Empower Results®

ESTUDIO ANUAL DE AON SOBRE CIBERSEGURIDAD Y GESTIÓN DEL RIESGO CIBER EN ESPAÑA

2021

HISCOX beazley GARRIGUES ANDERSEN

AIG AXA XL Insurance ZURICH TOKIO MARINE HCC QBE

ÍNDICE

1 Resumen ejecutivo

Principales conclusiones del estudio

Incremento de volumen de primas recaudadas:
A cierre 2020, el volumen de primas de Ciber recaudado es aproximadamente de unos 75 millones de €. El incremento respecto a 2019 se debe tanto a que sigue creciendo el número de empresas que transfieren el riesgo al mercado por primera vez, así como la propia tendencia alcista en primas como consecuencia del endurecimiento del propio mercado. En este sentido, identificamos un aumento de primas de renovación de entre el 25% y el 60%.

Novedades regulatorias:
Se ha producido un cambio de paradigma en materia de ciberseguridad debido a que la UE toma el papel de regulador global. Este tema pasa a ser una de las principales prioridades en su agenda y tiene claro cómo va a abordarla: mediante una intensa actividad regulatoria e inversión de gran cantidad de fondos europeos.

- Aprobaciones en 2020 por la UE: la Directiva sobre Resiliencia de Entidades Críticas (CER), el Reglamento de Resiliencia Digital Operativa (DORA), la Directiva NIS 2.

Inversión desigual en ciberseguridad y tecnología.
Existe una gran diferencia entre la inversión realizada por las distintas organizaciones en este ámbito, tanto en protección de sistemas como en digitalización.

- Aparición de barreras que impiden lograr los objetivos de negocio y que afectan a otras áreas: financiero, legal, innovación o reputacional.

Ransomware:
El factor COVID y la gestión del teletrabajo no se ha realizado aplicando todas las buenas prácticas desde el punto de la seguridad, lo que ha contribuido a un aumento de los casos de ransomware desde 2019 y durante todo 2020.
Las previsión de impacto económico de este tipo de ataques para 2021 está estimada en cerca de 20.000 millones de dólares, ya que el modelo de negocio está cambiando.

- Ya no se basa exclusivamente en 'pagar por descifrar' los datos, sino en pagar para evitar la publicación, así como impedir la interrupción del negocio.

- 2020:
  - 7 de cada 10 ataques de ransomware exfiltraron información sensible de la empresa y amenazaron con subastar el contenido en varios mercados de internet en caso de no pagar el rescate.
  - Se observaron variantes emergentes que inutilizaban los servidores y borraban los datos almacenados en ellos.

Siniestralidad:
Casi el 70% de la siniestralidad que se produce bajo las pólizas de seguro Ciber tiene su origen en ataques ransomware, compromiso de datos personales e ingeniería social.

- Entre 2017 y 2020 las notificaciones de siniestros por ataque de ransomware ha crecido un 200%.

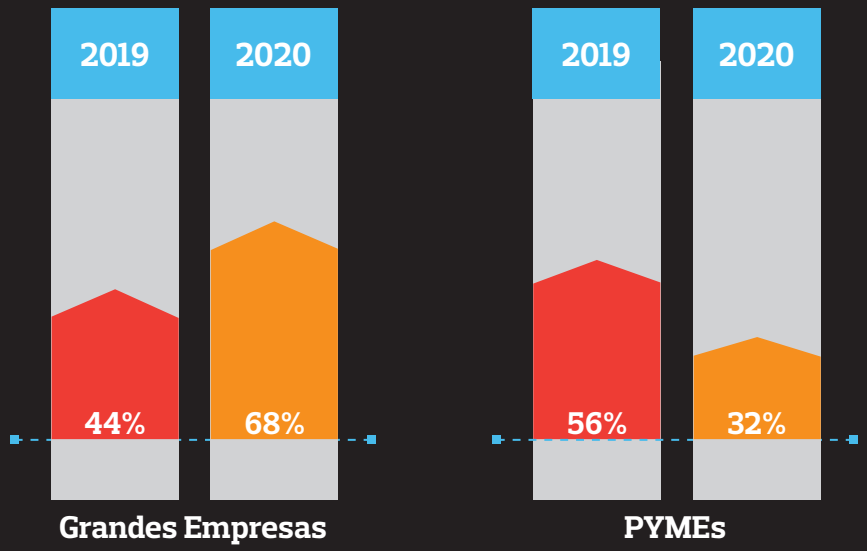
Contratación Seguros:
Las empresas con facturación superior a 250 millones de euros cada vez transfieren más su riesgo Ciber al mercado asegurador mediante la contratación de pólizas.

- En 2020 el segmento de Grandes Empresas representó un 68% de las contrataciones de Seguros Ciber en España, frente al 44% en 2019.

2020: 68%
2019: 44%

Sin embargo, el segmento PYME ha reducido la contratación de este tipo de seguros, pasando de un 56% en 2019, a un 32% en 2020 probablemente como consecuencia del impacto económico derivado de la pandemia.

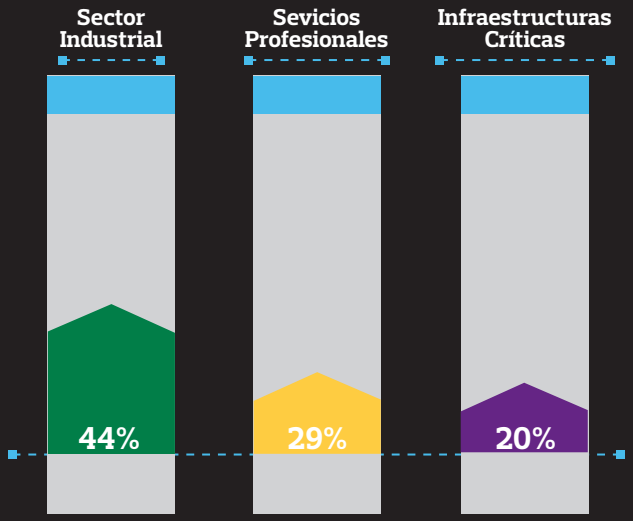
2020: 32%
2019: 56%



Sectores:
El sector más ciberatacado es el de la Administración Pública*.
Sin embargo se trata de un sector que apenas se protege mediante póliza de seguro, por lo que apenas existe siniestralidad registrada.

- El Sector Industrial es el que acumula mayor número de incidencias notificadas, con un 44% de las incidencias aportadas al mercado asegurador en 2020. Le siguen el sector de Servicios profesionales, con el 29% de siniestros declarados, e Infraestructuras Críticas (que incluye las entidades financieras) con un 20% de siniestralidad declarada.

Sector Industrial: 44%
Servicios profesionales: 29%
Infraestructuras Críticas: 20%



2 Estado de la Regulación en materia de Ciberseguridad: 2020 el gran cambio de paradigma

Vicente Moret Millás
Of Counsel Andersen
Letrado de las Cortes Generales

El 2020 será un año que no olvidaremos fácilmente entre otras cosas por la irrupción en nuestras vidas de una pandemia que ha hecho las funciones de cisne negro a escala global. Lo cierto es que uno de los efectos globales más destacados de la pandemia ha sido un cambio de paradigma en cuanto a la **aceleración y profundización de la transformación digital** de nuestras sociedades en todos sus aspectos; económicos, sociales e incluso culturales. Lo que se está digitalizando son nuestras vidas a un ritmo exponencial. Se habla ya no de una era de cambio, sino de un cambio de era que ha sido acelerado por la pandemia de un modo exponencial.

En el contexto de esta disrupción digital, la **preocupación por la ciberseguridad** ha ido en aumento. Al digitalizar de forma masiva todas las esferas de nuestras vidas estamos ampliando la superficie de ataque que tanto actores estatales como no estatales aprovechan para afectar a la seguridad de las redes y sistemas. La ciberseguridad ya estaba en todas las agendas como riesgo global antes de la pandemia. Ahora ocupa un lugar prioritario en las agendas de gobiernos, organismos internacionales y empresas. Cuando un riesgo se coloca con tanta fuerza entre las preocupaciones globales, una de las reacciones que los Estados y organizaciones internacionales ejecutan inmediatamente es la articulación de políticas públicas destinadas a mitigar ese riesgo mediante normas: tratados internacionales, leyes, reglamentos, directivas o recomendaciones.

La UE como regulador global de la ciberseguridad.

Este es precisamente uno los aspectos que más caracterizan el panorama actual de la ciberseguridad, la intensa actividad reguladora que se ha empezado a desplegar por algunos actores, especialmente la Comisión Europea, a la hora de intentar someter esa nueva realidad digital y especialmente la seguridad de ese nuevo medio, al Derecho, aplicando las categorías clásicas de derecho público a este nuevo entorno.

Con todas las dificultades que implica este intento por someter internet a los parametros de seguridad que exigimos en nuestra vida física, se está exigiendo a los Estados que actúen para proteger los derechos y libertades de los ciudadanos y el buen orden de la economía y de la actividad empresarial. Y ello es muy difícil precisamente porque la aplicación del Derecho en el ciberespacio tiene unas características especiales que hacen de ese esfuerzo una tarea muy compleja de ejecutar, empezando por la desaparición de la categoría central territorio, ámbito sobre el cual el Estado despliega su Soberanía.

Tampoco ayuda la categoría central de anonimato en la red que supone una dificultad añadida para la persecución del delito en la red y que es así mismo una categoría ajena al mundo de lo jurídico, ni la modificación del concepto tiempo, que en internet responde a una especie de eterno presente.

No obstante, se puede decir que pese a todo y especialmente tras la pandemia, las autoridades de todos los niveles han decidido empezar a regular en profundidad para proteger a sus ciudadanos y empresas y sus intereses, desde el prisma de la seguridad nacional. En este sentido 2020 ha sido un año lleno de novedades regulatorias, especialmente en el ámbito de la UE, en relación con la ciberseguridad y su marco normativo.

Si bien se puede decir que esa preocupación por regular cuestiones relativas a la ciberseguridad no es nueva, especialmente en el caso de la UE, lo cierto es que durante 2020 el ritmo, profundidad e intensidad de los cambios propuestos en el marco regulatorio han sido sorprendentes. Ya existía antes de 2020 un pilar regulatorio **NIS** que se colocaba al lado del otro gran pilar regulatorio en esta materia, el **RGPD**. Pero en 2020 ve la luz un nuevo pilar regulatorio llamado a colocarse al lado de los dos anteriores en cuanto a su importancia e impacto regulatorio: la Directiva Digital Operational Resilience Act (**DORA**).

En este sentido, 2020 ha supuesto un cambio de paradigma en cuanto al marco regulador de la UE en esta materia. En primer lugar, porque se ha colocado entre las mayores prioridades de la UE quien pretende articular un futuro cercano verde y digital. Por otra parte, porque **el concepto de riesgo** se coloca como eje central de cualquier actuación en este ámbito junto con su derivada que es la adopción del enfoque de defensa en profundidad basado en el triángulo tecnología, personas y procesos.

Además, otra línea general que se asienta con claridad es la de fortalecimiento de una **soberanía digital europea** frente a la predominancia en el ámbito digital de las empresas norteamericanas y chinas. Por último se puede decir que la UE está llevando a cabo una política en esta materia que ya le ha dado buenos frutos en otras áreas de regulación a nivel global: está intentando sentar las bases de una marco regulatorio que luego sea imitado a adoptado por países de fuera de la Unión, desplegando así una capacidad de influencia basada el soft power y que tenga como resultado la afirmación de los principios sobre los que se basa la UE: rule of law, protección de los derechos fundamentales y cumplimiento del derecho de competencia.

Por otra parte, y en cuanto a los Estados, especialmente los europeos, han decidido abordar esta nueva amenaza desde la óptica de la **seguridad nacional.** Una buena prueba de ello es la reciente Executive Order on Improving the Nation's Cybersecurity, de 12 de mayo, en la cual el Presidente Biden intenta dar respuesta a recientes incidentes de ciberseguridad como el que afectó a la red de oleoductos de la Costa Este en ese mismo mes de mayo de 2021.

La gran dependencia que tenemos de las redes y sistemas de información, hace imprescindible proteger al máximo las **infraestructuras consideradas como críticas,** que permiten funcionar adecuadamente a estas complejas realidades que son las sociedades modernas.

2020: el año en el cual la Ciberseguridad se colocó entre las prioridades políticas de la UE.

El contexto de la pandemia ha venido a acelerar la priorización de la ciberseguridad como pilar de la digitalización de la sociedad europea. En este sentido en el nivel Estratégico, es necesario comenzar por la publicación de la nueva Estrategia de ciberseguridad de la UE en diciembre de 2020.

Esta Estrategia, junto con la comunicación Shaping Europe's Digital Future, el Plan de Recuperación para Europa y la Estrategia de Unión de Seguridad de la UE constituyen el marco normativo de nivel estratégico que asienta las grandes líneas generales de cuales van a ser las actuaciones de la UE en esta materia.

1. A este respecto, es forzoso referirse a la **Estrategia de Seguridad de la UE para el período 2020–2025,** aprobada en julio de 2020, y que marca las líneas principales de acción en esta materia. La relevancia de la Estrategia reside en la fijación de unas prioridades que se traducirán en nueva normativa y políticas europeas, que su vez serán aplicadas por los Estados, los cuales siguen siendo los principales responsables de la seguridad de los ciudadanos.

   Entrando en el contenido de la Estrategia, se puede decir que de ella se extraen **dos grandes ideas:**

   - El ámbito digital y el físico se ponen en un plano de igualdad a la hora de garantizar la seguridad dada la tremenda dependencia de las redes y sistemas.
   - No se puede separar tajantemente la seguridad interior y exterior dado que las interconexiones son tales que forman un todo inseparable.

   Además, se señalan los ámbitos en los cuales la UE va a priorizar sus actuaciones de forma inmediata. Las **infraestructuras críticas** serán objeto de actuación para modificar y profundizar en el marco regulador ahora existente. Se impondrán nuevas obligaciones de protección y resiliencia a los operadores de estas infraestructuras físicas y digitales, entre otros, en cuanto al despliegue de las redes 5G conforme a las recomendaciones ya publicadas por la Comisión.

   También se señala como prioritaria una iniciativa sobre **resiliencia del sector financiero,** que más tarde se concretó con la publicación del borrador de la Digital Operational Resilience Act (DORA) y un nuevo marco regulador para los drones, con el objeto de evitar su uso con fines delictivos. Así mismo, se promoverá una más estrecha cooperación entre agentes públicos y privados para asegurar mayor protección de los espacios públicos.

   También en el ámbito de la ciberdelincuencia, la Estrategia marca como prioridad aprobar una serie de medidas relativas a la cuestión central de la **identidad en internet.** Se prevé una **revisión del Reglamento eIDAS** que ayude a reducir la usurpación de identidad, y evitar así el creciente impacto del fraude online. La Estrategia también señala la relevancia de la delincuencia organizada como enemigo a combatir, señalando tres frentes prioritarios; el tráfico de drogas, el tráfico de armas y el de personas. Estas tres prioridades contarán con planes de acción específicos.

   En definitiva, lo que se propone en esta Estrategia **es generar capacidades, cadenas de suministro propias y soluciones tecnológicas europeas** frente a unas amenazas que evolucionan y se transforman con gran rapidez.

2. La **nueva Estrategia de Ciberseguridad de diciembre de 2020** es el segundo documento a tener en cuenta a la hora de entender las grandes decisiones de la UE. Pretende intensificar su liderazgo en las normas y estándares internacionales en el ciberespacio basados en el estado de derecho, los derechos humanos, libertades fundamentales y valores democráticos.

   En este sentido la Comisión propone modificar las normas sobre seguridad de las redes y los sistemas de información, mediante una Directiva sobre medidas para un alto nivel común de ciberseguridad en toda la Unión (Directiva NIS 2), que mejore y amplié a la normativa NIS 1. Las medidas adicionales incluirán apoyo dedicado a las pequeñas y medianas empresas (PYME), en el marco de los Centros de innovación digital, así como un mayor esfuerzo para mejorar la cualificación de los recursos humanos, atraer y retener al mejor talento en ciberseguridad e invertir en investigación e innovación abierta.

   En el ámbito internacional la UE apuesta por promover un **ciberespacio global y abierto mediante una mayor cooperación.** Ello se consigue fortaleciendo la seguridad internacional y la estabilidad en el ciberespacio mediante normas y estándares internacionales que reflejen estos valores fundamentales de la UE, trabajando con sus socios internacionales en las Naciones Unidas y otros foros relevantes.

La UE se compromete a respaldar la nueva Estrategia de Ciberseguridad con un nivel de **inversión sin precedentes** en la transición digital de la UE durante los próximos siete años, a través del próximo presupuesto de la UE a largo plazo, en particular el Programa Europa Digital y Horizonte Europa, así como el Recovery Plan, es decir el Next Generation Plan.

Por otra parte, la Comisión, consciente de la posición retrasada que ocupa ahora en el mundo de la economía digital, por detrás de EEUU y China, se pone como objetivo **reforzar las capacidades industriales y tecnológicas de la UE en materia de ciberseguridad.** La UE tiene la oportunidad única de poner en común sus activos para mejorar su autonomía estratégica, es decir su soberanía digital, e impulsar un liderazgo en ciberseguridad en toda la cadena de suministro digital, incluyendo datos, nube y redes 5G y 6G.

3. NIS 2

La Directiva NIS 1 fue un gran avance en materia de ciberseguridad. Lanzada en 2016, ha supuesto por primera vez una acción legislativa coordinada en toda la UE. Supuso la trasposición de esta norma mediante normas de desarrollo nacionales que en el caso de España se materializaron en el RD-ley 12/2018 y en el RD 43/2021. No obstante, la Comisión también es consciente que la **trasposición fue muy irregular** según los Estados y el nivel de disparidad regulatoria generada es realmente inadmisible si se quieren reforzar la resiliencia total de la UE en su conjunto. Por ello, la Comisión publicó el borrador de Directiva NIS2 que pretende solventar muchas de esas deficiencias producidas con NIS 1.

Para responder a las crecientes amenazas debidas a la digitalización y la interconexión, la Directiva propuesta cubrirá entidades medianas y grandes de más sectores en función de su importancia para la economía y la sociedad. NIS 2 **refuerza los requisitos de seguridad** impuestos a las empresas incluyendo cambios en la gobernanza interna de la ciberseguridad como las nuevas responsabilidades del Consejo de Administración.

Además, prioriza, igual que DORA, la seguridad de **las cadenas de suministro** y las relaciones con los proveedores. Agiliza las obligaciones de información, introduce medidas de supervisión más estrictas para las autoridades nacionales y, sobre todo, tiene como objetivo armonizar los regímenes de sanciones en los Estados miembros.

4. La nueva Directiva sobre resiliencia de entidades críticas (CER)

La propuesta de Directiva sobre resiliencia de entidades críticas (CER) es otra de las novedades que ha visto la luz en 2020. Amplía, actualiza y profundiza respecto a la directiva europea de infraestructuras críticas de 2008, ahora en vigor. Se aplicará a diez sectores: energía, transporte, banca, infraestructuras del mercado financiero, salud, agua potable, aguas residuales, infraestructura digital, administración pública y espacio.

Especial preocupación en este sector genera llevar a cabo un despliegue seguro de las nuevas redes 5G sobre las cuales va a pivotar la sociedad digital europea. En este sentido la Comisión, alienta a los Estados miembros, con el apoyo de ENISA, a completar la implementación de la Toolbox 5G de la UU y a adoptar un enfoque integral y objetivo basado en el riesgo.

5. DORA

El 24 de septiembre, la Comisión Europea publicó la propuesta de Reglamento de Resiliencia Digital Operativa, (DORA) para el sector financiero. Se trata de **un antes y un después** en la regulación de la ciberseguridad en la Unión Europea. DORA supone la profundización en una senda ya iniciada con la Directiva NIS.

DORA establece un marco único europeo de obligaciones, principios y requerimientos en materia de ciberseguridad para uno de los sectores considerados estratégicos: el financiero. Así mismo, conviene resaltar que DORA es el primer paso, ya que la propia Comisión ha incluido en sus más recientes documentos la intención de extender a los demás sectores estratégicos, energía, agua, transportes y otros, los esquemas regulatorios incluidos en DORA.

Entre las novedades más desatacadas cabe resaltar: un nuevo enfoque de las actuaciones basado en el **riesgo;** la atribución de responsabilidad directas en esta materia al **consejo de administración** en relación con el establecimiento y cumplimiento de estrategias, políticas y protocolos adecuados; las nuevas responsabilidades del **CISO;** las políticas de identificación y clasificación de la información; el control del riesgo en la **cadena de suministro,** la obligatoriedad de los **planes de continuidad** de negocio en caso de ciberataque; o las correspondientes estrategias de **comunicación.**

A este respecto, es relevante resaltar la profundidad e intensidad del nuevo marco regulatorio que va mucho más allá de lo que hasta ahora había intentado la UE, fijando **vía reglamento** con efecto directo, una amplia variedad de nuevas obligaciones de cumplimiento normativo en materia de ciberseguridad. En este sentido, la propuesta de la norma, tal y como se ha publicado, imita el enfoque existente en el Reglamento de General Protección de Datos y establece como prioridad una gobernanza sólida de la ciberseguridad como un aspecto que debe ser parte integral de la organización. Se produce por tanto una **convergencia** entre las normativas encaminadas al cumplimiento normativo y seguridad de los datos (sean o no personales). Esta tendencia de plena conexión con el Reglamento General de Protección de Datos se refuerza si atendemos a los borradores de próximas normas a aprobar (NIS 2), que además refuerzan las sanciones (hasta un 2% de la facturación global del potencial infractor).

Otra novedad capital, que introduce nuevas obligaciones, son las relativas a los contratos de las entidades financieras con **terceros suministradores.** DORA establece un completo y exhaustivo marco descriptivo de esas relaciones contractuales, cuyo propósito es precisamente empoderar a las entidades financieras frente a las empresas tecnológicas que les prestan servicios.

Finalmente, el responsable interno elegido orgánicamente para dar respuesta a lo anterior es el **CISO** de la organización financiera. Si al DPO se le presuponía el dominio de la norma nacional y comunitaria y se le pedía un conocimiento en análisis de riesgo, consultoría de procesos, negocio y seguridad de la información, al CISO se le coloca en una posición relevante al tener responsabilidad sobre el cumplimiento normativo de los proveedores y al ser responsable frente a las Administraciones Públicas de determinadas obligaciones con amplias repercusiones legales, incluidas las de carácter sancionador.

En definitiva, DORA supone la introducción de un amplio elenco de nuevos principios y obligaciones que se suman al complejo y amplio marco regulador de la actividad de las entidades financieras. No obstante, si se tiene en cuenta el rápido e intenso proceso de transformación digital que estamos viviendo, y la exposición de las entidades financieras a los ciberataques, es coherente que la UE haya decidido comenzar a regular en profundidad. **Es el sector financiero el más preparado y avanzado** en materia de seguridad de las redes y sistemas. Las grandes inversiones que las entidades financieras realizan todos los años para mantener sus organizaciones y negocio protegidos, así como una sólida cultura de ciberseguridad interna, hacen que sea más factible empezar con este sector por los sólidos estándares de cumplimiento procedentes del marco regulatorio que están acostumbradas a afrontar.

Conclusión: 2020 es un Turning Point. La Ciberseguridad desde el principio en todos los sentidos.

La pandemia del Covid-19 ha sacudido a Europa y al mundo, poniendo a prueba los sistemas de asistencia sanitaria, las sociedades, las economías y en general, nuestra forma de vivir y trabajar. Por ello, la transformación digital acelerada ha irrumpido en nuestras vidas. Las nuevas tecnologías han mantenido a muchas empresas y servicios públicos en funcionamiento. Han ayudado a mantenernos conectados, a trabajar de forma remota y han permitido, entre otras, continuar con las actividades de formación en todos los niveles educativos. Este salto va a suponer cambios permanentes y estructurales en la vida social y económica y por ello la Comisión Europea, **obligada a actuar rápido para mantener el proyecto europeo acompasado con los tiempos digitales** que nos toca vivir y respecto a los cuales la UE ha quedado claramente atrás respecto a EEUU y China.

La UE es consciente de la necesidad urgente de **recuperar el tiempo perdido** y este 2020 nos ha traído la certeza de saber cómo lo va a hacer: mediante una intensa actividad regulatoria y mediante la inversión de gran cantidad de fondos europeos. El tiempo nos dirá si la estrategia fue la acertada. No obstante, y por lo que al presente se refiere, podemos estar seguros de una cosa: la regulación en materia de ciberseguridad va a tener un alto impacto regulatorio en las organizaciones y empresas. Especialmente en las más complejas.

Pero quizá la forma más inteligente de observar, entender y aplicar estos cambios regulatorios sea la de afrontar este nuevo paradigma legal no como una amenaza, no como obligación únicamente, sino como la oportunidad de convertir ese nuevo contexto regulatorio en palanca de cambio y transformación digital y de generación de una **nueva ventaja competitiva** que impulsará a las empresas que sepan entender estos nuevos tiempos.

3 Ciberseguridad y Privacidad

Alejandro Padín Vidal
Socio responsable del área de Privacidad,
Tecnología y Ciberseguridad de GARRIGUES

1. Introducción.

Vamos a tratar en este artículo de ofrecer unas líneas de aproximación a la relación entre la ciberseguridad y la privacidad. Para ello, expondremos inicialmente el marco regulatorio para, a continuación, desgranar las principales cuestiones en las que ambas materias se entrelazan. Por último, ofreceremos una visión práctica de algunos de los problemas que suelen ocurrir en el curso de ciberataques que afectan a organizaciones multijurisdiccionales. En estos casos, además de los problemas habituales de cualquier ciberincidente, se añaden otras dificultades derivadas del ámbito transnacional del evento.

2. Entorno regulatorio de la ciberseguridad.

Hasta no hace mucho tiempo, apenas había instrumentos regulatorios destinados específicamente a la ciberseguridad. Desde hace algunos años, sin embargo, a nivel europeo se ha elevado el nivel de sensibilidad institucional sobre esta materia y se han desarrollado diversas normas para conseguir incrementar la seguridad de las redes y sistemas de información y conseguir, de esta forma, reforzar la prevención, capacidad defensiva y resiliencia frente a ciberataques.

No es casualidad ese desarrollo normativo, sino el resultado de la constatación empírica de que la ciberseguridad es un elemento esencial de la seguridad en sentido amplio y del desarrollo social y económico de la Unión Europea.
De entre los diferentes mecanismos regulatorios existentes en la Unión Europea, se ha hecho uso tanto de la figura de la Directiva como, actualmente, del mecanismo del Reglamento. Como consecuencia de ello, tenemos en este momento un conjunto de normas de distintos tipos a nivel comunitario europeo y español[1], de entre las que, a los efectos el objeto del presente trabajo, queremos citar las siguientes:

- Directiva NIS (Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión).

- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (nos referiremos a estas normas que desarrollan la Directiva NIS como "normativa NIS").

Además, hay algunas normas en proceso de tramitación, como por ejemplo el futuro Reglamento DORA (sobre la resiliencia operativa digital del sector financiero), actualmente en fase de propuesta, que regulará a las entidades financieras, de seguros y todos sus proveedores de servicios tecnológicos.

[1] *Por su utilidad, hacemos referencia al Código de Derecho de la Ciberseguridad publicado por el Boletín Oficial del Estado, que contiene un amplio compendio de las normas aplicables en España en esta materia, y que se puede consultar aquí: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1*

3. Notificaciones a distintas administraciones derivadas de ciberincidentes.

Un elemento común a todas las normas anteriormente citadas es la existencia de obligaciones de notificación a determinadas autoridades administrativas.

Esta obligación es coincidente y paralela a la obligación de notificación de violaciones de seguridad de datos personales establecida en el RGPD cuando se ven afectados datos personales.

A. Plazo de notificación y consecuencias del incumplimiento

Los plazos que se establecen en la normativa son tremendamente exigentes. El RGPD establece un plazo de 72 horas, la normativa NIS señala que es obligatorio notificar los incidentes que son objeto de regulación a la mayor brevedad posible. La propuesta de Reglamento DORA, por su parte, establece un plazo de notificación dentro del mismo día hábil en que se produce el incidente o, en determinadas circunstancias, en las primeras 4 horas hábiles del día siguiente.

Como vemos se trata, en todos los casos, de plazos que no dejan capacidad de reacción si no se dispone de un procedimiento establecido y testado en la organización que permita cumplirlo.

B. Inicio del cómputo

Sabiendo que los plazos son tan cortos, la principal cuestión que se suele plantear cuando se produce un ciberincidente es la que, en términos jurídicos, se denomina el "dies a quo", es decir, a partir de qué momento hay que empezar a contar el plazo o cuándo ponemos el reloj a marcar la cuenta atrás.

Esta cuestión es esencial para una buena gestión de las consecuencias de un incidente, por varios motivos. En primer lugar, porque la buena gestión de la información necesaria para formular una comunicación temprana a las autoridades puede permitir extraer los elementos esenciales de la investigación en tiempo muy rápido, permitiendo centrar la investigación en las cuestiones más relevantes del incidente. En segundo lugar, el motivo es mucho más obvio, y es que la normativa establece graves consecuencias para el incumplimiento del plazo de notificación, que se reflejan en forma de sanciones.

Las sanciones pueden ir desde multas económicas de elevadísimos importes (hasta 20 millones de euros o el 4% del volumen de facturación global del grupo al que pertenece la entidad infractora durante el ejercicio financiero anterior, en el caso del RGPD) hasta sanciones penales, tal como prevé la propuesta de Reglamento DORA, que se podrían imponer, además, no solo a la entidad responsable, sino también a los miembros de los órganos de dirección o a otras personas físicas que sean responsables del incumplimiento.

Establecida, por tanto, la importancia de realizar la correspondiente notificación en plazo, ¿cuándo empezamos a contar ese plazo?

El plazo para el ejercicio de la notificación comienza, en el caso de la normativa de protección de datos personales, en el momento en que el responsable del tratamiento "haya tenido constancia" de la violación de la seguridad de datos personales. Como vemos, tampoco se establece de forma totalmente diáfana el inicio del cómputo. Por un lado, tenemos que tener muy claro qué debemos entender por una "violación de la seguridad de los datos personales"; por otro lado, tenemos que interpretar qué quiere decir la norma cuando habla del concepto de la "constancia" de la existencia de aquella.

Con respecto a la definición del concepto de violación de la seguridad de los datos personales, este se encuentra definido en el RGPD como "toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

En cuanto a en qué momento se puede entender que el responsable del tratamiento ha tenido constancia de la existencia de una violación de seguridad de los datos, habrá que estar al caso concreto. En algunos casos, esta constancia puede venir determinada por el resultado de la investigación forense de un incidente. En otras ocasiones, la constancia puede venir determinada por informaciones externas, bien del propio atacante que demuestra la exfiltración de los datos, o por la propia publicación de la información, si estamos ante un incidente causado por un ciberataque. Otros casos como la pérdida o destrucción de dispositivos, servidores o repositorios de datos, pueden ofrecer esa constancia de una forma mucho más directa.

En todo caso, habrá que estar al caso concreto y, sobre todo, ponerlo en relación con la propia excepción que ofrece la normativa: "a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas". Es decir, que la decisión final dependerá, también, del análisis de riesgos para los interesados que se pueda producir a raíz del incidente.

Como vemos, no se trata de una decisión sencilla o fácilmente identificable a priori. Sin embargo, debemos tener en cuenta que, tan importante como cumplir el plazo de notificación, es no adelantarse a una notificación intempestiva e innecesaria. Por ello, con el fin de poder cumplir el plazo de notificación de forma adecuada, y acertar, dentro de lo posible, con la decisión de realizar la notificación, es necesario disponer en la organización de un protocolo detallado en el que se establezcan los criterios, metodología y puntos clave para tomar la decisión, y se identifique perfectamente quién tiene la última palabra para tomar esa decisión.

Este protocolo ayudará a que esta línea de trabajo, una de las más importantes en caso de ciberincidentes, pueda desarrollarse fuera del fragor de la batalla que se plantea durante las acciones de respuesta ante este tipo de situaciones, evitando conflictos innecesarios y riesgos de errar en el análisis.

C. Notificaciones complementarias

Para poder cumplir con unos plazos tan rigurosos, suele ser necesario construir una notificación inicial que contiene tan solo la información preliminar del incidente, y suele ser imposible que en ella se pueda incluir información de detalle resultado de la investigación que, en el momento de esa primera notificación, normalmente todavía está en una fase muy preliminar.

Una vez realizada la notificación inicial, por tanto, suele ser necesario realizar una o más notificaciones posteriores de detalle, hasta llegar a la notificación de cierre del incidente, en la que se deberá trasladar a la autoridad todo el detalle del incidente y, en su caso, copias de los informes ejecutivos de la investigación. En la práctica, cuando la AEPD inicia un expediente de investigación preliminar tras una notificación, suele requerir la aportación de este tipo de informes.

Las autoridades designadas por la normativa NIS también solicitarán información de detalle y copias de los informes para poder analizar los detalles relevantes del incidente.

4. Incidentes multijurisdiccionales. Recomendaciones.

Hemos visto la dificultad de cumplir con la normativa en cuanto a las notificaciones a efectuar a los distintos reguladores cuando se produce un incidente de seguridad. Imaginemos ahora la problemática de cumplir esas mismas obligaciones cuando el incidente afecta a más de una jurisdicción.

Sobre todo, cuando el incidente de seguridad se ha producido por un ciberataque y si estamos en un grupo de sociedades, es habitual que los efectos del ciberataque se extiendan por todas o gran parte de las sociedades que forman parte del grupo. En grupos multinacionales, esto implica tener que lidiar con normativa aplicable en distintas jurisdicciones. Los incidentes más complejos son aquellos que, además, implican diversas jurisdicciones en distintos continentes (por ejemplo, varios países de la Unión Europea, Asia y Latinoamérica), puesto que los enfoques normativos pueden ser muy diferentes en cuanto a la exigencia de notificación, contenido de la misma y plazos.

En nuestra experiencia, la única forma de poder atender de una forma eficaz una situación de este tipo es contar con una preparación adecuada. Esta preparación pasa por disponer de un grupo de trabajo intragrupo en el que estén representados responsables con capacidad de dirigir equipos en distintas jurisdicciones, que hayan preparado una situación similar y sepan cómo responder llegado el momento.
En cierto modo, estaríamos ante la misma problemática que se plantea para responder ante otro tipo de riesgos tales como los incendios u otras eventualidades imprevistas y graves. Sin preparación no puede haber una respuesta eficaz.

D. Organización, coordinación y liderazgo

Además de esa preparación, o formando parte de la misma, es necesario contar con un buen asesoramiento local, pero coordinado de forma centralizada. Establecer un equipo de trabajo y una coordinación clara es clave para una gestión adecuada del incidente. Normalmente, y en nuestra experiencia, la mejor forma de acometer estas situaciones es disponer de un asesor legal cercano al centro de decisión del grupo, que será el encargado de involucrar y coordinar asesores locales en todas y cada una de las jurisdicciones afectadas. De esta forma, se puede simplificar enormemente el proceso de toma de decisiones, facilitando el entendimiento ordenado de la situación en cada país y la normativa aplicable en cada jurisdicción.

Hay un elemento fundamental para que todo esto funcione de forma ágil, es un elemento muy sencillo que, por desgracia, en muchas ocasiones perece bajo el pánico que surge en un ciberincidente y el caos que se produce. Ese elemento esencial es una correcta interlocución y actualización continua entre el equipo de investigación y el equipo de análisis y asesoramiento jurídico.

Ambas partes son fundamentales en la gestión de un ciberincidente. Desde luego, el asesor jurídico necesita de forma crítica conocer los avances y hallazgos de la investigación para poder dar el asesoramiento correcto. Pero también el equipo de investigación necesita orientar sus acciones hacia lo que es necesario buscar desde el punto de vista jurídico.

Cierto es que, cuando estamos en plena urgencia, las prioridades se suelen enfocar en la recuperación de la actividad y la continuidad del negocio. Por supuesto, esa línea de trabajo es fundamental. Pero no es menos crítica la línea de trabajo de investigación forense y la de asesoramiento legal. Todas ellas deben estar perfectamente definidas por adelantado y deben coordinarse y retroalimentarse de forma dinámica hasta que el incidente haya sido cerrado con garantías.

Imaginemos un ciberincidente como un accidente en un buque que navega por el océano, provocado por un iceberg que forma parte de una corriente de rocas heladas que se ha desprendido de los polos. Imaginemos que tenemos un agujero en el casco, daños graves en los motores, miles de pasajeros en pánico que necesitan seguir subsistiendo y un puente de mando que tiene que dirigir la estrategia de la situación de forma coordinada. Si los esfuerzos se centran únicamente en tapar el agujero del casco, pero desatendemos los daños de los motores, la ruta del buque y el cuidado y alimentación de los pasajeros, posiblemente conseguiremos tapar el agujero que hemos identificado, pero no podremos continuar navegando, no podremos evitar el hundimiento por otras rocas que impacten contra el casco y puede que algunos pasajeros se mueran de inanición. Será necesario que un equipo especializado se centre en cerrar el primer agujero, otro repare y ponga en marcha los motores, otro investigue la procedencia de los icebergs para establecer una ruta segura y otro se ocupe de tranquilizar y alimentar a los pasajeros. Todo ello, de forma coordinada y paralela.

5. Resoluciones en materia de ciberseguridad emitidas por supervisores en Europa.

Cuando acabamos de celebrar el tercer aniversario desde la fecha en que el RGPD es de aplicación obligatoria, tenemos ya algunas resoluciones de supervisores europeos en materia de protección de datos relacionadas con notificaciones de brechas de seguridad.

Vamos a referirnos a dos de ellas, las más relevantes por la cuantía de la sanción, que han sido tramitadas por el supervisor británico de protección de datos, la Information Commissioner's Office (ICO), con anterioridad al Brexit y, por tanto, bajo la plena aplicación del RGPD.

En primer lugar, tenemos una sanción a la compañía British Airways, a la que la ICO abrió un expediente por un importe inicial de 200 millones de libras esterlinas, del que resultó una sanción finalmente de alrededor de 20 millones de libras en el año 2020. El motivo, en este caso, en opinión de la ICO estaba relacionado con una supuesta falta de medidas de seguridad, que no habrían impedido que unos atacantes se infiltraran en la plataforma de venta de billetes de la compañía para robar información de pago que incluía números de tarjetas de crédito.

La segunda sanción que citaremos también fue impuesta por la ICO en el año 2020, esta vez a la cadena hotelera Marriot. Se trata de una multa de 18 millones de libras esterlinas, en un expediente iniciado con una posible sanción de 100 millones de libras. El motivo de esta sanción tiene un elemento adicional de enorme importancia, y está relacionado con la necesidad de verificar el estado de cumplimiento de una empresa en el momento de compra de esa empresa por otra, en el marco de las operaciones que se llaman de fusiones y adquisiciones (M&A, por sus siglas en inglés). La cadena Marriott había comprado en el año 2016 la cadena hotelera Starwood Hotels. Posteriormente, en 2018, Marriott conoció la existencia del ciberataque sufrido por Starwood en el año 2014, en el que habían resultado exfiltrados datos de millones de clientes. Marriott procedió a notificar la brecha de seguridad en 2018. La ICO considera que existió una falta de medidas de seguridad suficientes. En este caso, como se puede advertir, resulta esencial que en un proceso de compra de empresas la revisión que el comprador hace de la sociedad comprada no se quede en una mera revisión formal, al menos en lo que respecta a materias de ciberseguridad y protección de datos.

6. Conclusiones

Estamos en un entorno cambiante y en continua evolución, tanto desde el lado de los cumplidores como desde el lado de los incumplidores. Los riesgos son inherentes al uso de la tecnología, y la normativa se va adaptando de forma paulatina al entorno en el que se desarrolla la economía digital y sus vicisitudes.

Como colofón de todo lo mencionado recordaremos la importancia de conocer la normativa en materia de ciberseguridad, la existencia de interrelaciones muy directas con la normativa de privacidad y la necesidad de una buena gestión de un ciberincidente para evitar riesgos jurídicos, especialmente en cuanto a la posible notificación obligatoria de las violaciones de seguridad de los datos a las autoridades de supervisión.

4 Estado del arte: Gestión y tratamiento del riesgo cibernético

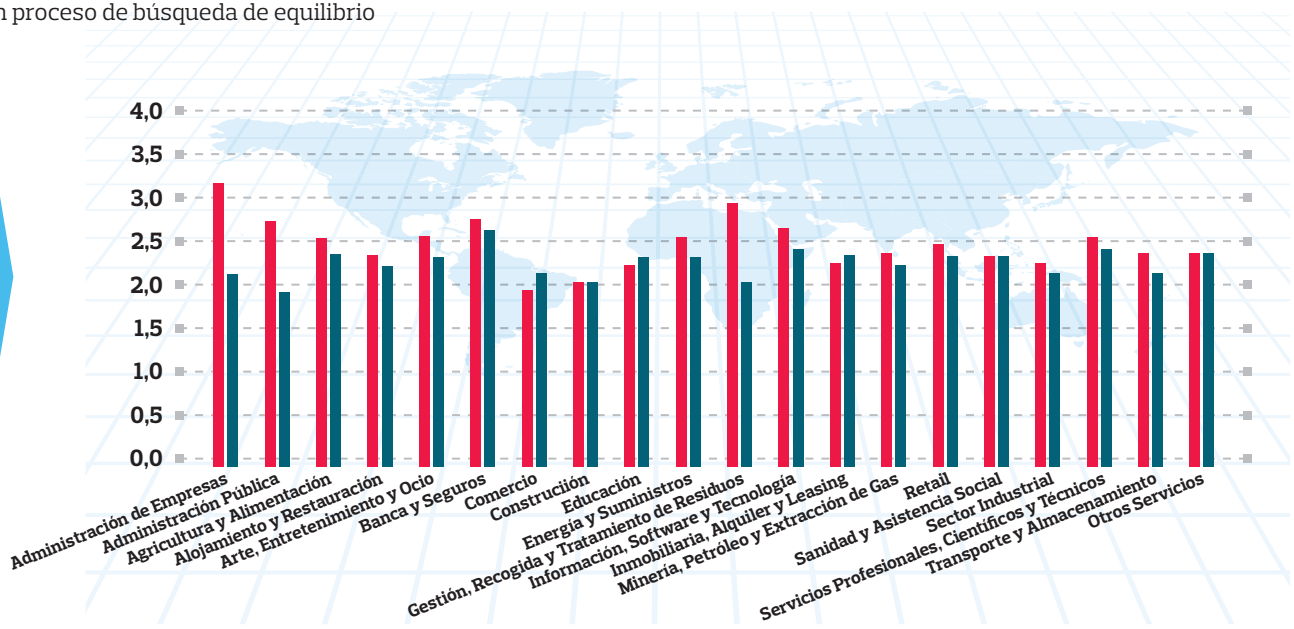
A medida que avanzamos en el tiempo, observamos cómo organizaciones y empresas, sobre todo aquellas consideradas como pymes o SME, mantienen una relación compleja con la ciberseguridad ya que deben permanecer en constante evolución y a la vanguardia de la innovación para tratar de alcanzar un nivel base suficiente y competitivo, presente y demandado por el mercado.

La inversión en ciberseguridad y tecnología, en cuanto a los sistemas de información se refiere, es desigual. Esto puede suponer y supone la aparición de barreras que impiden la obtención de los beneficios deseados, llegando a afectar a otros componentes de negocio, por ejemplo, a nivel financiero, legal o reputacional. El riesgo cibernético es amplio. Ahora más que nunca, los líderes empresariales se encuentran bajo una presión creciente. Los ingresos disminuyen y los presupuestos son limitados. A ello debemos añadir la constante presión por transformarse, la cual obliga a que las organizaciones asuman nuevos riesgos y retos, entre ellos ponerse al día en el ámbito de la ciberseguridad. Es un proceso de búsqueda de equilibrio entre el riesgo y la oportunidad.

La mayoría de las ciberamenazas a las que se enfrentan las organizaciones hoy en día no son nuevas: el uso de la tecnología, los dispositivos conectados, el ransomware y el riesgo interno, estarán siempre presentes. Apoyados en datos propios y en la visión de los expertos, este informe presenta el estado del arte del riesgo cibernético en España como comparativa y referencia dentro de entornos como el europeo o global, dado que el riesgo cibernético y sus amenazas anexas, no entienden ni de geografías o idiomas, ni tampoco de volúmenes de facturación.

Dentro del estudio, hemos identificado industrias, actividades y sectores de operación de referencia en nuestra geografía, y analizado su evolución a lo largo del último año. Se han considerado un total de 995 organizaciones y un total de más de 11.000 fuentes de datos para su elaboración, sirviendo como punto clave de referencia en el ámbito de la ciberseguridad.

Evolución de la Madurez de Controles de Ciberseguridad



Haciendo referencia al gráfico, se puede observar cómo tan solo el sector del 'Comercio' y la agrupación de sectores englobados bajo la actividad de 'Inmobiliaria, Alquiler y Leasing' han mejorado mínimamente durante este año. Otros como, por ejemplo, 'Construcción' y 'Sanidad y Asistencia Social' igualan valores a los identificados en el pasado año. El resto de los sectores, industrias y actividades de operación, reducen sus niveles de gestión y actuación con respecto a valores previos.

Todos ellos, no obstante, deben reforzar sus presupuestos de ciberseguridad durante el presente año, garantizando una adecuada gestión del riesgo bajo el establecimiento de niveles mínimos a lo largo de todas y cada una de las organizaciones abarcadas por estos.

Enfocándonos en concreto sobre cada una de las áreas bajo estudio, identificamos aquellas que en la actualidad están siendo más atendidas o, visto desde otro prisma, reciben mayor volumen de presupuesto y recursos para abordar y garantizar su seguridad y tratamiento en el tiempo.

Destacan por encima del resto los dominios de seguridad de 'Control de Acceso', 'Seguridad Física' y 'Seguridad de la Red'. Por el contrario, existen otros dominios y áreas que deben abordarse con urgencia. Podemos destacar entre ellas los dominios de 'Seguridad de Datos', Seguridad de Aplicación', 'Resiliencia de Negocio' y 'Proveedores'.

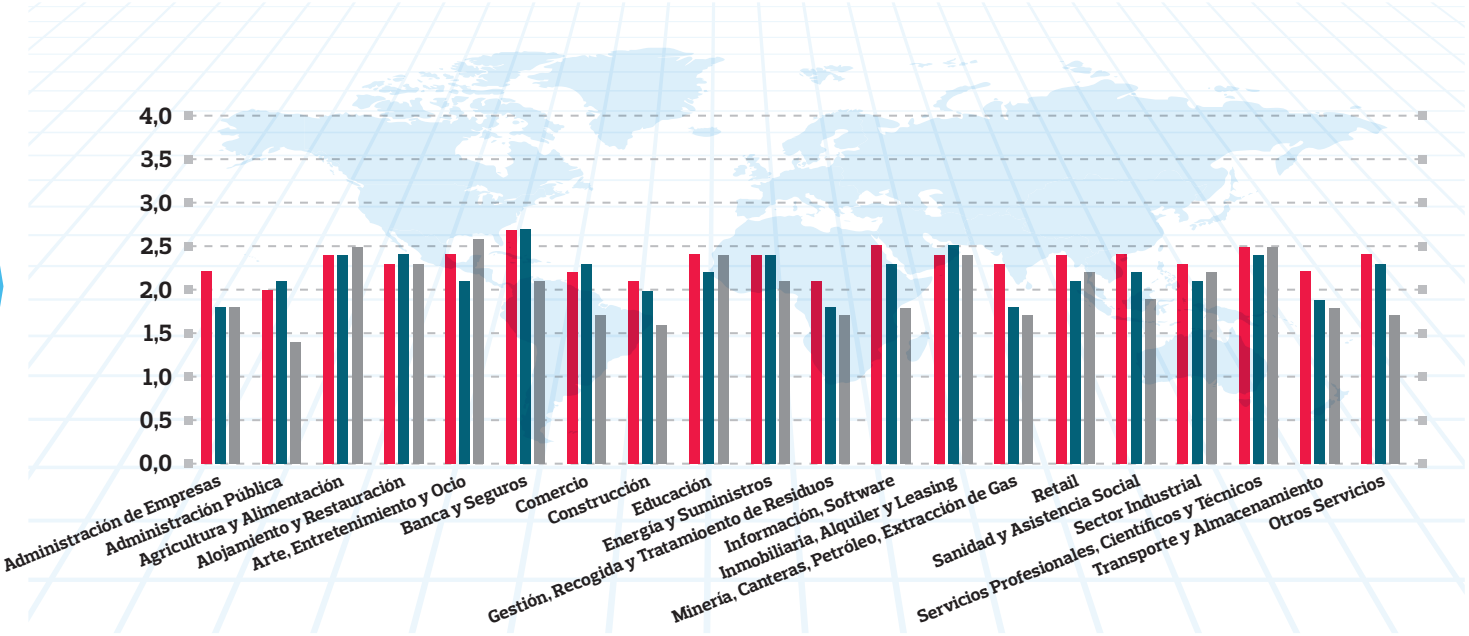
Todos ellos son ámbitos ampliamente agravados por el escenario de riesgos y amenazas actuales. La rápida evolución digital, el surgimiento de nuevas normativas y regulaciones o las amenazas concretas relativas al ransomware y riesgo de proveedores, confirman la patente necesidad de abordar rápidamente estos ámbitos, así como su previa identificación particular, caso a caso.

Los datos demuestran que las organizaciones, con independencia de su franja de facturación y sector, tienen un rendimiento inferior a valores aconsejables cuando se trata de gestionar la ciberseguridad corporativa y con ello la continuidad del negocio. Como era de esperar, los sectores considerados históricamente como agregadores de datos – Instituciones Financieras y Tecnología, Medios de Comunicación y Telecomunicaciones (TMT) – obtienen resultados más favorables que el resto. Sin embargo, ningún sector ha alcanzado un nivel de madurez en el que la gestión de los riesgos de ciberseguridad esté arraigada en la mayor parte de la organización.

Comprendida la tendencia general y asumidas las áreas de análisis cubiertas por este estudio, podemos identificar tanto aquellos sectores que aplican un mejor tratamiento de estos riesgos, como aquellos otros que tienen una gran oportunidad para abordar.

En términos generales y localizando el riesgo en España, desde un enfoque práctico, vemos como los valores asumidos internamente por las organizaciones siguen aún difiriendo de niveles mínimos y aconsejables, motivo por el cual es necesario abordar y facilitar servicios adaptados al mercado que proporcionen una identificación, mejora y, en definitiva, ganancia rápida de mayores niveles de gestión de riesgos. Asimismo, los recientes casos publicados en medios sobre ciberataques a empresas de estos sectores considerados 'más débiles' o incluso la propia Administración Pública, supone una ausencia de concienciación en este sentido. Todas y cada una de las empresas, públicas o privadas, con o sin ánimo de lucro, se ven impactadas y el panorama, al menos de momento, no presenta variaciones a presente y futuro.

Benchmarking Corporativo



Riesgo Crítico
Riesgo Moderado

	Valoración Global	Valoración EMEA	Valoración ESPAÑA
Administración de Empresas	2,2	1,8	▼ 1,8
Administración Pública	2,0	2,1	▼ 1,4
Agricultura y Alimentación	2,4	2,4	= 2,5
Alojamiento y Restauración	2,3	2,4	= 2,3
Arte, Entretenimiento y Ocio	2,4	2,1	= 2,6
Banca y Seguros	2,7	2,7	= 2,1
Comercio	2,2	2,3	▲ 1,7
Construcción	2,1	2,0	= 1,6
Educación	2,4	2,2	= 2,4
Energía y Suministros	2,4	2,4	▼ 2,1
Gestión, Recogida y Tratamiento de Residuos	2,0	2,1	▼ 1,4
Información, Software y Tecnología	2,5	2,3	= 1,8
Inmobiliaria, Alquiler y Leasing	24	2,5	▲ 2,4
Minería, Canteras, Petróleo, Extracción de Gas	2,3	1,8	= 1,7
Retail	2,4	2,1	= 2,2
Sanidad y Asistencia Social	2,4	2,2	= 1,9
Sector Industrial	2,3	2,1	= 2,2
Servicios Profesionales, Científicos y Técnicos	2,5	2,4	= 2,5
Transporte y Almacenamiento	2,2	1,9	▼ 1,8
Otros Servicios	2,4	2,3	= 1,7

Importancia de la Función de Gestión de Riesgos.

Esta función y sus departamentos anexos deben mantener una visión clara y amplia de todos aquellos riesgos presentes en el contexto de la organización, facilitando la asignación de recursos y su administración. Por ello, es adecuado contar con políticas, procedimientos y herramientas que faciliten esta labor y garanticen el adecuado seguimiento, tratamiento y automatización de estos, de forma que esto permita reducir y evitar incidentes e impactos, aportando valor a las actividades y descargando la carga de trabajo sobre aquellos aspectos más burocráticos y administrativos. Es por ello, por lo que este es un requisito esencial tanto de los estándares y marcos de Seguridad de la Información más importantes como de las mejores prácticas sectoriales.

La gestión de los riesgos cibernéticos es la siguiente evolución en términos de seguridad y riesgo tecnológico para las organizaciones que dependen, cada vez más, de procesos digitales y de innovación para administrar y garantizar la continuidad de las operaciones, más aún si cabe en el caso de pymes y SME.

Un buen gobierno corporativo permite la definición de una estrategia de gestión de riesgos garantizando la adopción de un enfoque alineado y organizado. Si el enfoque es correcto, reducirá los niveles de riesgo asociados a sus activos de información, protegiendo el negocio frente a algunas de las ciberamenazas actuales más comunes como el ransomware o el riesgo de proveedores, asumido y retenido internamente.

La Seguridad de la Información como marco de gestión corporativo.

La Seguridad de la Información es un elemento clave e integral de la gestión de riesgos que tiene por objetivo la protección del recurso más valioso para una organización, la información. En los últimos años, ha existido un debate sobre la relación coste-beneficio que esta provee al negocio, y por ello, esto ha influido en la práctica de la ciberseguridad, donde el aumento de los riesgos no ha supuesto un aumento igual o similar en términos de presupuesto disponible.

El valor de esta gestión debe justificar los costes de protección, por ello, el ajuste y la rentabilidad son elementos clave y necesarios para su conocimiento y alineación bajo los objetivos estratégicos, siendo necesario contar con procesos de identificación y evaluación, mejora continua, cuantificación, transferencia y respuesta. La correcta definición e implantación de estos procesos garantizará en mayor o menor medida la limitación de impactos no solo tecnológicos sino también legales, regulatorios, financieros y reputacionales.

En el proceso de identificación y evaluación, los riesgos son identificados, analizados y evaluados. Los resultados de este análisis se documentan para posteriormente ser priorizados, incluyendo amenazas y vulnerabilidades. También deben asignarse propietarios de riesgo e identificar las consecuencias que, tanto en términos de probabilidad e impacto, podrían afectar al negocio.

Tras la etapa de identificación y evaluación, nos situaríamos dentro del proceso de tratamiento y mejora del riesgo. Para ello, es necesario haber evaluado correctamente los riesgos y sus consecuencias durante la anterior etapa, ya que dentro de esta se prevé identificar e incluso definir objetivos de control y controles que permitan reducir el nivel de riesgo previamente identificado. En caso de no haber llevado a cabo una correcta evaluación, la respuesta provisionada al riesgo no será efectiva e integral.

El resultado de este proceso es una lista con medidas y objetivos de control, un plan de tratamiento de riesgos que incluye la aceptación de niveles de riesgo residuales, la definición o implementación de controles y solicitudes de cambios.
Tras ello, llega el momento de evaluar el impacto de los riesgos en términos financieros, y para ello el proceso de cuantificación es clave. Este proceso implica realizar un análisis detallado para determinar las consecuencias financieras resultantes en caso de pérdida sobre aquellos escenarios de riesgo cibernético identificados, valorando y cuantificando tanto la pérdida máxima estimada como de pérdida máxima probable de cara a facilitar la toma de decisiones y la posible transferencia del riesgo al mercado asegurador.

Como última etapa identificada dentro de la gestión de la ciberseguridad, identificamos el proceso de respuesta cuyo objetivo es detectar, informar, evaluar y gestionar incidentes. Los resultados de este proceso se utilizan para mejorar y fortalecer otras actividades como la gestión de cambios y la concienciación y formación a empleados.

La concienciación en materia de ciberseguridad debe basarse en el establecimiento de un programa de concienciación, formación y educación para garantizar que todo el personal reciba la educación necesaria en materia de ciberseguridad, mitigando el riesgo y reduciendo los niveles residuales aplicables.

Asimismo, a medida que los servicios son externalizados cada vez en mayor medida y grado, estos necesitan ser gestionados y controlados, no solamente delegados. Para ello es importante disponer de un proceso informado que permita definir procedimientos de selección, homologación y auditoría de proveedores.

Preguntas Clave y Reflexiones.

¿Cómo pueden las organizaciones estar mejor preparadas y protegidas? Además de concentrarse en las áreas de control de la seguridad identificadas en los cuatro temas clave de los ciberriesgos, a continuación, se ofrece un plan para ayudar a las organizaciones a formularse las preguntas adecuadas.

Evaluación

- ¿Cuál es el estado actual de nuestra seguridad y controles, en particular, en lo que se refiere a la evolución digital, el riesgo de proveedores, el ransomware y el riesgo normativo?
- ¿Cuáles son los activos más importantes que debemos proteger?
- ¿Cuáles son las amenazas más probables?
- ¿Cómo equilibramos las necesidades del negocio con los riesgos cibernéticos?

Cuantificación

- ¿Conocemos el tipo y la importancia de nuestras pérdidas potenciales? En el caso del ransomware, ¿conocemos esto más allá del riesgo de encriptación de datos?
- ¿Conocemos los principales requisitos normativos y los costes asociados al incumplimiento?
- ¿Cómo tomamos las decisiones de inversión en seguridad?
- ¿Podemos medir la eficacia de nuestra actual gestión de riesgos y seguros, en términos de coste total del riesgo (TCoR)?

Aseguramiento

- ¿Conocemos nuestros riesgos?
- ¿Disponemos de una estrategia eficaz para mitigar las pérdidas?
- ¿Debemos transferir una parte de nuestro riesgo al mercado de seguros o considerar estrategias alternativas de transferencia del riesgo?

Preparación para la Respuesta ante Incidentes

- ¿Tenemos un plan de respuesta ante incidentes apropiado, actualizado y en curso? En caso afirmativo, ¿está el equipo de respuesta formado y preparado para actuar?
- ¿Tenemos las herramientas, procesos y procedimientos de seguridad y forensics adecuados?
- ¿Hemos configurado correctamente nuestra tecnología de ciberseguridad?
- ¿Podemos responder rápida y eficazmente a un incidente?

5 Ransomware

Es innegable que los ataques de ransomware son la mayor fuente de dinero del cibercrimen, no solo actualmente si no en épocas pasadas. Los diferentes grupos criminales lanzan cada vez ataques más agresivos y amenazan con publicar los datos si no se procede al rescate, el cual puede superar el millón de euros.

A este escenario hay que añadirle el factor COVID y la gestión del teletrabajo, algo nuevo para muchas empresas. Esta gestión no se realizó aplicando todas las buenas prácticas desde el punto de la seguridad y han permitido un aumento de los casos de ransomware desde el 2019 y durante todo el 2020.

Las previsiones del impacto económico de este tipo de ataques para el 2021 está estimado cerca de los 20 mil millones de dólares, ya que el modelo de negocio está cambiando. Ya no se basa exclusivamente en 'pagar por descifrar' los datos, si no en pagar para evitar la publicación, así como impedir la interrupción del negocio.

Al finalizar el año 2020 se observó que 7 de cada 10 ataques de ransomware exfiltraron información sensible de la empresa y amenazaron con subastar el contenido en varios mercados de internet en caso de no pagar el rescate. También se observaron variantes emergentes que inutilizaban los servidores y borraban los datos almacenados en ellos.

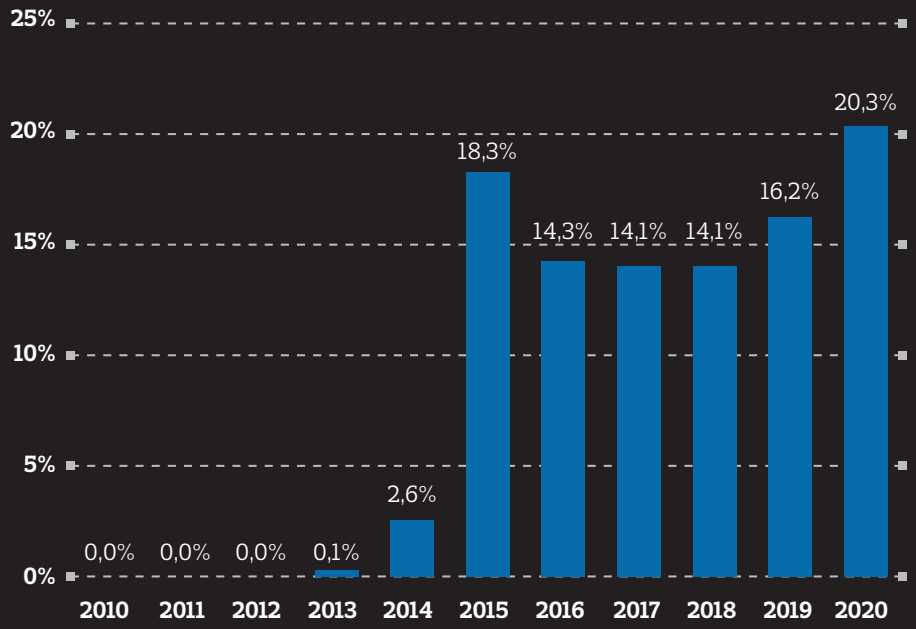


Ilustración 1. Incremento del uso de ransomware por años.

Durante este año 2021 se han visto diferentes ataques usando variantes del ransomware Ryuk y REvil. El primer malware ha estado activo desde 2018 y sigue en constante desarrollo y utilizado el grupo del que recibe su nombre mientras que el segundo apareció directamente en el 2019 como 'Ransomware as a Service''.

En España, el servicio público de empleo estatal (SEPE) fue atacado por Ryuk en marzo, dejando inutilizada la web, sistema de citas, correo, sistemas y bloqueando el trabajo a las oficinas presenciales y telemáticas en mitad de una crisis económica y pandémica. La falta de previsión ante este incidente provocó que los departamentos de sistemas tuviesen que restaurar una copia de seguridad almacenada en Archive.org, una organización sin ánimo de lucro que se dedica a recopilar todos los sitios web accesibles con la intención de documentar en vivo la historia de la red.

Según el director general del SEPE, no se solicitó ningún tipo de rescate, lo cual contradice la naturaleza de este tipo de ataques.

En Francia 2 hospitales han sido atacados con este tipo de ransomware en la misma semana de febrero. Una vez infectados, los departamentos de IT limitaron los intercambios de información, redes internas y conexiones con los demás hospitales de la red para evitar una propagación e impacto mayores. Aun así, varias operaciones tuvieron que ser pospuestas y varios pacientes tuvieron que ser reubicados en otros hospitales. También se vieron afectados los servicios de radioterapia y radiología, ya que los equipos quedaron inutilizados.

En este caso, el director general de la agencia de salud regional tachó de "barbaridad despreciable" atacar este tipo de infraestructuras y se negó a pagar el rescate, ya que "el pago no garantiza la recuperación de los datos" y que además "esto solo animaría a los piratas a atacar otros hospitales".

Total value received by ransomware addresses associated with sanction risk by ransomware strain, 2016–2020

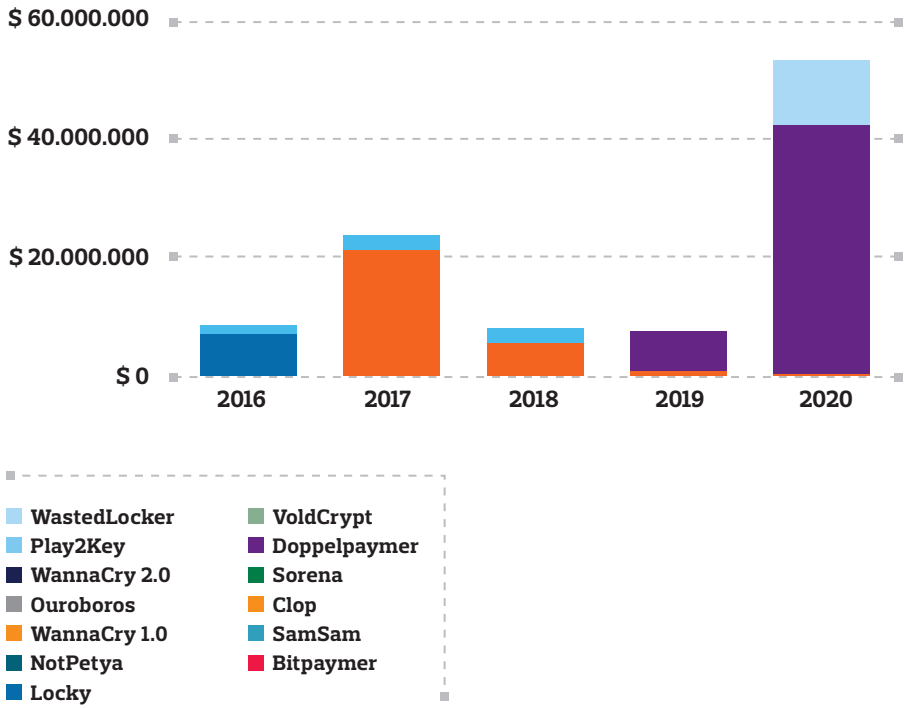


Ilustración 2. Cantidades pagadas a cuentas relacionadas con ataques de ransomware.

La agencia nacional de sistemas de seguridad de la información francesa (ANSSI) cree que este tipo de ataques usando el ransomware Ryuk ha sido un trabajo de un grupo ruso conocido por actividades similares.

También otro grupo ruso llamado Darkside se ha visto implicado en un ataque reciente a "Colonial Pipeline", en Estados Unidos, usando REvil como servicio. Esta empresa de oleoductos tuvo que parar sus casi 9.000km de tubería debido al ataque informático. Esta empresa contaba con sistemas muy vulnerables y conectados de manera "pobre" entre ellos y a la red, permitiendo una propagación más rápida y eficaz del ransomware.

Pese a la recomendación de no pagar, ya que no hay garantía de éxito, como comentó el director general de los hospitales mencionados antes, esta empresa reaccionó aceptando y negociando el pago. En este caso, se pagó alrededor de 5 millones de dólares a cambio de la herramienta para descifrar los archivos. Los delincuentes mandaron su herramienta para descifrar los archivos, pero era inservible debido a la lentitud con la que recuperaba los archivos originales.

Los expertos mencionan que los ataques usando ransomware seguirán creciendo en sofisticación, frecuencia y coste para las víctimas a no ser que se haga algo para evitar el pago a los criminales.

¿Qué puede hacer tu empresa? Es complicado indicar acciones de mitigación del riesgo concretas en este aspecto. Lo que sí es seguro es que se debería reducir la huella y exposición de demasiados servicios en internet, así como minimizar el impacto o robo de información sensible mediante mantenimientos, políticas, auditorias y revisiones de estas. Para ello, recomendamos contratar profesionales cualificados en identificar vulnerabilidades, establecer planes de continuidad del negocio y ofrecer una respuesta ante incidentes, sin dejar de lado otros vectores de ataque a las organizaciones como el phishing.

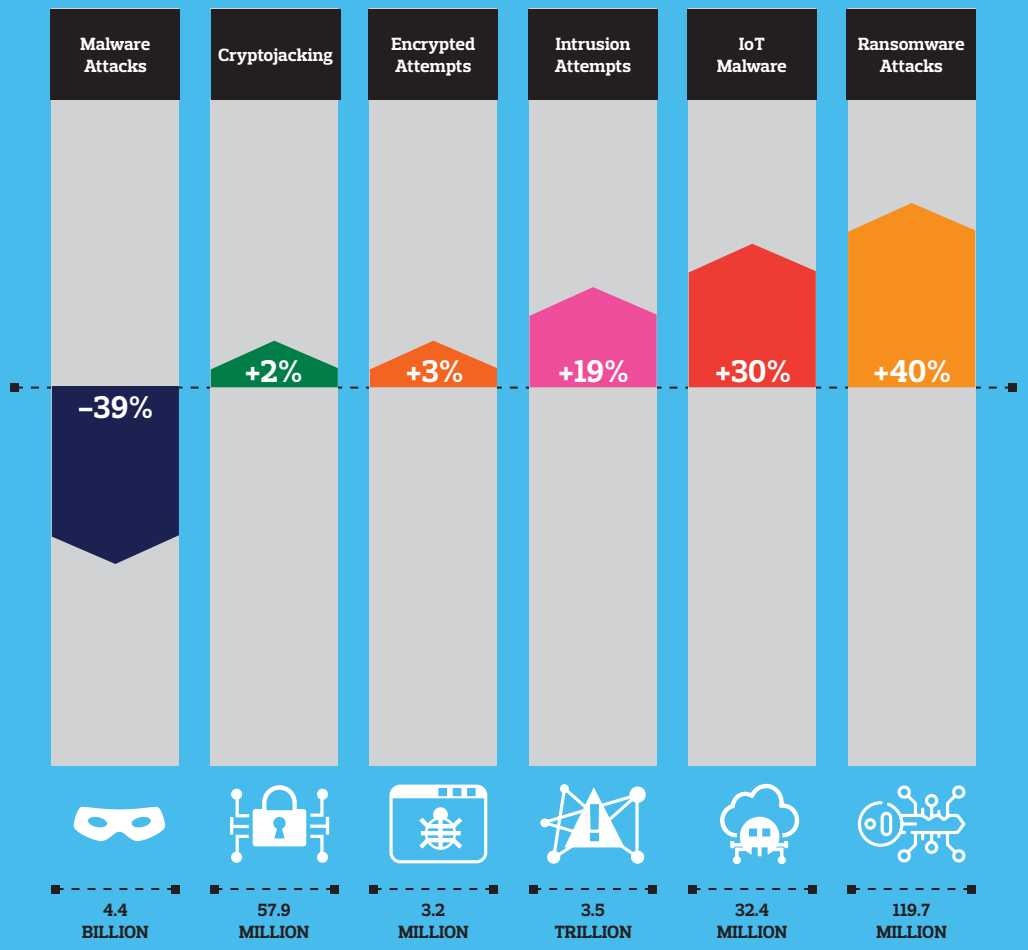


Ilustración 3. Análisis de tendencias en ciberataques.

6 Cómo las tendencias del 2020 han afectado a la suscripción del riesgo en España

Durante 2020, las aseguradoras alcanzaron, y en muchos casos superaron, un punto de inflexión a medida que la frecuencia y la gravedad de los siniestros superaban la mejora de la selección de riesgos y el aumento limitado de las primas. Este cambio se relaciona principalmente con la actividad del ransomware en todos los segmentos de empresas, pero principalmente en el espacio del mercado medio.

Las principales tendencias que identificamos en 2020 son:

1. Frecuencia de siniestralidad: durante el pasado año se registró un aumento de 3 nuevos siniestros por día hábil, a nivel mundial. Esto supone un aumento del 100% con respecto a 2019. Cabe destacar que este incremento estuvo relacionado sobre todo con ataque ransomware.

2. Siniestralidad de impacto: el impacto medio de las pérdidas fue en aumento a cada trimestre de 2020, destacando las pérdidas como consecuencia de ransomware, que llegaron a ser de 8 cifras. Muchos de estos siniestros siguen revisándose este año para cerrar las cifras que corresponden a pérdida por interrupción de actividad y se litigan reclamaciones por responsabilidad.

3. Primas: los incrementos en 2020, con respecto a 2019, fueron moderados, entre el 5 – 10% para mercado medio, mientras que, para grandes cuentas, con facturaciones anuales superiores a 500 Millones, el incremento se ha movido entre 25–40%. No obstante, la siniestralidad ocurrida ha venido a demostrar que fueron aumentos insuficientes.

4. Selección del riesgo: las aseguradoras han estado reforzando, durante 2020, las herramientas a su alcance para efectuar una selección del riesgo adecuada. Muchos están utilizando los cyber scan para buscar vulnerabilidades que puedan ser objeto de ciberamenazas, y se han incluido nuevos cuestionarios específicos sobre ransomware. Estos esfuerzos se centran en mejorar los controles de los riesgos asegurados, así como en mejorar la selección de riesgos.

¿Qué les preocupa a las aseguradoras y dónde ponen el foco en su análisis de riesgo?.

1. Ciber extorsión: el robo y el uso indebido de información personal identificable ya no es el objetivo principal de los cibercriminales. Los ataques de ransomware han evolucionado para incluir no sólo el cifrado de datos sensibles (incluida la IPP y la información corporativa confidencial) sino también la amenaza de exposición de dichos datos en Internet. Este tipo de ataques puede dar lugar a tiempos de inactividad de la empresa debido a las redes cifradas, así como a posibles consecuencias de responsabilidad en términos de sanciones administrativas o demandas de terceros.

2. El riesgo del proveedor: a medida que las organizaciones continúan adaptándose al entorno empresarial actual y a las necesidades del mercado asociadas, la dependencia de la tecnología de terceros y de las aplicaciones de back-end son mayores que nunca. Las normas de ciberseguridad de los proveedores son una parte fundamental de esta ecuación. El compromiso de SolarWinds y las recientes vulnerabilidades de Microsoft Exchange demuestran la complejidad de las relaciones con los proveedores de tecnología y cómo aumenta el riesgo frente a la ciberseguridad.

3. Trabajo en remoto: el teletrabajo ha contribuido a aumentar las vulnerabilidades potenciales como el software del Remote Desktop Protocol (RDP), la seguridad del acceso remoto, la dependencia de terceros proveedores de servicios de IT y la comunicación digital como el principal medio para compartir información.

4. Tecnología no cubierta: la coyuntura que se deriva de la pandemia COVID-19 ha acelerado las iniciativas de transformación digital de muchas organizaciones. La aparición de servicios y productos tecnológicos en sectores más tradicionales representa una exposición de IP potencialmente "descubierta" que puede no estar contemplada desde el punto de vista de la responsabilidad y las pérdidas financieras.

5. Incumplimiento de la normativa: el entorno normativo sigue creciendo en complejidad. Las recientes multas impuestas en virtud del Reglamento General de Protección de Datos (RGPD) de la Unión Europea demuestran que las organizaciones deben ser conscientes del impacto de una violación de datos. Más de 160.000 violaciones de datos se han notificado desde que el GDPR entró en vigor el 25 de mayo de 2018. Las **sanciones aumentaron casi un 40% en 2020**, alcanzando la cifra de 158,5 millones de euros, **siendo la mayor sanción de 35 millones de euros emitida por el regulador alemán**. La evolución en este ámbito podría traer consigo mayores problemas financieros desde el punto de vista de las multas y sanciones.

Consideraciones a la cobertura.

En respuesta a las tendencias de riesgo y siniestralidad descritas anteriormente, las aseguradoras están ajustando su enfoque de suscripción, revisando los términos y condiciones de la cobertura y reevaluando el despliegue de la capacidad.
Los siguientes son ejemplos específicos de consideraciones de cobertura que los asegurados están teniendo en consideración en 2021:

1. Cobertura de ransomware: las pérdidas asociadas son citados por muchas aseguradoras como un factor importante que impacta en sus ratios de siniestralidad. Si no se proporciona la información de suscripción adecuada, o si la información proporcionada se considera desfavorable, las aseguradoras pueden tratar de limitar su cobertura para las pérdidas por eventos de ransomware de la siguiente manera:
   - Varias aseguradoras están adoptando una estrategia en la que pueden limitar el agregado que ofrecen a algún factor del límite total de la póliza.
   - Se está proponiendo el coaseguro (con el asegurado), en algunos casos, junto con un sublímite.
   - Se están revisando los periodos de espera para los acuerdos de seguro de interrupción de la actividad empresarial relacionados con eventos de ransomware, que en algunos casos pueden llegar a ser de 24 horas.
   - En los casos más extremos, cuando faltan controles críticos, las aseguradoras pueden tratar de incluir exclusiones de "eventos de ransomware" en las pólizas.

Es fundamental tener en cuenta que, aunque las aseguradoras están utilizando estos enfoques para limitar su exposición, estas restricciones de cobertura no están diseñadas para aplicarse únicamente a un acuerdo de seguro de ransomware o ciberextorsión. Más bien, la restricción está redactada de tal manera que se aplica al ransomware como vector de ataque, y por lo tanto puede aplicar la limitación a cualquier pérdida que se derive de tal ataque.

2. Interrupción del negocio: El compromiso de SolarWinds ha hecho que las aseguradoras revisen su exposición global a los riesgos sistémicos, agregados y correlacionados, relacionados con la cadena de suministro de software, por lo que varias aseguradoras están revisando la amplitud de la cobertura ofrecida para las pérdidas por interrupción de la actividad, con la intención de limitar la exposición financiera a un evento sistémico de las siguientes maneras:
   - Reconsideración de los periodos de espera. En muchos casos, los periodos de espera se han negociado entre 6 y 8 horas (y en algunos casos se han eliminado por completo).
   - El mercado está empezando a presionar para que los periodos de espera se acerquen a las 24 horas.
   - Limitación de la exposición al límite agregado. Esto se está consiguiendo mediante la reintroducción de sublímites o la exigencia de coaseguro.
   - Incorporación de exclusiones específicas para SolarWinds, así como para el uso de sistemas obsoletos.

3. Proveedores de Primera Respuesta: A medida que los índices de siniestralidad se deterioran, las aseguradoras están revisando de cerca los costes de los proveedores de terceros en los que se incurre para investigar y responder a los incidentes cibernéticos.
   Para reducir (o al menos combatir el aumento de) estos costes, **las aseguradoras están demostrando menos flexibilidad en el uso de proveedores no pertenecientes al panel** o preacordados. Cada vez es más frecuente que las aseguradoras sólo reembolsen una cantidad igual a la que habrían pagado a un proveedor de panel teniendo que asumir el asegurado el resto de la factura de honorarios. Así mismo, **algunas aseguradoras han empezado a aplicar franquicia** en la cobertura de Primera Respuesta.

7 Evolución en la contratación de la póliza Ciber

Capacidad y dimensión del mercado español.

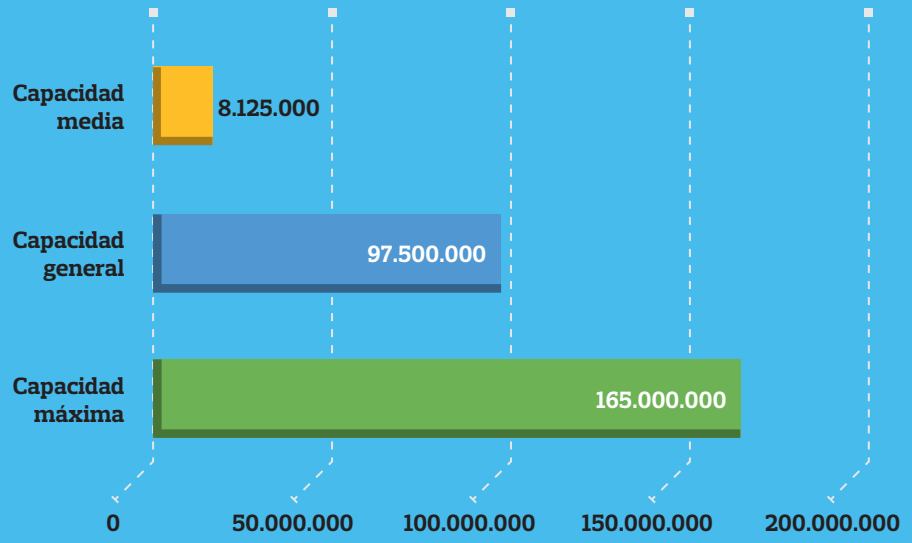
El mercado asegurador español tiene una **capacidad general para suscribir el riesgo ciber cercana a los 100 Millones €, pudiendo llegar la capacidad máxima a ser de 165 Millones €** en 2020, como mostramos en el gráfico 1.

Con respecto a 2019, identificamos una **reducción del 45% en la capacidad máxima y del 60% en la capacidad general,** dado que las capacidades máxima y general manejadas hasta entonces eran de 300 Millones y 250 Millones respectivamente.

Es obvio que esta restricción es consecuencia del aumento de siniestralidad, muy concentrado en ataque ransomware, que es consecuencia, en parte, de la coyuntura generada por la pandemia mundial y los siguientes decretos de estado de alarma habidos, que llevaron a la mayoría de las empresas a instaurar de manera rápida e improvisada el teletrabajo, lo que ha supuesto una reducción de los perímetros de seguridad y la fortaleza de las infraestructuras.

Esta situación ha puesto de manifiesto un endurecimiento del mercado, en cuanto a la suscripción del riesgo Ciber, dando lugar en primer lugar, a la reducción de capacidad. No obstante, cabe destacar que todavía se dispone de suficiente para cubrir los programas que más capacidad requieren ahora mismo en España, programas vinculados a las infraestructuras críticas y sector retail.

CAPACIDAD DEL MERCADO ESPAÑOL



Fuente: elaboración propia.

Contratación del Seguro Ciber por volumen de facturación.

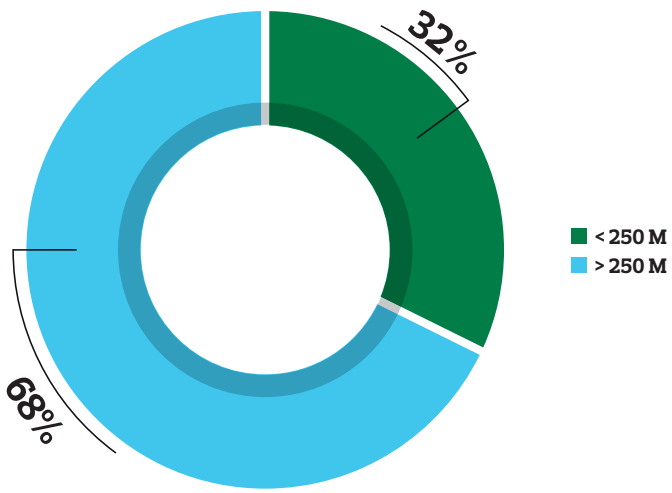
La importancia de transferir el riesgo al mercado, entre otras razones, debido a la cada vez mayor severidad de la legislación con respecto a las brechas de seguridad y a los compromisos de datos personales, así como la aceleración de la digitalización que contribuye al aumento de los ciber ataques, han seguido impulsando la contratación de pólizas Ciber como en los últimos años.

Si comparamos la contratación de pólizas Ciber entre sociedades que facturan más de 250 Millones € y sociedades que facturan por debajo de esta cifra, vemos, con respecto al estudio publicado el año pasado, como las sociedades con más recursos económicos (facturación >250M €) tienden a transferir el riesgo al mercado en mayor medida que empresas con mensos recursos (facturación <250M €).

En ese sentido, cabe destacar que mientras en 2019 solo el 44% de las sociedades con facturación >250M contrataban póliza, ahora lo hace el 68%.

Sin embargo, las sociedades con facturación <250M han reducido la contratación desde 2019, 56%, al 32% que identificamos en 2020, tal y como mostramos en el gráfico 2.

Distribución contratación por facturación



Fuente: elaboración propia.

Contratación del Seguro Ciber por sectores de actividad.

El sector de Infraestructura crítica ha sido líder en la contratación de seguros Ciber pasando del 17% en 2019 al 28% en 2020. Forman parte de este sector, las Entidades Financieras (bajo la constante vigilancia de los organismos reguladores y en el punto de mira de las leyes de privacidad de datos); así como las Energéticas (su papel en las infraestructuras críticas y su influencia financiera la convierten en un objetivo atractivo para las naciones extranjeras, el espionaje económico y los hacktivistas); y por último, las Telcos (dan soporte al resto de industrias, la demanda de sus productos y servicios es más pronunciada que nunca, lo que aumenta su foco sobre la ciberseguridad).

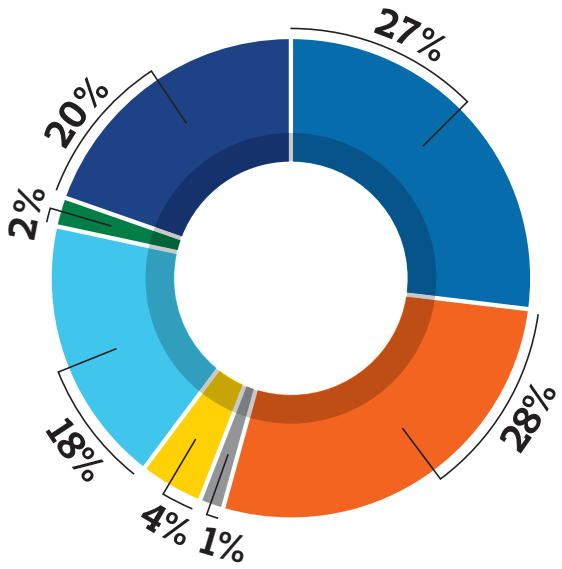
Le sigue el sector Industrial, con una contratación actual del 27% (frente al 25% que publicábamos en el estudio del año pasado) que está viviendo un cambio tecnológico que se manifiesta en las cadenas de suministro global y en los sistemas de control industrial (SCI), conectados a Internet de forma directa o indirecta, y que las expone a un mayor número de vectores de ataque cibernético.

Y, en tercer lugar, encontramos al sector de Servicios Profesionales que cubre el 18% de la contratación. No obstante, este sector ha reducido la compra de póliza Ciber con respecto a 2019, cuando el 24% de las pólizas comercializadas eran adquiridas por empresas de servicios profesionales.

Cabe destacar, una significativa caída en la contratación de póliza por parte de la industria del Ocio y Turismo, que pasa a ser el adquiriente del 4% de las pólizas que se comercializaron en 2020, frente al 18% de 2019. Probablemente la explicación está en la caída de la actividad que ha supuesto para este sector la pandemia, siendo una de las industrias más afectadas.

Por último, debemos poner de manifiesto que AA.PP y Salud siguen la misma tendencia que en los últimos años. Compran el 3% de las pólizas que se han vendido durante 2020 (porcentaje muy similar a 2019). Aun siendo uno de los sectores más ciber atacados, siguen siendo los que menores recursos destinan a proteger sistemas y transferir el riesgo al mercado. También es cierto que, la baja inversión en ciberseguridad conlleva la falta de apetito del mercado asegurador hacia la administración y empresas públicas.

Distribución contratación ciber por sectores de actividad



Fuente: elaboración propia.

Conclusiones.

A cierre 2020, el volumen de primas de Ciber recaudadas es aproximadamente de unos 75M €. El incremento respecto a 2019 se debe tanto a que sigue creciendo el número de empresas que transfieren el riesgo al mercado por primera vez, así como la propia tendencia alcista en primas como consecuencia del endurecimiento del propio mercado. En este sentido, identificamos un aumento de primas de renovación entre el 25% y el 60%.

Desde el inicio de 2021 la tendencia de suscripción del seguro Ciber está viviendo tiempos sin precedentes. Ante la constatación de un panorama de siniestralidad creciente, con mucha concentración en los ataques de ransomware, las aseguradoras que lideran la suscripción de este riesgo, notablemente preocupadas por el impacto de posibles cúmulos, y con tal de frenar el loss ratio combinado y dar una dirección positiva a sus inversiones, observamos que la suscripción empieza a caracterizarse por:

1. **Cambios constantes en sus guías de suscripción:** se sublimitan garantías y se aplican nuevas exclusiones y limitaciones)

2. **Limitación de la validez de las cotizaciones** a 30 días. Deben revisarse las propuestas tras expiración del plazo.

3. **Tendencia alcista en las primas:** de enero a junio de 2021, las primas de renovación han sufrido un incremento de hasta el 60%.

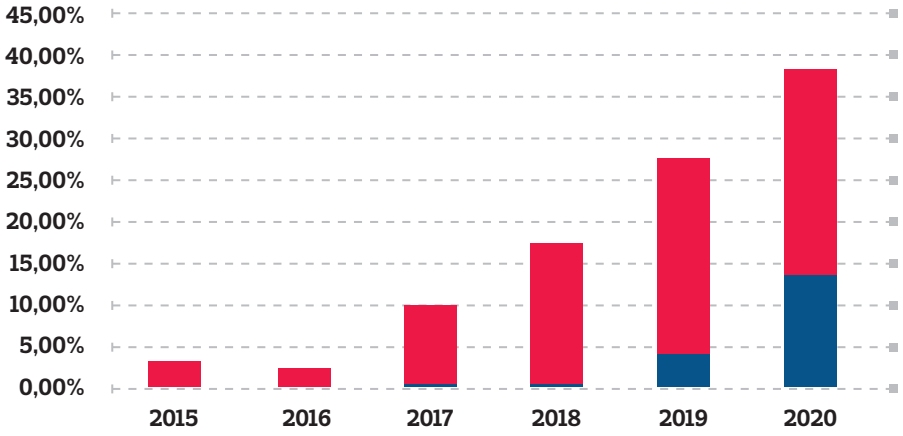
4. **Reducción de capacidad máxima del mercado** pasando de 165 a 130 Millones.

8 Evolución de la siniestralidad en España

1. Introducción. Siniestros abiertos y cerrados:

Analizando la siniestralidad desde el año 2015 al año 2020 se observa que más de un 80% de los expedientes se encuentran cerrados, siendo las anualidades de 2019 y 2020 las que mayor número de expedientes tienen en proceso de gestión y/o liquidación.

Siniestralidad a 5 años

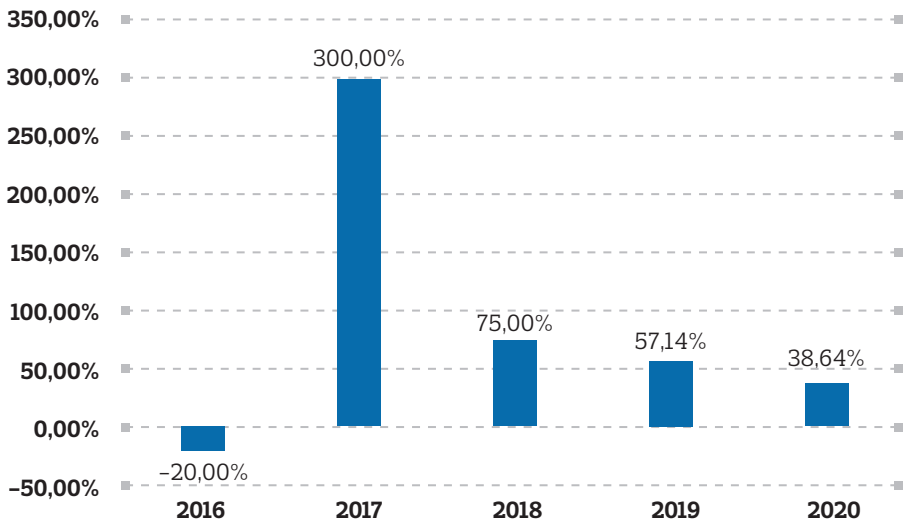


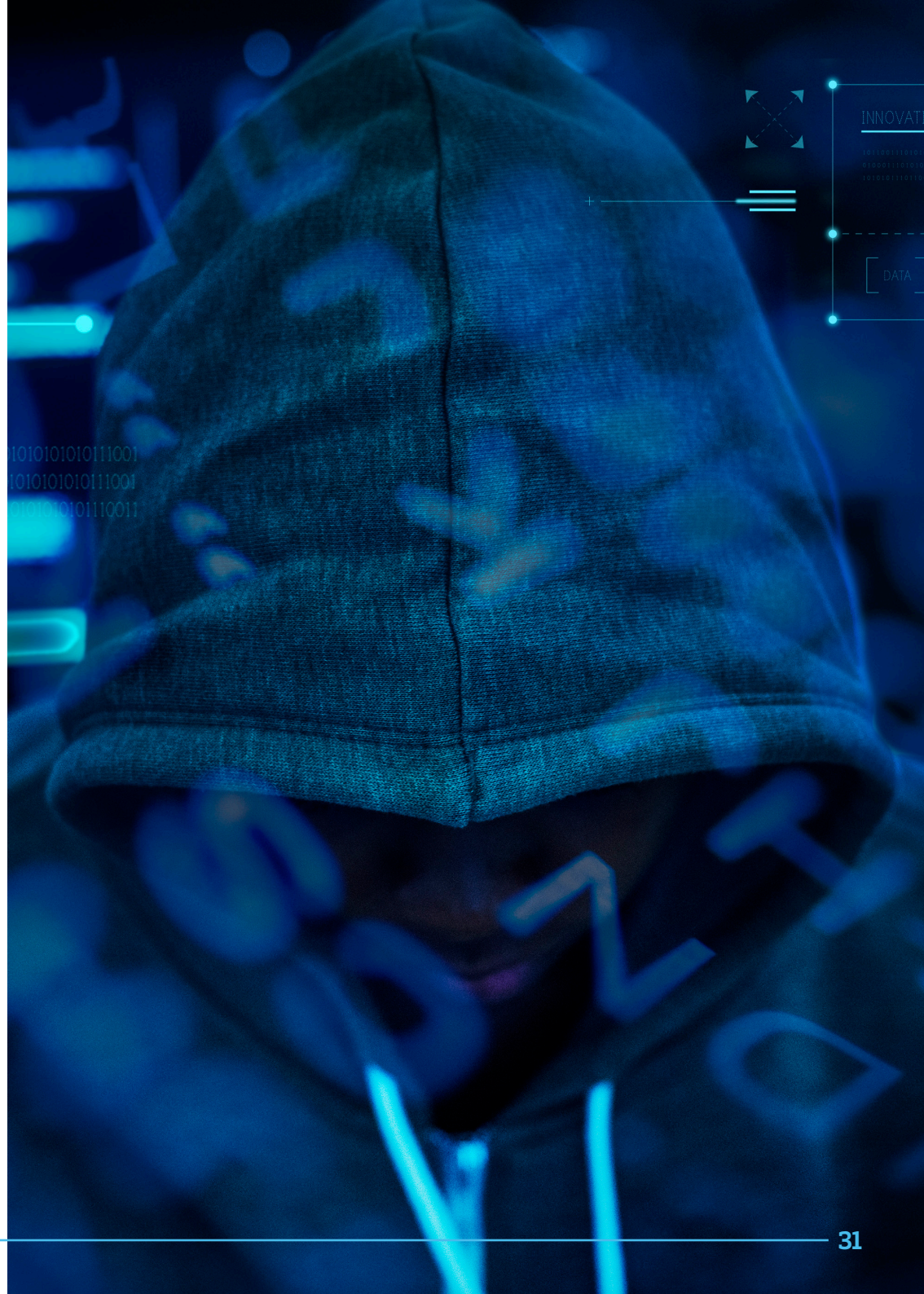
AÑOS	ABIERTO	CERRADO	TOTAL GENERAL
2015	0,00%	3,16%	3,16%
2016	0,00%	2,53%	2,53%
2017	0,63%	9,49%	10,13%
2018	0,63%	17,09%	17,72%
2019	4,43%	23,42%	27,85%
2020	13,92%	24,68%	38,61%
Total general	**19,62%**	**80,38%**	**100,00%**

La variación porcentual entre el año 2015 y el año 2020, asciende al 1.120%. Esto puede dar una idea de la evolución que han seguido los siniestros de este ramo.

Con respecto a la variación porcentual en los últimos 5 años – tomando como punto de partida 2016– destaca la importante subida de siniestros que se produce entre las anualidades de 2016 a 2017. Los números relativos a la variación porcentual de las siguientes anualidades arrojan la conclusión de que la tendencia en la declaración de siniestros no se reduce, sino que se consolida al alza.

Valoración porcentual a 5 años





2. Principales causas de siniestralidad:

A nivel global en nuestro estudio precedente se señalaban como principales causas la ciber extorsión y el empleo de códigos dañinos, seguido por las pérdidas derivadas de la intrusión en sistemas o datos y fallos de seguridad.

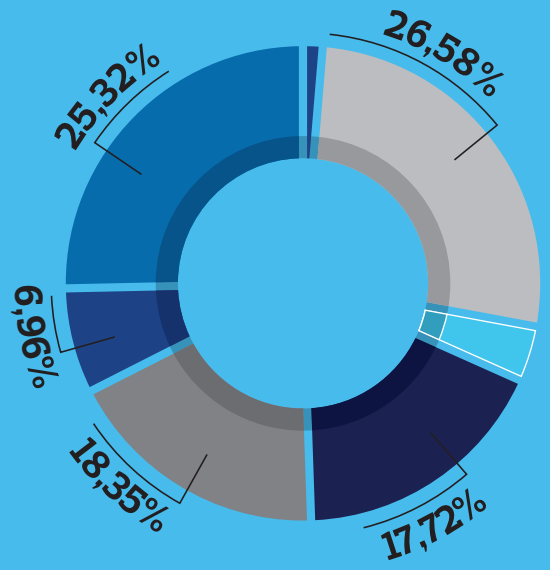
El panorama no ha variado especialmente con respecto a las tipologías que abarcan un mayor número de incidentes, siendo la ciber extorsión la más destacada junto con los fallos de seguridad que suponen un compromiso en los datos.

Tipología Global

Ciberextorsión/Código dañino **Compromiso de datos/Obtención de Información**
Contenido abusivo **Fallo de seguridad/Intrusión** **Pérdida de Beneficios**
Fraude

Entrando en un mayor nivel de detalle los resultados que se generan tras un estudio de nuestros datos nos ofrecen la siguiente visión:

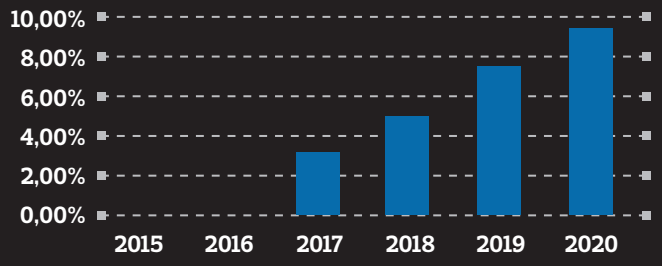
Tipología a 2020



Ataque de denegación de servicio **Data breach** **Fallo de sistema**
Ingeniería social **Intrusión o manipulación de sistemas o datos**
Otras violaciones de la normativa de datos **Ransomware, virus, malware**

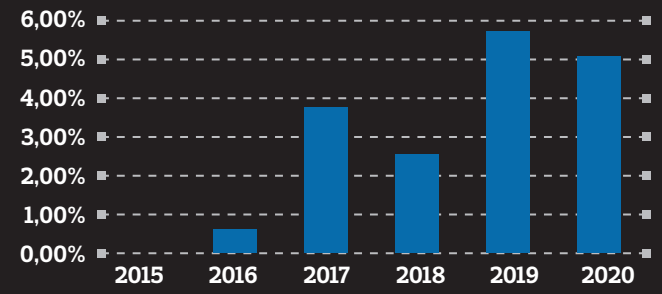
Por otra parte, tomando como referencia el período comprendido entre los años 2015 a 2020, el ransomware, ha sido una de las tipologías de incidente con mayor peso entre los siniestros registrados. Estos han mantenido una tendencia de crecimiento constante desde el año 2017, llegando a experimentar una variación porcentual de un 200%.

Ransomware, virus, malware.

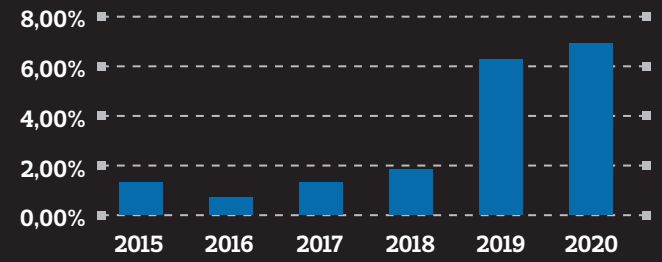


Junto con el ransomware, los incidentes con mayor relevancia son los originados con motivo de Ingeniería Social, y de intrusión o manipulación de sistemas o datos, teniendo este último una evolución especialmente acusada en los últimos años.

Ingeniería global

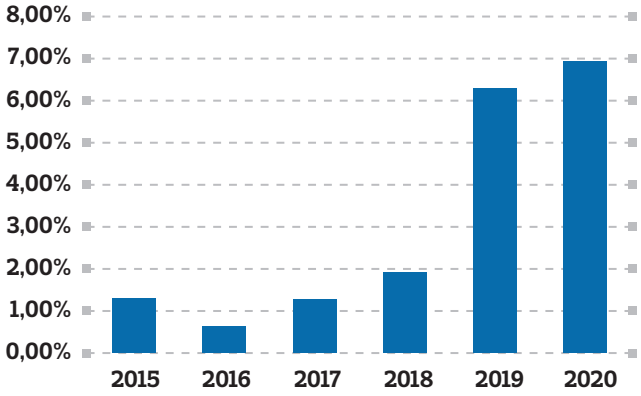


Intrusión o manipulación de sistemas de datos



Especial mención merece el compromiso de datos, que junto con el ransomware encabeza el listado de siniestros con mayor número.

Intrusión o manipulación de sistemas de datos



Las cuatro tipologías mencionadas aglutinan entre ellas la cifra de 87,97% de los siniestros ocurridos.

Centrándonos en el período comprendido entre los años 2019 y 2020, observamos que la evolución de la siniestralidad sigue siendo similar a los antecedentes del presente estudio. El ransomware continúa evolucionando al alza, sin embargo, este movimiento es más visible aún en sede de compromisos de datos.

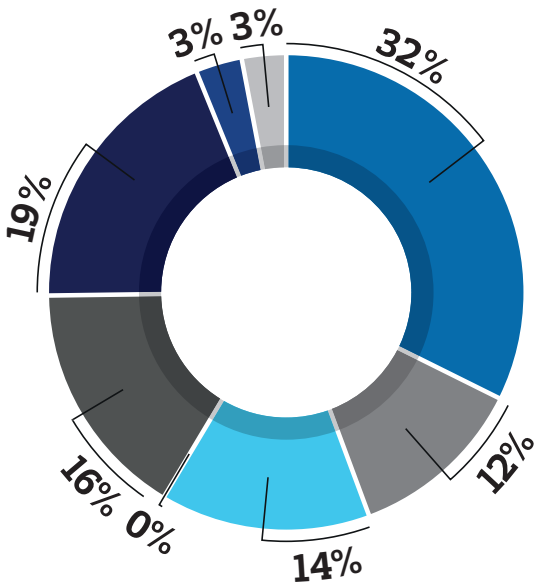
Por lo que respecta a la ingeniería social y a la intrusión y manipulación de datos, su crecimiento se ha mantenido estable, aunque es notablemente mayor en relación con años anteriores.

3. Principales coberturas afectadas.

Debido a la propia naturaleza de estos siniestros, la principal cobertura que se activa en el momento en que se sospecha o se tiene ya la certeza de que ha ocurrido un incidente, es la cobertura de primera respuesta.

Este patrón se mantiene como una constante con respecto a nuestro anterior Estudio, según los datos manejados hay una media de más de un 30% de los incidentes que precisan la activación de dicha cobertura.

Principales coberturas afectadas



- Primera Respuesta / Gastos de gestión incidente
- Gastos de recuperación de datos
- Sanciones en materia de protección datos
- Sanciones PCI
- Ciberextorsión
- Pérdida Beneficios
- Responsabilidad Civil derivada de fallo de seguridad
- Responsabilidad Civil derivada de fallo de privacidad

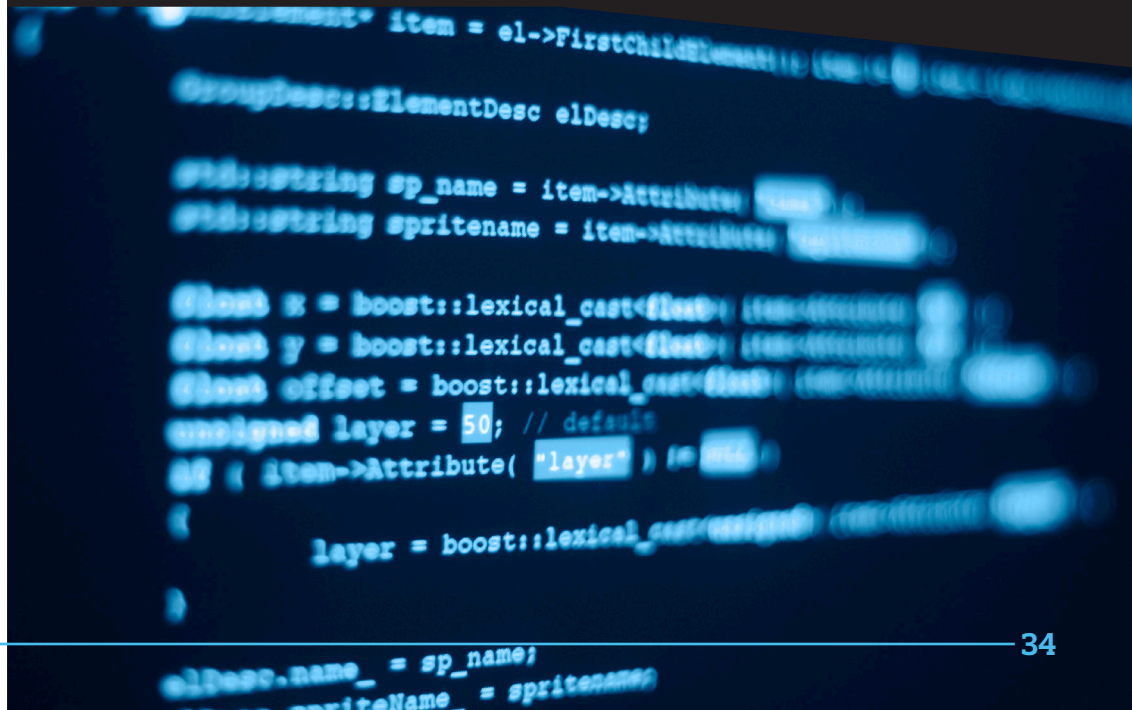
Igualmente, con motivo de la naturaleza de estos incidentes, la siguiente cobertura cuya activación se demanda, es la de recuperación de datos. Esto guarda coherencia con el hecho de que muchos de estos incidentes provocan una afectación en las bases de datos de los asegurados.

Para aquellos supuestos donde no es posible la recuperación de estos datos se acude a la tercera de las coberturas de mayor peso según nuestros datos, la de ciber extorsión.

Por otra parte, los datos obtenidos para el presente estudio, otra de las coberturas cuya activación se requiere mayoritariamente es la de pérdida de beneficios, dado que los ciber incidentes suelen afectar la continuidad de los negocios.

La cobertura en materia de sanciones de protección de datos, aunque porcentualmente no encabece el actual listado de coberturas afectadas, es una de las que hemos observado que especialmente que ´en el último trimestre el pasado año, ha acaparado siniestros de gran impacto por su importe.

En la misma del estudio precedente, encontramos un porcentaje de incidentes residuales, producto de la aún poca litigiosidad por parte de terceros, lo que supone una no muy elevada de la activación de la cobertura de responsabilidad civil.



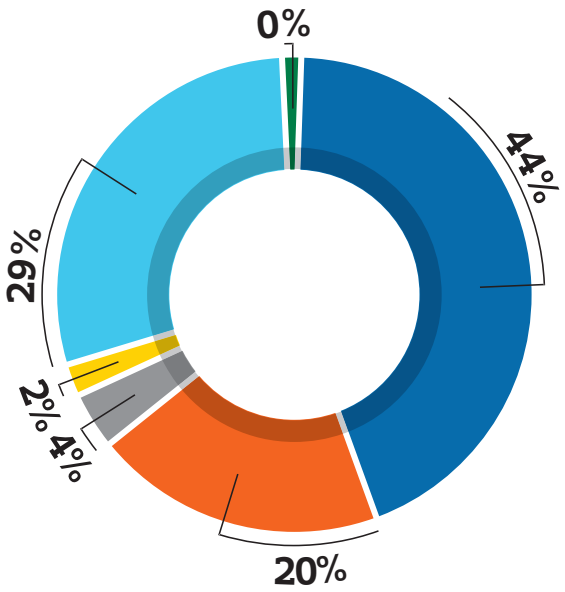
4. Siniestralidad por sectores.

De manera global con la respecto al desglose de los ciber incidentes según el tipo de sector involucrado, se mantiene encabezando la lista al igual que en nuestro anterior estudio, el sector "Industria" que constituye el 44%.

A título seguido se encuentra como el siguiente sector más afectado por este tipo de siniestros, el de los servicios profesionales con un 29%, seguido muy de cerca por el de la infraestructura crítica que cuenta con un 20%.

Obsérvese que, entre los tres, se alcanza un 93% de la totalidad de los casos con relevancia en el ámbito ciber.

Distribución de la siniestralidad según industria

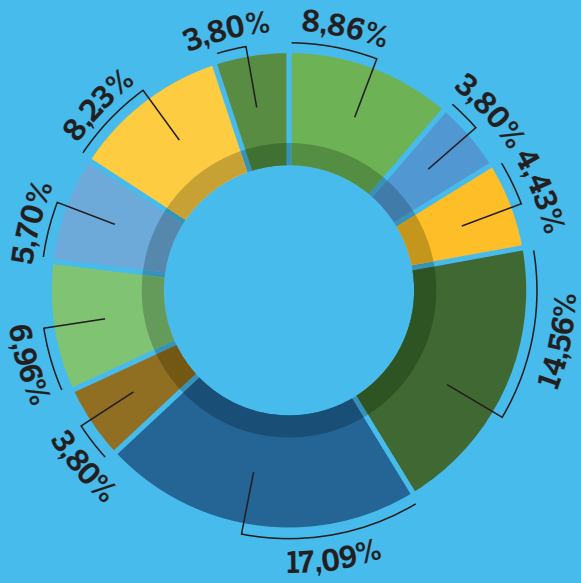


Industrial · Infraestructura Crítica · Salud · Ocio / Hoteles · Servicios Profesionales · AA PP · Otros

Entrando en un mayor nivel de detalle, se ha investigado qué cuál es el comportamiento que, dentro de las diversas áreas de la actividad económica, tienen este tipo de incidentes.

Así de acuerdo con los datos obtenidos, el sector de las instituciones financieras o de la maquinaria diversa son los que encabezan el listado, junto con el turismo.

Áreas



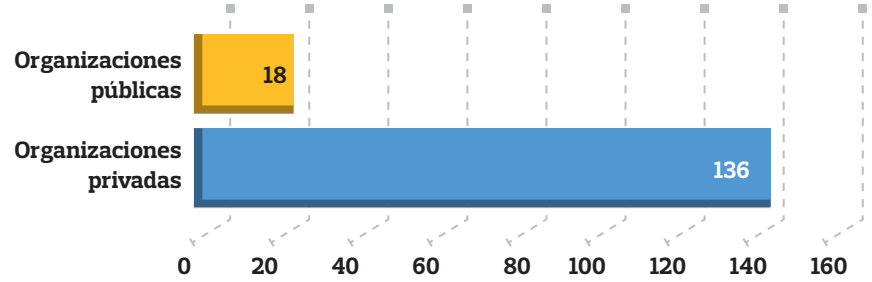
Construcción · Electricidad · Inmobiliarias · Inst. Financieras · Maquinaria diversa · Minoristas · Productos alimenticios y tabaco · Servicios Generales · Servicios Informáticos · Turismo

www 5. Notificaciones de compromisos.

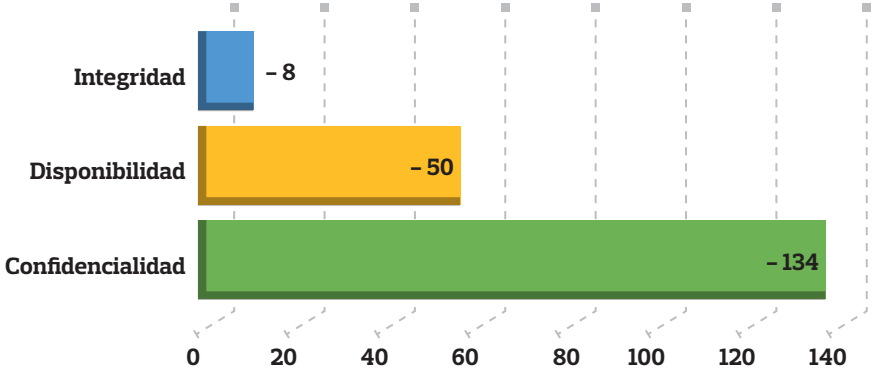
En el ámbito europeo, si se consulta en la web de la European Data Protection Board, las noticias más relevantes en materia de protección de datos, sorprenderá cantidad[2] y las impactantes cifras que han generado este tipo de incidencias en España. Como se indicaba con anterioridad la AEPD, ha estado especialmente activa en el último trimestre del pasado año, tendencia que ha mantenido.

Siguiendo el informe elaborado por este organismo supervisor en su memoria de Julio de 2020, las notificaciones que ha recibido la misma en dicho período se distribuyen de la siguiente manera:

1. Por tipo de organización

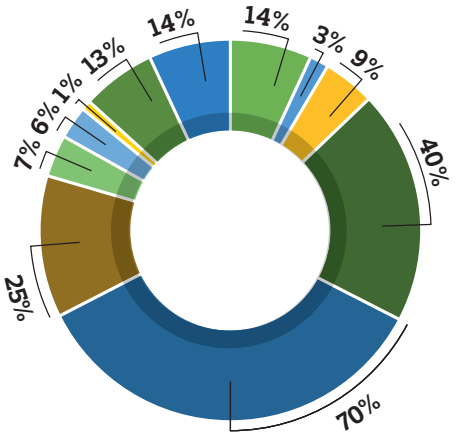


2. Por tipología de la brecha:



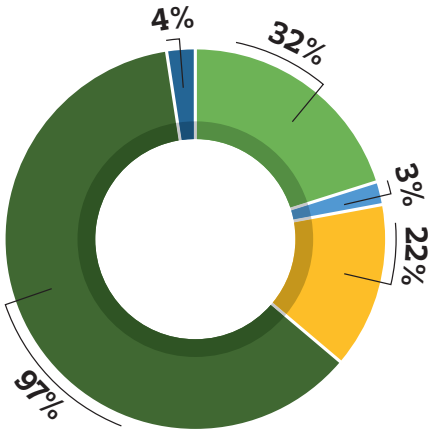
[2] *https://edpb.europa.eu/news/news_en?news_type=2&field_edpb_member_state_target_id=93*

3. Con respecto a las causas de las brechas:



Dispositivo perdido/robado · Documentación perdida/robada · Correo perdido · Hacking · Malware · Phishing · Datos personales mostrados · Publicación no intencionada · Revelacion verbal · Datos personales enviados · Otros

4. Contexto de la brecha



Interno (no intencionado) · Interno (intencionado) · Externo (no intencionado) · Externo (intencionado) · Otros

Conclusiones.

- El incremento de la actividad en el ámbito de internet de individuos o empresas que antes no tenían presencia online ha intensificado tanto el número de ataques y sus consecuencias dañosas.
- Los confinamientos y el mencionado aumento de la presencia online, ha ido de la mano de la rápida adaptación de las tradicionales actividades de ciber crimen de los atacantes.
- Se ha detectado una mayor sofisticación en los ataques perpetrados mediante la ingeniería social, tendencia que se prevé no sólo que se sostenga, sino que se acentúe.
- La actividad sancionadora del supervisor en el ámbito de protección de datos ha sufrido un cambio de tendencia y es es esperable un importante incremento.

9 METODOLOGIA

Este Estudio ha sido elaborado con información propia y datos del mercado asegurador obtenidos mediante cuestionarios multirrespuesta 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 el año pasado, lo que nos permitirá comparar la evolución de esta modalidad aseguradora en términos de contratación y, sobre todo, en términos de siniestralidad. Esto último, es uno de los factores que nos va a hacer evolucionar la póliza tanto en términos de nuevas garantías como de desarrollo de clausulado y exclusiones.

Todos los datos de primas, pólizas y siniestralidad están cerrados a 31 de diciembre de 2020.

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.

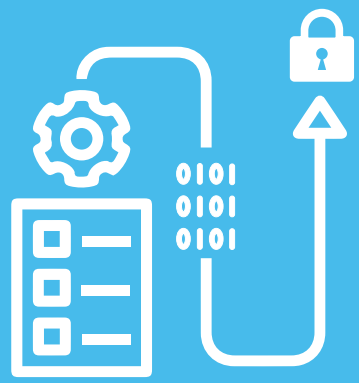
En relación con el volumen de primas, la cifra resultante comprende las cantidades que corresponden a las principales aseguradoras del mercado, utilizando los siguientes criterios:

- Se han incluido tanto primas de cartera como de nuevo negocio suscrito en 2020, 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 2020, del seguro Ciber en España.



10 TENDENCIAS 2021

A lo largo del desarrollo del informe que ahora cerramos hemos puesto de manifiesto el impacto que la pandemia ha tenido en la transformación digital de las empresas durante 2020, y cómo este escenario ha dado lugar a un contexto mucho más complejo y agresivo para todos.

Viviendo ya los últimos coletazos del Covid-19 y resituándonos en el nuevo contexto social, económico y político es momento para reflexionar y evaluar la situación dando lugar a una predicción de las principales tendencias que se están produciendo este año con respecto a la gestión y transferencia del riesgo cibernético:

1. Ha aumentado la **frecuencia y la virulencia de los siniestros Ciber**, de manera que ya estamos viendo cómo fallos de seguridad (sobre todo centrados en ataques ransomware) dan lugar a unas **pérdidas que consumen la totalidad del límite de la póliza e incluso, los asegurados deben asumir pérdidas por encima del límite contratado**. Esto pone de manifiesto también que las capacidades que se compran bajo los contratos de seguro son pequeñas e insuficientes para asumir las pérdidas generadas tras un incidente Ciber.

2. En cuanto al **ámbito legislativo**, destacamos la actividad por parte de los reguladores europeos en la aplicación del RGPD, dado que la otra cobertura más afectada en póliza y, que contribuye de manera significativa al consumo de la totalidad del límite de las pólizas, está siendo las **sanciones administrativas en materia de protección de datos**. Hasta hace poco, este tipo de pérdidas era residual en el ramo. Así mismo prevemos que **podría haber cambios en el marco legal vinculados al pago de rescates por ransomware** e incluso cambios en la propia cobertura introducidos a iniciativa de las propias aseguradoras.

3. Una de las primeras consecuencias que se derivan de los puntos anteriores es que **se mantiene e incrementa la tendencia alcista de primas**, identificando un **incremento medio en 2021 del 60%** de las primas de renovación. De momento no prevemos una estabilización de los precios dado que el objetivo principal del mercado es corregir y rentabilizar el ramo para poder mantener una suscripción óptima.

4. El aumento significativo de la siniestralidad en tan poco tiempo ha dado lugar a una **reducción de capacidad aseguradora** (en 2019 identificábamos una capacidad general de 250 Millones y ahora apenas llegamos a los 100 Millones en el mercado español). Dado que continua **el incremento sostenido de pérdidas, así como la incerteza ligada a posibles cúmulos de riesgo y otros factores, inciden en que durante los próximos meses no se prevea la entrada de nuevo capital** en el ramo que contribuya a armonizar los precios de la capacidad.

5. Los ramos de Daños materiales y Responsabilidad Civil General están incluyendo de manera generalizada exclusiones para evitar posibles vacíos de cobertura con respecto a lo que se ha dado en llamar ***Ciber silenciosa***. Este es un trabajo pendiente de resolver por parte del mercado asegurador que debe dar solución a esas posibles coberturas pasivas, que pueden incluir o no excluir expresamente los riesgos Ciber bajo pólizas tradicionales. De momento **identificamos algunas soluciones, pero muy incipientes, y que se encuentran con el problema principal de que no hay capacidad suficiente para asumir los daños materiales y corporales** que se deriven de un incidente Ciber.

El mercado asegurador no identifica ningún parámetro que permita prever una reducción de la siniestralidad en el corto plazo por lo que recomendamos a las empresas ser muy proactivas en la gestión del riesgo cibernético y, en la medida de lo posible, cuenten también con un programa de seguros que les permita garantizar la continuidad de su negocio a pesar de las pérdidas que pudieran derivarse de un evento Ciber.

11 GLOSARIO DE TERMINOS

GLOSARIO DE LOS PRINCIPALES TERMINOS TÉCNICOS UTILIZADOS

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
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.

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.

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.

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 para gestionar y garantizar el gobierno central de una organización, la administración de 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.

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.

Inyección de código
Término general para ataques cuya tipología consiste en la introducción de código que es interpretado o ejecutado por aplicaciones provocando una ejecución malintencionada.

Inyección SQL
Método de infiltración de código que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

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.

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.

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.

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.

Payload
Conjunto de datos transmitidos que hacen referencia al mensaje enviado.

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.

GLOSARIO DE LOS PRINCIPALES TERMINOS DE SEGURO UTILIZADOS

Actividades en Medios Digitales
La publicación o difusión de contenidos en Medios Digitales en el portal web del Asegurado, incluyendo portales en medios sociales.

Acto Informático Malicioso
Cualquier acto deshonesto cometido contra el Sistema Informático de la Sociedad que conlleve la introducción, alteración o destrucción de sus Datos, que no implique ningún daño físico al Sistema Informático o a sus equipos e infraestructuras de telecomunicaciones.

Asegurado

(i) La Sociedad;

(ii) Cualquier persona física que sea administrador, directivo o socio (incluido cualquier Directivo responsable) de la Sociedad en la medida en que dicha persona actúe o haya actuado como tal;

(iii) Cualquier persona física que sea o haya sido empleada por la Sociedad;

(iv) Cualquier representante legal o del caudal hereditario de cualquier Asegurado descrito en los puntos (i), (ii) y (iii) de esta definición cuando se presente una Reclamación en su contra con respecto a un acto, error u omisión de dicho Asegurado.

Algunos condicionados pueden incluir expresamente

(v) Cualquier contratista independiente que se halle bajo la dirección o supervisión de la Sociedad, pero solo con respecto a los servicios prestados por el contratista independiente a la Sociedad; y

Asesor de respuesta

Cualquier consultor designado por la Aseguradora, o cualquier otra firma de abogados designada por el Asegurado, cuyo cometido es coordinar a los especialistas en TI, Legal y Comunicación, que intervendrán en la gestión del ciber incidente.

Ciberextorsión

Amenazas contra el sistema informático o contra los datos con el objetivo que la víctima realice un acto en perjuicio propio o ajeno.

Ciberterrorismo

El uso premeditado de actividades perjudiciales contra cualquier red o Sistema informático del Asegurado, o la amenaza expresa de utilizar dichas actividades con la intención de causar daños y perseguir otros objetivos sociales, ideológicos, religiosos, políticos o de índole similar, o de intimidar a cualquier persona para promover dichos objetivos. Ciberterrorismo no abarca, en ningún caso, actividades que formen parte de operaciones militares, bélicas o cuasi bélicas.

Control de identidad / Control de crédito

Servicios contratados a fin de identificar cualquier posible uso inadecuado de Información personal como resultado de un acceso no autorizado real o presunto a Información Confidencial.

Cupones descuento (Goodwill)

Descuento o reembolso a personas afectadas para compra futura de productos o servicios que sean ofrecidos por la sociedad.

Datos

Cualquier información, hecho o programa almacenado, creado, empleado o transmitido en cualquier hardware o software informático que permita que un ordenador o cualquiera de sus accesorios funcione, incluidos sistemas y aplicaciones de software, discos duros y disquetes, CD–ROM, cintas, unidades, células, dispositivos de procesamiento de datos y demás medios que se emplean junto con equipos controlados electrónicamente u otros dispositivos electrónicos de copia de seguridad. Los Datos no constituirán una propiedad tangible.

Fallo de seguridad

Es una de las definiciones a destacar en cualquier condicionado, ya que, dependiendo de la amplitud de su definición, el ámbito de cobertura será mayor o más restrictivo. A continuación, indicamos una que podemos considerar óptima. Cualquier intrusión en el Sistema informático del asegurado, acceso no autorizado o uso no autorizado de dicho sistema, así como la pérdida de Datos como resultado del robo o la pérdida física de hardware controlado por el mismo.

Fallo en el sistema

Es una de las definiciones a destacar en cualquier condicionado, ya que, dependiendo de la amplitud de su definición, el ámbito de cobertura será mayor o más restrictivo. A continuación, indicamos una que podemos considerar óptima. Fallo en el sistema informático del asegurado por cualquier acto u omisión accidental, negligente o fortuito por parte de un empleado del asegurado o un empleado de cualquier proveedor de servicios externo mientras gestiona, actualiza o realiza tareas de mantenimiento en el Sistema informático del asegurado.

Fondo para recompensas

Suma ofrecida por información que lleve al arresto y condena de cualquier persona que cometa o intente cometer cualquier acto ilegal relacionado con la protección de datos.

Fondo de Compensación del Consumidor

Importe que el Asegurado se encuentra legalmente obligado a depositar en un fondo en concepto de compensación equitativa para el pago de las reclamaciones de los consumidores derivadas de una sentencia o resolución adversa de un Procedimiento Normativo. Este fondo no incluirá ningún importe abonado en concepto de impuestos, multas, penalizaciones, requerimientos o sanciones.

Fraude informático

Acceso no autorizado al sistema informático y que resulte en órdenes de transferencia fraudulentas.

Fraude telefónico

Acto informático malicioso o uso o acceso no autorizado por un tercero al sistema telefónico del asegurado que puede resultar en importantes cantidades facturadas.

Gastos para mitigar la pérdida de beneficios
Costes y gastos incurridos para mitigar o reducir una interrupción grave

Incidencia de datos electrónicos
Cualquier daño o destrucción accidental del sistema informático del asegurado causado por motivos técnicos nominados en póliza según asegurador (sobre carga de la tensión eléctrica, caída de rayo, etc) y que provoquen que los datos no puedan ser leídos por una máquina.

Incumplimiento del deber de notificación a afectados
Error u omisión de la notificación en base a los requisitos establecidos por el órgano regulador pertinente.

Incumplimiento de deber de protección de información confidencial
Revelación o transmisión no autorizada de Información confidencial del Asegurado.

Información confidencial
Información corporativa e Información personal que se halle bajo el cuidado, la custodia o el control del asegurado o titular de información o de las que un asegurado o titular de información sea legalmente responsable.

Información corporativa
Información de cualquier tercero que no sea de dominio público y/o secretos comerciales, datos, diseños, previsiones, fórmulas, prácticas, procesos, registros, informes y documentos objeto de protección contractual o legal.

Información personal
Cualquier información relativa a una persona física o no pública capaz de identificar individualmente a dicha persona física. Información personal se refiere, pero no se limita, al nombre, dirección de correo electrónico, número telefónico, número de tarjeta de crédito o tarjeta de débito, cuenta u otra información bancaria, información médica o cualquier otra información de una persona física que se halle protegida por leyes o reglamentos en materia de confidencialidad de datos.

Interrupción de sistema informático
Suspensión o degradación del sistema informático del asegurado o la imposibilidad de acceder a los datos de este.

Interrupción de sistemas en un proveedor externo de servicios tecnológico
Suspensión o degradación del sistema informático del proveedor externo o la imposibilidad de acceder a los datos de este.

Medios Digitales
Cualquier contenido digitalizado, incluyendo texto, gráficos, audio y video, que puedan ser transmitidos a través de Internet o una red de comunicación de datos.

Multas por incumplimiento de deber de protección de datos
Cualquier multa y/o penalización asegurable por ley cuyo pago sea impuesto por un Organismo regulador a una Sociedad por un incumplimiento de la Normativa de protección de datos, así como los gastos razonables y necesarios incurridos por un experto consultor contratado por un Asegurado en relación con la investigación de un Incidencia asegurada por orden de un Organismo Regulador.

Multas por incumplimiento de deber de protección de datos no incluirá ningún otro tipo de multa o penalización civil o penal.

Normativa de Protección de Datos
La normativa relativa al cuidado, la custodia, el control y el uso de Datos de Carácter Personal.

Notificación de incidentes / Gastos de notificación
Costes asociados a la creación y gestión de centros de llamadas, preparación y notificación a las personas interesadas y a cualquier organismo regulador pertinente y la investigación y recopilación de información como consecuencia de un Incumplimiento de deber de protección de información confidencial real o presunto.

Organismo regulador
Organismo legalmente establecido de conformidad con la Legislación en materia de protección de Datos en cualquier jurisdicción, que tenga la potestad de velar por el cumplimiento de tal normativa en relación con el tratamiento o control de la Información personal o Información Corporativa si fuese pertinente.

Pérdida de beneficios del asegurado
(i) La disminución de los ingresos netos que se habrían obtenido en caso de no haber sufrido la interrupción del sistema informático;

(ii) Gastos en los que se incurra para asegurar la continuidad de los procedimientos operativos normales de la Sociedad.

Periodo informativo
Periodo para notificar reclamaciones e incidencias aseguradas tras la finalización del contrato de seguro (sujeto a no renovación o sustitución del contrato)

Protección de datos personales (privacidad)
Deber de proteger la información importante de la corrupción y/o pérdida y de establecer medidas de seguridad y acciones para proteger el dominio cibernético frente a las amenazas vinculadas con sus redes interdependientes y su infraestructura de información, o que puedan afectar a estas.

Proveedor de servicios externo
Una entidad que no sea propiedad, no esté gestionada o controlada por la Sociedad y que esta última haya designado para prestar servicios específicos (incluidos, a título enunciativo pero no limitativo, alojamiento web, procesamiento de pagos, recopilación de datos de seguridad informática, procesamiento de datos, delegación de procesamiento de datos, almacenamiento de datos y/o eliminación o destrucción de datos, o acceso bajo demanda de alojamiento de infraestructuras tecnológicas o plataformas informáticas.

Con respecto al proveedor de servicio cloud computing, la definición varía entre los distintos condicionados analizados.

Recreación/Restauración de datos, recarga de software con licencia y gastos de limpieza o descontaminación de sistemas
Medidas adoptadas para identificar datos retenidos, recuperarlos o volver a crearlos cuando sea posible y recargar y/o personalizar software cuando estuviera dañado.

Responsabilidad derivada de la publicación de contenidos digitales
Reclamaciones por intromisión en la intimidad o daño a la reputación de las personas por las causas nominadas en póliza (ej. Infracción de derechos de autor, plagio, calumnias...) siempre y cuando no sea intencionado y únicamente en el curso de actividades en medios digitales

Respuesta a afectados
Call center para atender a afectados y brindarles respuesta/recomendaciones acerca de la gestión del compromiso de sus datos personales, así como de cualquier aspecto de la propia incidencia de seguridad.

Sanciones PCI (tarjetas de pago)
Sanciones de medios de pago y bancos por incumplimiento de normas de seguridad de tarjetas de pago

Servicios informáticos
Medida adoptada por un Especialista en TI para:

(i) Confirmar si un Fallo de seguridad o Fallo en el sistema se ha producido, cómo se ha producido y si continúa produciéndose;

(ii) Identificar si dicho Fallo de seguridad o Fallo en el sistema ha resultado en un Incumplimiento de un deber de protección de Información confidencial e identificar Datos en riesgo;

(iii)Determinar hasta qué punto podría haberse visto afectada la Información confidencial; y

(iv) Atajar y resolver una Incidencia asegurada y hacer recomendaciones para prevenirla o mitigarla.

Servicios jurídicos
Servicios prestados por un Asesor de respuestas con el objeto de:

(i) Coordinar al Especialista en TI o los Consultores expertos en comunicación, e informar, notificar y cumplir con cualquier requisito de notificación con cualquier Organismo regulador pertinente; o

(ii) Hacer un seguimiento de quejas presentadas por Personas interesadas y asesorar al Asegurado acerca de respuestas a una Incidencia asegurada con el fin de minimizar los daños para la Sociedad, incluyendo medidas adoptadas para mantener y restablecer la confianza pública en la Sociedad.

Servicios de protección de la reputación
Asesoramiento y apoyo de un Consultor experto en servicios de comunicación y de crisis para mitigar o prevenir los posibles efectos adversos o daños a la reputación de un Suceso de interés mediático, incluido el diseño y la gestión de una estrategia de comunicaciones.

Sistema informático de la Sociedad
(i) Cualquier hardware, firmware o software informático o cualquiera de sus componentes vinculados mediante una red de dos o más dispositivos accesibles a través de Internet o una red interna o conectados a través de dispositivos de almacenamiento de datos u otros dispositivos periféricos propiedad de la Sociedad o gestionados, controlados o arrendados por dicha Sociedad.

(ii) Cualquier dispositivo personal de un empleado utilizado para acceder a un Sistema informático de la Sociedad o Datos contenidos en dicho sistema; y

(iii) Cualquier servicio de nube u otros recursos informáticos alojados utilizados por la Sociedad y puestos en funcionamiento por un proveedor de servicios externo conforme a un contrato escrito entre el proveedor de servicios externo y la Sociedad.

Sistema informático de proveedor de servicios externo
Cualquier hardware o software informático o cualquiera de sus componentes que estén vinculados a través de una red de dos o más dispositivos accesibles a través de Internet o una red interna o que estén conectados a través de dispositivos de almacenamiento de datos u otros dispositivos periféricos que sean propiedad de un Proveedor de servicios externo o estén gestionados, controlados o arrendados por el mismo.

Uso o Acceso No Autorizado
La entrada o acceso al Sistema Informático de la Sociedad por un tercero no autorizado, o por cualquier Empleado o entidad autorizada que sobrepase sus autorizaciones de acceso.


AON
Empower Results®
AIG
beazley
AXA
XL Insurance
TOKIO MARINE HCC
HISCOX
ZURICH
QBE
GARRIGUES
ANDERSEN