras el “compromiso” del sistema informático vino el extraordinario compromiso de los empleados, de los proveedores de maquinaria industrial y de los proveedores de servicios de IT. Se cortaron las comunicaciones de las conexiones de red de las máquinas de las sedes, se aislaron sistemas, se reinstalaron sistemas operativos y softwares de control de maquinaria desde cero.

Participaron innumerables empresas de servicios de IT. Algunas eran las que utilizaba habitualmente la empresa en su día a día, otras fueron contactadas ex profeso.

Como anécdota, un proveedor de maquinaria incluso pidió a uno de sus empleados que recientemente se había jubilado, quien en su día había instalado el software de control de una máquina, que acudiese para ayudar a recuperar dicha máquina.

La actividad se vio seriamente afectada durante dos semanas. El impacto en la producción y ventas duró dos meses.

Mientras no se recuperaban los diferentes sistemas, volvieron a realizarse de forma manual muchos procesos que estaban automatizados.

Se pudieron expedir algunos productos volviendo a utilizar métodos manuales de trabajo, si bien la gestión de los stocks también estaba afectada. La logística tuvo que llevarse “como antes” y sin perder la trazabilidad de los lotes.

La empresa sufrió pérdida de ventas y tuvo que incurrir en costes adicionales durante el periodo de trabajo en manual.

El proceso de reclamación a la aseguradora requirió del aporte de gran volumen de documentación y cálculos.

5.3. Algunos puntos relevantes.

- Importancia del doble factor de autentificación
- Considerar la seguridad de los equipos asociados a control de maquinaría
- Capacidad de reacción de los equipos
- La asistencia de expertos en el cálculo, justificación y preparación de la reclamación al seguro es fundamental

En situaciones de ciber ataque, las decisiones se han de tomar rápidamente y el proceso normal de licitación de compras no suele llevarse a cabo. Es recomendable, en todo caso, documentar en la medida de lo posible qué va a hacer cada una de las empresas de IT que va a ayudar con la incidencia.

También es necesaria la comprensión por parte de la aseguradoras de que el asegurado no va a tener el habitual desglose de todos los gastos incurridos.

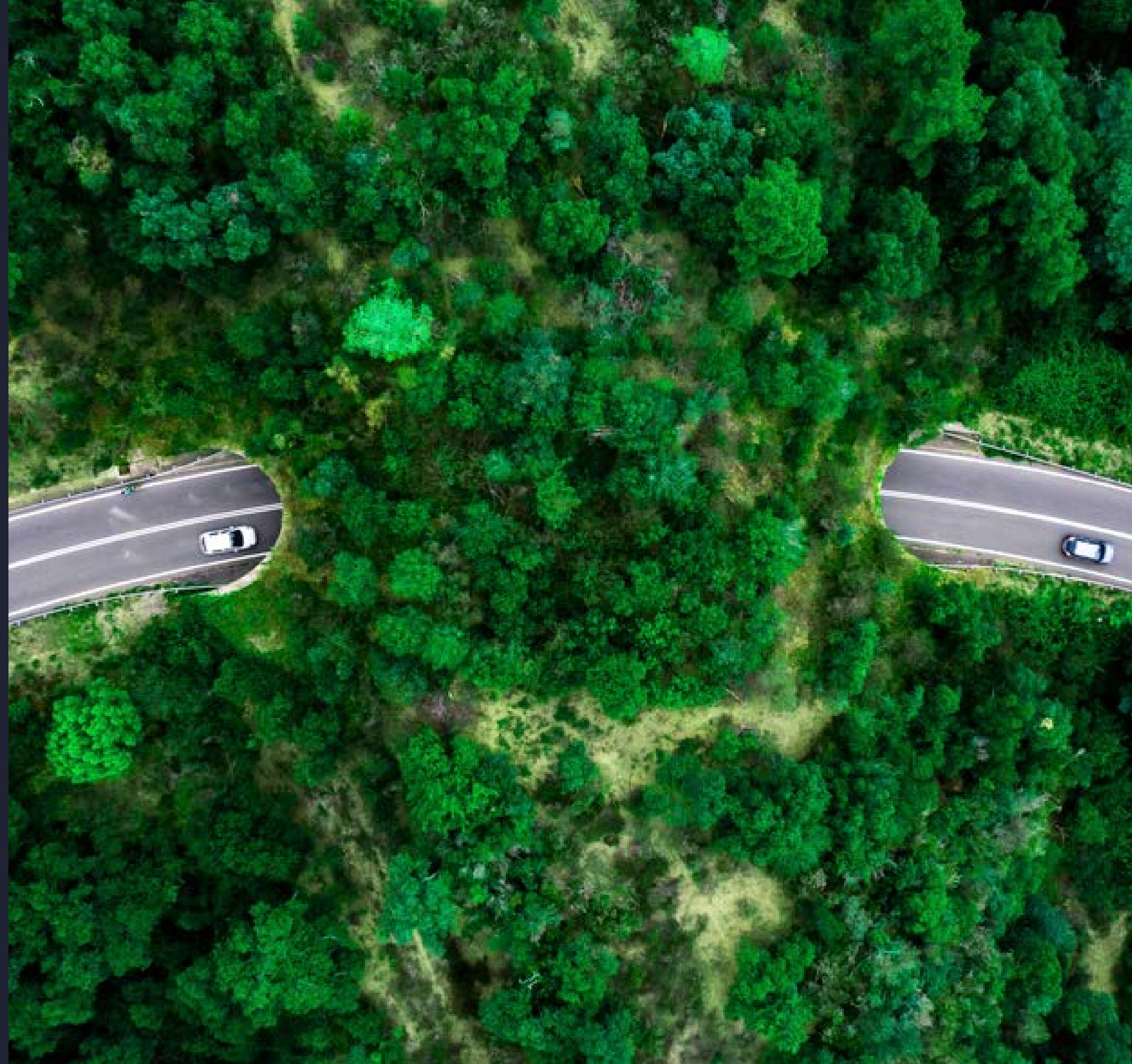
Se trata de evitar conflictos en los dos puntos más habituales de fricción en los procesos periciales en cuanto a los gastos de respuesta al incidente: costes habituales y mejoras.

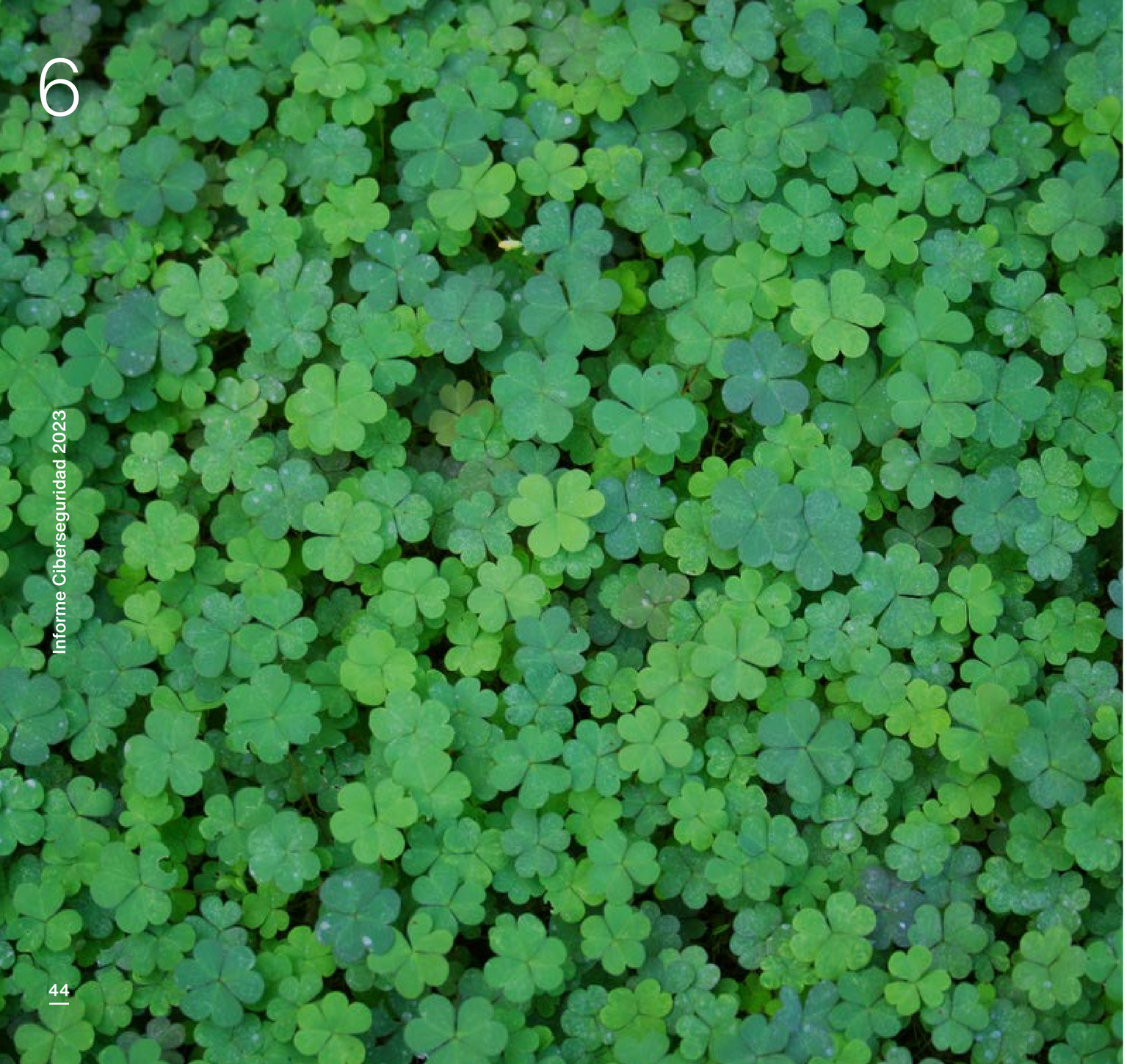
Nexo causal entre el incidente y la pérdida de beneficios: en casos de ciber ataque, cobra especial relevancia el explicar bien el mecanismo por el cual el ataque deviene en pérdidas que no sean evitables.

6

La relevancia de ciberseguridad y privacidad de datos en ESG

Claudia Gómez, Executive director Specialty ESG, y **Anna Clavarino,** Associate Specialty ESG.





La relevancia de ciberseguridad y privacidad de datos en ESG

6.1. ESG se convierte en un criterio significativo para las empresas

En los últimos años, los factores medioambientales, sociales y de gobernanza (ESG) se han convertido en consideraciones importantes para las empresas. A medida que el cambio climático se convierte en una preocupación cada vez más acuciante y que se están introduciendo más legislaciones y normas obligatorias de reportaje, el desempeño ESG de una empresa se ha convertido en un diferenciador competitivo para todos los stakeholders.

Unos temas que a menudo se pasan por alto en los debates sobre ESG son la ciberseguridad y la protección de datos. Sin embargo, dados los importantes riesgos que las amenazas cibernéticas plantean a las empresas y a sus stakeholders, cada vez está más claro que la ciberseguridad y la protección de datos son aspectos esenciales y críticos de ESG.

Los riesgos de ciberseguridad pueden suponer una amenaza significativa para las empresas. No sólo los datos personales de clientes, empleados y otros stakeholders, sino también la información empresarial sensible, la propiedad industrial y los secretos comerciales son a menudo objetivo de los ciberdelincuentes. Las consecuencias de estas violaciones de datos pueden tener graves repercusiones para la empresa y dar lugar a robos de identidad, fraudes financieros, pérdida de ventajas competitivas o daños a la reputación.

Dada la importancia actual de la inversión y la innovación en sostenibilidad, especialmente la pérdida de ventajas competitivas (tecnologías, etc.) puede retrasar o impedir los objetivos estratégicos.

Los numerosos ciberataques de los últimos años ilustran las consecuencias de las violaciones de datos y las interrupciones de la cadena de suministro causadas por medidas deficientes de protección de datos. Estos eventos resultaron no sólo en enormes pérdidas financieras, debido a los costes de reparación, denuncias (o demandas) judiciales y la pérdida de ingresos, sino también en los daños reputacionales significativos que, a su vez, han producido pérdidas serias de clientes, socios e inversores.

Sin embargo, el impacto de los riesgos cibernéticos no se limita a las empresas individuales: Los ciberataques pueden tener repercusiones sociales y medioambientales más amplias, sobre todo cuando afectan a infraestructuras críticas como redes eléctricas, sistemas de abastecimiento de agua o redes de transporte, razón por la cual sigue siendo una de las mayores preocupaciones de la actualidad. Estos tipos de interrupciones pueden tener serias consecuencias sociales y medioambientales y, por tanto, es esencial que las empresas den prioridad a la ciberseguridad como parte de sus iniciativas y estrategias de ESG.

Los 10 Mayores Riesgos

Global Risk Management Survey 2021 de Aon

1	Ciberataques/violación de datos	6	Cambios normativos/legislativos
2	Interrupción del negocio	7	Riesgo de pandemia/crisis sanitaria
3	Desaceleración económica/lenta recuperación	8	Fallo en la cadena de suministro o distribución
4	Riesgo de precio de las materias primas/escasez de materias primas	9	Competencia creciente
5	Daños a la reputación/marca	10	Incapacidad para innovar o satisfacer las necesidades de los clientes

6.2 El vínculo entre ciberseguridad, privacidad de datos y ESG.

La ciberseguridad y la privacidad de datos están estrechamente vinculadas a las dimensiones de ESG por varias razones.

En el ámbito medioambiental, los ciberataques pueden tener importantes repercusiones indirectas sobre el medio ambiente. Por ejemplo, si un ciberataque interrumpe las operaciones de una empresa que produce o transporta mercancías, puede provocar un aumento de la actividad de transporte y logística, lo que conlleva mayores emisiones de carbono. Además, los ciberataques contra infraestructuras críticas, como las redes eléctricas o los sistemas de abastecimiento de agua, pueden causar interrupciones que pueden producir daños medioambientales indirectos, como la contaminación provocada por las fuentes de energía de reserva o las interrupciones en las instalaciones de tratamiento de aguas.

La ciberseguridad es un componente crítico de la gestión de la cadena de suministro, especialmente dada la gran dependencia que tienen las empresas de proveedores críticos de nube y las posibles interrupciones que podrían producirse en el futuro. Las empresas también deben evaluar este riesgo y asegurarse de que sus socios y proveedores tomen las medidas adecuadas para proteger sus sistemas y datos. Unas prácticas de ciberseguridad eficaces pueden ayudar a evitar violaciones de datos que supongan un derroche de recursos y energía, como los costes asociados a la recuperación de datos perdidos o la sustitución del hardware comprometido.

Desde la perspectiva social, la privacidad de los datos y la ciberseguridad están directamente relacionadas con los derechos humanos y la responsabilidad social. Tras varias violaciones de datos en los últimos años, el uso ético y responsable de los datos personales se ha convertido en una exigencia creciente de clientes y consumidores. Un ejemplo de violaciones graves serían los ciberataques a infraestructuras sanitarias críticas, como los hospitales, que pueden interrumpir servicios esenciales, poner en peligro la salud y la seguridad públicas y generar desconfianza entre los stakeholders. Garantizar que los datos personales están protegidos de las ciberamenazas es, por tanto, un componente importante de la responsabilidad social corporativa de una empresa, y un factor crítico en su desempeño general en materia de ESG.

Desde la perspectiva de gobierno, el incumplimiento de normativas sobre la privacidad de datos, la ciberseguridad de infraestructuras críticas (dispositivos médicos, etc.) u otras leyes sobre la protección de datos, puede tener graves repercusiones legales, financieras y reputacionales para el negocio. Las empresas deben evaluar los riesgos normativos potencialmente provocados por la falta de medidas adecuadas y mantenerse al corriente de las nuevas tendencias tecnológicas, como el uso creciente de la inteligencia artificial (IA) por ejemplo, para mejorar sus estrategias y resultados en materia de ESG.

Aunque la IA se está convirtiendo en una herramienta cada vez más importante en la lucha contra los ciberataques, también se ha convertido en uno de los mayores retos a la hora de garantizar la protección de datos y la ciberseguridad. Los ciberdelincuentes y hackers pueden perfeccionar sus técnicas de ciberataque basadas en la IA y disponen de las herramientas necesarias para desarrollar ciberamenazas más sofisticadas en forma de correos electrónicos de phishing más creíbles o códigos maliciosos, por ejemplo. Además, la IA puede producir resultados sesgados y tomar decisiones sin supervisión humana (automatización), lo que en algunos casos puede resultar en falsas identificaciones, comportamientos discriminatorios o mala toma de decisiones. Las consecuencias que puede tener esta tecnología en cuanto a privacidad de la información deben ser analizadas bajo todas las perspectivas – ambiental, social y de gobernanza – para garantizar la correcta gestión de riesgos en caso de ciberataques impulsados por la IA.

Perspectiva Medioambiental

Perspectiva Social

Perspectiva de Gobierno

6.3. Conclusiones

En resumen, la protección de datos y la ciberseguridad son componentes esenciales de ESG y, por tanto, pueden contribuir al buen gobierno corporativo.

La creciente preocupación por el cambio climático, la introducción de nuevas legislaciones, el auge de nuevas tendencias (como la IA) y la creciente demanda por parte de todos los stakeholders de un uso ético y responsable de sus datos personales han convertido la implementación de medidas seguras de ciberseguridad no sólo en una ventaja competitiva, sino también en un criterio significativo para el desempeño positivo en materias de ESG. Estas medidas son fundamentales para garantizar la estabilidad financiera, salvaguardar las infraestructuras críticas y para defender los derechos humanos.

Los riesgos de ciberseguridad pueden derivarse a menudo de prácticas de gobernanza deficientes, como una gestión inadecuada de riesgos, la falta de supervisión por parte del consejo de administración o la ausencia de controles apropiados, lo que puede provocar daños legales, financieros y reputacionales. Al aplicar políticas y prácticas sólidas de ciberseguridad como parte de sus iniciativas ESG, las empresas pueden demostrar su compromiso con la responsabilidad social, la gobernanza eficaz y el crecimiento sostenible, mitigando al mismo tiempo los riesgos asociados a los ciberataques y las violaciones de datos.

7

Mercado Asegurador: Principales Cambios y Tendencias en 2022

7

Mercado Asegurador: Principales Cambios y Tendencias en 2022

Antes de exponer la situación del mercado asegurador en un futuro inmediato y las tendencias que se prevén para este año 2023, consideramos importante recordar de dónde venimos para entender la situación actual y por qué hemos llegado hasta aquí.

Desde 2020, llevamos un período, que en términos asegurador denominamos de “mercado duro”, que se aceleró en 2021, en un entorno post-pandemia y con el crecimiento de manera exponencial de los ataques de ransomware y de phishing. La transformación digital acelerada por el Covid-19 aumentó el riesgo empresarial ante el cibercrimen.

La actividad delictiva en la red hizo que el ramo entrara en déficit, dado que las aseguradoras contabilizaban ratios de rentabilidad negativos, al indemnizar más siniestros vs las primas que ingresaban. Ello hizo que las aseguradoras pusieran el foco en las medidas de seguridad con procedimientos de suscripción mucho más rigurosos, con exigencias mínimas muy estrictas, por debajo de las cuales no estaban dispuestas a suscribir determinados riegos. El resultado fue el de reducción de capacidades, incremento de primas, incremento de franquicias y limitando coberturas sobre todo en cuanto a ransomware se refería. Pero vamos por partes analizando los motivos de este cambio de tendencia.

Aon's Cyber Solutions registró durante 2020 una secuencia de 3 nuevos siniestros por día hábil, a nivel mundial. Esto es un incremento de casi el 100% con respecto 2019, y casi todos ellos relacionados con ransomware. **El impacto medio de las pérdidas aumentó cada trimestre de 2020.** En muchos casos, las pérdidas relacionadas con ransomware llegaron a ser de ocho cifras.

El Parlamento Europeo considera que el ransomware es "la amenaza más preocupante en la actualidad". En 2021 el coste global por este tipo de ataque fue de 18.000 millones de euros, 57 veces más que en 2015, con un pago medio de 150.000 euros. Para 2031 se espera que el ransomware costará $ 265.000 Millones anuales.

Las reclamaciones derivadas de la vulneración de ley de Protección de datos también han sido y son, una fuente de pérdidas para las Aseguradoras, junto con el trabajo en remoto y la dependencia de la tecnología de terceros.

Las medidas de ciberseguridad con los proveedores se convirtieron en una parte fundamental de esta ecuación, el compromiso de **Solar Winds** y las vulnerabilidades de **Microsoft Exchange** demostraron la complejidad de las relaciones con los proveedores de tecnología y cómo aumentó el riesgo frente a la ciberseguridad.

Todo ello tuvo una **repercusión inmediata en el coste del seguro** y se produjo un incremento de las primas de manera drástica. Aunque el incremento medio de prima se inició en un temprano 2019 con incrementos moderados, éstos no fueron suficientes para compensar el aumento de la frecuencia y el impacto de los siniestros y aparte de incrementar las primas de manera exponencial, tuvieron que **modificar sus criterios de suscripción poniendo el foco en las medidas de seguridad** de sus riesgos.

18.000 Millones

En 2021 el coste global por este tipo de ataque fue de 18.000 millones de euros.

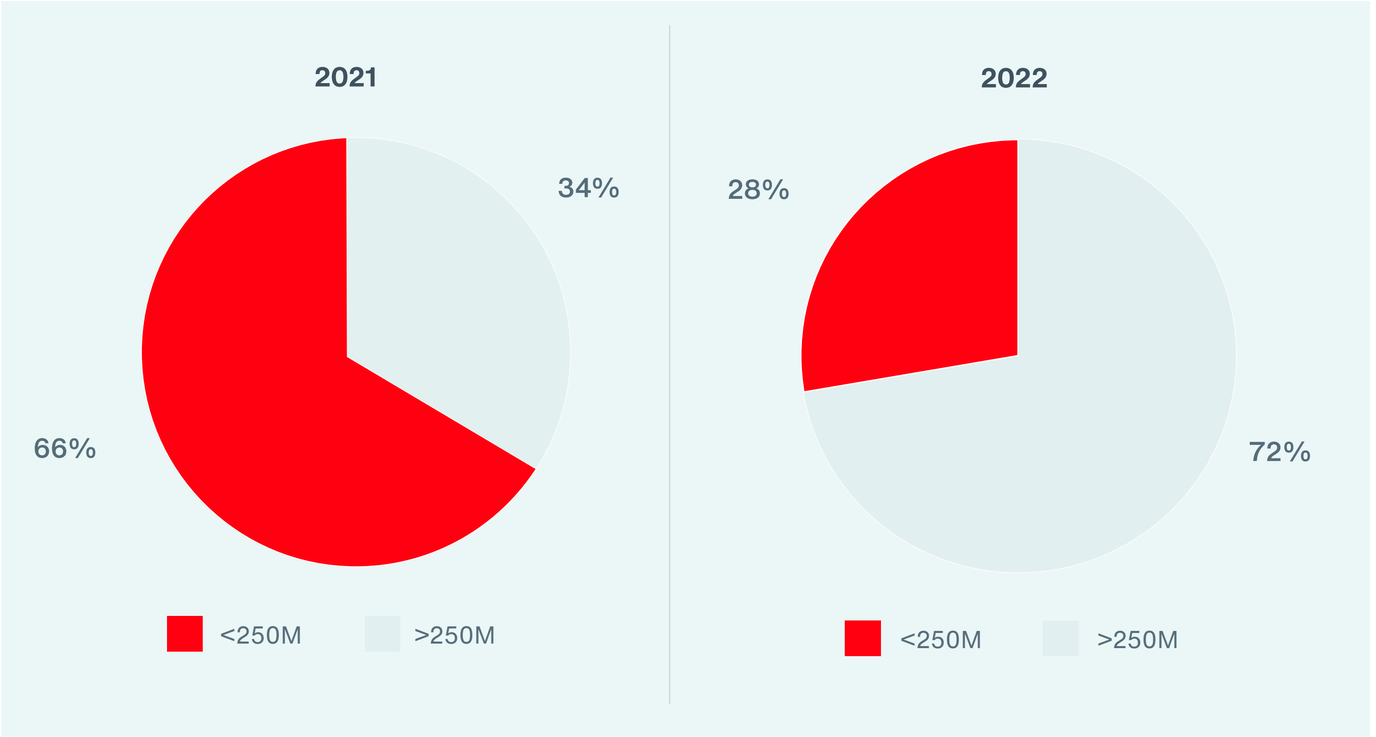
El Parlamento Europeo considera que el ransomware es la "amenza más preocupante en la actualidad".

7.1. Evolución del mercado asegurador en España en 2022.

El mercado asegurador experimentó un cambio significativo de tendencia a finales del año pasado. El primer semestre de 2022 continuó una tendencia de incremento drástico en primas, sin embargo, durante la segunda mitad de 2022, se observaron incremento más moderados, primeros síntomas de la tendencia a la estabilización. A medida que avanza el año 2023, esta tendencia se mantiene.

- **Contratación del Seguro de Ciberriesgos según el Volumen de Facturación:**

A raíz de los múltiples y sofisticados ataques cibernéticos que han tenido lugar en los últimos tiempos, las organizaciones han intensificado su preocupación por el impacto económico potencial de estas amenazas. Al analizar la distribución de las pólizas contratadas en función del volumen de facturación, se observa un considerable incremento en el número de empresas que superan los 250 millones de euros en comparación con el periodo anterior.



- **Contratación del seguro de Ciberriesgos por sectores de actividad:**

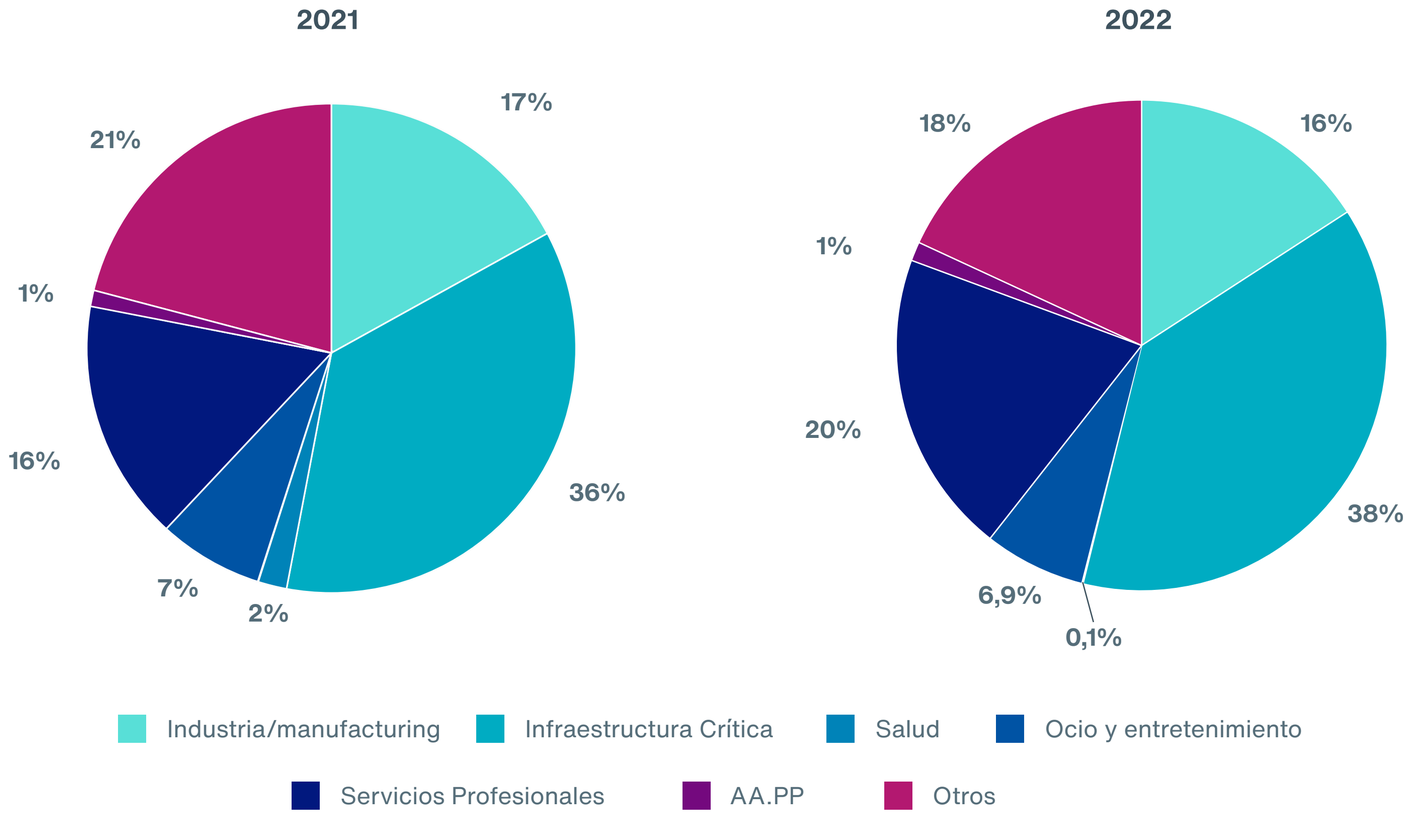
En el grafico siguiente podemos observar la distribución por sectores. En este caso incluye mucho la política de suscripción de cada aseguradora, siendo la administración pública el sector que menos contrata, en parte por el escaso apetito del mercado a estos riesgos.

El sector de infraestructuras críticas continúa liderando en términos de concienciación sobre ciberseguridad y en la generación de contrataciones anuales. Esto se debe a que los atacantes perciben un claro potencial de beneficio, ya sea económico o social, en estas empresas.

En segundo lugar, se ha observado un notable aumento en el sector de servicios profesionales en comparación con años anteriores. Esto debido en parte a que uno de los sectores más afectados y la gran demanda de nuevos servicios de consultoría IT.

Por otro lado, el sector industrial ha experimentado una disminución gradual en los últimos años. En 2020, representaba el **27%** de la participación, luego descendió al **21%** en 2021 y finalmente alcanzó el **18%** en 2022.

En línea con años anteriores, los sectores de administración pública y salud siguen manteniendo una participación limitada y han experimentado una menor contratación en comparación con años anteriores.

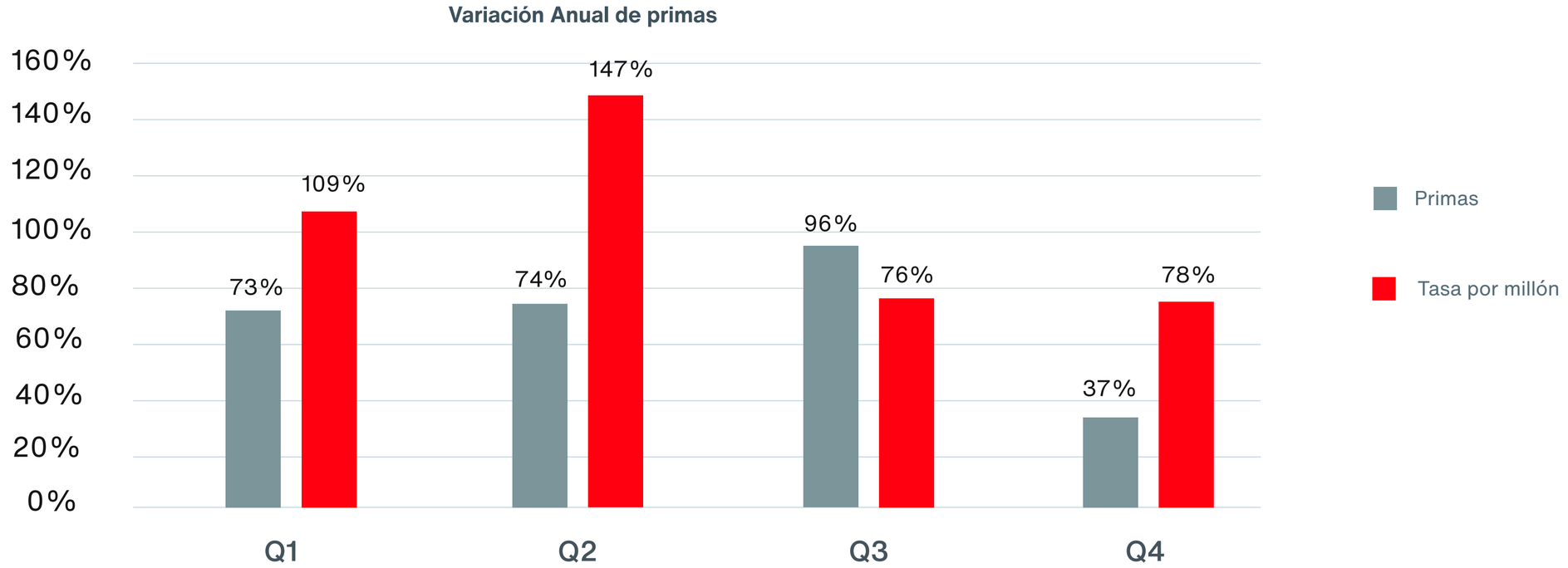


- **Volumen de primas:**

El aumento de las primas es una realidad generalizada en todos los sectores y actividades. Si bien algunas industrias pueden verse más afectadas que otras, la mayoría de los clientes han experimentado un incremento considerable en sus primas. Observamos que los mayores aumentos se dieron durante el primer y segundo trimestre de 2022, donde se registraron incrementos superiores al 100% en las primas. Esto se debe a que las aseguradoras comenzaron a ajustar las tasas que no habían sido modificadas anteriormente. A finales de 2021, todavía existían muchas pólizas que se renovaban automáticamente, sin cambios en las condiciones desde 2019.

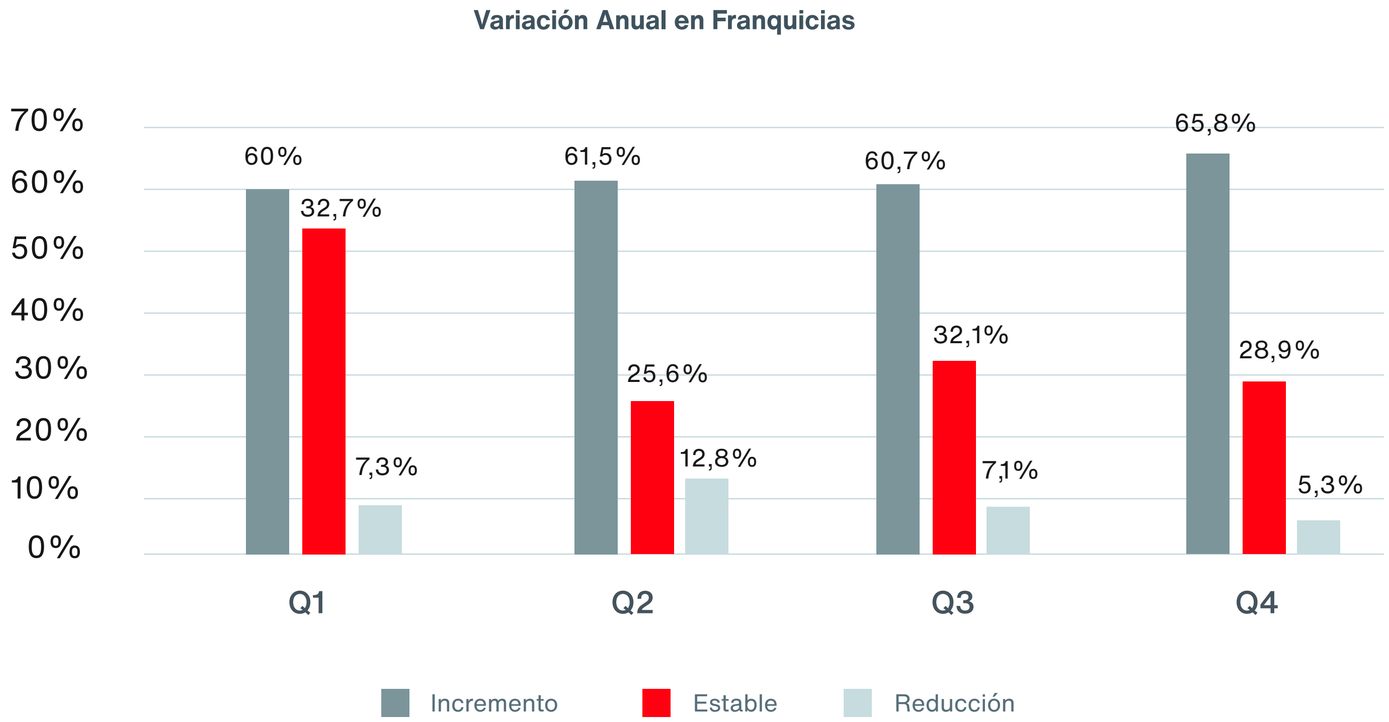
Se espera que, debido a la estabilización del mercado, los aumentos de las primas se detengan o si continúan en algunos casos sean con porcentajes menores.

Por otra parte, el volumen de primas del mercado en general continúa aumentando tanto por el incremento en nuevas contrataciones como por el incremento en límite de los clientes que ya tienen suscrita una póliza.



- **Límites y Retenciones/Franquicias:**

En este 2022 los clientes continúan experimentando cambios en las estructuras de sus programas para mantener el riesgo. Las aseguradoras han adaptado los programas para que sean mutuamente beneficiosos. En el año 2022, se observó un notable incremento en las retenciones, lo cual ha sido una medida significativa.

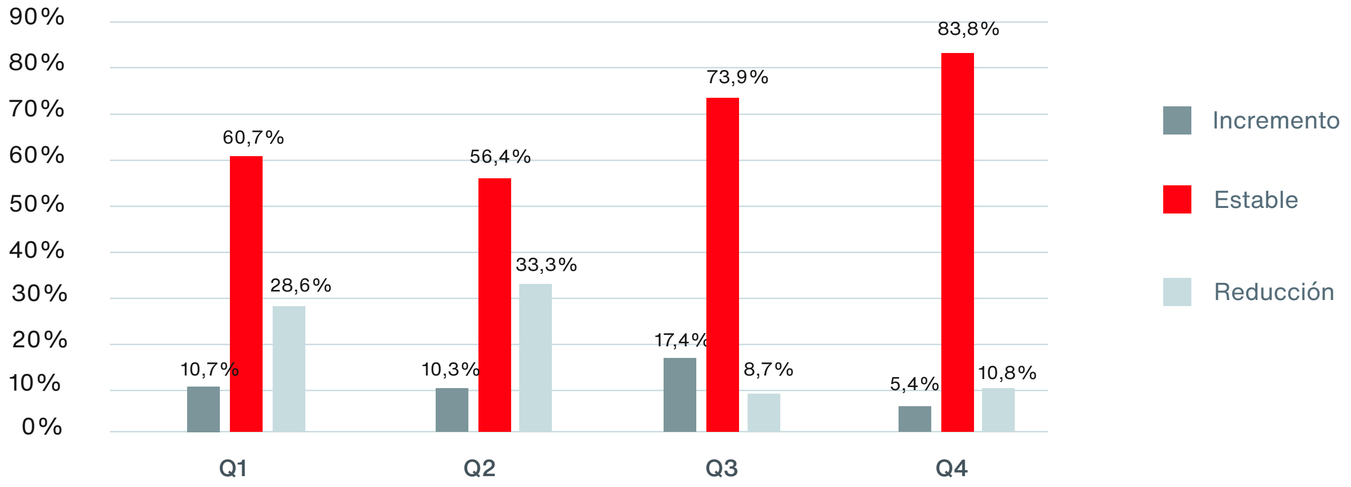


En el proceso de renovación, aproximadamente el 60% de los clientes experimentaron un incremento en sus franquicias, mientras que un 8% experimentó una reducción. Este último caso, que antes no se había observado en una medida significativa, resulta notable.

A finales de 2022, se pudo observar una estabilización del mercado, lo que llevó a que los clientes mantuvieran sus límites en comparación con el resto del año. Este patrón se hizo más evidente a principios de 2023, gracias a la flexibilidad que están mostrando las aseguradoras. Estas compañías están ofreciendo límites similares a los anteriores, pero aumentando las franquicias.

Este cambio de tendencia ha afectado también al proceso de suscripción. Las Aseguradoras tuvieron que reforzar durante 2021-2022, las herramientas a su alcance que les ayudara en la selección de sus riesgos. Muchos, utilizando los cyberscan para buscar vulnerabilidades que pudieran ser objeto de ciberamenazas, y se ampliaba la solicitud de información requiriendo cuestionarios específicos muy exhaustivos con cuestionarios diferenciados para el riesgo de ransomware.

Estos esfuerzos se centraron en mejorar los controles de los riesgos asegurados, así como en mejorar la selección de estos.



Este proceso desencadenó también en **revisión de términos y condiciones de cobertura y reevaluación del despliegue de capacidades.**

Cobertura para eventos de ransomware:

Las aseguradoras establecieron sublímites en la cobertura para eventos ransomware, lo que limita la capacidad de la póliza a un porcentaje reducido, generalmente entre el 30% y el 50%, del límite total contratado. Esto significa que, en caso de un evento de ransomware, la cobertura disponible puede ser considerablemente menor que el límite principal de la póliza. Además, algunas aseguradoras pueden introducir la figura del coaseguro, que implica que la compañía que adquiere la póliza debe asumir un porcentaje del impacto financiero del siniestro. Estos sublímites y la incorporación del coaseguro son medidas que se implementan para mitigar el riesgo asociado a los eventos de ransomware y equilibrar la carga financiera entre la aseguradora y la compañía asegurada. Es importante comprender estas condiciones y evaluar cuidadosamente los términos de la póliza, para tener una visión clara de la cobertura real y los costos que podrían enfrentar en caso de un incidente de ransomware.

Inclusión de cláusula de exclusión de Guerra:

A medida que los ciberataques se han vuelto cada vez más sofisticados y agresivos debido a la situación que se vive actualmente, las compañías de seguros han empezado a considerar la inclusión de cláusulas de exclusión de guerra en las pólizas. Estas cláusulas buscan proteger a las aseguradoras y limitar su responsabilidad en caso de ciberataques relacionados con conflictos bélicos.

La inclusión de dichas cláusulas en los contratos de ciberseguro es una respuesta comprensible por parte de las aseguradoras, ya que el entorno geopolítico puede tener un impacto significativo en el riesgo cibernético. A medida que aumenta la tensión en una región específica o en un conflicto internacional, el potencial de ciberataques patrocinados por gobiernos o grupos afiliados a ellos también se intensifica. En este contexto, las aseguradoras buscan salvaguardar sus intereses y evitar posibles reclamaciones masivas relacionadas con eventos de guerra cibernética.

Es importante destacar que las cláusulas de exclusión de guerra no son algo nuevo. En el pasado, en situaciones de conflictos bélicos o tensiones geopolíticas, las aseguradoras han implementado este

tipo de cláusulas en diversos tipos de seguros, incluidos los de daños y responsabilidad civil. Sin embargo, su inclusión en los seguros cibernéticos es un reflejo de la creciente relevancia de los ciberataques en el ámbito de la seguridad global y de la necesidad de evaluar y mitigar los riesgos asociados. Sin olvidar que desde 1 de Abril de este 2023 es algo impositivo en el mercado de Londres y de los principales proveedores de capacidad de reaseguro.

Capacidad disponible:

Es un aspecto que cambió mucho a lo largo del año, pasando de un inicio con mucha dificultad para conseguir capacidad a un final de año con nuevos aseguradores interesados en aumentar sus carteras de ciberseguros, respondiendo a la creciente demanda en este ámbito. Ha cambiado también la tendencia a lo largo del año, pasando de querer participar en capas de exceso muy altas a tener más interés en capas de exceso inferiores poniendo especial foco en el primer exceso.

Información de suscripción

La suscripción de seguros cibernéticos continúa siendo rigurosa, lo que implica la necesidad de recopilar una amplia cantidad de información sobre los riesgos involucrados. No se espera que esta rigurosidad se reduzca en un futuro cercano. Sin embargo, la naturaleza de la información requerida se ha vuelto cada vez más específica, y el valor agregado de las preguntas es cada vez más evidente. Los seguros cibernéticos actúan como incentivo para las inversiones en seguridad informática, ya que el retorno de la inversión en este ámbito se aprecia especialmente en las empresas que se sitúan por encima de la media.

En términos de las necesidades de información, los cuestionarios son comunes, y se centran principalmente en consultas relacionadas con el ransomware y la privacidad. También son habituales los escaneos de vulnerabilidades no invasivos, que permiten evaluar el nivel de riesgo de la organización asegurada.

La flexibilidad por parte de las aseguradoras varía según el caso, pero en general, las respuestas relacionadas con el ransomware suelen tratarse de manera muy estricta. Si no se cumplen los criterios mínimos establecidos, los riesgos pueden ser rechazados o pueden imponerse restricciones significativas en la cobertura.

Cobertura para eventos de ransomware:

Inclusión de cláusula de exclusión de Guerra:

Capacidad disponible:

Informe de suscripción

7.2. Siniestralidad en España en 2022.

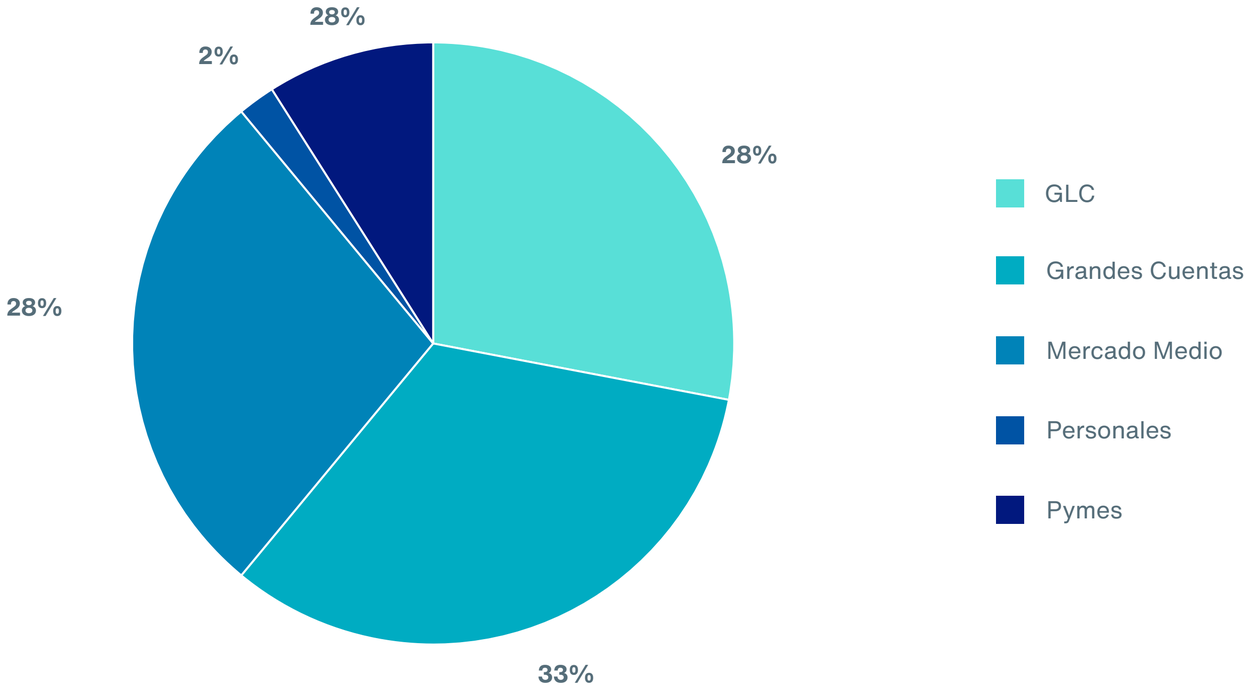
No podemos olvidarnos que el principal actor que ha determinado llegar a esta situación ha sido la siniestralidad.

En el grafico a continuación podemos observar como se ha ido incrementando la comunicación de siniestros a lo largo de los años y como esta comunicación se ha mantenido en los años 2021 y 2022.

Correspondiendo la gran mayoría de estas comunicaciones a grandes cuentas y clientes multinacionales globales. El mercado medio representa el **28%** de las notificaciones y de manera minoritaria las pymes o seguros personales.

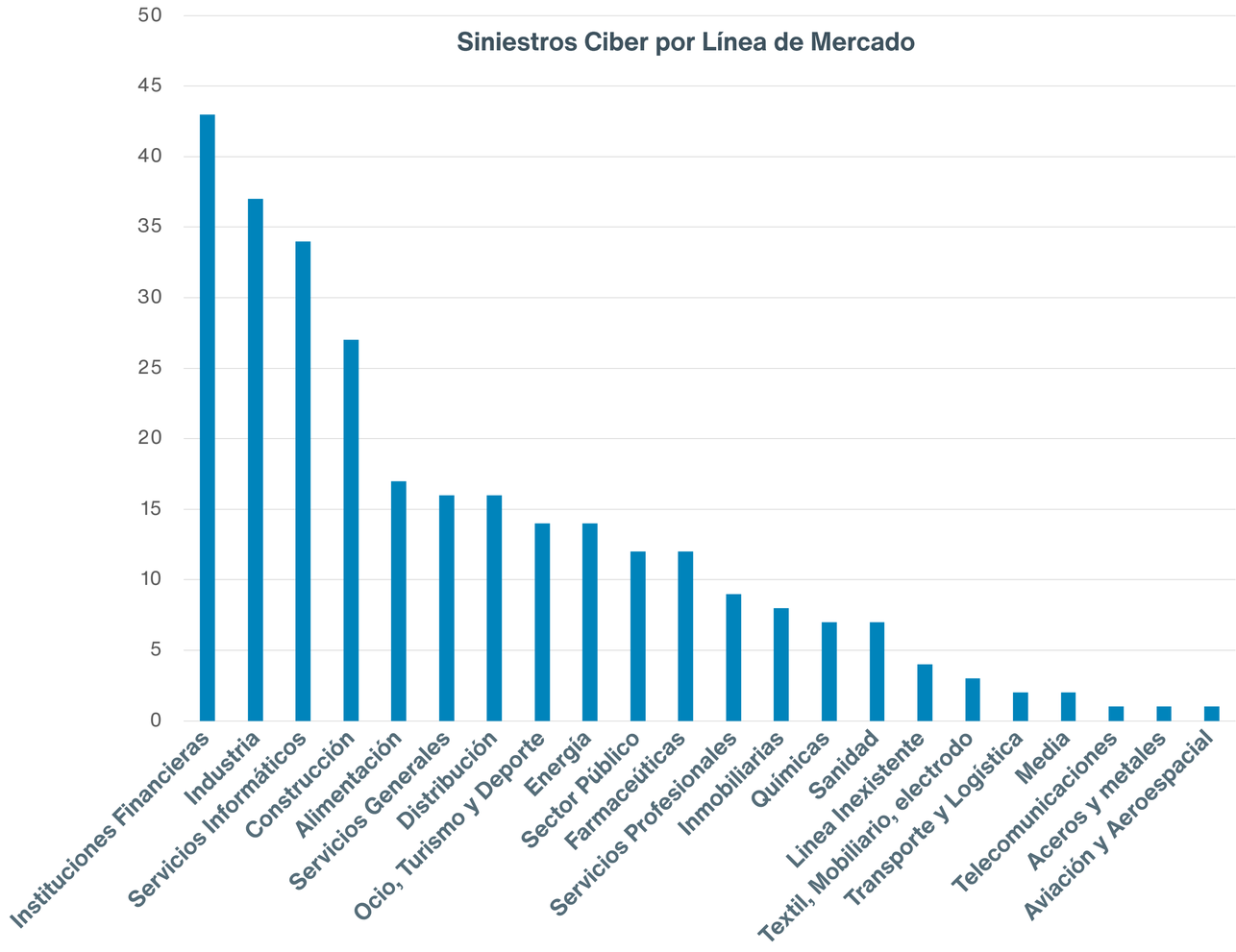
Grandes cuentas	**33%**
GLC	**28%**
Mercado Medio	**28%**
Personales	**9%**
Pymes	**2%**

Siniestros por Segmento de Mercado



Por otra parte, y también referenciado con el perfil de clientes que contratan este tipo de pólizas mayoritariamente, está el perfil de empresas con mayor número de notificaciones, según podemos observar en el gráfico a continuación.

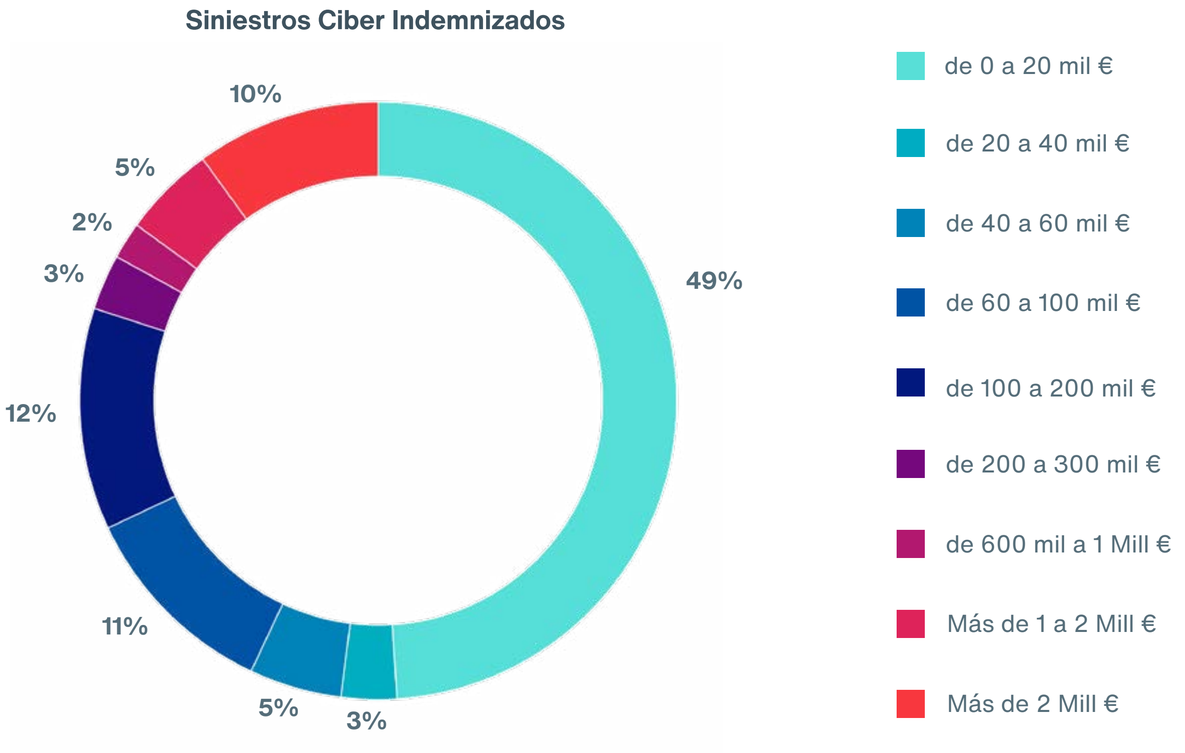
TOP SINIESTROS POR LÍNEA DE MERCADO
Instituciones Financieras
Industria
Servicios Informáticos
Construcción
Alimentación



En cuanto al tipo de eventos que se reportan son variados, siendo las más comunes instrucciones fraudulentas, compromisos de email y ransomware. También se han incrementado considerablemente en el último año los casos de cyber extorsión con exfiltración de datos.

Por último, nos gustaría centrarnos en el impacto económico que todas estas comunicaciones están teniendo en el mercado, donde en algunos casos, los límites contratados resultan insuficientes para cubrir la pérdida total sufrida. Hemos observado siniestros con indemnizaciones de más de 8 dígitos, lo que hace muy difícil mantener rentable un mercado relativamente maduro con un volumen de primas importante, pero en el entorno de los **EUR 120-140M anuales.**

El 10% de los siniestros indemnizados supera los 2M de euros de indemnización, teniendo en cuenta la tasa de prima por millón de la mayoría de las industrias, observamos que se puede convertir en un negocio no rentable.



7.3. Transferencia del riesgo al mercado asegurador.

A la hora de transferir este riesgo al mercado asegurador, el papel del bróker ha sido clave para trasladar a las aseguradoras toda la inversión realizada por las organizaciones en medidas de seguridad y los esfuerzos realizados en aras de generar relaciones de confianza y alianzas con las aseguradoras para que asuman determinados riesgos.

La inversión en ciberseguridad se ha convertido en uno de los principales indicadores de la relevancia de este aspecto para las organizaciones. A lo largo de los años, se ha observado un aumento significativo en el presupuesto que las empresas españolas destinan a la ciberseguridad. Específicamente, se ha registrado un incremento considerable en el año 2022, debido al crecimiento de los ciberataques, que se desarrollan de manera cada vez más sofisticada. Aunque, existe una notable variación entre los sectores en términos de inversión, algunos, como el de infraestructuras críticas, dedican un porcentaje considerable de sus recursos a fortalecer su ciberseguridad, en comparación de otros como puede ser el ocio y entretenimiento, el cual tiene una participación más lineal en términos de ciberseguridad.

Estos datos reflejan una mayor conciencia por parte de las organizaciones sobre la importancia de destinar recursos adecuados a la protección de su infraestructura digital. A medida que las amenazas cibernéticas continúan evolucionando, se espera que la inversión en ciberseguridad siga creciendo, tanto en términos absolutos como en la asignación de presupuesto por parte de las empresas. Esto permitirá fortalecer la capacidad disponible en el mercado asegurador y proporcionar una protección más sólida ante los riesgos cibernéticos.

Ya se hacía hincapié la pasada edición de las **principales áreas en las que estaban enfocando las aseguradoras para analizar los riesgos.** Ese mismo escrutinio no solo, ha continuado, sino que se ha intensificado. Medias como control de accesos, resiliencia del negocio, protección de los endpoints con EDR, copias de seguridad, manejo de las cuentas privilegiadas, protección del correo electrónico, segmentación de redes, tratamiento de datos, siguen siendo claves para poder transferir el riesgo al mercado. Veamos ahora en detalle cada aspecto.

1. Control de Accesos: con multifactor de autenticación, ha sido y sigue siendo unos de los controles esenciales para prevenir ataques de ransomware, especialmente en relación con accesos remotos por parte de empleados y terceros, así como usuarios privilegiados. Sin estas medidas, ya nos solo en correo electrónico y en remoto, sino para todas las aplicaciones, la mayoría de las aseguradoras del mercado ya no accedían a evaluar el riesgo.

2. Protección y respuesta en el endpoint (EDR): El uso de soluciones de protección y respuesta en el endpoint es esencial para detectar y responder rápidamente a posibles amenazas cibernéticas que puedan afectar los dispositivos y sistemas utilizados por la organización.

3. Ejercicios de phishing y capacitación en concientización cibernética: Por todos es conocido que el empleado es el eslabón más débil de la cadena, la formación de los empleados y tener establecidos programas de concienciación en materia de ciberseguridad para los empleados, es otro aspecto para destacar para prevenir los ataques de phishing. La protección del Correo Electrónico y la Web, disponer de herramientas que permitan filtrar correos y detectar adjuntos y enlaces potencialmente maliciosos, así como bloquear sitios web dañinos o sospechosos tanto dentro como fuera de la red corporativos se consideran básicos para tener el riesgo controlado en este aspecto.

4. Gestión de parches y vulnerabilidades de día cero: La implementación de un proceso efectivo de gestión de parches y la capacidad de abordar las vulnerabilidades de día cero de manera oportuna son considerados criterios esenciales para reducir el riesgo de explotación de vulnerabilidades conocidas.

5. Acceso seguro a través de RDP/VPN: Las aseguradoras esperan que las organizaciones utilicen métodos seguros de acceso remoto, como la configuración adecuada de Protocolo de Escritorio Remoto (RDP) o una red privada virtual (VPN), para proteger las conexiones externas a los sistemas de la empresa.

6. Plan de respuesta a incidentes y ejercicios de ransomware: La existencia de un plan de respuesta a incidentes, así como la realización de ejercicios específicos para hacer frente a ataques de ransomware, demuestran la preparación de una organización para responder de manera efectiva y mitigar los impactos de un incidente de seguridad.

7. Control de acceso y cuentas de servicio: Otro aspecto que preocupa a las compañías a la hora de revisar sus riesgos es el manejo de Cuentas Privilegiadas. Tener implementadas herramientas PAM (Privileged Access Management) es otro aspecto importante que permite a las compañías asegurarse de que cada usuario tenga el nivel de acceso necesario para ejecutar sus labores. Es importante que las cuentas privilegiadas cuenten con MFA para el acceso.

8. Recuperación ante desastres y copias de seguridad: La existencia de un plan de recuperación ante desastres y mantener copias de seguridad offline y segmentadas del resto de la red, es otro aspecto donde las aseguradoras están poniendo el foco, dado que permite a las organizaciones recuperar sus datos íntegramente, reponerse de un ataque y evitar el eventual pago de una demanda de extorsión. Mantener una estrategia de seguridad para backups debe ser parte de la política de gestión de riesgo de las compañías.

9. Gestión de riesgos en la cadena de suministro: Las aseguradoras valoran la implementación de medidas de gestión de riesgos en la cadena de suministro para identificar y abordar posibles vulnerabilidades y amenazas derivadas de los proveedores externos.

10. Segmentación de redes y monitoreo de red (IT/OT): La segmentación de redes por geografía y/o funciones comerciales y el monitoreo tanto de los sistemas de tecnología de la información (IT) como de los sistemas de tecnología operativa (OT) son considerados criterios esenciales para limitar el impacto de un incidente en la infraestructura de una organización y detectar actividad anómala.

Otro punto importante es el **tratamiento de Datos Personales** e Información Sensible: Las políticas en materia de protección de datos deben estar alineadas con los requisitos de las normativas aplicables en cada uno de los territorios donde la compañía tenga intereses. La cantidad de registros almacenados y procesados debe estar identificada y actualizada.

En conclusión, el principal riesgo es aquel para el que se está menos preparado y la concienciación y la inversión en ciberseguridad siguen siendo las piezas claves.

7

En cualquier caso, y para poder transferir el riesgo de manera adecuada al mercado consideramos importante tener en cuenta lo siguiente:

1 Encontrar valor a través de la colaboración:

Es fundamental colaborar con expertos internos y externos, como profesionales de seguridad de la información, abogados y corredores de seguros, para priorizar los riesgos que la empresa considera relevantes y transferibles. Combinar este diálogo con un análisis financiero del impacto ayuda a desarrollar un marco que priorice los objetivos del programa de seguros.

2 Establecer objetivos a largo plazo para el programa:

El seguro ciber continúa proporcionando valor a los asegurados, aunque los cambios en el lenguaje de las pólizas propuestos por las aseguradoras pueden resultar frustrantes en algunos casos. La creciente competencia brinda a las empresas la oportunidad de considerar opciones de cobertura alternativas.

3 Mantenerse al tanto de las nuevas tendencias:

Los controles de seguridad clave que reducen la probabilidad de un evento de ransomware son parte fundamental del diálogo y del proceso de suscripción. Es importante tener una visión de futuro y estar al tanto de las nuevas tendencias.

8

Visión hacia el futuro: El fin del mercado duro

Visión hacia el futuro: El fin del mercado duro

En una década de comercialización del seguro de Ciber en España hemos pasado ya por diferentes etapas, desde su origen donde sorprendía a los asegurados la fácil contratación de estos seguros facilitando únicamente los datos del tomador y facturación, hasta un mercado duro sin precedentes, donde únicamente aquellos riesgos considerados **"best in class"** tenían opciones de contratar un seguro de ciber riesgos y a unas condiciones, no tan favorables como los asegurados esperaban. Todo ello tras someterse a rigurosos análisis de información y medidas de seguridad.

A lo largo de este 2023 estamos observado un mercado mas estable y favorable. Esta evolución está generando nuevas oportunidades para las empresas.

Son varios los factores de mercado que contribuyen a este cambio de tendencia.

Mejora de rentabilidades: Si analizamos la evolución de las primas vs la siniestralidad ésta continúa siendo de alto impacto, pero ha frenado la frecuencia.

Los incrementos de los últimos años en primas y franquicias han hecho que las aseguradoras mejoraran sus ratios de rentabilidad y ganaran en confort a la hora de suscribir riesgos nuevos, queriendo crecer en este ramo.

Los mercados nuevos y de retorno han aportado **nuevo capital** y competencia, lo que ha llevado a una mayor desaceleración de las tasas. Una capacidad sustancialmente nueva contribuirá a suavizar el mercado.

Aunque la capacidad sigue siendo limitada, sobre todo en capas primarias, ya no se limita de manera generalizada, sino en función del sector de actividad y las medidas de protección del riesgo analizado en concreto.

Las capacidades medias se mantienen en 5M por riesgo y 10M de manera excepcional. No obstante, están entrando nuevos mercados para proporcionar capacidad en capas de exceso por lo que se está empezando a impulsar una **mayor competencia.** Mercados internacionales se están estableciendo en España con alto interés en suscribir este ramo.

La mayoría de los aseguradores busca activamente el crecimiento, en particular en el segmento de grandes empresas con exceso elevado. En este primer trimestre de 2023 se ha observado **más recursos de suscripción** con importantes previsiones de crecimiento en este ramo por parte de las aseguradoras.

Según fuente del mercado asegurador, se estima un crecimiento del mercado global de seguros ciber de alrededor del **20%-30%** anual durante el 2023.

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. Pero esto se hace extensible a las Pymes, que también están en el punto de mira de los ciber atacantes desde hace un tiempo, por lo que se estima que este factor impulse la adopción de nuevos productos de seguros ciber por parte de este nicho de 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.

En 2023 estamos observando un mercado más estable y favorable.

Ciertas amenazas continúan preocupando al mercado asegurador como sigue siendo el entorno regulatorio cada vez más estricto (NIS2, CRA, Dora Directiva sobre acciones colectivas, Regulación sobre IA), desarrollo de nuevos malware y amenazas a partir de Inteligencia artificial, sigue la sofisticación de los ataques de Ransomware; y preocupa especialmente el riesgo de vulneración de activos de información a medida que avanza el desarrollo de la computación cuántica.

Los suscriptores siguen vigilando de cerca el entorno geopolítico, con preocupaciones específicas relacionadas con el posible aumento de los siniestros cibernéticos relacionados con acontecimientos bélicos en Europa del Este.

Las exclusiones de guerra, de infraestructuras y de “eventos generalizados” siguen estando en el punto de mira de los términos y condiciones.

Desde el 31 de marzo, el mercado del Lloyd’s de Londres exigió que todas las pólizas de seguro cibernético excluyan específicamente la cobertura de las pérdidas relacionadas con ataques o actos de guerra tras los que se encuentre un Estado. Esta imposición del mercado de Londres se está viendo reflejada en España, donde la mayoría de las aseguradoras están adoptando también la misma exclusión de guerra, en muchos casos, impuesta por su tratado de reaseguro.

Existe una inquietud generalizada en el mercado asegurador en relación con el potencial impacto de un evento catastrófico.

El **riesgo sistémico** tradicionalmente ha estado relacionado con el ramo de daños materiales, donde catástrofes naturales como terremotos, huracanes o inundaciones tienen impactos generalizados que afectan a muchos asegurados, pudiendo llegar a agotar la capacidad disponible de los aseguradores en el ramo. Igualmente puede ocurrir con un ataque cibernético que puede afectar a miles de asegurados diferentes en diferentes partes del mundo, teniendo que soportar pérdidas millonarias un mercado no tan maduro como otros ramos tradicionales. Esto unido a la falta de estadísticas en siniestralidad y los rápidos avances en tecnología hace que los mercados suscriban el riesgo sistémico con gran incertidumbre.

El crecimiento de este riesgo está directamente correlacionado con una mayor dependencia de proveedores SaaS por parte de las compañías, aspecto identificado por los hackers como una oportunidad que los ha llevado a concentrar sus esfuerzos en atacar sistemas interconectados complejos. Si pensamos en un incidente en algunos de los grandes proveedores en nube o proveedores de servicios de internet que prestan servicio a la gran mayoría de asegurados a nivel global, el impacto podría se devastador para el ramo.

Otra área donde incrementa cada vez más la atención, derivado en gran parte de las múltiples interpretaciones de la legislación americana que varía por estados, es la gestión que se hace de los **datos biométricos**, sobre todo, en determinados sectores que manejan un alto volumen de datos altamente sensibles. Debido a un aumento en las demandas colectivas resultantes de la recopilación, uso o retención indebidos de dicha información, cada vez, son más los mercados, que están analizando la exposición al riesgo, la gestión, recopilación y divulgación de información que se lleva a cabo mediante los datos biométricos, y establecen limitaciones e incluso exclusiones de reclamaciones derivadas de la gestión negligente de estos datos.

A pesar de que el proceso de suscripción siga siendo riguroso, es más ventajoso para las empresas, que están bien posicionadas y han invertido en seguridad con un riesgo considerado maduro. Reunir al equipo adecuado e invertir los recursos adecuados en toda la organización puede ayudar a conseguir mejores resultados de cobertura en la renovación.

En definitiva, durante el primer trimestre del 2023 estamos observamos que los precios empiezan a estabilizarse, sí es cierto que dependerá de la exposición al riesgo, del sector y de los incidentes sufridos y un aspecto muy importante, de las medidas de protección que hayan implementado esa organización, a raíz de los siniestros sufridos. Por otra parte, existe cierta incertidumbre o incluso miedo por parte de las aseguradoras de que esta estabilización no pueda perdurar en el tiempo, teniendo que volver en el corto plazo a una nueva rectificación de condiciones.

Riesgo sistémico

Datos biométicos

Factores que influyen en la estabilización de los precios:

- Exposición al riesgo
- Sector
- Incidentes sufridos
- Medidas de protección implementadas

9

Metodología

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 2022.

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 70% 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 2022, con independencia del tamaño y sector de actividad, por lo que comprende tanto el negocio del segmento medio como el correspondiente a 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.

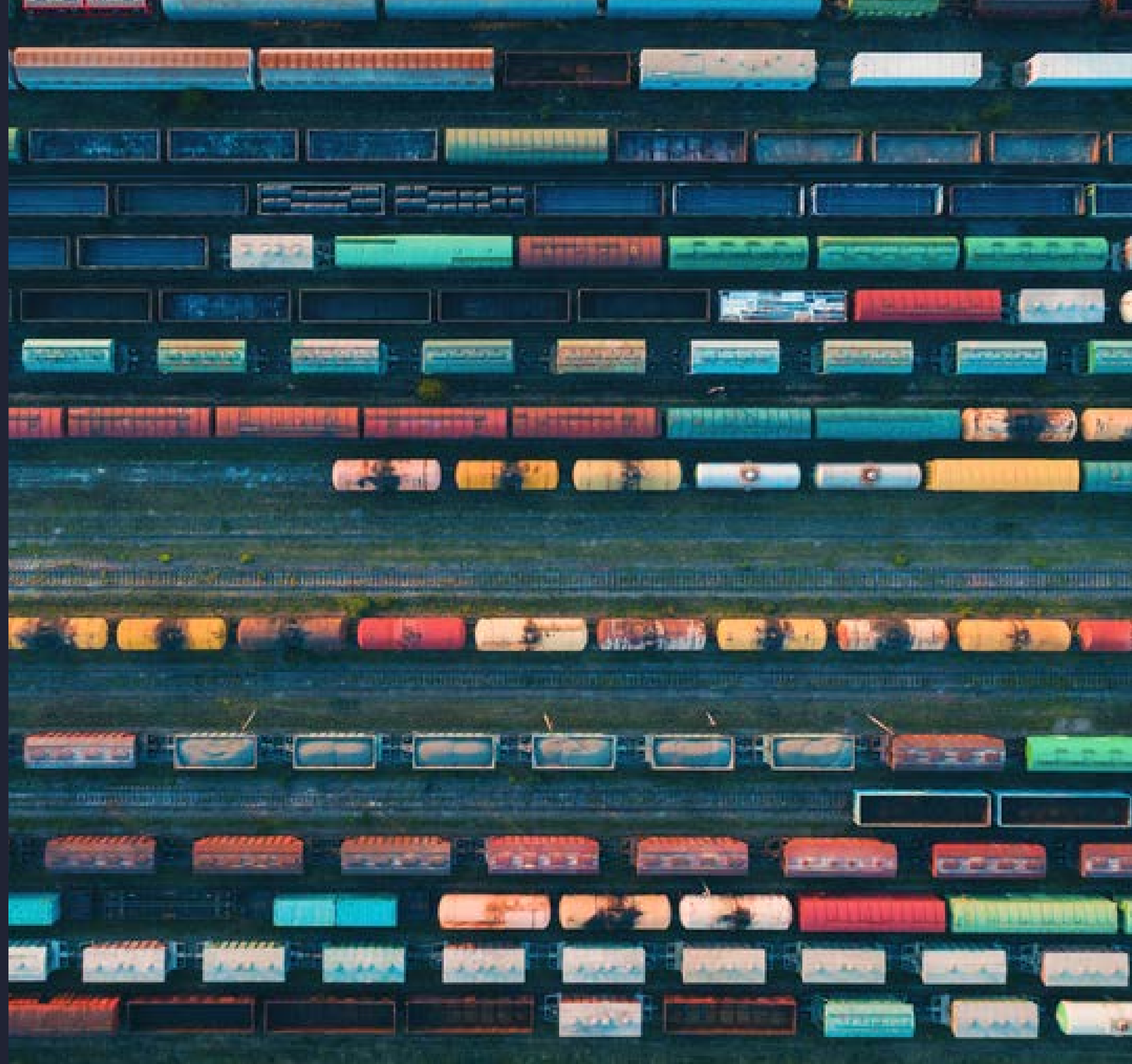
La cifra de primas permite conocer el volumen que corresponde a riesgos españoles de Ciber, con independencia de su tamaño, sector de actividad, ubicación geográfica o nacionalidad del asegurador.

Por tanto, este Estudio ofrece una radiografía nítida y precisa, a 31 de diciembre 2022, del seguro Ciber en España.

10

Glosario de términos

Glosario de los principales términos técnicos



10 Glosario de términos

Acuerdo de nivel de servicio (SLA): Contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para garantizar la calidad de dicho servicio.

Activo de información: Cualquier información o sistema relacionado con el tratamiento de esta que contenga valor para la organización (procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes, redes, equipamiento auxiliar o instalaciones).

Activo intangible: Activo que posee naturaleza no física, como por ejemplo patentes, derechos de autor, procesos o imagen de marca.

Activo tangible: Cualquier activo que posee naturaleza física, como por ejemplo sistemas o equipos informáticos.

Adware: Programa o contenido software utilizado para presentación de publicidad al usuario y que en ocasiones y dada su naturaleza puede contener archivos maliciosos o malware. Se convierte en malware en el momento en que empieza a recopilar información sobre el ordenador donde se encuentra instalado.

Algoritmo de cifrado: Operación o función matemática aplicada a un texto para cifrarlo (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida. Podemos diferenciar entre cifrado simétrico y cifrado asimétrico.

Amenaza: Cualquier acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Amenaza persistente avanzada (APT): Conjunto de procesos orquestados de forma sigilosa y continua, dirigidos a penetrar la seguridad informática de una entidad específica.

Análisis de impacto de negocio (BIA): Evaluación de criticidad y sensibilidad de los activos de información que determina el impacto por la pérdida de cualquier recurso, establece el escalado de la pérdida a lo largo del tiempo e identifica y prioriza los recursos mínimos necesarios para su recuperación.

Análisis forense: Proceso de recolección, evaluación, clasificación y documentación de la evidencia digital para facilitar la identificación de la amenaza, el alcance del compromiso y la metodología empleada.

Antivirus: Programa o contenido software específicamente diseñado para detectar, bloquear y eliminar código malicioso o malware.

Ataque de denegación de servicio (DDoS): Ataque a un servicio desde un único origen que provoca su desbordamiento debido al elevado número de peticiones y solicitudes, provocando la parada total o ralentización de este.

Ataque de fuerza bruta: Procedimiento automatizado que consiste en probar todas las combinaciones posibles de forma iterativa hasta hallar la contraseña o combinación correcta. También conocido como ataque de diccionario si se combina con ciertas expresiones o términos más específicos, reduciendo por tanto el número de combinaciones.

Ataque combinado: Procedimiento que se vale de métodos y técnicas sofisticadas que combinan diferentes tipos de virus informáticos, gusanos, troyanos y códigos maliciosos, entre otros y que se caracteriza por utilizar servidores y vulnerabilidades conocidas para iniciar, transmitir y difundir el ataque extendiéndose rápidamente y ocasionando graves daños, en su

mayor parte, sin requerir intervención humana para su propagación.

Auditoría de seguridad: Estudio que comprende el análisis y gestión de sistemas con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de los equipos de trabajo, redes de comunicaciones, servidores y/o aplicaciones.

Autenticación: Procedimiento de comprobación de que alguien es quién dice ser cuando accede a un repositorio y/o servicio.

Autenticación de doble factor (2FA): Método de autenticación basado en el uso de dos factores de autenticación independientes (contraseña y clave SMS, por ejemplo).

Autoridad de certificación: La Autoridad de Certificación (AC o CA, por sus siglas en inglés, Certification Authority) es una entidad de confianza cuyo objeto es garantizar la identidad de los titulares de certificados digitales y su correcta asociación a las claves de firma electrónica.

Autoridad de registro: Entidad que informa de la vigencia y validez de los certificados electrónicos creados y registrados por una Autoridad de Registro y por una Autoridad de Certificación.

Backdoor: Punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.

Backup: Copia de seguridad que se realiza sobre ficheros o aplicaciones con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Bomba lógica: Código software insertado de forma intencionada en un programa o sistema informático que permanece oculto hasta que se cumple la condición que se le programó, momento en el cual ejecuta una acción maliciosa.

Botnet: Conjunto de ordenadores, controlados de forma centralizada y remota, utilizados tanto para envío de spam como para la realización de acciones maliciosas o ataques de denegación de servicio.

Bug: Error o fallo inesperado en un programa de dispositivo o sistema de software que desencadena un resultado indeseado.

Centro de respaldo: Centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia.

Checksum: Valor calculado que se asigna a un fichero o archivo que garantiza que ni este ni su contenido ha sido alterado o modificado.

Ciberespionaje: Acto por el cual se obtiene información secreta, confidencial o personal sin permiso a través de la red o mediante el uso de técnicas complejas.

Ciberseguridad: Procesos, procedimientos y acciones orientadas a velar por la protección de activos de información, así como de la información procesada, almacenada y transportada por estos.

Cifrado simétrico: Técnica de codificación matemática que utiliza la misma clave para cifrar y descifrar la información. También conocido como “de clave privada”.

Cifrado asimétrico: Técnica de codificación matemática que utiliza un par de claves diferentes para el cifrado y

descifrado de información, garantizando el no repudio, así como la confidencialidad e integridad. También conocido como “de clave pública”.

Cloud computing: Alternativa para la provisión de servicios bajo demanda, basados y desplegados vía internet.

Confidencialidad: Función corporativa de seguridad de la información o atributo que garantiza que la información y los datos no serán divulgados a personas o sistemas no autorizados.

Contramedida: Cualquier acción o actividad implementada o dirigida a reducir el impacto de una amenaza o vulnerabilidad.

Cookie: Fichero que recolecta información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que se puede consultar la actividad previa y hábitos de navegación de este.

Criptografía: Técnica de cifrado de mensajes e información.

Cross-site scripting (XSS): Vulnerabilidad clásica que permite a un tercero inyectar contenido malicioso en páginas web visitadas por el usuario.

Command and Control (C2C): Herramientas y técnicas utilizadas por los atacantes de ransomware para mantener el control sobre los sistemas comprometidos una vez iniciado el exploit de los mismos.

Dark Web: Partes cifradas de Internet que no están indexadas por los motores de búsqueda y que son utilizadas por todo tipo de delincuentes, para comunicarse y compartir información sin ser detectados o identificados por las fuerzas de seguridad.

Data Loss Prevention (DLP): El objetivo de la DLP es evitar que los datos sensibles caigan en manos no autorizadas o malintencionadas, mediante diversas técnicas, como estrictos controles de acceso a los recursos, el bloqueo o la supervisión de los archivos adjuntos al correo electrónico, la prevención del intercambio de archivos de red con sistemas externos, el bloqueo de cortar y pegar, la desactivación del uso de redes sociales y el cifrado de los datos almacenados.

Disponibilidad: Función corporativa de seguridad de la información o atributo que garantiza que podemos acceder a la información y los datos cuando sea necesario haciendo uso de los canales adecuados siguiendo los procesos formalizados y comunicados.

EDR (Endpoint Detection and Response): Sistemas utilizados para el monitorio y recolección de datos en tiempo real, con un sistema de respuesta automatizado ante amenazas. Estos sistemas EDR además, son capaces de eliminar o contener amenazas, mientras se notifica a los equipos de seguridad.

Enmascaramiento: Técnica informática empleada para bloquear la visualización de información secreta, confidencial o sensible, como por ejemplo contraseñas o datos personales.

Equipo de respuesta a emergencias informáticas (CERT): Grupo y función especializada en responder y dar soporte en caso de contingencia tecnológica. Su misión principal es la de aplicar controles correctivos y eficaces, además de actuar como punto de contacto único en caso de ciberincidentes y en asuntos relacionados con los sistemas de información.

Escaneo de puertos: Acto de descubrimiento con el fin de identificar puertos abiertos en equipos y sistemas.

Escaneo de vulnerabilidades: Proceso orientado a la identificación proactiva de las debilidades de seguridad en una red o sistema de información.

Evaluación de riesgos: Proceso que comprende la identificación de activos informáticos y sus vulnerabilidades, así como las amenazas a las que se encuentran expuestos, su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Evento: Suceso que anticipa o sugiere la identificación de una amenaza posterior contra un activo de una manera que tiene el potencial de causar daño directamente.

Evidencia: Información que aprueba o desaprueba un problema determinado.

Exploit: Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto.

Firewall: Dispositivo de seguridad de red que controla las conexiones entrantes y salientes, decidiendo si autoriza o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad.

Firma electrónica: Conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico, permitiendo la identificación y garantizando la integridad y el no repudio.

Freeware: Software disponible de forma gratuita y uno de los principales medios de propagación de riesgos.

Fuga de datos: Pérdida de la confidencialidad de la información privada de una persona o empresa.

Función hash: Operación o función matemática que asigna o traduce un conjunto de bits a otro de modo que un mensaje produce siempre el mismo resultado utilizando el mismo mensaje como entrada, siempre y cuando no haya sido modificado o alterado.

Gateway: Dispositivo de red encargado de dar paso y entrada a redes internas o externas.

GDPR: GDPR (Reglamento General de Protección de Datos) es una ley de privacidad de datos que entró en vigor en la Unión Europea en mayo de 2018. La GDPR establece reglas para la recopilación, el uso y el almacenamiento de datos personales de los ciudadanos de la UE. El objetivo principal de la GDPR es proteger los derechos de privacidad de los individuos y aumentar la responsabilidad de las empresas que manejan datos personales.

Gestión de la configuración: Función orientada a gestionar la configuración de sistemas, aplicaciones y procesos a lo largo del ciclo de vida de estos.

Gestión de parches: Función de monitorización de sistemas que contempla la revisión, prueba e instalación de parches (y actualizaciones) en un sistema informático gestionado, con el objetivo de mantenerlo constantemente actualizado minimizando por tanto los riesgos de seguridad.

Gestión de riesgos: Función orientada a la coordinación de actividades para dirigir y controlar una empresa con respecto al riesgo.

Gobierno: Función propia del consejo de administración y ejecutivos que consiste tanto en el liderazgo como en la gestión de las estructuras organizacionales y procesos que aseguran y fortalecen los objetivos estratégicos de la empresa.

Gobierno, Riesgos y Cumplimiento (GRC): Estrategia

riesgos empresariales y el cumplimiento de las regulaciones, garantizando la protección de los activos y las operaciones.

Gusano: Código o software malicioso que tiene como característica principal su alto grado de dispersión.

Hacker: Persona con amplios conocimientos cuyo objetivo es el de obtener acceso no autorizado a un sistema informático.

Hacktivismo: Utilización no violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos.

Hijacking: Explotación y secuestro de una sesión de red válida para fines no autorizados.

IA:La Inteligencia Artificial (IA) en el entorno de la ciberseguridad se refiere al uso de algoritmos y modelos de aprendizaje automático para proteger los sistemas informáticos y las redes de ataques maliciosos y violaciones de datos. La IA en ciberseguridad puede ayudar a detectar y prevenir amenazas de seguridad en tiempo real, identificar patrones de actividad sospechosa y mejorar la capacidad de respuesta ante incidentes de seguridad

Impacto: Magnitud o nivel de pérdida resultante de una amenaza que explota una vulnerabilidad.

Incertidumbre: Dificultad para predecir un resultado debido al conocimiento limitado de componentes y recursos.

Incidente: Cualquier evento que no es parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción, o una reducción en la calidad de dicho servicio.

Indicador clave de riesgo (KRI): Referencia altamente relevante para la identificación de problemas y cuyo uso se centra en la rápida transmisión de información a nivel de reporting en términos de gestión de riesgos.

Informática forense: Proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial.

Infraestructura como servicios (IaaS): Provisión de acceso a recursos informáticos basados en un entorno virtualizado a través de una conexión pública.

Infraestructura crítica: Instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas.

Infraestructura de clave pública (PKI): Conjunto de procesos y tecnologías que permiten relacionar claves criptográficas y entidades de emisión de estas.

Ingeniería social: Práctica empleada para la obtención de información confidencial a través de conocimiento previo y la manipulación de usuarios legítimos.

Integridad: Función corporativa de seguridad de la información o atributo que garantiza que la información y datos son correctos y no han sido modificados, manteniéndose exactamente tal cual fueron generados, sin manipulaciones ni alteración por parte de terceros.

Intruso: Persona o individuo que obtiene acceso a la red, sistemas o recursos sin autorización.

Investigación: Proceso de recolección y análisis de las evidencias con el objetivo de identificar al intruso o responsable de un ataque, así como el posible uso o acceso no autorizado.

IoT: El término Internet de las cosas (IoT) se utiliza para describir objetos cotidianos que están conectados a internet y son capaces de recoger y transferir datos automáticamente, sin necesidad de interacción humana.

Keylogger: Software empleado para la recolección de toda actividad realizada mediante pulsaciones de teclado.

Latencia: Concepto utilizado para identificar el tiempo exacto que una orden necesita para ser transmitida a través de una red.

Mainframe: Equipo de alta velocidad y grandes dimensiones, da soporte a numerosas estaciones de trabajo o periféricos.

Malware: Software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.

MFA (Multi-Factor Authentication): En español, autenticación multifactor. Aplicación de diferentes categorías de credenciales para acceder a un sistema. Puede realizarse mediante un token físico o un token virtual que se envía a un segundo dispositivo.

Medio extraíble: Cualquier tipo de dispositivo de almacenamiento que puede ser extraído del sistema mientras está en uso.

Metadatos: Conjunto de datos relacionados con un fichero o archivo y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión.

Métrica de seguridad: Medición utilizada en la gestión de actividades relacionadas con la seguridad.

NIST Framework: Guía diseñada para ayudar a las organizaciones a mejorar su seguridad cibernética. Proporciona un conjunto completo de pautas, mejores prácticas y estándares de seguridad para proteger la información y los sistemas de una organización contra amenazas cibernéticas y ataques malintencionados. El marco se divide en cinco categorías principales: identificar, proteger, detectar, responder y recuperarse, cada una de las cuales aborda diferentes aspectos de la ciberseguridad.

No repudio: Envío de información a través con capacidad de demostrar la identidad del emisor de dicha información.

Normalización: Estructuración de la información y eliminación de datos no relevantes.

Objetivo de punto de recuperación (RPO): Volumen de datos en riesgo de pérdida que la organización considera tolerable.

Objetivo de tiempo de recuperación (RTO): Tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

Ofuscación: Codificación de textos y mensajes para que no evitar su entendimiento y contenido en caso de ser capturado.

PAM (Privileged Access Management): Herramienta para la gestión de identidades con capacidades de acceso especiales, generalmente para cuentas de mayor privilegio.

Paquete: Conjunto de información que contiene información de enrutamiento y de datos.

Parche de seguridad: Conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos.

Pentest: Prueba de ataque especializado a un sistema software o hardware con el objetivo de detectar vulnerabilidades para su posterior corrección.

Perímetro de seguridad: Límite que define el área de interés de la seguridad y la cobertura de la política de seguridad.

Pharming: Ataque informático que aprovecha una vulnerabilidad del software de los servidores DNS y que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

Phising: Estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir información confidencial de usuarios legítimos (contraseñas, datos bancarios, etc.) de forma fraudulenta.

Ping: Comando o una herramienta de diagnóstico que permite llevar a cabo una verificación del estado de una determinada conexión de un sistema de forma remota en una red.

Plan de continuidad de negocio (BCP): Plan que recoge la práctica documentada de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

Plan de recuperación frente a desastres (DRP): Proceso de recuperación documentado que cubre los datos, el hardware y el software crítico, para que un negocio pueda restaurar sus operaciones en caso de desastre, contingencia o acciones deshonestas por parte de terceros.

Plan de respuesta ante incidentes: Componente operacional de una gestión de incidentes que incluye procedimientos documentados y alineados para la definición de la criticidad de los incidentes, los procesos de presentación de informes y su escalado, así como los procedimientos de recuperación.

Plataforma como servicio (PaaS): Provisión de plataformas basadas en un entorno virtualizado a través de una conexión pública.

Política de seguridad: Documento que recoge y da soporte a las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos.

Privacidad: Atributo en términos de tecnología de la información que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos pueden ser compartidos con terceros, evitando su cesión no controlada o robo.

Probabilidad: Magnitud o nivel de ocurrencia resultante de una amenaza que explota una vulnerabilidad.

Procedimiento: Documento que contiene una descripción detallada de los pasos necesarios para llevar a cabo operaciones específicas en conformidad con los estándares aplicables.

Programa de seguridad de la información: Combinación global de medidas técnicas, operacionales y de

procedimiento y estructuras de gestión implementadas para proporcionar la confidencialidad, integridad y disponibilidad de la información en base a los requerimientos del negocio y el análisis de riesgos.

Protocolo: Conjunto de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier medio.

Proxy: Equipamiento o software encargado de proveer servicio y conectividad de forma segura, haciendo de intermediario entre las peticiones de los equipos de la red local propia hacia Internet.

Ramsonware: Software malicioso que una vez ejecutado facilita la toma de control por parte de un ciberdelincuente, secuestrando y cifrando la información del usuario de tal forma que esta permanece ilegible si no se cuenta con la contraseña de descifrado.

Red de área local (LAN): Red informática de alcance local y acotado al ámbito de una empresa o grupo de trabajo.

Red privada virtual (VPN): Tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada.

Resiliencia: Capacidad de un sistema o red para resistir a fallas o para recuperarse rápidamente frente a cualquier interrupción, generalmente con mínimos efectos.

Responsable de Seguridad (CSO): Figura responsable de todos los aspectos de seguridad de una organización, tanto físicos como digitales.

Responsable de Seguridad de la Información (CISO): Figura responsable de la seguridad de la información de una organización.

Riesgo: Combinación de probabilidad de un evento y su impacto.

Riesgo inherente: Nivel de riesgo o exposición base.

Riesgo residual: Nivel de riesgo o exposición resultante tras la aplicación de controles y medidas de mitigación y respuesta.

Rootkit: Conjunto de software diseñado para facilitar a un intruso el acceso administrativo no autorizado a un sistema informático.

Segmentación de red: Implementación de seguridad de red consistente en dividir la red de la organización en zonas que pueden ser gestionadas, controladas, monitorizadas y protegidas de forma independiente.

Segregación de funciones: Control interno básico que previene y detecta errores e irregularidades mediante la asignación de responsabilidades diferenciadas por usuario contribuyendo al registro de transacciones y acciones, así como a la custodia de los activos.

Sensibilidad: Medida del impacto que puede suponer la divulgación indebida de información.

Sistema de detección de intrusiones (IDS): Sistema empleado para supervisar la actividad de red e identificar patrones sospechosos que puedan suponer un ataque de red o sistemas.

Sistema de prevención de intrusiones (IPS): Sistema empleado para la protección de sistemas frente a ataques de red o sistemas.

Sistemas de Información: Combinación de las actividades estratégicas, gerenciales y operativas involucradas en la recolección, el procesamiento, el almacenamiento, la distribución y el uso de la información y sus tecnologías relacionadas.

Software como servicio (SaaS): Provisión de aplicaciones basadas en un entorno virtualizado a través de una conexión pública.

Spam: Conjunto de mensajes y emails no solicitados y

generados de forma automatizada que pueden contener riesgo de seguridad conforme a su contenido.

Spear Phising: Ataque de tipología phishing, donde se emplean técnicas de ingeniería social para hacerse pasar por un ente fiable para obtener información o contraseñas de la víctima.

Spoofing: Técnica de suplantación de identidad llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o mediante el uso de malware.

Spyware: Software malicioso que recopila información local y después la envía de forma remota sin el conocimiento o consentimiento.

Suplantación de identidad: Actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso o robo.

Token: Dispositivo o identificación que se utiliza para autenticar a un usuario de forma temporal.

Troyano: Software malicioso que se caracteriza por carecer de capacidad de autorreplicación.

Vector de amenaza: Camino o ruta utilizada por el adversario para obtener acceso al objetivo.

Vector de ataque: Camino o ruta utilizada por el adversario para obtener acceso al objetivo de forma activa.

Virus: Software malicioso diseñado para que, al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo y propagando su impacto.

Vulnerabilidad: Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas.

Vulnerabilidad 0-day: Vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y desconocidas por fabricantes y usuarios.

About Aon

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