Cuadernos de Dirección Aseguradora

243

Contratación de la póliza de Ciberriesgos, tratamiento del siniestro y la importancia del reaseguro

Máster en Dirección de Entidades Aseguradoras y Financieras

UNIVERSITAT DE BARCELONA

Munich RE

UNIVERSITAT DE BARCELONA

243

Contratación de la póliza de Ciberriesgos, tratamiento del siniestro y la importancia del reaseguro

Estudio realizado por: Guillermo García Marcén
Tutor: Manuel Huerta

Tesis del Máster en Dirección de Entidades Aseguradoras y Financieras

Curso 2018/2019

Esta publicación ha sido posible gracias al patrocinio de

Cuadernos de Dirección Aseguradora es una colección de estudios que comprende las tesis realizadas por los alumnos del Máster en Dirección de Entidades Aseguradoras y Financieras de la Universidad de Barcelona desde su primera edición en el año 2003. La colección de estudios está dirigida y editada por el Dr. José Luis Pérez Torres, profesor titular de la Universidad de Barcelona, y la Dra. Mercedes Ayuso Gutiérrez, catedrática de la misma Universidad.

Presentación y agradecimientos

Quisiera agradecer a mi familia y a mi pareja su ánimo y apoyo incondicional en el transcurso de este año académico.

Dar las gracias también a Seguros Catalana Occidente por darme la oportunidad de participar en este máster, y en especial a Manuel Martinez por confiar en mi persona.

Por último, quería realizar una mención especial a todos mis compañeros del máster, gente excepcional y grandes profesionales.

Resumen

El mundo se encuentra en constante evolución, y en los últimos años se ha debido principalmente a internet y las nuevas tecnologías. Las empresas han sido las grandes beneficiadas, pero por otro lado la aparición de nuevas amenazas provenientes del ciberespacio ha supuesto que deban estar preparadas para protegerse e intentar mitigar sus posibles efectos. La póliza de ciberriesgos se percibe como la solución más adecuada.

Lo que se pretende con esta tesis es realizar un estudio exhaustivo sobre qué son los ciberriesgos, cuáles son las principales amenazas que nos encontramos actualmente y qué consecuencias pueden tener sobre las personas, empresas e incluso gobiernos e instituciones públicas. Por otro lado, se explicará a través de una breve guía metodológica como contratar este seguro, y en caso de siniestro como realizar un adecuado tratamiento y gestión del mismo. Además de informar del papel fundamental que juega el reaseguro en el seguro de ciberriesgos.

Palabras Clave: internet, nuevas tecnologías, empresas, ciberespacio, póliza ciberriesgos, siniestro, reaseguro.

Resum

El món es troba en constant evolució, i en els últims anys ha estat degut, principalment, a internet i les noves tecnologies. Les empreses han sigut les grans beneficiades però, per altra banda, l'aparició de noves amenaces provinents del ciberespai ha fet que hagin d'estar preparades per a protegir-se i intentar mitigar els seus possibles efectes. La pòlissa de ciberriscos es percep com a la solució més adequada.

El que es pretén amb aquesta tesi és realitzar un estudi exhaustiu sobre què són els ciberriscos, quines són les principals amenaces amb què ens trobem actualment i quines conseqüències poden tenir sobre les persones, empreses o, fins i tot, governs i institucions públiques. D'altra banda, s'explicarà a través d'una breu guia metodològica com contractar aquesta assegurança, i en cas de sinistre com realitzar un tractament i una gestió adequades del mateix. A més d'informar del paper fonamental que juga la reassegurança en l'assegurança de ciberriscos.

Paraules Clau: internet, noves tecnologies, empreses, ciberespai, pòlissa de ciberriscos, sinistre, reasseguro

Summary

The world is undergoing constant evolution, driven in recent years by advances in new technologies and the internet. Business has been the main beneficiary of these advances but the appearance of new threats from cyberspace has meant that they must take steps to protect themselves and to mitigate possible negative effects. To this end, the cyber risk policy has emerged as the most appropriate solution.

The aim of this thesis is to undertake an exhaustive study of cyber risks, of the specific threatsthat they pose to individuals, companies, governments and public institutions alike, and of their consequences. In addition, the thesis provides a brief methodological guide explaining how to contract cyber risk insurance, and how to successfully manage a claim. Finally, the fundamental role played by reinsurance in relation to cyber risk policies is explained.

Keywords: internet, new technologies, business firms, cyberspace, cyber-risk policy, insurance claims, reinsurance

Indice

Contratación de la póliza de ciberriesgos, tratamiento del siniestro y la importancia del reaseguro

1. Introducción

El desarrollo de las nuevas tecnologías y las telecomunicaciones están suponiendo un cambio trascendental en nuestra sociedad, pues se trata de una sociedad permanentemente comunicada. La tecnología está cada vez más extendida, es más fácil de utilizar y está al alcance de todos. A su vez entraña nuevas amenazas de carácter cibernético, o lo que es lo mismo la existencia de los llamados ciberriesgos. Pero, ¿Qué es exactamente un ciberriesgo? En mi opinión, un ciberriesgo es cualquier amenaza a nuestro entorno digital, pudiendo ser local o remota, de carácter accidental o doloso, y la cual afecta a la tecnología actual, entendiendo como tal equipos y sistemas informáticos, redes y/o cualquier dispositivo que se pueda conectar a internet. Todos ellos son susceptibles de ser atacados en cualquier momento y desde cualquier parte del mundo siempre que se encuentren conectados.

Hoy en día los expertos ya hablan de una cuarta revolución industrial, la cual está basada en el blockchain[1], y que deriva en la ausencia de intervinientes humanos con el objetivo de eliminar intermediarios, para así simplificar procesos y a su vez ahorrar costes a todas las partes de la transacción. La clave de esta tecnología es que es de carácter totalmente transparente, descentralizada e inmutable. Para entender el potencial del blockchain hay que hablar de smart contracts[2], o contratos que son capaces de ejecutarse y hacerse cumplir por sí mismos, de manera autónoma y automática, sin intermediarios ni mediadores, y con validez propia ya que no dependen de las Autoridades, pues se trata de un código visible por todos y cuyo contenido no se puede alterar. Las posibilidades y mejoras que implican tanto para las personas, como para las empresas e incluso gobiernos son altísimas. Pero como contrapartida supone nuevas amenazas cada vez más complicadas de identificar, tratar y resolver.

Su origen, puede deberse como a consecuencia de acciones realizadas por personas (ciberdelincuentes o empleados), incidentes fortuitos, o por errores y fallos de sistemas (por ejemplo, un fallo de alimentación eléctrica en un servidor. En realidad, tanto las personas como cualquier empresa se encuentran en peligro, ya sean grandes o pequeñas empresas. Ninguna está exenta de sufrir un incidente, por lo que se conforma como mejor opción es ceder parte de ese riesgo a una compañía de seguros, ya que las pymes y los particulares no pue-

[1] Blockchain (cadena de bloques en inglés): en palabras de Marc Andreessen, creador de Netscape, es esencialmente solo un registro, un libro mayor de acontecimientos digitales que está “distribuido” o es compartido entre muchas partes diferentes. Solo puede ser actualizado a partir del consenso de la mayoría de participantes del sistema y, una vez introducida, la información nunca puede ser borrada.

[2] Smart contracts (contratos inteligentes en inglés): son códigos informáticos escritos con lenguajes de programación que no se pueden cambiar al existir sobre la tecnología blockchain.

den mantener el nivel de exigencia y los costes que requiere la seguridad electrónica, y por eso se deben apoyar en un tercero.

Por lo tanto, desde el mercado asegurador la solución actual que se plantea frente a estas ciberamenazas es la contratación de una póliza de ciberriesgos, la cual se estudiará en detalle y se analizará si ofrece un conjunto de garantías adecuadas para los activos que se quieren proteger, así como una capacidad suficiente para atender correctamente la ocurrencia de un evento o siniestro.

1.1. Origen de los ciberriesgos

Los riesgos asociados al ciberespacio[3] datan aproximadamente de la década de los ochenta, a través de riesgos de tipo código dañino o malware. Según informa la enciclopedia de Kaspersky, uno de los más relevantes fue Suriv-3 o virus Jerusalem, como se conoce hoy en día. Fue detectado el viernes 13 de mayo de 1988, sacudiendo a todo el mundo, pero los Estados Unidos, Europa y el cercano Oriente fueron los más afectados. Jerusalem destruyó todos los archivos guardados en las máquinas infectadas de empresas, oficinas del Gobierno e instituciones académicas de todo el mundo, causando una gran epidemia. Su difusión fue como consecuencia de factores humanos.
Por aquella época las compañías que proveían de programas antivirus a empresas y particulares eran particularmente pequeñas y contaban con pocos recursos. Su software consistía en simples escáneres que realizaban búsquedas para detectar secuencias de código de virus. Pero no eran suficientes, ya que se quedaban obsoletos y no conseguían hacer frente a los nuevos virus que iban apareciendo.

En los noventa aparecieron nuevas amenazas en forma de virus, gusanos y troyanos que estaban especialmente diseñados para robar información de los ordenadores. Cabría destacar el Virus informático CIH, creado por Chen Ing Hau, un estudiante de Taiwán que buscando dejar en evidencia a compañías muy importantes de software que presumían de sus programas antivirus, acabó ocasionando uno de los mayores ataques cibernéticos de la historia, afectando a equipos informáticos de medio mundo.

No obstante, los expertos en la materia apuntan a cuatro hechos relevantes en la década de los 2000 para identificar el origen de los llamados ciberriesgos:

- *El efecto 2000.* Se llamaba así ya que se pensaba que cuando llegara el año 2000 los sistemas informáticos colapsarían creando una catástrofe empresarial sin precedentes a nivel global. Finalmente, no ocurrió nada, pero se adoptaron posibles medidas por si colapsaban los sistemas informáticos de todo el mundo.

- *Las empresas Puntocom.* Principalmente empresas americanas cuyo negocio estaba relacionado con internet. En aquella época suponía un

[3] Ciberespacio: ente o lugar virtual donde se realizan las conexiones globales a internet, así como una trasferencia continúa de todo tipo de datos.

nuevo modelo de negocio y se desconocía el potencial que hoy en día tiene. En este contexto, empresas americanas como Amazon, Google, Yahoo, o eBay, se convirtieron en potenciales clientes de las aseguradoras americanas y de su nuevo producto, el ciberseguro.

- *Crimen organizado en la red.* Los criminales han traspasado el mundo físico para dedicarse también al mundo virtual de internet. Actualmente existe un mercado negro de información personal y económica tanto de individuos como de empresas llamado Deep Web[4]. En dicho mercado digital se compran y venden datos de identificación personal, datos médicos, números y claves de tarjetas de crédito de personas, e información confidencial y privada de empresas. Lo más alarmante es que el cibercrimen nunca descansa y opera 24 horas/365 días al año aprovechándose de posible vulnerabilidades y brechas de seguridad de sus víctimas para poder actuar.

- *Ley SB1386 o Ley sobre notificación de la vulneración de las medidas de seguridad.*[5] Esta ley obligaba a que toda empresa que diera a conocer de forma accidental o evitable información personal de cualquier residente de California, debía revelar este hecho a la persona afectada dentro de un período razonable. Tal y como está formulada la ley, cualquier empresa que mantuviera relaciones comerciales con cualquier residente de California también estaba obligado a cumplir dicha ley. Esto significa que no solo las empresas residentes en California tuvieran el obligado cumplimiento, sino que ninguna empresa americana estaba exenta. Esta nueva normativa supondría que aquellas empresas que estuvieran afectadas por esta ley quisieran transferir este nuevo riesgo al mercado asegurador. Las pólizas de seguro cibernéticos comenzaron a incluir entre sus coberturas los costes directos asociados con el cumplimiento de las leyes de notificación, incluyendo honorarios de abogados, gastos de investigación forense, costes de notificación y envío, gastos de call center[6], etc. ya que todos estos gastos de notificación son directos e inevitables.

A efectos del mercado asegurador el primer seguro de ciberriesgos lo lanzó la compañía aseguradora AIG en 2012. El seguro se llamaba CyberEdge, y se trataba de un seguro, como apunta INESE[7], que buscaba disminuir algunas de las consecuencias que potencialmente producen tanto una violación de seguridad como una fuga de datos. Dentro de las coberturas básicas ofertaban la responsabilidad por el uso y tratamiento de información que ampara los perjuicios y los gastos de defensa relacionados con una violación de datos personales o de información corporativa. Posteriormente en el año 2000, el conocido mercado británico de seguros Lloyds definió las políticas relativas al sector.

[4] (Deep Web) Web profunda en castellano. Se denomina así por no estar indexada a los motores de búsqueda tradicionales de internet.
[5] El 1 de julio de 2003 se aprobó en el Estado de California la Ley sobre notificación de la vulneración de las medidas de seguridad, también conocida como Ley SB1386.
[6] (Call Center) Centro de llamadas telefónico.
[7] INESE: Instituto de Estudios Superiores Financieros y de Seguros.

Por lo tanto, fue en Estados Unidos donde comenzó a ofertarse el seguro de ciberriesgos. Allí empresas de todos los tamaños suscriben desde hace mucho tiempo este tipo de pólizas ya que son conscientes de los imprevisibles riesgos que entraña la red. En Europa y España, como se verá más adelante, el seguro de ciberriesgos se está empezando a consolidar y ya goza de cierta relevancia dentro del sector.

1.2. Tipos de ciberriesgos, ciberamenazas y sus consecuencias

A continuación, se identificarán los principales tipos de ciberriesgos, así como una representación de la gran cantidad y variedad de ciberamenazas existentes, y las consecuencias que pueden acarrear a personas, empresas y gobiernos. Se ilustrará cada tipo de ataque con una noticia de actualidad.

Los ciberriesgos son tres principalmente:

- *Operacional*. Es la interrupción no física del negocio, es decir, cuando sucede un acontecimiento que está fuera del control de la empresa y es capaz de restringir o incluso cancelar las operaciones relacionadas con su negocio.
- *Reputacional*. Pudiendo afectar a la imagen y reputación de la empresa.
- *Regulatorio*. Multas de Organismos Públicos y reclamaciones de terceros.

En cambio, las ciberamenazas pueden ser muchísimas y de naturaleza muy diferente, tal y como se identifica a continuación.

1.2.1. Fuga y/o robo de información

Es la filtración de información confidencial, deliberada o de forma involuntaria, a una persona o medio de comunicación sin su consentimiento. Es uno de los mayores ciberriesgos que pueden sufrir las empresas, por la importancia que tiene hoy en día el uso y manejo tanto de la información propia como de información de terceros. La mayoría de la información sustraída es de carácter confidencial y privada.

En el caso de las empresas, la fuga o robo de información puede provenir tanto de fuera de la organización, a través del ataque de un cibercriminal o hacker a los sistemas informáticos de la empresa por vulnerabilidades de los sistemas de información; o puede venir de dentro de la organización, como a consecuencia de un descuido de un empleado, o por su mala intencionalidad.

Las consecuencias pueden llegar a ser muy importantes en cualquier empresa ya que casi siempre derivan en pérdidas económicas y financieras, daños en la operativa del negocio, pérdida de nuevas oportunidades de negocio, daños de imagen de marca y reputacionales, y/o sanciones administrativas, civiles e incluso penales.

Afecta a todo tipo de sectores empresariales, pero haciendo mayor hincapié en aquellos que dispongan de información de medios de pago o información confidencial valiosa.

En el caso de Gobiernos y Administraciones Públicas el robo de datos tendrá un motivo financiero y/o de espionaje. Hasta las ciudades están empezando a ser atacadas mediante el secuestro de datos, pero sin que estos sean robados, y principalmente para percibir un rescate económico cuantioso. El problema es que este tipo de ataque no está afectando simplemente a simples usuarios, sino que también golpea directamente a los sistemas críticos de la ciudad: policía, bomberos, hospitales, empresas que gestionan la luz, el agua o el gas e, incluso el propio Gobierno municipal.

En el caso de las personas el robo de información puede implicar una posterior extorsión que vulnere la imagen de la víctima, y busque adicionalmente conseguir un beneficio económico. Muy popular fue el caso de Ashley Madison, una web de citas para personas infieles, que sufrió un robo de datos masivo de sus clientes para luego hacerlos públicos al no cerrar de inmediato la web como exigían los ciberdelincuentes.

Otro ejemplo de fuga importante de información fue el caso de Facebook y Cambridge Analítica. A principios de 2018 se filtró una noticia informando que en 2014 la información de millones de usuarios de la red social Facebook había sido compartida sin su consentimiento con una empresa británica llamada Cambridge Analytics. Los datos fueron utilizados por la empresa británica para que a través de un programa informático predijera las decisiones de los votantes durante las elecciones de los Estados Unidos de 2016 y a su vez lanzara mensajes influyentes tratando de alterar su intención de voto.

Según una noticia del diario El País del 24 de abril de 2019[8], como a consecuencia de este hecho la Comisión Federal de Comercio estadounidense anticipaba una multa de hasta 5.000 millones de dólares a la compañía Facebook, en su mayoría de costes legales de la investigación del regulador, al violar el compromiso por proteger la privacidad de sus usuarios.

1.2.2. Malware, Ramsomware y Spyware

El malware es un programa informático que tiene efectos no deseados o maliciosos. Suele actuar sin que el usuario del equipo se dé cuenta, entrando a través del correo electrónico, descargas de software en sitios maliciosos o mediante la copia de ficheros en medios extraíbles (como dispositivos USB o discos duros).

El ransomware es un tipo de “malware” cuyo principal objetivo es infiltrarse en los sistemas informáticos de las empresas para bloquearlos o cifrarlos. Se caracteriza porque inutiliza y bloquea determinados archivos del sistema pidiendo un rescate económico (normalmente en moneda virtual del tipo Bitcoin[9]) para recuperar la información.

[8] Pozzi, S. (24 abril 2019). Facebook anticipa una multa de hasta 5.000 millones por la fuga de datos. El País.
[9] (Bitcoin) Moneda virtual aceptada para determinados pagos en internet.

Existen muchos tipos de ransomware, entre los que destacan aquellos que provocan el secuestro del ordenador (imposibilidad de usarlo), y el cifrado de sus archivos, sea cual sea el soporte en que esté (equipos individuales, en red, en nube, etc.) Ahora además se adapta y ataca también a los nuevos dispositivos o gadgets (wearables) que están conectados a internet.

Según un estudio de la compañía Symantec[10] ya en el año 2015 se detectaron 430 millones de nuevas variantes de malware. Esto prueba que los ciberdelincuentes cada vez son más profesionales y persistentes intentando encontrar posibles brechas en los sistemas operativos de las empresas. El informe revela que España es el octavo país de Europa y el decimonoveno del mundo en ciberamenazas. Respecto a ramsomware recibe casi 300 ataques diarios, la mayor parte de estos ataques lo sufren las pymes, siete de cada diez. Los sectores favoritos son el sector servicios, banca y seguros (acumulando 8 de cada 10 ataques).

El spyware o programa espía es otro tipo de malware cuyo objetivo es recopilar información de un equipo informático para después transmitir dicha información a una entidad externa sin el conocimiento o el consentimiento del usuario.

Este tipo de ataques han crecido exponencialmente entre los usuarios, destacando en los últimos años los sectores de energía (persiguiendo la interrupción del suministro), gubernamentales, sanitario, telecomunicaciones, domésticos, negocios, e incluso servicios críticos como hospitales o centrales energéticas, de acuerdo al estudio anterior de Symantec.

El caso más importante de ataque por malware fue el ramsomware WannaCry. Ocurrió en mayo de 2017 y afectó a escala mundial a más de 360.000 ordenadores de personas, instituciones públicas y empresas de todo el mundo: Se vio comprometido el Servicio Nacional de Salud británico, la empresa americana FedEx o aquí en España Telefónica, Iberdrola y Gas Natural entre otras.

El malware WannaCry gracias a una vulnerabilidad revelada por la Agencia de Seguridad Nacional estadounidense permitía atacar aquellos ordenadores con el sistema operativo Microsoft Windows que no estuvieran debidamente actualizados. Muchos ordenadores que no tenían las actualizaciones de seguridad MS17-010 quedaron afectados, sus archivos cifrados y mostrando un mensaje en pantalla que exigía un rescate de 300 dólares en bitcoins a cambio de descifrar los archivos.
Un informe de Deloitte[11] sobre este caso, estimó que el impacto económico podría superar los 200 millones de dólares.

1.2.3. DDoS

El término Distributted Denial of Service (DDoS en sus siglas en inglés) consiste en provocar un colapso de los sistemas de información de una empresa mediante la saturación del servicio. Se busca sobrecargar los servidores de la em-

[10] Informe sobre amenazas a la seguridad de internet de Symantec (ISTR)
[11] Informe ¿Qué impacto ha tenido el ciberataque de WannaCry en nuestra economía?

presa para impedir el normal funcionamiento, ya que los sistemas de información de las empresas no están dimensionados para gestionar un tráfico desproporcionado.

Los ataques DDoS son muy populares por su bajo coste y sencillez. Basta darse una vuelta por la deep web para encontrar decenas de páginas que ofrecen estos servicios desde muy poco dinero. Según la empresa de ciberseguridad Kaspersky Lab, quienes han analizado los servicios DDoS disponibles en el mercado negro, un ataque DDoS puede tener un coste mínimo de 6,5 euros por hora.

Por otro lado, no siempre las amenazas se dirigen a grandes compañías. Más bien al revés. Ahora se dirigen en su mayoría a las pymes y comercios que utilicen internet como medio de negocio, empresas con web dedicadas al comercio online, portales de compra venta de bienes y servicios, webs online de apuestas y juegos de azar, etc.
Estos ataques también pueden ser realizados con motivos políticos (hacktivistas) y terroristas contra los gobiernos e instituciones críticas del país, así como de extorsión contra particulares y empresas.

Un evento importante, según apunta Kaspersky en su blog online[12], fue el relacionado con la caída del servidor DNI, servidor de compañías online como Twitter, Spotify, PayPal o Reddit. Según se redacta, “El 21 de octubre de 2016, muchos americanos descubrieron que sus páginas web favoritas no estaban disponibles. Sin ver Netflix, sin realizar transferencias mediante PayPal, sin juegos en línea con PlayStation. Y ni siquiera pudieron tuitear sobre el problema ya que Twitter también estaba caído. En resumen, 85 webs principales funcionaban ralentizadas o, simplemente, no respondían. Resultó que el problema fue una serie de ataques (tres en total) contra la estructura americana de internet.”

1.2.4. Phishing

El término phishing se refiere a una estafa realizada por cibercriminales para suplantar la identidad de un sitio web con el objetivo de obtener la información confidencial de sus usuarios (claves, contraseñas y datos bancarios), para realizar pagos y transferencias de dinero a través de internet. Quien se ve más afectado por este tipo de ataques son los particulares y las pymes.

Para citar un ejemplo respecto de este tipo de ataques y el cual haya afectado directamente a un particular, me gustaría relatar una experiencia personal, la cual me ocurrió hace aproximadamente un año y donde fui víctima de un intento de fraude. Recuerdo querer acceder con mi ordenador personal a la supuesta página web oficial de una entidad bancaria con la que trabajaba por aquel entonces. Accediendo a internet a través del portal web de Google di “click” a la primera opción que aparecía, tras introducir mi usuario y contraseña en la página principal del banco como era habitual, apareció un mensaje indicando que por favor informase de unos números secretos de mi tarjeta de claves banca-

[12] Blog online Kasperky, https://www.kaspersky.es/blog/attack-on-dyn-explained/9420/

rias. Me quedé muy sorprendido en ese mismo instante porque nunca antes el banco me las había solicitado, y por lo tanto desconfié. Inmediatamente después busqué en internet información relativa a lo que me acabada de pasar y sorpresa, mucha gente estaba comentando lo mismo. Decían que era una estafa y que bajo ningún concepto diéramos nuestras credenciales. El caso es que la página web en cuestión a la que estaba accediendo anteriormente no era la página web oficial del banco, sino una muy similar, a excepción de unos mínimos detalles que a priori pasaban inadvertidos.

1.2.5. Suplantación de identidad – Fraude del CEO

La suplantación de identidad es un tipo de ataque mediante el cual una persona consigue hacerse pasar por otra persona para cometer un fraude. Suele afectar principalmente a las personas, pero también puede ocurrir en empresas. La suplantación difiere del robo en que no accede a las contraseñas u otros datos personales. Se utiliza bastante las credenciales filtradas, y se limita a crear un perfil paralelo con la información publicada.

El actuario Fabián Romo Zamudio[13], advierte que para este tipo de ataques existen dos tipos de datos de ser susceptiblemente robados, “Los datos corporativos y los personales. Transacciones, números de cuenta bancarios, planes financieros, desarrollos, innovaciones, invenciones —el llamado espionaje industrial— datos de usuarios, como cuentas y contraseñas. En el segundo son la identidad digital, números de cuenta bancarios, cuentas y contraseñas, y otros tipos de datos personales como domicilio, información de redes sociales, imágenes, videos, documentos. En lo general, cualquier tipo de dato es susceptible de ser extraído”[14].

En lo que se refiere al impacto y consecuencias que tienen estos ataques sobre las empresas, en mi opinión se produce principalmente como a consecuencia de una mala educación organizativa en lo referente a la seguridad cibernética dentro de la empresa. Ya que como a consecuencia de errores humanos voluntarios e involuntarios se producen la mayoría de estos ataques. Pero también es cierto que se pueden producir como a consecuencia de suplantación del correo y/o la web sin que el usuario sea consciente de ello. No obstante, tal y como se puede deducir de un artículo del blog Kaspersky[15] se están dando los primeros pasos en materia de concienciación en ciberseguridad (Cybersecurity Awareness en inglés), principalmente en Estados Unidos y Europa, y cuyo objetivo principal es promocionar la educación en temas de ciberseguridad, seguridad y privacidad online.

Por sectores, los que se encuentran más afectados por este tipo de ataques son instituciones bancarias y financieras.

[13] Director de Sistemas de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la Universidad Nacional Autónoma de México (UNAM).
[14] Zamudio, F. (8 de abril de 2019). Robo de identidad es un ciberdelito que va en aumento en México. La Verdad Diario.
[15] Blog Kaspersky (5 octubre 2017). Mes de la concienciación en ciberseguridad.

Por otro lado, si hacemos referencia al ataque conocido como *Fraude del CEO*, se trata de un tipo de ataque relacionado con el comentado anteriormente y en el que los cibercriminales aprovechan la facilidad de suplantación de identidad para incitar a un empleado, previamente elegido como víctima, a realizarles una transacción sensible (financiera o de información), sin el estafado saberlo. Simplificándolo, los estafadores envían un correo electrónico a un empleado el cual suele pertenecer a las áreas de finanzas o contabilidad de la empresa. El correo supuestamente lo recibe de alguna persona de la alta dirección de la empresa, como el Director General (o CEO, de ahí el nombre del fraude), y le solicita sin levantar ninguna sospecha que envíe dinero o realice el pago de una factura a una cuenta bancaria bajo el control de los estafadores, la cual estará ubicada en algún país donde resulte prácticamente imposible seguir su rastro, principalmente paraísos fiscales, y donde no se podrá recuperar el dinero.

Los procedimientos y controles internos de las compañías, en ocasiones demasiado laxos, no logran detectar el fraude hasta ya pasado un tiempo, con todos los posibles daños y perjuicios económicos que implicará para la empresa. Según aconseja el Cuerpo Nacional de Policía para evitar esta estafa "las empresas tendrían que establecer protocolos de actuación respecto a las transferencias de dinero y un sistema de doble verificación antes de ejecutar órdenes sensibles. También se deben adoptar medidas de seguridad en las comunicaciones como cautela al abrir cualquier email de desconocidos; valorar la información empresarial que se publica en las redes; mantener el software de los equipos utilizados por el CEO actualizados y tener especial atención con las conexiones a través de redes wifi abiertas".

Este fraude afecta principalmente a las empresas, sobre todo a aquellas con un alto número de empleados, y/o grandes corporaciones. Además, todos los sectores empresariales son susceptibles de verse afectados, ya que las estructuras jerárquicas de las empresas son muy similares en general.

Tal y como informaba el periódico local de Canarias[16], la empresa Guaguas Municipales, y varias empresas canarias fueron víctimas de este ataque a principio de 2018. Solo la compañía municipal de transportes perdió 982.765 euros por dos pagos falsos. Guaguas Municipales más tarde lo denuncio a la Policía Nacional y llevaron el caso a los tribunales. Gracias a ello ya han recuperado una parte del dinero perdido.

1.2.6. Ciberbullying o ciberacoso

El evento más típico en el ámbito personal es del ciberbullying o ciberacoso, una práctica cada vez más extendida en todos los países y afectando sobre todo a las figuras públicas y las personas más jóvenes. Se da principalmente a través de las redes sociales o mediante aplicaciones de mensajería como WhatsApp. El ciberdelincuente en un principio genera contenidos negativos de su víctima para denigrar y desfavorecer su reputación online. Finalmente le pe-

[16] Darriba, J. (24 de abril de 2019). Guaguas Municipales fue víctima de la «estafa del CEO. Canarias7.

dirá un rescate a cambio de eliminar dicha cuenta falsa, buscando con ello obtener un beneficio económico por el fraude realizado.

Por último, y si atendemos al último estudio[17] realizado por Unespa, Cepime y Cepreven, tres autoridades de reconocido prestigio en el mundo asegurador en España, los ataques que se dan con mayor frecuencia son la denegación de servicio (DDOS), programas maliciosos (malware) y de secuestro de datos (ransomwares).

A modo de conclusión, y centrándome únicamente en las empresas, considero oportuno resumir y concretar cuáles son las principales consecuencias de recibir un ataque cibernético.

- *Pérdida y/o robo de datos.* Según qué tipo de datos se vean afectados determinará la magnitud del suceso. Si se sustraen datos financieros o personales se podrá reparar en su justa medida, pero si el robo o la pérdida son de datos de carácter confidencial, privado y/o relacionado con proyectos estratégicos de la compañía podría llegar a tener unas consecuencias catastróficas para la empresa.
  Perder información privada y sensible de la empresa puede afectar gravemente tanto a su patrimonio como a su reputación, por eso transferir este riesgo al mercado asegurador sería muy conveniente para conseguir una rápida recuperación de los datos y una recuperación de la imagen pública de la empresa.

- *Pérdida económica.* Casi todos los ataques informáticos que he expuesto con anterioridad tienen como fin último obtener un beneficio económico. Todo tipo de empresas, independientemente del sector y del tamaño de las mismas, son susceptibles de sufrir una pérdida económica. Y en las empresas pequeñas las consecuencias pueden ser mayores debido a la escasez de recursos que destinan a la seguridad informática y sus sistemas.

- *Pérdida de confianza y reputación.* Cuando una empresa sufre un ataque cibernético puede llegar a derivar en una pérdida de credibilidad y confianza, afectando tanto internamente a sus socios, accionistas y empleados, como externamente a sus clientes y proveedores. Ello puede dar lugar desde a empleados inseguros y desconfiados, a pérdidas de clientes y a una mala imagen pública en el sector, pudiendo acarrear consecuencias irreparables si no se atienden a tiempo y en su justa medida.

- *Cambio en el modelo de negocio.* Y con ello me refiero a la reorganización interna necesaria en el ámbito de la ciberseguridad de la empresa. Tras recibir un ataque, es necesario replantearse la forma en que se tratan, almacenan y protegen los datos y la información sensible para asegurarse de que los sistemas informáticos existentes no vuelvan a ser vulnerables. De hecho, en ocasiones se opta por no volver a almacenar los datos personales especialmente sensibles, así como los datos finan-

[17] Estudio 'Ciberriesgos, su impacto en las PYMES' (08 de octubre del 2018)

cieros de sus clientes por el riesgo que ello conlleva de cara a las potenciales multas y sanciones. Otra posible medida a realizar sería trasladar los servidores a un proveedor externo para no tener toda la información en el mismo sitio, y así minimizar el riesgo.

1.3. Ataques cibernéticos a gobiernos, infraestructuras críticas, personas y empresas

En el presente capitulo se informará quienes son los principales causantes de las ciberamenazas anteriormente descritas, y cómo estas impactan y perjudican a gobiernos, infraestructuras críticas, personas y empresas. Así como los mecanismos existentes en el presente para combatirlas.

Actualmente, como ya ocurre en el mundo físico, los ataques cibernéticos pueden ser llevados a cabos por diferentes agentes.

- *Los Estados*, y en particular los Servicios de Inteligencia y Contrainteligencia, con el fin de robar y obtener información sensible de otros países y de sectores estratégicos. Disponen de muchos medios tecnológicos y muy avanzados, además de personal muy cualificado.

- *Terroristas*. Los grupos terroristas emplean el ciberespacio hoy en día como medio de propaganda y reclutamiento, o para obtener financiación para sus actividades terroristas. Se trata de una amenaza que recae principalmente sobre Estados, Gobiernos y Naciones.

- *Grupos extremistas*. Personas con intereses ideológicos, étnicos, religiosos y/o políticos que persiguen perjudicar principalmente a grupos de personas con intereses en común, también conocidos como lobby. Es lo que se conoce como Hacking Político o Patriótico.

- *Crimen organizado*. Estas organizaciones también han comenzado a trasladar sus acciones al ciberespacio, realizando actividades relacionadas con el robo de información de carácter individual y financiero. Su objetivo principal es la obtención de información sensible de personas y empresas para su posterior uso fraudulento y extorsión, y así conseguir grandes beneficios económicos. En consecuencia, se requerirá a las aseguradoras considerar los incidentes y consecuencias derivados de un fraude o extorsión como garantías asegurables en el seguro de ciberriesgos.

- *Espionaje industrial*. Gobiernos y empresas de origen tecnológico e industrial principalmente que tienen interés en disponer de información crítica de desarrollos tecnológicos e industriales, así como de procesos de fabricación de productos de la competencia con el objetivo de obtener ventajas y secretos comerciales. El mercado asegurador deberá contemplar esta amenaza como una posible garantía a ofrecer a las empresas en la póliza de ciberriesgos.

- *Personas individuales* (hackers). Personas con conocimientos muy avanzados en las tecnologías de la información e internet. La naturaleza de los ataques puede ser muy heterogénea y por diferentes motivos, fundamentalmente, personal, de creencias y por valores, pero principalmente económicos. A mi parecer, son la amenaza más letal que existe hoy en día, ya que tanto personas, como gobiernos, infraestructuras críticas, y principalmente empresas de todos los sectores y tamaños son objetivo de estos ciberdelincuentes. Son ellos los creadores de virus, malware o archivos maliciosos que tanto daño hacen a nivel global. El fraude, la ciberextorsión y la pérdida y/o robo de información propia y de terceros serán los riesgos a intentar transferir principalmente por parte de las compañías.

1.3.1. Gobiernos y Administraciones Públicas

Los expertos informan de que en el mundo actual se está librando una guerra cibernética a gran escala, y fomentada principalmente por las grandes potencias mundiales. Los principales países implicados son Estados Unidos, Rusia y China. Gracias a sus grandes recursos económicos disponen de los recursos tecnológicos más avanzados. La batalla se ha trasladado al ciberespacio, e implica nuevas amenazas nunca antes vistas. La capacidad de reacción que tengan los países se presume crítica si no quieren verse gravemente perjudicados.

En lo que concierne a España hay que decir que también se están realizando grandes esfuerzos a nivel de Estado para combatir las nuevas amenazas del ciberespacio. Una noticia de marzo de 2019 del diario El País[18] se hacía eco de ello e informaba el modo en que está cambiando la delincuencia en España y cuales son ahora las principales amenazas. “La delincuencia está cambiando. Los métodos para combatirla, también. La recién publicada Estrategia Nacional contra el Crimen Organizado detalla cuáles serán las principales amenazas de los próximos años y señala el cibercrimen y el riesgo de ataques informáticos a gran escala como las mayores preocupaciones de los expertos policiales”. Ello significa que se está produciendo un cambio de paradigma, y tanto en el presente como en el futuro los ataques más críticos posiblemente provengan del ciberespacio. Supone un reto sin precedentes para Gobiernos y Administraciones Públicas.

En nuestro país contamos principalmente con dos instituciones para combatir las ciberamenazas:

Instituto Nacional de Ciberseguridad de España (INCIBE). Es una sociedad dependiente del Ministerio de Industria, Energía y Turismo. Su misión es reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en ge-

[18] Lopez-Fonseca, O. (10 de marzo de 2019). ‘Interior alerta del “riesgo alto” de sufrir ciberataques a gran escala’. El País.

neral. En el presente juega un papel fundamental en la ayuda para la ciberseguridad de las pymes en España.

Centro Criptológico Nacional (CCN). Es el organismo encargado de la ciberseguridad bajo la dirección del Centro Nacional de Inteligencia (CNI). Según destacaba una noticia del diario La Vanguardia de junio de 2019[19] dicho organismo esperaba que para este año 2019 aumenten los ciberataques patrocinados por diferentes Estados y los especialmente dirigidos a la cadena de suministro y a la nube (por la gran cantidad de datos que contiene).

Entre los organismos internacionales europeos cabría destacar la agencia europea *ENISA* (European Network Information Security Agency) que coordina las diferentes Agencias Nacionales de Seguridad en el ámbito de la Unión Europea. No obstante, aún son pocos los países europeos que cuentan con Agencias Nacionales en el ámbito de la ciberseguridad.

A mi juicio, la seguridad del ciberespacio tiene que ser un objetivo primordial para la seguridad nacional de cada país. Debería centralizarse la gestión de la ciberseguridad mediante la creación de un organismo responsable de coordinar a todas las entidades públicas y privadas de dicho país. Así como la cooperación internacional entre países, y el fomento de una cultura de ciberseguridad en el conjunto de la población y los trabajadores de las empresas. Se debe destinar cada vez más recursos económicos y humanos a la defensa del ciberespacio por parte de Gobiernos y Naciones. Solo así se podrá luchar frente a estas nuevas amenazas.

Por otro lado, entiendo inviable una cobertura adecuada en el actual mercado asegurador privado que pueda proteger de los ataques cibernéticos que afectan a Gobiernos y ciertos Organismos Públicos, como por ejemplo en materia de Defensa.

1.3.2. Infraestructuras críticas

Las infraestructuras críticas son el conjunto de recursos, redes, servicios y tecnologías de la información que en caso de sufrir un ataque causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento de la Nación.

Las amenazas a las infraestructuras críticas siempre han existido en tiempos de guerra o conflicto, pero los escenarios de amenazas incluyen ahora ataques en tiempos de paz por delincuentes anónimos, tanto individuales como el crimen organizado, terroristas e incluso Gobiernos.

Un ejemplo del impacto que podría tener un ataque de estas características sería un ataque a las redes eléctricas de un país. Como le ocurrió a Venezuela a mediados de marzo de 2019, y donde según indicaban muchos medios de comunicación locales e internacionales podría haber sido como consecuencia de un ciberataque. Tenemos que reflexionar y pensar que sin electricidad

[19] Grau, X. (13 de junio de 2019). 'Estas son las tendencias de futuro en ciberataques'. La Vanguardia.

prácticamente todo en un hogar y en la vida cotidiana dejaría de funcionar. El país dejaría de prestar servicios públicos tan importantes como los transportes públicos o servicios básicos en los hospitales. Una pérdida de energía durante unos pocos días, puede producir daños económicos devastadores en la economía de un país.

En España las infraestructuras críticas se agrupan en 12 sectores importantes: Administración, salud, sistema financiero y tributario, energía, agua, alimentación, industria nuclear, industria química, instalaciones de investigación, transporte, espacio y tecnologías de la información y las comunicaciones. Actualmente existen unas 3.700 infraestructuras críticas, de las que el 80% de ellas pertenecen al sector privado. Todos estos sectores se apoyan en el ciberespacio, tanto en su gestión interna como para ofrecer sus servicios a los usuarios y clientes. Esa dependencia tecnología es constante y no admite fallos prolongados, debe estar siempre disponible y ser fiable.

La Secretaría de Estado de Seguridad (SES) en España es el órgano responsable de la dirección, coordinación y supervisión de la protección de infraestructuras críticas nacionales, de la creación del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), como órgano competente en la protección de las infraestructuras críticas, director y coordinador de dichas actividades. Este Centro (CNPIC) y el Instituto Nacional de Ciberseguridad (INCIBE) son los órganos encargados de dar respuesta también a incidentes para las tecnologías de la información de las infraestructuras críticas ubicadas en España. Ambas entidades han puesto en marcha un equipo de respuesta a incidentes de seguridad especializado en el análisis y gestión de problemas e incidencias de seguridad tecnológica. De este modo, este equipo de respuesta se convierte en la unidad especializada en la gestión de incidentes relacionados con las infraestructuras críticas a nivel nacional. Europa aprobó en 2004 el Programa para la Protección de la Infraestructuras Críticas (PEPIC).

Podríamos decir que España se está profesionalizando y especializando a pasos agigantados en seguridad cibernética. Prueba de ello se recoge en una publicación del diario Expansión[20] donde se menciona que “España es el primer país de la UE en desarrollar la Guía de Gestión de Ciberincidentes”. Este manual busca ser una descripción detallada del proceso de notificación, con 38 tipos de ataques, agrupados en 10 clases y 5 correspondientes niveles de peligrosidad, así como 6 de impacto. En el ámbito de protección de infraestructura críticas, designados así en la aplicación de la Ley 8/2011, PIC, establece incluso rangos temporales obligatorios de notificación y entrega de informes de incidentes, dependiendo de los niveles de peligrosidad o impacto. Además, incluye una propuesta de métricas para el proceso de gestión de incidentes que, según el tamaño de la entidad y el nivel de madurez en seguridad, podrían reflejarse en plan de adecuación al Esquema Nacional de Seguridad (ENS).

El citado Centro Criptológico Nacional (CCN) hizo frente en 2018 a 38.192 ciberataques, el 57% dirigidos contra redes de las Administraciones Públicas. El Instituto Nacional de Ciberseguridad (INCIBE) gestionó también 111.519 inci-

[20] De las Heras, Mar. (27 de febrero de 2019). ‘España, primer país de la UE en desarrollar la Guía de Gestión de Ciberincidentes’. Expansión.

dentes, de los que 722 afectaron a operadores estratégicos críticos, es decir, gestores de servicios esenciales para la sociedad. En los últimos cinco años, estos últimos han sufrido más de 2.300 ataques. Los sectores financieros, energético y de transportes suman más de la mitad de los casos.

Según el último informe Global de Riesgos del Foro Económico Mundial[21], la tendencia creciente consiste en el uso de ciberataques que apuntan a infraestructura esencial y sectores industriales estratégicos, lo cual hace temer que en el peor de los casos posibles, los atacantes podrían provocar el colapso de sistemas que mantienen a sociedades enteras en funcionamiento.

A efectos del mercado asegurador, únicamente las compañías aseguradoras de ámbito internacional pueden estar interesadas y tener el apetito suficiente como para poder asegurar este tipo de sectores estratégicos tan importantes. La forma de aseguramiento será ciertamente mediante contratos de coaseguro[22] y reaseguro.[23] Hay que tener en cuenta que la información que poseen y la actividad que realizan es clave para el buen funcionamiento de la sociedad. Un robo o pérdida de información esencial, o una ciberextorsión inutilizando temporalmente los equipos hasta que no se produzca el pago exigido, se perciben como críticos. Y lo que podría ser incluso peor, un ataque terrorista con el único objetivo de causar el mayor desastre y daños posibles a toda la sociedad.

1.3.3. Personas

El ciberdelito más común que se da contra las personas es el de la ciberextorsión y el ciberbullying. A través de la ciberextorsión los atacantes intimidan a sus víctimas a través de internet para obtener de ellas información de carácter personal y sensible o para que realicen un pago económico a su favor. El delincuente y la víctima normalmente no se conocen y no suelen tener contacto directo más allá del mantenido en la red para pedir la cantidad a abonar. Según la Guía de la Fundación Mapfre[24] los casos más comunes en los que se da la ciberextorsión son:

- Bloqueo de la información o de programas informáticos que impida la realización normal de la actividad.
- Secuestro de acceso a teléfonos móviles.
- Bloqueo de cuentas personales en diferentes redes sociales.
- Amenazas de publicación de información obtenida de la víctima.
- Envío de comunicados solicitando información personal bajo amenazas.

El caso del ciberbullying es distinto, suele darse entre jóvenes adolescentes de ambos sexos, con el ánimo de ofender, intimidar y deshonrar la imagen de la víctima. Normalmente el atacante y su víctima sí que se conocen y guardan algún tipo de relación previa. Se han llegado a producir casos de suicidios como a consecuencia de este ciberacoso. La paradoja que se da es que hoy en

[21] 'Informe Global de Riesgos, 2018'. Foro Económico Mundial.
[22] Coaseguro: Reparto del riesgo entre las diferentes compañías aseguradoras que participan del mismo.
[23] Reaseguro: Transferencia de parte del riesgo o su totalidad a otra compañía aseguradora o reaseguradora.
[24] 'Guía para proteger tu negocio frente a los ciberriesgos'. Fundación Mapfre, 2017.

día además de que te puedan acosar físicamente en el mundo real puedes ser también acosado y extorsionado a todas horas en el mundo digital de internet.

Otro ataque muy común que se da últimamente entre las personas son los delitos de phishing, y donde a través de correos electrónicos de suplantación de identidad y webs falsas se engaña a los usuarios para robar sus datos personales y bancarios.

En mi opinión, animo a las compañías aseguradoras a que empiecen a ofertar garantías especificas contra la extorsión y el ciberacoso en las pólizas de hogar, y con el objetivo de ayudar a las víctimas a través de medidas preventivas contra la ciberextorsión y el acoso. Si no otra opción podría ser formular una nueva póliza de ciberriesgos que ampare únicamente este tipo de amenazas. Cabría resaltar en este ámbito la ayuda que pueden aportar las empresas tecnológicas de servicios a las compañías de seguros, a través de expertos profesionales que saben cómo actuar ante este tipo de situaciones. Ya que uno de los principales problemas que se da entre las víctimas es la incapacidad de reacción ante las situaciones de acoso y extorsión.

1.3.4. Empresas

Todas las empresas que dependan de los sistemas de información, y que almacenan datos de carácter confidencial y privado son susceptibles de sufrir ataques cibernéticos. Porque la pregunta que se tienen que hacer no es si van a recibir un ataque cibernético, sino cuando se va a producir. De todos los agentes descritos anteriormente, las empresas son las que sufren más ciberataques. En realidad, por el hecho de poseer información de carácter sensible tanto propia como de terceros (proveedores y clientes), hacen que estén más expuestas a ser atacadas por hackers, cibercriminales e incluso Gobiernos.

Según un estudio realizado por IBM Security y el Instituto Ponemon[25] a 447 compañías de los sectores más relevantes de ámbito mundial, y que sufrieron una violación de datos en los últimos 12 meses, se determina, como indica el grafico a continuación, que la mayor frecuencia de casos se dan en el sector financiero, tecnológico, industrial y de servicios.

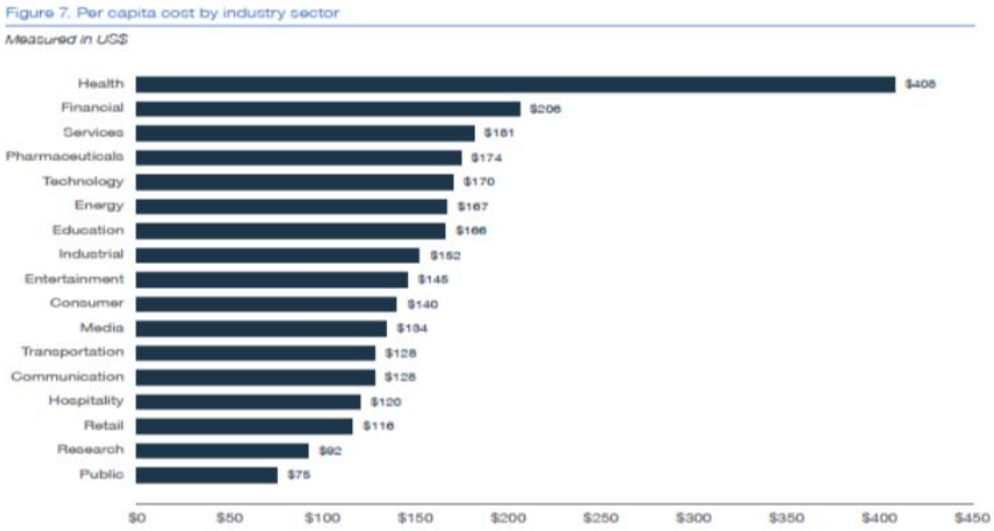
[25] Estudio ‘Costes de Violación de datos (Data Breach)’. IBM Security e Instituto Ponemom. 2018.

Gráfico 1. Frecuencia de ataques de violación de datos por sector

Fuente Estudio realizado por IBM Security y el instituto Ponemon de 2018 sobre “Costes de Violación de datos (Data breach)”

Sin embargo, como se puede apreciar en el siguiente gráfico, los costes más elevados como a consecuencia de dichos ataques se dan en el sector salud principalmente, pero tambien en el financiero, servicios, tecnológico, energético y farmacéutico.

Gráfico 2. Costes de ataques de violación de datos por sector.



Fuente, Estudio realizado por IBM Security y el instituto Ponemon de 2018 sobre “Costes de Violación de datos (Data breach)”

En el ámbito empresarial, existen sectores más sensibles ante las ciberamenazas. Por consiguiente, los empresarios tratarán de ceder parte de estos riesgos al mercado asegurador. Los principales sectores afectados son:

- *Compañías bancarias y aseguradoras.* Históricamente ha sido el sector que ha sufrido más ataques cibernéticos, así como un mayor número de violaciones y brechas de seguridad, ya que poseen información de carácter personal y económico muy relevante, como nombres, números de teléfonos, direcciones físicas, detalles de tarjetas de débito y crédito, historiales de crédito, además de otros datos financieros.
  El crecimiento de la banca por internet y el uso de aplicaciones bancarias en el teléfono móvil han expuesto el sector aún más a nuevas ciberamenazas.

  Estarán interesados en transferir al mercado asegurador principalmente los riesgos asociados con la pérdida y/o robo de datos de clientes y el uso indebido de las tarjetas de crédito o débito.

- *Las empresas de telecomunicaciones.* Procesan y transmiten gran cantidad de información a través de sus servidores, y son responsables de la seguridad de dicha información. Desde 2002 y de acuerdo con la Directiva europea 2002/58/CE[26], en muchos países de la UE, entre ellos España, las empresas de telecomunicaciones tienen la obligación legal de notificar cualquier violación en la seguridad de datos, lo que supone unos gastos de notificaciones elevados, además de posibilidad de recibir multas y/o sanciones administrativas y reclamaciones de terceros.

  Por lo tanto, los costes asociados a la responsabilidad civil de la empresa por violación de confidencialidad y privacidad de terceros, así como la propia seguridad de su red, tienen que ser contemplados en la póliza de ciberriesgos.

- *Hoteles y ocio:* Disponen de una base de datos de consumidores muy amplia, tanto de carácter personal como financiero, ya que está vinculada a las ventas y las reservas online. Tienen que ser especialmente cautos respecto al cumplimiento de la normativa relativa a la industria de tarjetas de crédito. Deberán ser además muy precavidos en cuanto a la protección de la información confidencial de sus clientes y la protección de las comunicaciones entre empresa y sus proveedores. Los gastos de reclamación por la pérdida y/o robo de datos de los clientes, el fraude con las tarjetas de crédito, o el fraude en su comercio electrónico son riesgos a ceder a las compañías aseguradoras.

- *Centros de salud y hospitales:* Los ciberataques a instituciones sanitarias pueden causar la pérdida de datos personales, alteraciones en el histo-

[26] Ley BOE: Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

rial clínico de los pacientes e incluso modificaciones de la prescripción de medicamentos que consumen, con las implicaciones que tendría sobre el paciente. Generando a su vez un daño muy importante a la imagen y reputación del centro sanitario por la pérdida, robo y/o manipulación de estos datos. Por lo tanto, los costes asociados a la pérdida y/o robo de datos de pacientes y empleados, y la consecuente pérdida reputacional son riesgos que se intentarán transferir al mercado asegurador. Aunque solo muy pocas compañías aseguradoras y que tienen un conocimiento muy profundo de este negocio se deciden a asegurarlos. Cabe recordar a su vez que, tal y como apuntaba el estudio anterior, los costes asociados a sufrir una ciberamenaza en este sector eran los más elevados.

- *Centros educativos*: Escuelas privadas, concertadas, públicas, guarderías, academias y centros de formación, recogen gran cantidad de información confidencial de sus alumnos y padres. Nombres, direcciones, teléfonos de contacto, y otros más íntimos como datos sobre la salud o creencia religiosa, expedientes académicos, números de tarjetas de crédito, cuentas bancarias de los padres, información contractual. La pérdida y/o robo de datos de padres y alumnos, con sus correspondientes reclamaciones y costes por violación de la privacidad, los gastos asociados a recuperar la imagen del centro, o el fraude por robo de información de tarjetas de crédito, son riesgos a analizar en el seguro de ciberriesgos.

- *Prestadores de servicios* (despachos de abogados, gestorías, consultorías, etc.) Son excelentes objetivos para los ataques cibernéticos por la naturaleza de la información que manejan. Datos financieros, estrategias de negocio, secretos de marca, transacciones comerciales e información personal de terceros.

  Un ejemplo muy sonado fue el caso de los papeles de Panamá que afectó a la firma de abogados Mossack Fonseca en abril de 2016, dejando al descubierto información muy sensible sobre cómo evadían millones de impuestos algunos particulares y empresas.

  Los altos costes asociados a la información sensible y confidencial que manejan, hacen que casi ninguna aseguradora del mercado esté dispuesta a otorgarles una cobertura adecuada.

- *Comercios:* Tienen acceso a una gran cantidad de información sobre sus clientes, entre la que figura, datos de identificación personal y números de tarjetas de crédito. Además, en muchos comercios se realizan ventas online, y las páginas web son susceptibles de sufrir ciberataques.

  El riesgo más importante a valorar por un comercio en general es sufrir una ciberextorsión que le bloquee sus sistemas y no le permita continuar con su actividad ordinaria o su negocio online. La póliza de ciberriesgos deberá incluir la ciberextorsión entre sus coberturas.

- *PYMES:* Trabajan con gran cantidad de datos de clientes, proveedores y trabajadores, así como información confidencial de la propia empresa. Si se pierde o sustrae esta información puede resultar útil a la competencia, como por ejemplo estrategias de precios, situación financiera de la empresa, campañas publicitarias, etc. Asimismo, cada vez dependen más del entorno digital e internet para llevar a cabo sus operaciones más frecuentes y cotidianas, como el control y gestión de gastos, control y gestión de stocks, cadena de suministros y la comercialización de productos y servicios. Esta dependencia y el hecho de que las pymes suelen tener un gran desconocimiento de las amenazas a las que están expuestas y pocos conocimientos y recursos avanzados de carácter informático, aumenta sus niveles de riesgo.

  Las pymes son el perfil más buscado por las compañías aseguradoras para comercializar su póliza de ciberriesgos. Deberán tratar de mitigar los costes anteriormente descritos a través de las diferentes coberturas de la póliza.

2. Transferencia del riesgo al mercado asegurador, el ciberseguro

2.1. Introducción

Los mercados y las empresas están evolucionando constantemente y con ello el tipo de riesgos a los que se exponen. Hoy en día cualquier empresa, como se ha observado en el punto anterior, es susceptible de recibir un ataque cibernético en cualquier momento e independientemente de donde se encuentre. Con el objetivo de mitigar dichas ciberamenazas las empresas buscan transferir parte del riesgo a las compañías aseguradoras y en particular a través del seguro de ciberriesgos. Como el nivel de exposición al riesgo no se puede reducir, a no ser que se apagasen las máquinas y equipos informáticos, se pretenderá a través del contrato de seguros aminorar y controlar el nivel de impacto frente a estos riesgos, así como el perjuicio económico que supone para las empresas las posibles pérdidas financieras, de interrupción de negocio u otros daños derivados del uso de sistemas de información y comunicación.

Además, con la nueva normativa europea de 2016[27], relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, las empresas están obligadas a informar sobre cualquier brecha de seguridad y notificar a terceros las violaciones por robo y/o pérdida de sus datos. Por lo tanto, a través de la póliza de ciberriesgos se tratará también de aminorar la responsabilidad frente a terceros como a consecuencia de la pérdida y/o robo de información, con los consecuentes costes y gastos judiciales y de defensa asociados. Así como las posibles multas y/o sanciones de los organismos reguladores de protección de datos

Es evidente que empresarios y órganos directivos de las empresas han de tomar medidas adecuadas para transferir parte de estos nuevos riesgos a las compañías aseguradoras. A través de una adecuada gerencia de riesgos deberán analizar y valorar los costes derivados de una pérdida o robo de datos de carácter sensible, la pérdida de beneficios derivada de no poder comercializar sus productos y servicios a través de su plataforma digital, o la repercusión económica derivada de no poder acceder a sus propios datos o a los datos de sus proveedores y clientes. Sin descuidar, que estando en un entorno totalmente interconectado, las empresas suelen trabajar con proveedores de servicios tecnológicos más pequeños y es por ahí precisamente por donde puede venir un ciberataque con una posterior repercusión legal que puede afectar gravemente a la empresa en cuestión.

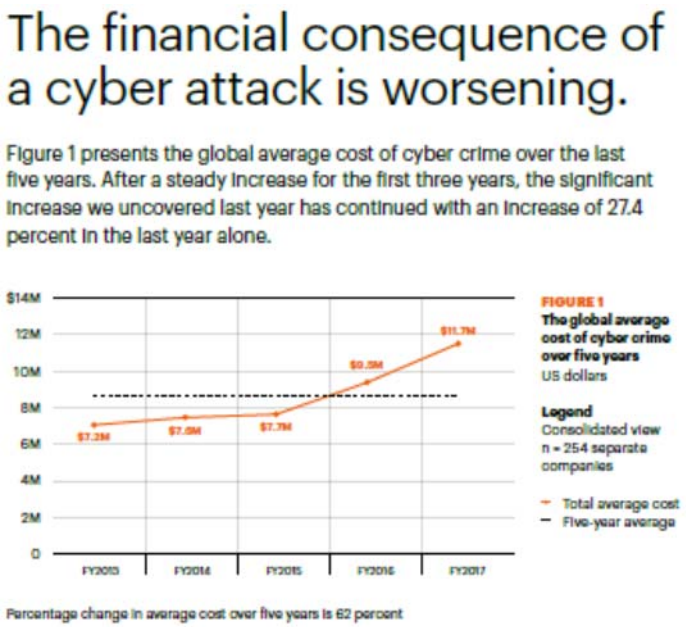
Por otro lado, ante un robo o una pérdida de datos de terceros podría implicar para la empresa una serie de costes de recuperación de dichos datos o costes de contratar asesores legales para que le informen sobre como notificar el inci-

[27] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

dente a sus clientes. Y lo que sería más grave aún, la pérdida de confianza de los clientes y usuarios afectados por el ataque con los consecuentes costes asociados de campañas publicitarias posteriores para intentar restaurar la imagen de la empresa.

Tal y como avala un estudio realizado por Accenture y el Ponemon Institute,[28] las consecuencias financieras para las empresas de recibir un ciberataque se están incrementando significativamente en los últimos años. Como se muestra en el siguiente gráfico, los costes financieros relacionados con ciberataques se han ido incrementando en los últimos 5 años, pero de forma mucho más significativa en los últimos 2 años del estudio, 2016 y 2017. Las compañías deberán de tomar por lo tanto medidas internas y externas de protección y resiliencia frente a los ciberriesgos.

Figura 1. Costes globales de recibir un ataque cibernético.



Fuente, estudio realizado por Accenture y el Ponemon Institute '2017CostCybercrime'.

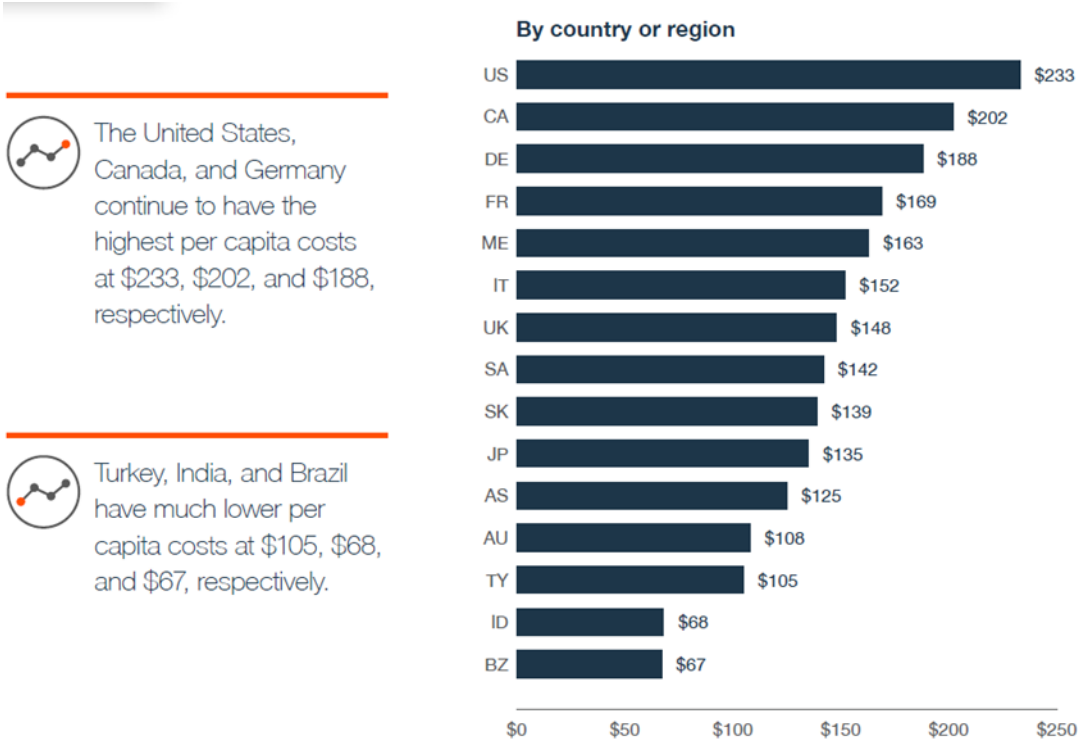
A nivel macro, y según informa INCIBE, España es el tercer país con más ciberataques del mundo tras Estados Unidos y Reino Unido. Solamente en 2018 se registraron más de 100.000 ciberataques. Suponiendo, según afirmaba el CNI, un aumento del 43% respecto al año anterior.

Pero si atendemos a los costes específicos que implican para las empresas recibir un ciberataque, un estudio realizado por el instituto Ponemon con la colaboración de la compañía IBM Security[29] nos arroja resultados sorprendentes. Los resultados del estudio concluyen que el coste medio de recuperar cada

[28] Estudio '2017CostCybercrime'. Accenture y el Ponemon Institute
[29] Estudio 'Costes de Violación de datos (Data Breach)'. IBM Security e Instituto Ponemom. 2018.

dato que fue sustraído fue de 148 dólares. No obstante, cabe aclarar que es mucho más costoso el coste de recuperar un dato en Estados Unidos o Canadá, sobre unos 233 dólares, que en India o Brasil, aproximadamente unos 67 dólares. Esto se debe a los altos costes de notificar la pérdida de datos en Estados Unidos; pues mientras que en Estados Unidos es obligatorio por ley notificarlo e informarlo a los afectados no ocurre lo mismo en India o Brasil.

Figura 2. Costes financieros de recibir un ataque cibernético, en dólares.



Fuente, estudio realizado por el Instituto Ponemon con la colaboración de la compañía IBM Security, “2018 Cost of a Data Breach”

Otra de las claves que desvela el estudio es que cuanto antes se identifique y contenga una violación de datos mucho menor serán los costes. El tiempo medio en identificar una violación fue de 197 días y de contenerla unos 69 días. Es decir, de media pasan casi 9 meses desde que la empresa en cuestión identifica que ha sufrido una brecha o violación de datos de datos hasta que finalmente la puede contener. Finalmente, y respecto al impacto económico que supone una brecha de seguridad en función del número de datos que almacena una empresa, indica que una violación de más de un millón de datos ha supuesto de media un coste total de 40 millones de dólares, y si la violación ha sido de más de 50 millones de datos el coste total ha sido de unos 350 millones de dólares. Por lo tanto, aquellas empresas que manejan y almacenan gran cantidad de datos necesitarán contratar un seguro de ciberriesgos, y con cobertura suficiente.

España no se contemplaba en el estudio anterior, pero según informa el Instituto Nacional de Ciberseguridad en 2018 un ciberataque tuvo un coste medio de 75.000 euros en España, lo que supuso unos 14.000 millones de euros para las empresas.

Con todos estos datos relacionados con el impacto que supone para una empresa recibir un ciberataque quiero hacer especial hincapié en la relevancia que tiene para las empresas transferir parte de estos riesgos al mercado asegurador, pues es cierto que en caso de violación de datos los costes asociados a su identificación y recuperación pueden impactar significativamente sobre la cuenta de resultados de la compañía. Por no hablar del valor objetivo y emocional que puede suponer una mala imagen de marca o una pérdida reputacional.

Cabe esperar por lo tanto que, con el creciente número de incidentes cibernéticos, la continua transformación digital en equipos informáticos, teléfonos móviles y gadgets tecnológicos, así como las nuevas iniciativas reguladoras en la Unión Europea y en España, aumente la concienciación de particulares y empresas de cara a protegerse e impulse a su vez la demanda de los ciberseguros

2.2. Primera barrera, la resiliencia cibernética de las empresas

Cuando se produce un ataque cibernético la mayoría de las organizaciones no están preparadas y no tienen los suficientes recursos o un plan de respuesta real y consistente ante estos incidentes. Esta es la principal conclusión que se ha extraído del último estudio anual realizado por el Instituto Ponemon e IBM[30]. El cual revela que el 77% de los encuestados aún carecen de un plan formal de respuesta ante incidentes de ciberseguridad (CSIRP). Asimismo, se define el concepto “resiliencia cibernética” como la capacidad que tiene una organización para protegerse y defenderse de los ciberataques. Las organizaciones altamente resilientes atribuyen esta percepción de mayor ciberresistencia a su capacidad para contratar personal cualificado, pero el factor tecnológico también es muy relevante según relata el estudio.

Por lo tanto, las empresas deberían de actuar de forma más proactiva ante estas nuevas amenazas del ciberespacio, constatando la necesidad de un cambio de paradigma al gestionar los riesgos cibernéticos. La ciberseguridad de la empresa se basará en el análisis y resolución de estos nuevos riesgos del ciberespacio y la implementación de una política resiliente acorde. La cual deberá ser aplicada desde un punto de vista organizativo y humano, que debe abordarse desde diferentes líneas de acción, haciendo partícipes a todas las personas que trabajen interna y externamente en la empresa. Pues la mayor parte de los problemas de seguridad provienen de dentro de las propias organizaciones, y no de fuera como se piensa comúnmente. En algunos casos, por usuarios malintencionados, pero en muchos otros casos, por simple desconocimiento en las acciones que realizan.

A continuación, se dará a conocer una serie de medidas básicas que se deberían adoptar en las empresas con el fin de evitar o mitigar en la medida de lo posible los riesgos cibernéticos.

[30] Estudio ‘Cyber Resilient Organization’. Instituto Ponemon e IBM. 2018

FACTORES HUMANOS

El personal de la empresa, socios y demás colaboradores deben estar sensibilizados y concienciados en la aplicación de las siguientes normas y buenas prácticas dentro de la empresa. Entre las medidas a aplicar:

- No responder e-mails o llamadas solicitando información confidencial de la compañía.
- Estar alerta ante los posibles e-mails o links a páginas web que recibamos de destinatarios no identificados.
- No utilizar equipos informáticos que no sean los proporcionados por la empresa.
- No dejar información confidencial en el escritorio del trabajador, todo debe ser archivado y guardado.
- Bloquear todos los dispositivos, fijos y móviles, cuando no se utilicen.
- No dejar a la vista contraseñas en los lugares de trabajo.
- Tener contraseñas de acceso a los diferentes equipos con claves complicadas, haciendo uso de minúsculas, mayúsculas, números y caracteres especiales.
- Establecer una política de utilización segura del correo electrónico (documentos adjuntos dudosos, hipervínculos o enlaces extraños.)
- No instalar USB, soportes de almacenamiento u otro tipo de dispositivos personales (hardware) en los equipos informáticos de la empresa.
- Evitar la utilización de accesos remotos o móviles no protegidos (wifi, bluetooth)
- No instalar programas informáticos o aplicaciones (software) en los equipos informáticos de la empresa sin el permiso del administrador.

Es importante resaltar en este punto que estas medidas tienen que afectar no solo a los trabajadores en nómina de la empresa, sino también a sus trabajadores temporales, estudiantes en prácticas, y otros posibles socios y colaboradores.

Debe realizarse también una adecuada concienciación a los proveedores y prestadores de servicios, y a través de las siguientes medidas:

- Establecer una política de utilización segura del correo electrónico (documentos adjuntos dudosos, hipervínculos o enlaces extraños).
- Al disponer nuestros proveedores de datos sensibles de la empresa, se debería establecer clausulas en los contratos y controles necesarios para garantizar que los datos se encuentren protegidos y pedir responsabilidades en caso de incidente. En particular esta acción se debería realizar siempre con los siguientes tipos de proveedores:

    - Proveedores de servicios tecnológicos (aquellos que ofrecen servicios como alojamiento web, emisión de certificados, pasarelas de pago, almacenamiento en la nube, soporte informático).

- Proveedores de servicios no tecnológicos, pero con acceso a datos corporativos (proveedores de servicios financieros, viajes, publicidad y marketing).
- Proveedores de productos tecnológicos, es decir, de los que adquirimos los equipos ofimáticos, los componentes y las aplicaciones informáticas (software).

En efecto, si vamos a trabajar con proveedores de servicios externos, será necesario que nuestra información disponga de los mecanismos de protección y seguridad suficientes, tanto en su acceso, como en su uso.

FACTORES ORGANIZATIVOS:

- No se debe descuidar nunca la gestión de redes y sistemas. Muchas empresas descuidan el mantenimiento de la seguridad de sus servidores y redes, dispositivos de red vulnerables o servidores sin actualizar desde hace años. Estas brechas de seguridad la utilizaran los hackers para llevar a cabo sus ciberataques.
- Antivirus/cortafuegos (firewall): Son la base de la protección de todos los sistemas de información. Limitan el acceso a redes internas a usuarios no autorizados. Deben actualizarse de forma periódica.
- Realizar copias de seguridad diarias o periódicas. Evitar a su vez localizar las copias de seguridad en el mismo sitio donde se almacenan los sistemas y datos a proteger.
- Actualización de aplicaciones: Cuanto más actualizadas se encuentren las aplicaciones de todos los equipos ofimáticos de la empresa y de sus trabajadores, mayor seguridad ante un posible ataque cibernético.
- Cifrar siempre información almacenada que contengan datos sensibles. El cifrado ayuda a guardar la información en caso de que los dispositivos se pierdan o sean robados, o si la información termina en manos ajenas no deseadas.
- Control de acceso a la información. Será de gran importancia contar con una política de seguridad en la que se defina y clasifique la información, dejando claro quién y en qué condiciones accederá a qué tipo de información. Este control tendrá como objetivo impedir fugas de información y que personal no autorizado acceda a información confidencial.
- Elaborar un listado con todos los equipos fijos y móviles existentes en la empresa, e indicando que equipo móvil se ha llevado cada empleado para un control total.
- Notificar siempre cualquier incidente de carácter malicioso tanto a las Fuerzas de Seguridad, en el caso español a la Policía, como a INCIBE (instituto Nacional de Ciberseguridad). Ellos sabrán cómo ayudar a la empresa.
- Transferir el riesgo siempre que sea posible a las aseguradoras a través de mediadores de seguros especializados en ciberriesgos: Cada empresa requiere sus propios niveles de seguridad adaptados a sus procesos, sistemas y modelo de negocio. Por ello, se recomienda el asesoramiento profesional externo para la identificación y obtención de las medidas de seguridad que necesita la organización (en algunos casos dependerá de las capacidades económicas o de personal).

Además de estas medidas, sería muy aconsejable tener en la empresa un encargado de la Seguridad de la Información (CISO). Un experto en seguridad CISO se responsabiliza de la protección de datos de la compañía y tiene responsabilidad centralizada sobre la gestión de los mismos. Debe dirigir y coordinar la respuesta de la empresa frente a un ciberataque, desde la Dirección Ejecutiva, a la Asesoría Legal, Gestoría de Riesgos, Relaciones Públicas, y/o departamento de Marketing. La seguridad de la red y de los datos es un riesgo que tiene que involucrar a toda la empresa y no sólo al departamento de Informática. Esta persona debería formar parte del IRP (Plan de Respuesta a Incidentes).

El Plan de Respuesta a Incidentes debe ser una estrategia con directrices claras, transparentes y documentadas que funcionen para administrar el riesgo de un incidente cibernético. Una organización que tiene un plan IRP bien confeccionado e implementado será capaz de tomar medidas rápidas y concretas cuando se requiera para aminorar posibles intrusiones y minimizar el daño financiero que pueda ocasionar a la empresa. Además, y a efectos legales, tendrá una mayor probabilidad de poder responder con exactitud y celeridad a lo que se le exige.

Ahora, y de acuerdo al Reglamento General de Protección de datos (RGPD), cualquier organización que sufra un incidente de seguridad debe notificarlo a la autoridad competente y a los afectados en un máximo de 72 horas, si los datos afectados entrañan un riesgo para su privacidad.

Todas estas medidas podrían venir recogidas en el Plan de Contingencia y de Continuidad de Negocio de la empresa, el cual nos ayudará a saber cómo actuar correctamente cuando sufrimos un ataque. Desde analizar, tratar y solucionar un incidente, a evitar una posible interrupción de negocio de la empresa.

2.3. Panorama actual del seguro de ciberriesgos

No fue hasta principios de la década anterior cuando se empezaron a ofertar los ciberseguros en Estados Unidos, y principalmente como a consecuencia de una nueva ley sobre notificación de la vulneración de las medidas de seguridad, pues obligaba a notificar brechas de seguridad cuando hay datos de carácter personal comprometidos. Desde entonces y hasta ahora el seguro de ciberriesgos se ha ido asentando en dicho país siendo además uno de los ramos del mercado asegurador con más perspectiva de crecimiento.

En Europa, y más particularmente en España, ha tardado más en comercializarse. Este proceso se ha conseguido gracias al conocimiento aportado por mediadores especializados y compañías aseguradoras de ámbito internacional (Estados Unidos y Reino Unido preferentemente), los cuales han sabido adaptarse a las especificaciones y particularidades de cada mercado local donde se iba introduciendo este seguro. Hoy en día mediadores y aseguradoras de ámbito nacional, como Seguros Catalana Occidente o Mapfre, ya comercializan

también los ciberseguros en España, siendo un producto más de su línea de negocio.

Tal y como indica el último informe de la compañía Lloyd's[31], aunque la contratación de seguro es significativamente mayor en las economías desarrolladas que en regiones emergentes, el nivel de ciberseguro en Europa es inferior al de Estados Unidos. En 2016, la tasa de adopción de ciberseguro se situó en un 30% en Alemania y en un 36% en el Reino Unido frente al 55% registrado en Estados Unidos. Estos datos ponen de manifiesto la sensibilización actual de los empresarios americanos frente a los riesgos cibernéticos, comparado con las empresas europeas. También hay que tener en cuenta que en Estados Unidos las empresas llevan ya muchos años sujetas a una mayor regulación, ya que es el país que recibe más ataques de esta índole.

Mientras, en España las empresas que constituyen el Ibex 35 ya están empezando a contratar estos seguros. Según apuntaba el Diario 5 días en una noticia de marzo de 2019[32] cierta parte del selectivo ya se estaba blindando frente a las ciberamenazas a través de la contratación de productos de seguro específicos. Así, Telefónica había contratado seguros de ciberriesgos por 405 millones de euros. Iberdrola desvelaba que cuenta con protección aseguradora específica para este tipo de amenazas desde 2017 y además dando cobertura al grupo en los distintos países donde opera. El programa se contrata en capas con grupos aseguradores internacionales de primer nivel y cuenta con la participación de Iberdrola Re, reaseguradora del grupo. La compañía admitía que en 2018 detectaron y lograron bloquear cientos de eventos e intentos de ataque, aunque asegura que no registró ningún incidente significativo que resultase en una pérdida financiera o reputacional. En su informe anual sí cuantifica que ha tenido 364 reclamaciones "fundamentadas" por violación de la privacidad o fuga de datos de clientes (la mayoría en Reino Unido y algunas pocas en España). CaixaBank, Indra, Repsol, Santander, Amadeus y Bankia también tienen contratados seguros de ciberriesgo, y Ferrovial asegura que lo "está valorando".

Hasta ahora se pensaba que el seguro de ciberriesgos se había centrado únicamente en aquellas empresas que en un principio podían encontrarse más expuestas a los riesgos cibernéticos y las cuales necesitaban mayores niveles de protección, es decir, grandes compañías multinacionales. Sin embargo, cada vez hay más aseguradoras que centran su mirada en el sector de la pequeña y mediana empresa, y para ello están intentando adaptar su oferta a su realidad y sus necesidades. El problema que sigue habiendo hoy en día con las pymes es la falta de concienciación existente por parte de los empresarios respecto al nivel de exposición e impacto económico y reputacional asociado con una amenaza cibernética. Algunas razones que suelen dar los empresarios para no contratar este seguro son:

[31] Informe 'Un mundo en riesgo. Informe global de infraseguro'. Lloyd's. 2018
[32] Jimenez, M. (9 de marzo de 2019).'Así se protegen las empresas del Ibex 35 ante los ciberataques'. Cinco Dias.

- *Me encuentro protegido frente a las ciberamenazas con mi sistema de protección anti virus*. Cuando en realidad esta medida es totalmente insuficiente para hacer frente a todas las posibles amenazas.

- *Tengo un especialista informático en la empresa*. La existencia de un especialista si no dispone de recursos tecnológicos necesarios no permitirá resolver el problema.

- *El precio del seguro de ciberriesgos es caro*. No es cierto, ya que la póliza se adecua en función de los parámetros del solicitante y las coberturas que solicita contratar.

- *El coste de sufrir un ciberataque no es muy alto*. Está equivocado, pues en función de la magnitud y tipología del ciberataque puede llegar a suponer para la empresa cuantiosas pérdidas económicas, o una posible interrupción de negocio, o incluso una pérdida reputacional.

- *Desconocimiento de las nuevas leyes de notificación en caso de recibir una violación de datos o una brecha de seguridad.* No exime al empresario de sus obligaciones legales. Esa falta de conocimiento le puede acarrear pérdidas económicas inesperadas como a consecuencia de recibir una reclamación por parte de terceros.

- *Mi actual seguro de Daños y/o Responsabilidad Civil seguro que ya me da cobertura para esta tipología de riesgos*. Los seguros de Daños y/o Responsabilidad Civil no contemplan actualmente el riesgo cibernético entre sus coberturas, por lo que este seguro se debe contratar en una póliza aparte.

En conclusión, aunque la demanda del seguro de ciberriesgos a día de hoy aún no es muy significativa, desde mi punto de vista se va a producir un cambio radical en su contratación en los próximos años, y por dos motivos fundamentalmente. El primero y más importante a raíz de la introducción de la nueva ley RGPD y sus requisitos de obligado cumplimiento respecto a la notificación de brechas de seguridad. En segundo lugar, según vayan apareciendo nuevos ciberataques y de gran envergadura, fomentará que los empresarios sean más susceptibles de contratar la póliza.

2.4. Legislación aplicable al seguro en La Unión Europea y España

Respecto a los ciberriesgos el proyecto legislativo de mayor trascendencia ha sido el del Consejo de Europa, el cual nombró en 1997 un Comité de Expertos del ciberespacio, integrado por policías, juristas e informáticos, y al que se invitó a participar a países no europeos, pero con un peso importante en la sociedad de la tecnología de la información global (Estados Unidos, Canadá, Japón y Australia), para debatir los problemas relativos al ciberespacio. Tras cerca de cuatro años y más de veinte borradores se logró crear un convenio sobre ciberdelincuencia, aprobado y abierto a la firma por el Plenario del Con-

sejo de Ministros en Budapest, el 23 de noviembre de 2001. Este hecho fue el inicio de un nuevo marco legislativo común para todos los Estados miembros de la Unión Europea. El convenio define los delitos informáticos agrupándolos en cuatro grupos:

- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.
- Delitos relacionados con la informática. Se definen la falsificación y el fraude informático.
- Delitos por su contenido. Comprende las conductas englobadas en los delitos relacionados con la tenencia y distribución de contenidos de pornografía infantil en la red.
- Delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines.

El fin último de este convenio es la persecución de un delito global, que no entiende de fronteras terrestres ni virtuales. Según se define en el BOE[33] el presente Convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable.

No obstante, la ciberseguridad en España tal como indica el Ministerio de Defensa Español en su cuaderno de Estrategia sobre ciberseguridad[34], y a diferencia de otros países de nuestro entorno, no ha sido definida todavía en una legislación específica y completa en materia de ciberseguridad, aunque si existe legislación distribuida en distintos ámbitos ministeriales pero no se ha desarrollado todavía una política común que refleje el ámbito nacional y estratégico de la ciberseguridad. Únicamente en el ámbito de las Administraciones Públicas se ha trabajado en este aspecto, y con el objetivo de asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias. Dicha competencia se recoge en el Real Decreto 3/2010 del BOE[35].

Por otro lado, deberemos conocer cuáles son las responsabilidades en materia de cumplimiento legal por parte de las empresas que operan en el ámbito de la Unión Europea. Es decir, todas las empresas deben cumplir con la legislación del país en la que esté fiscalmente establecida o bien la de aquel en el que ofrezca sus productos o servicios. Hay que tener en cuenta que hoy en día par-

[33] Ley BOE: Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.
[34] Ministerio de Defensa: Cuadernos de estrategia. Número 149. Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio.
[35] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

te de las ventas ya no se realizan únicamente en un lugar físico, sino que también se pueden realizar a través del mundo virtual de internet, como el correo electrónico, tiendas online, aplicaciones móviles o redes sociales, y desde hace algún tiempo wereables (o tecnología vestible).

A su vez, el 25 de mayo de 2018 entró en vigor el nuevo Reglamento Europeo en materia de Protección de Datos Personales (R.G.P.D. por sus siglas en ingles). Este hecho ha producido un cambio en el ámbito de los ciberriesgos en Europa y su tratamiento. Esta regulación aplica por igual a todos los países y compañías miembros de la Unión Europea, y/o cualquier empresa dentro o fuera del ámbito europeo que procese datos de ciudadanos de la Unión Europea. Esto quiere decir, que el reglamento es aplicable a aquellos responsables que no están en la Unión Europea, pero que ofrecen productos o servicios dentro de ella. Todas las organizaciones que traten datos de carácter personal deben conocer la normativa existente en materia de protección de datos y adoptar las medidas necesarias para garantizar su cumplimiento.

Se ha producido pues una homogeneización de la regulación legal de Protección de Datos llevada a cabo por parte de la Unión Europea a través del mencionado Reglamento, de cumplimiento obligatorio para los Estados miembros a partir del 25 de mayo de 2018.

Los principios sobre los que se rige esta nueva ley son:

- *Principio de licitud, lealtad y transparencia.* Los datos personales no pueden ser recogidos de forma fraudulenta, desleal o ilícita. Además, el responsable debe facilitar al interesado toda la información sobre el tratamiento de forma concisa, transparente, inteligible y de fácil acceso.

- *Principio de limitación de la finalidad.* Los fines para los que se recogen los datos personales deben ser determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines.

- *Principio de minimización de datos.* Los datos deben ser adecuados, pertinentes y limitados a los fines para los que se recogen.

- *Principio de exactitud de datos.* Los datos han de ser exactos, correctos y completos, suprimiéndose o rectificándose, sin dilación, los que no estén actualizados o sean inexactos.

- *Principio de limitación del plazo de conservación de los datos*, debiendo mantenerse de forma que se permita la identificación del interesado durante no más tiempo del necesario.

- *Principio de integridad y confidencialidad*, es decir, los tratamientos han de garantizar una seguridad adecuada de los datos.

El consentimiento del titular de los datos personales es uno de los instrumentos que legitiman el tratamiento de datos personales. Cabe destacar que el mismo:

- Deberá otorgarse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal.

- La solicitud de consentimiento deberá presentarse diferenciada de los demás asuntos, de forma inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo.

- El interesado tendrá derecho a retirar su consentimiento en cualquier momento, debiendo ser tan fácil retirar el consentimiento como fue darlo.

El consentimiento tácito no es válido, de modo que el silencio del interesado no constituye consentimiento.

Por otro lado, las obligaciones más relevantes que se fijan en el reglamento son las son las que se mencionan en los artículos 33 y 34.

- El *artículo 33* de dicho reglamento establece la obligación de notificar una violación de la seguridad de los datos personales a la autoridad de control por parte del responsable de los datos, sin dilación, y a más tardar 72 horas después de haber tenido conocimiento de la violación de seguridad de los datos personales.

- El *artículo 34* establece la obligación de comunicar una violación de la seguridad de los datos personales al interesado siempre que entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Dicho reglamento establece un nuevo régimen sancionador por incumplimiento de las obligaciones y principios establecidos en el mismo. Las multas económicas se incrementan respecto de los rangos establecidos hasta la fecha en nuestra normativa nacional recogida en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, pudiendo alcanzar:

- Hasta 10.000.000 € o el 2% del volumen de negocio total anual global del ejercicio anterior, pudiendo elegir la autoridad competente la imposición de la cifra más elevada, y como a consecuencia de infracciones relativas a:

  - Incumplimiento de las obligaciones del responsable y encargado.
  - Obligaciones de los organismos de certificación.
  - Obligaciones de la autoridad de control.

Un ejemplo sería una falta de notificación.

- Hasta 20.000.000 € o el 4% del de negocio total anual global del ejercicio anterior, pudiendo elegir la autoridad competente la imposición de la cifra más elevada, y como a consecuencia de infracciones relativas a:

  - Principios básicos del tratamiento.
  - Derechos de los interesados.

- Transferencias de datos personales.
- Incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por la autoridad de control.
- Incumplimiento de las resoluciones de la autoridad de control.

Un ejemplo sería una transferencia de datos a terceros países.

No obstante, existen ciertas excepciones a la obligación de comunicar/notificar:

- Cuando se han adoptado y aplicado medidas técnicas y organizativas apropiadas.
- Cuando se han adoptado medidas que garanticen que no existe posibilidad de que se vulneren derechos y libertades.
- Cuando la necesidad de comunicar supone un esfuerzo desproporcionado (comunicación pública).
- Relativo al plazo máximo de 72 horas. Si las empresas no pudieran aportar toda la información en el plazo de 72 horas, se podrá hacer de forma gradual en distintas fases. En este sentido, la primera notificación se realizará siempre en las primeras 72 horas.

En mi opinión esta ley ha entrado en vigor tarde, hubiera sido necesario tener una ley específica en materia de ciberriesgos mucho antes, pero es cierto que las medidas que en ella se recogen han sido acertadas y adecuadas si con ello se consigue elevar el nivel de concienciación en ciberseguridad de las empresas que operen no solo en España, sino también en la Unión Europea. Es muy importante que con el desarrollo de las nuevas tecnologías y la continua innovación que se da en los mercados, los usuarios nos encontremos lo más protegidos posibles respecto a la seguridad de nuestros datos personales y nuestra privacidad. Además, si la comparamos con el impacto que tuvo en su día en Estados Unidos la Ley SB1386, podríamos llegar a pensar que su existencia dará lugar a una mayor demanda del seguro de ciberriesgos por parte de las empresas de la Unión Europea.

Otras leyes que aplican y pueden afectar a empresas y autónomos desde el punto de vista de la seguridad informática y las cuales podrían ser recogidas en el contrato del seguro son:

- *LSSI-CE (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico).* Regula aspectos jurídicos de las actividades económicas o lucrativas derivadas del comercio electrónico, es decir, de aquellos servicios relacionados con internet y el comercio o la contratación electrónica, información y publicidad y servicios de intermediación.

  Si además desde páginas y aplicaciones webs se hace uso de las «cookies»[36] habrá que informar al usuario para que dé su consentimiento y permita la instalación en su equipo. Las cookies permiten a los prestadores de servicios almacenar información en el dispositivo del cliente o del usuario.

[36] (cookies) Archivos que contienen información sobre los usuarios.

- *LPI (Ley de Propiedad Intelectual)* que regula los derechos relativos a las creaciones de tipo artístico, científico, literarias, o creaciones en formato digital, tales como imágenes, vídeos, contenido multimedia, etc. Protege los derechos de los autores, tanto derechos morales como patrimoniales. Por lo tanto, las empresas y autónomos no podrán utilizar obras protegidas sin pagar derechos de autor, y deberán proteger los derechos de las creaciones propias o de los empleados, respetando siempre el derecho del creador de reconocerse como autor de la obra.

Por último, y respecto a las pólizas de ciberriesgos, la normativa actual a efectos de legislación aplicable se basa en las siguientes leyes:

- *Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).* Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas. Es decir, el fin es la protección de la privacidad de las personas y sus datos personales.

  La mayoría de empresas y autónomos utilizan datos personales, ya sean de clientes, proveedores o empleados. Esto implica que deberán cumplir con esta legislación.

- *Real Decreto 1720/2007*, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal.

- *Reglamento UE 2016/679 del Parlamento Europeo y del Consejo,* relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

2.5. Agentes que participan en el seguro de ciberriesgos

Actualmente los agentes que participan en el mercado de los ciberseguros son el propio asegurado, mediadores, aseguradoras, reaseguradoras y empresas tecnológicas de servicios especializados.

Figura 3. Cadena de valor del seguro de ciberriesgos

Fuente: Elaboración propia

2.5.1. Asegurados

Cualquier persona física (autónomos) y/o jurídica (empresas) que busca una solución aseguradora frente a las ciberamenazas con el objetivo de evitar en la medida de lo posible un impacto económico y/o reputacional en su negocio.

El perfil actual del asegurado es muy amplio, desde pequeñas y medianas empresas hasta empresas de mayor tamaño que trabajan con gran cantidad datos propios y de terceros.

Se está produciendo un cambio de paradigma, a través de una equiparación en términos de sensibilización por parte del asegurado respecto a los riesgos tradicionales de los seguros de empresas, tales como sufrir un incendio, daños relacionados con el agua, o daños como a consecuencia de riesgos de la naturaleza.

En el presente, cualquier tipo de organización se puede encontrar amenazada frente a los riesgos y amenazas tanto del ciberespacio como de dentro de su propia empresa y como consecuencia de sus propios empleados. Por lo tanto, las empresas a través de una adecuada gerencia de riesgos tendrán que decidir cuál quieren evitar, transferir al mercado asegurador o incluso aceptar.

2.5.2. Mediadores

Los mediadores de este tipo de seguros suelen ser tanto brokers como agentes tradicionales. No obstante, las grandes corredurías de ámbito internacional como a consecuencia de su amplia experiencia aportan un valor añadido respecto al resto de sus competidores, como corredurías de seguro de menor tamaño y los agentes tradicionales de las compañías aseguradoras.

Son los grandes corredores internacionales los que tienen un conocimiento profundo de este negocio, ya que la mayoría de estas corredurías se encuentran en el mercado norteamericano, el cual como se ha comentado con anterioridad, fue el pionero en buscar soluciones aseguradoras para los seguros de ciberriesgos. Ofrecen una gestión eficiente y soluciones de transferencia del riesgo que permitirá evaluar, gestionar y responder de forma efectiva a las ciberamenazas a las que pudiera enfrentarse la empresa, desarrollando una estrategia transversal y que engloba todos los servicios de la empresa. Desde operaciones, a cumplimiento legal y normativo, finanzas y comunicaciones.

Además, el hecho de que estos grandes corredores se encuentren establecidos en toda la geografía mundial permite que el asegurado encuentre soluciones globales para la diseminación de riesgos que tengan, es decir, los diferentes países donde pudieran encontrarse también establecidas sus filiales. Así como un amplio conocimiento respecto a la legislación local de cada país donde se quiera suscribir el riesgo, ya que cada país tiene su propia legislación, y suelen encontrarse diferencias significativas entre ellos, como por ejemplo la obligatoriedad o no de notificar una brecha de seguridad a un tercero.

Estos mediadores suelen disponer de equipos de especialistas que asesoran, coordinan y gestionan la respuesta en caso de sufrir una vulneración de datos, fallo de seguridad o amenaza de extorsión. Además, suelen contar con herramientas web propias para la formación de los empleados de las empresas aseguradas en materias de ciberseguridad y medidas de protección básicas.

2.5.3. Aseguradoras

Frente a estas nuevas amenazas las aseguradoras han encontrado un nuevo nicho de mercado en el mundo de los seguros generales (o seguros de no vida). Es un mercado relativamente nuevo en el que hay que estar muy especializado y tener un equipo de especialistas que sepan bien cuáles son las necesidades reales que pueden tener sus asegurados; ya que el primero que desconoce los riesgos potenciales a los que se enfrenta es el propio asegurado. Por ello, deben ser las aseguradoras y sus especialistas los que ayuden a realizar una correcta gestión de riesgos. Más complicado aún se prevé determinar una prima acorde al seguro contratado y un tratamiento adecuado del siniestro.

2.5.4. Empresas de servicios tecnológicas especializadas

En el seguro de ciberriesgos es especialmente relevante y aconsejable que la compañía aseguradora cuente con un proveedor tecnológico especializado que preste una respuesta inmediata al asegurado en caso de que se produzca un ciberataque. Pero también para que de forma preventiva realice sobre los asegurados un análisis de riesgos relativos a su ciberseguridad y su seguridad informática. Por lo tanto, ejercen una doble función, servicio previo a sufrir una ciberamenaza y servicio de gestión de incidentes una vez la empresa sufre un ataque de esta índole.

Los servicios preventivos que ofrecen estas empresas son los siguientes:

- Análisis de vulnerabilidades internas (vulnerabilidades IP y de redes).
- Análisis de vulnerabilidades de páginas web.
- Corrección de vulnerabilidades a través de asistencia remota.
- Aplicación antisecuestro.
- Evaluación del cumplimiento de la LOPD.
- Asistencia a la adecuación a la LOPD.
- Vigilancia digital y reputacional online.

El conjunto de servicios preventivos ofrece a las empresas aseguradas, de una manera indirecta, información de carácter vital para el conocimiento del estado de su infraestructura informática y legal, así como a elementos de protección que intentaran evitar la parada o interrupción del negocio.

Una vez el asegurado contrata la póliza el proveedor tecnológico ya procede a prestarle los siguientes servicios:

- Asistencia informática online 24 horas/365 días al año.
- Descontaminación de antivirus.

- Verificación y configuración del wifi, firewall, antivirus, antispyware y malware.
- Soporte sobre cuentas de correo electrónico, en aplicaciones informáticas y navegadores de internet.
- Copias de seguridad.
- Recuperación de datos de discos duros o sistemas de almacenamiento.

Por lo tanto, el asegurado no solo está contratando una póliza de seguros, sino que también está protegiendo la seguridad informática y cibernética de su empresa, un activo de importantísimo valor.

Más tarde, si finalmente el asegurado notifica un siniestro, y siempre que ocurra en el periodo de vigencia del contrato, los servicios que pueden llegar a prestar estas empresas de servicios son:

- Peritación del siniestro: identificación del tipo de incidente o evento de seguridad con la emisión del correspondiente informe del incidente.
- Limpieza del software infectado.
- Revisión y restablecimiento de los sistemas de comunicación.
- Revisión de las políticas de contraseñas.
- Comprobación de las políticas de las copias de seguridad.
- Restablecimiento de los sistemas infectados o perjudicados, así como revisión del resto de sistemas.
- Recuperación de datos.
- Rescate de datos en el caso de robo de información.
- Certificaciones electrónicas forenses, así como informes técnicos forenses.
- Respecto a la posible pérdida de riesgo reputacional del asegurado se realizará un borrado específico de apariciones no deseadas.

Los servicios necesarios para la gestión de siniestros se deben basar en las coberturas contratadas en la póliza, ofreciendo soluciones específicas tanto a los asegurados, como a las compañías aseguradoras, y garantizando la correcta peritación del daño y la asistencia al asegurado.

2.5.5. Reaseguradoras

Las reaseguradoras, como se verá reflejado en el último capítulo de esta tesis, son totalmente necesarias, brindando una ayuda esencial a las aseguradoras tanto en la elaboración del contrato del seguro de ciberriesgos, como en la suscripción, tarificación y posterior tratamiento de los siniestros. Además, y relativo a la suscripción, resultará que no todos los riesgos son a priori suscribibles y solo se podrán asegurar a través del reaseguro.

3. Guía metodológica de contratación del seguro y posterior tratamiento del siniestro

El propósito de este capítulo es redactar, desde el punto de vista de una compañía aseguradora, una breve guía metodológica sobre el contrato de ciberseguros, la suscripción del seguro de ciberriesgos, y posteriormente el tratamiento y resolución de siniestros.

En la actualidad, los riesgos y amenazas cibernéticas no están cubiertos en los seguros tradicionales de las pólizas de daños o de responsabilidad civil, puesto que estos riesgos están tipificados como una exclusión en ambos contratos, teniendo que contratar una póliza de ciberriesgos específica a parte.

Generalmente una póliza de ciberriesgos es un contrato que vincula y obliga legalmente a una compañía aseguradora ante la ocurrencia de determinados cibereventos, los cuales están definidos en el contrato, y que pueden acarrear unas pérdidas económicas y/o reputacionales al asegurado, pagándole una cantidad económica especifica como a consecuencia de una reclamación. En contraprestación, el tomador del seguro paga una prima (o precio del seguro) a la compañía aseguradora. El contrato es firmado por ambas partes e incluye aspectos como tipos de coberturas y límites contratados, franquicias, exclusiones, definiciones y, en los casos que proceda, la evaluación en términos de seguridad informática del asegurado.

El valor de la prima a pagar es dependiente del valor y suma de los activos, del tipo de negocio, tamaño de la compañía, nivel de exposición digital, volumen de datos digitales que almacena y nivel de seguridad de la empresa a asegurar. A su vez, la posible siniestralidad acumulada que se dé a lo largo de los años readecuará el valor de la prima futura. Pero es cierto que debido a la escasa información siniestral que existe hoy en día sobre esta tipología de siniestros se determina difícil fijar una valoración exacta de la prima.

A continuación, se describirán aquellos aspectos relativos al contrato de seguros que considero más importantes cuando se formaliza una póliza de ciberseguros entre una compañía de seguros y el solicitante del seguro en cuestión.

3.1. Suscripción de la póliza de ciberriesgos

3.1.1 Perfil del solicitante del seguro

El mercado de ciberseguros en España está dirigido principalmente a personas físicas (autónomos), pequeñas y medianas empresas. Algunas aseguradoras de ámbito internacional también se focalizan en grandes compañías.

El objeto de este estudio está dirigido principalmente al mercado de las pequeñas y medianas empresas, tanto las que se encuentren en territorio nacional,

como aquellas empresas que a su vez disponen de filiales en el extranjero, intentando ofrecer una solución global a sus necesidades.

3.1.2 Actividad del asegurado

Conocer la actividad que realiza el solicitante del seguro es fundamental. La compañía aseguradora debe saber en qué tipo de sector se encuentra la empresa en cuestión, cuales son los procesos que realiza, que tipo y cantidad de datos propios y de terceros maneja. Es decir, analizar en qué nivel de exposición se encuentra frente al mundo digital y los riesgos que implica.

De hecho, las aseguradoras valoran su apetito del riesgo no solo en función de la actividad del solicitante, sino que también tienen en cuenta los siguientes parámetros de la empresa:

- Número de empleados.
- Volumen de facturación.
- Productos y venta online y que porcentaje supone sobre el total de la facturación.
- Si gestiona datos sensibles de tarjetas de pago.
- Si tiene filiales en el extranjero, y en caso afirmativo cuanto factura cada una.
- Si tiene o no activos y cuanto factura en determinados países como pueden ser Estados Unidos y Canadá.
- Si procesa y almacena datos personales de ciudadanos de determinados países como Estados Unidos y Canadá.
- Si gestiona algún dato sensible de salud personal o propiedad intelectual.
- Qué volumen de registros gestiona y controla.
- Afirma disponer de contraseñas en sus sistemas, de software antivirus, antispyware o protección contra el malware, original y debidamente actualizado en todos los equipos y servidores.
- Afirma disponer de sistemas de firewall para los servidores accesibles desde internet o para los equipos que accedan a internet.
- Afirma disponer de un sistema de copia de seguridad o “Backup” para la recuperación de la información diaria.
- Afirma no haber tenido ningún incidente de seguridad en los últimos meses relacionados con los siguientes casos:

    - Violación o brecha de seguridad de sus sistemas informáticos.
    - Daños a la red de la empresa.
    - Pérdida o robo de datos de la empresa.
    - Posible sanción por parte de la Agencia Española de Protección de Datos.

En función del cumplimiento de estos criterios y de la actividad del asegurado la compañía aseguradora determinará si la suscripción puede ser automática o condicionada. Será de suscripción automática en el caso de que el solicitante del seguro cumpla con los criterios de suscripción arriba solicitados y además

su negocio se encuentre entre las tipologías de riesgo que tiene tipificadas la compañía aseguradora como automáticas.

Tipos de riesgos que podríamos considerar de suscripción automática:

- Pequeños comercios cotidianos, en los que no se trabaja con gran cantidad de datos.
- Supermercados e hipermercados de cadenas nacionales, sin ámbito global.
- Negocios relacionados con la pequeña hostelería como pueden ser hoteles locales, que no pertenecen a grandes cadenas multinacionales.
- Negocios relacionados con el ocio: cines, discotecas, teatros, etc.
- Pequeñas agencias de viaje, autoescuelas, academias de estudios, de baile, etc.
- Algunos despachos de profesionales, como por ejemplo los arquitectos.
- Industrias sin tratamiento de datos de carácter sensible.

Sin embargo, existen otros tipos de riesgos que podríamos considerar de suscripción condicionada:

- Empresas que impliquen infraestructuras críticas, como pueden ser centrales eléctricas, energía solar o eólica, depuradoras de agua, etc.
- Centros gubernamentales como consulados, embajadas, ayuntamientos.
- Centros hospitalarios, por la gran cantidad y sensibilidad de datos médicos y personales de terceros que tienen en su poder.
- Estudios de televisión, cine y radio. Por la sensibilidad de los datos con los que trabajan.
- Todo tipo de agencias de prensa, marketing o inmobiliarias con tratamientos de datos sensibles o en gran cantidad.
- Despachos de abogados, corredores, asesores y auditores.
- Entidades bancarias y de seguros.

La suscripción del riesgo pasará a ser condicionada en el caso de que el solicitante del seguro no cumpla con los criterios previos de contratación o la actividad sea considerada condicionada. Siendo así necesario cumplimentar un cuestionario adicional por parte de la empresa. Dicho cuestionario valorará cuestiones relacionadas con la información personal y de seguridad informática de la compañía:

- *Información de la compañía / del solicitante*. Dirección web, sector de la industria en el que se encuentra, posibles filiales, datos relativos al comercio electrónico que desarrolla la empresa, etc.

- *Tipo y cantidad de datos sensibles que maneja y/o procesa la compañía*. Cabría distinguir entre información de identificación personal, información relativa a tarjetas de pago (PCI), información de salud personal, propiedad intelectual, etc.

- *Servicios prestados por terceros respecto a la seguridad informática de la empresa*. Quién gestiona sus sistemas informáticos, sus redes, o fun-

ciones relacionadas con la seguridad informática como copias de seguridad y almacenamiento externo, procesamiento de datos o almacenamiento de datos en la nube. Además, si también trabajan con aplicaciones móviles sería conveniente saber quién es su proveedor de servicios por si el asegurado requiere solicitar a su vez cobertura para todos sus proveedores de externalización.

- *Seguridad informática de la empresa*. Sin duda alguna este es el punto del cuestionario de carácter más invasivo para las empresas, ya que están informando sobre su nivel de protección y seguridad informática, pero también exponen sus posibles vulnerabilidades.

- Se realizan preguntas sobre *medidas organizativas y técnicas de protección de la empresa*. Por un lado, cuestiones relativas al personal encargado de la seguridad informática, que medidas de concienciación realizan sobre la seguridad informática dentro de la empresa a sus empleados, así como que medidas antiphishing efectúan, o que políticas tienen de cambio y periodicidad de contraseñas personales. Por otro lado, preguntas relacionadas con las capacidades técnicas de la empresa frente a amenazas web y capacidad de reacción en caso de sufrir un ciberataque que genere una interrupción del negocio. Se le solicitará información acerca de las actualizaciones que realiza en materia de antivirus, anti malware y contra brechas de seguridad. Qué número y periodicidad de copias de seguridad realiza, etc.

- *Información relativa a los incidentes de seguridad informática y sus posibles pérdidas económicas*. Otro apartado delicado de cara a la información sensible que se solicita a las empresas. Ya que pueden llegar a pensar que si informan de un siniestro y sus consecuencias económicas la compañía aseguradora puede rechazar su solicitud de suscripción. No obstante, esto no es cierto y se requiere dicha información para poder ayudar a la empresa a ampliar y mejorar su seguridad informática. Labor que realiza conjuntamente la aseguradora con la empresa especializada de servicios tecnológicos.

- *Consentimiento a través de la firma*. Donde el firmante del cuestionario declara ser representante debidamente autorizado de la compañía, y en calidad de director, gerente o propietario.

El cuestionario no es una oferta vinculante ni otorga cobertura de seguro. Cumplimentarlo por parte del solicitante no obliga a la compañía de seguros a ofrecer una cobertura. Por lo que en mi opinión es entendible el posible rechazo y reticencia que puede generar a ciertas empresas ofrecer este tipo de información privada a las compañías de seguros si finalmente no se formaliza el seguro.

3.1.3 Solución aseguradora: Coberturas, límites y exclusiones de la póliza

Una vez realizada la suscripción automática o condicionada, le corresponderá ahora a la compañía aseguradora ofertar a su asegurado aquellas coberturas que mejor se ajusten a las necesidades de su negocio.

En este punto es muy importante el análisis de riesgos y el asesoramiento que puedan ofrecer los mediadores especializados, corredores de seguros y agentes exclusivos especialistas en ciberseguros que pueden contribuir a contratar las garantías adecuadas para proteger la empresa y, sobre todo, gestionar el siniestro y/o reclamación cuando esta suceda.

Respecto a aquellas empresas de carácter multinacional y con filiales en el extranjero que el asegurado quiera incluir, se requiere un esfuerzo conjunto por parte del mediador y la aseguradora para encontrar una solución global adecuada e integral que permita al asegurado tener cobertura localmente admitida y en armonía con las leyes locales, los requisitos reguladores, el idioma y garantías propias de cada país donde solicite asegurarse. También sería recomendable contar con la ayuda de expertos y gabinetes locales de cara a la tramitación de siniestros y gestión de demandas en cada país.

En una póliza de ciberseguros nos encontramos varios bloques de garantías donde podremos diferenciar entre garantías contratables obligatorias y opcionales. A su vez existen garantías que afectan a la propia empresa (1st party loss) como son los daños propios y la interrupción de negocio; y los daños que afecten a terceros (third party loss) – responsabilidad civil.

Dentro de los daños propios encontramos dos bloques de garantías, cobertura de datos e interrupción de negocio, los cuales se pasan a detallar a continuación.

1. Cobertura de Datos

Dependiendo de la compañía aseguradora puede ofrecerse de manera obligatoria u opcional. Comprende los siguientes supuestos:

1.1 *Alteración, pérdida o robo de datos*

Se garantizan los costes como consecuencia de pérdida o robo de datos o denegación de servicio en los sistemas informáticos del asegurado, y ocasionados directamente por un acto informático doloso[37], malware, o error humano[38] que se produzca en el propio sistema informático del asegurado.

[37] (Acto informático doloso) Todo acto indebido llevado a cabo con la intención de causar daño o conseguir acceso ilegitimo a datos, sistemas informáticos o redes informáticas mediante el uso de cualquier sistema informático o red informática.

[38] (Error humano) Entendido como tal, cualquier error de operación informática cometido por negligencia o involuntariedad, incluido un error en la elección del software a emplear, un error de configuración o cualquier otra operación indebida llevada a cabo por un empleado de la empresa.

Se indemnizarán a su vez los siguientes costes:

- Costes de restauración y recreación de los datos perdidos o robados. Tanto para recuperar, restaurar o recrear el software dañado como para adquirir licencias de sustitución de software. Así como para buscar o recopilar datos disponibles en copias informáticas de seguridad, comúnmente denominado “Backup”.

- Descontaminación de malware o código maligno informático. Con el objetivo de limpiar y restaurar datos, copias informáticas de seguridad y medios electrónicos debidamente afectados.

- Costes de investigación e indagación, para identificar el origen y las circunstancias del evento, y con el fin de limitar el impacto en costes y gastos que pueda originar.

- Costes de restauración del sistema de control de accesos y del perímetro de seguridad del sistema informático del asegurado. Y así evitar futuras brechas de seguridad.

Por otra parte, cabría atender a las exclusiones específicas para esta garantía, como por ejemplo las pérdidas como resultado de cualquier mejora, rediseño o reconfiguración de los sistemas informáticos del asegurado; o la exclusión de recuperación de datos que pudieran ser consecuencia de un daño físico del dispositivo de almacenamiento, un incendio, o la manipulación por personal no cualificado.

1.2 *Violación de la privacidad*

Se garantizan los costes como consecuencia de pérdida, robo o revelación a terceros no autorizados de datos de carácter personal confiados al cuidado, custodia y control del asegurado, ocasionados directamente por un acto doloso, malware o error humano que se produzca en el propio sistema informático del asegurado. Por esta cobertura se garantizan los siguientes costes, los cuales están siempre relacionados con la protección de datos de carácter personal:

- Costes de investigación e indagación para identificar el origen y las circunstancias del evento, y siempre que forme parte de un procedimiento regulatorio.

- Costes de notificación y comunicación.

- Costes de defensa legal[39].

[39] (Costes de defensa legal) Todos los costes, gastos y honorarios a pagar a expertos, abogados, profesionales, comparecencia ante tribunales, investigación, verificación y/o procedimientos necesarios para la defensa en los sectores civil, comercial, administrativo y/o criminal de la empresa.

- Multas administrativas por el incumplimiento de la legislación de protección de datos personales (LOPD).

- Costes de gestión de requisitos regulatorios.

1.3 *Seguridad de datos en la industria de tarjetas de pago (PCI)*

Al igual que en el punto anterior, se garantizan los costes como consecuencia de pérdida, robo o revelación a terceros no autorizados de datos de carácter personal confiados al cuidado, custodia y control del asegurado, ocasionados directamente por un acto informático doloso, malware o error humano que se produzca en el propio sistema informático del asegurado.

Se garantizan los siguientes costes:

- Costes de investigación e indagación para identificar el origen y las circunstancias del evento asegurado.

- Costes de los honorarios de expertos para la preparación de informes sobre el cumplimiento de PCI DSS, o lo que es lo mismo estándares de seguridad de datos aceptados y publicados por la industria de las tarjetas de pago.

- Costes adicionales para la expedición de cualquier tarjeta de crédito, débito o prepago, así como para la obtención de certificación de PCI DSS (control de calidad del manejo de datos de tarjetas de crédito o débito).

Dentro del apartado de exclusiones, las compañías aseguradoras no darán cobertura como a causa de cualquier pérdida, robo o revelación a terceros no autorizados de datos de carácter personal ocurridos cuando el asegurado no esté en posesión de una certificación válida PCI DSS expedida por un Asesor Cualificado de Seguridad.

1.4 *Extorsión cibernética*

Se asegura cualquier extorsión cibernética[40] que sufra el asegurado de carácter creíble, real, inminente y verificable. Dicha extorsión puede originar desde una denegación de servicios en los sistemas del asegurado, a una pérdida de datos confiados al cuidado, custodia y control del asegurado en sus sistemas informáticos, o un robo o la revelación de datos a un tercero no autorizado.

Se garantizan los costes y gastos razonables en relación a cualquier acción a tomar para proteger los sistemas informáticos del asegurado y aminorar las consecuencias de una amenaza de extorsión cibernética, realizada por cualquier persona o entidad ajena al asegurado que solicite una cantidad, rescate o acción como condición para no llevar a cabo dichas amenazas.

[40] (Extorsión cibernética) Cualquier uso ilegal e intencionado de una amenaza dirigida por un extorsionador contra los datos y/o los sistemas informáticos de la empresa afectada para obtener un rescate económico.

Entre las exclusiones más comunes se encuentran las extorsiones que pudieran venir de una entidad gubernamental o autoridad pública. Y cualquier hecho delictivo perpetrado por un directivo, accionista y/o empleado del asegurado.

Para esta cobertura las compañías de seguro suelen fijar un límite máximo de indemnización, y no se suele asegurar a valor total como en el resto de coberturas analizadas hasta el momento.

1.5 *Fraude cibernético*

Se asegura a través de esta garantía cualquier fraude informático, por robo de identidad o por ingeniería social que pudiera sufrir el asegurado.

- Fraude informático: Se le indemnizará al asegurado cualquier pérdida financiera resultante del robo de dinero como a consecuencia de una manipulación o un uso fraudulento o deshonesto del sistema informático del asegurado por parte de un tercero. O el robo de dinero del asegurado, o del cual es responsable, que hubiera sido ingresado en una cuenta corriente de una entidad financiera y que hubiera sido transferido de dicha cuenta siguiendo instrucciones supuestamente dadas por el asegurado, pero que en realidad hubieran sido fraudulentamente transmitidas o emitidas por un tercero.

- Fraude por robo de identidad: Se entiende como tal la acción por la que una parte distinta del asegurado pudiera llegar a un acuerdo con terceros y haciéndose pasar por el asegurado.

- Fraude por ingeniería social: Es decir, cualquier transferencia de dinero realizada de buena fe por un asegurado siguiendo instrucciones fraudulentas presuntamente dadas por un cliente o un proveedor, o por supuestos directivos de la propia empresa (Fraude del CEO) pero que en realidad hubieran sido emitidas por un impostor sin el conocimiento o el consentimiento del asegurado, el cliente o el proveedor.

Para esta cobertura, al igual que en el punto anterior, las compañías de seguro suelen fijar un límite máximo de indemnización, y no se suele asegurar a valor total.

1.6 *Riesgo reputacional*

Se aseguran principalmente los costes asociados a la publicación de cualquier información negativa en los medios de comunicación, y que con ello se pudiera ver perjudicada la imagen y/o reputación del asegurado. Siempre que el origen de tal evento sea una pérdida de datos de los sistemas informáticos del asegurado y como consecuencia de un acto informático doloso, malware o error humano; o por el robo de datos y denegación de servicios de los sistemas informáticos del asegurado.

En caso de siniestro las empresas de servicios tecnológicos tendrán que trabajar conjuntamente con la aseguradora para intentar minimizar todos los costes razonables de la gestión de la crisis en los medios de comunicación a través de campañas publicitarias y el borrado de apariciones no deseadas.

2. Interrupción del negocio

Se trata de una garantía también contratable de forma opcional. Se indemnizará al asegurado por las posibles pérdidas económicas que sufra como a consecuencia de una paralización o interrupción total o parcial de los sistemas informáticos. Dicha pérdida tendrá que dar lugar a una reducción del volumen de negocio o un aumento del coste de explotación en la empresa por los gastos adicionales soportados. En este caso se asegura la pérdida de beneficios y/o posibles costes extraordinarios que tenga que soportar el asegurado durante el periodo de restablecimiento de su actividad.

Es común que se sub límite esta garantía mediante la aplicación de un límite máximo de indemnización. Aunque también se podrá negociar para que se ofrezca a valor total.

Últimamente el mercado asegurador también está ofreciendo la garantía adicional de pérdida de beneficios derivada de proveedores externos de servicios. Ya que el origen de muchos de los ataques que sufren las empresas provienen de sus proveedores externos y no de la propia empresa asegurada. Para contratar esta garantía se pregunta previamente en el cuestionario de suscripción si la empresa dispone de proveedores externos de servicios, por si solicita asegurarlos. El asegurador indemnizará por lo tanto la pérdida de beneficios y los posibles costes extraordinarios que tuviera que soportar el asegurado durante el período de interrupción y que fuera ocasionada por una interrupción del servicio, siempre que dicha interrupción sea consecuencia directa y exclusiva de un incidente de privacidad y/o incidente de seguridad ocurrido en el sistema informático del proveedor de servicios, y que conllevan la pérdida de datos protegidos o que impidan acceder a los datos o servicios que presta.

Además de las garantías de daños propios anteriormente descritas, las compañías de seguro ofrecen la cobertura de responsabilidad civil por reclamaciones y/o perjuicios ocasionados a terceros.

3. Responsabilidad Civil

Es la única garantía contratable de forma obligatoria en el seguro de ciberriesgos. Se asegura la responsabilidad civil del asegurado frente a terceros y como consecuencia de los siguientes supuestos:

3.1 *Responsabilidad Civil contra la violación de la confidencialidad y de la privacidad*

Se aseguran los perjuicios ocasionados a terceros, de los que esté obligado legalmente a responder el asegurado, como consecuencia directa de reclamaciones derivadas de la pérdida, robo o la revelación a terceros no autorizados de información confidencial y/o privada confiada al cuidado, custodia y control del asegurado en sus propios sistemas informáticos y causada por un acto informático doloso, malware o error humano.

Se indemnizará el abono a los perjudicados de las indemnizaciones a que diera lugar la responsabilidad civil del asegurado, los gastos de defensa y pago de las costas y gastos judiciales o extrajudiciales inherentes al siniestro, así como la constitución de las fianzas judiciales exigidas al asegurado para garantizar su responsabilidad civil.

Como se ha ido cavilando a lo largo de este estudio, debido a que los costes de notificar y comunicar una brecha de seguridad a terceros pueden llegar a ser muy costosos para la empresa, se hace indispensable que el asegurado tenga esta cobertura contratada en la póliza. Resultará esencial para mitigar un impacto económico en su balance.

3.2 *Responsabilidad Civil por la seguridad de la red*

Se aseguran los perjuicios ocasionados a terceros, de los que esté obligado legalmente a responder el asegurado, como consecuencia directa de reclamaciones derivadas de la pérdida y/o robo de datos en un sistema informático de terceros, o la denegación de servicios al sistema informático de terceros; siempre que sea causada por un acto informático doloso, o un malware que se produzca en el propio sistema informático del asegurado debido al fallo o violación del entorno de seguridad de sus sistemas informáticos.

Al igual que en el punto anterior, se indemnizará el abono a los perjudicados de las indemnizaciones a que diera lugar la responsabilidad civil del asegurado, los gastos de defensa y pago de las costas y gastos judiciales o extrajudiciales inherentes al siniestro, así como la constitución de las fianzas judiciales exigidas al asegurado para garantizar su responsabilidad civil.

En esta garantía se tendrá que valorar la exclusión relacionada con cualquier reclamación presentada por un proveedor de servicios de IT prestados al asegurado, ya que podría contratarse opcionalmente.

3.3 *Responsabilidad frente a organismos reguladores*

Se aseguran las sanciones administrativas impuestas por un organismo regulador al asegurado por el incumplimiento involuntario de la normativa vigente en materia de protección de datos de carácter personal (LOPD) con motivo de una investigación y siempre que dichas multas y sanciones administrativas sean legalmente asegurables, y que dicha investigación resulte de un incidente.

En el conjunto de garantías de responsabilidad civil anteriormente descritas la póliza indemnizará:

- El abono a los perjudicados de las indemnizaciones por responsabilidad civil del asegurado.
- Los gastos de defensa y pago de los costes y gastos judiciales.
- Las fianzas judiciales exigidas al asegurado para garantizar su responsabilidad.

4. Servicios adicionales

La mayoría de compañías aseguradoras, a través de sus proveedores tecnológicos de servicios, están ofreciendo actualmente a sus asegurados una serie de servicios preventivos sobre la seguridad de sus sistemas que les ayuda a mejorar su capacidad de protección frente a posibles vulnerabilidades. Los servicios más comunes son:

- Análisis de vulnerabilidades internas, tanto en los sistemas operativos como en las aplicaciones que utilice el asegurado. El servicio permite la revisión del sistema informático del asegurado, así como la detección y eliminación de malware, archivos temporales, cookies y servicios que ralenticen o pongan en peligro los datos o el funcionamiento de los ordenadores propiedad del asegurado y cubiertos en póliza. Además, de forma remota se realizará un análisis de las vulnerabilidades de los dispositivos conectados a internet. También se analizan todas las posibles vulnerabilidades que haya en el sistema informático del asegurado, como pueden ser licencias caducadas, actualizaciones del sistema, puertos abiertos, etc.

- Análisis de vulnerabilidades de páginas web del asegurado en busca de fallos que pueda comprometer la seguridad del asegurado.

- Corrección de vulnerabilidades en remoto: Asistencia tecnológica en la que el asegurado recibirá atención directa de técnicos especializados para asistirle con las configuraciones de las vulnerabilidades detectadas. Dentro de este apartado podemos encontrar:

    - Actualización del equipo informático (siempre que se disponga de licencia).
    - Verificación de las conexiones.
    - Restablecimiento de los sistemas informáticos del asegurado.
    - Verificación y configuración de antivirus, firewall, antispyware y malware del sistema.
    - Configuración de contraseñas del asegurado.
    - Configuración segura de la red wifi del asegurado.
    - Geolocalización de smartphones, tablets y portátiles.
    - Copia de seguridad en la nube.
    - Limpieza de virus y spyware.

- Aplicación anti secuestro de la información: El asegurado se podrá instalar una aplicación en sus sistemas para evitar el secuestro de los ordenadores y de la información de la que dispone, para evitar y prevenir el

ransomware o el malware que infecte los sistemas del asegurado y que encripte y secuestre los principales archivos de información.

- Vigilancia digital y reputación online. Se realiza un exhaustivo análisis de búsqueda en internet para conseguir conocer las apariciones que haya de la empresa y su marca en internet. A partir de allí se le generara al cliente un informe con los resultados y apariciones obtenidas.

- Evaluación del cumplimiento de la LOPD. El asegurado, a través de una herramienta digital que le facilite la empresa de servicios, podrá comprobar el grado de cumplimiento que realiza con respecto a la legislación de la LOPD. Esta herramienta le ofrecerá las funcionalidades necesarias para la correcta adaptación de la empresa a la legislación, ofreciéndole:

    - Asistente de medidas técnicas y organizativas.
    - Gestor automático de documentación técnico-legal (documentos de seguridad, contratos).
    - Servicios de actualización y mantenimiento de la LOPD.
    - Gestor de incidencias.
    - Generación de documentación para cumplir con la ley (documento de seguridad, contratos con terceros, trabajadores, clausulas).

Por lo tanto, y a modo de conclusión, se puede afirmar que una vez la aseguradora realice un estudio exhaustivo respecto a las necesidades reales del solicitante del seguro, tendrá que ofertar las garantías que considere más oportunas y fijar los límites que se quieran contratar. Podrán ser tanto a valor total como a primer riesgo. E incluso es habitual en este seguro ver límites de indemnización conjuntos para diversas garantías con el ánimo de minimizar el impacto del siniestro, ya que un solo siniestro podría afectar a varios bloques de garantías. Es importante analizar estas limitaciones para que mantengan cierta coherencia respecto al límite general de indemnización contratado en la póliza.

A su vez, las aseguradoras suelen establecer una franquicia general y/o franquicias específicas para ciertas garantías con el objetivo de reducir costes de gestión y así rebajar sus costes operativos; y por otro lado como medida para ahorrarse siniestros de poca cuantía, lo que genera a su vez que el propio asegurado no efectué la reclamación inicial.

Tanto los límites como las franquicias contratadas, implican para la aseguradora el deber de fijar un precio adecuado respecto a la prima a pagar por parte del asegurado.

3.1.4 Otros aspectos relativos al contrato de seguros

En un seguro de ciberriesgos además de las coberturas, límites y franquicias a contratar, encontramos ciertos aspectos en las condiciones generales que definen el alcance y objeto del contrato.

3.1.4.1. Objeto del seguro

En este punto se indica que el asegurador indemnizará al asegurado conforme a los términos, condiciones, límites, franquicias y exclusiones contenidas en las condiciones particulares y generales de la póliza. Delimita a su vez el lugar donde se pueden formular reclamaciones contra el asegurado. En el caso que nos concierne España y ante tribunales españoles y, por hechos ocurridos en territorio de la Unión Europea (salvo que se pacte lo contrario).

3.1.4.2. Definiciones relativas a terminología del contrato de seguros

Definiciones relacionadas con la terminología que aparece en el contrato de seguros, y que hace referencia tanto a términos relacionados con la propia póliza (tomador, asegurador, prima, franquicia, etc.) como a eventos relacionados con el seguro (virus informáticos, malware, terrorismo cibernético, extorsión cibernética, etc.)

3.1.4.3. Ámbito territorial

Es muy importante determinar el ámbito territorial en función de donde se encuentre la empresa y las filiales que se quieran asegurar. Lo más común es que las coberturas del contrato apliquen a incidentes ocurridos y reclamaciones recibidas en todo el mundo, excepto en los Estados Unidos y Canadá, por su exigente y diferente regulación. Pero para aquellos asegurados de ámbito internacional, con presencia también tanto en Estados Unidos como en Canadá, se podría negociar con la aseguradora para ampliar el ámbito territorial a mundial.

3.1.4.4. Jurisdicción

El contrato de seguro debe quedar sometido a la legislación de cada país donde se suscribe el riesgo.

3.1.4.5. Exclusiones generales

Punto muy importante dentro de las condiciones generales de la póliza y donde se indican los eventos que quedan expresamente excluidos. Encontramos exclusiones análogas a cualquier otra póliza de seguros generales (seguros de no vida), pero también específicas para esta tipología de riesgos. Las exclusiones más comunes son:

- Incendio, daños causados por el agua, eventos de la naturaleza como el impacto de rayo, vendaval, tormenta de granizo, inundación, hielo, nieve, actividad volcánica, temblores de tierra, etc. Estos riesgos son propios de las pólizas de daños materiales.

- Cualquier responsabilidad contractual que exceda de la propia responsabilidad legal.

- Actos terroristas. Guerra civil o internacional, invasión, actos de enemigo extranjero, conflictos armados nacionales o internacionales, haya o no mediado declaración oficial. Así como cualquier huelga legal o ilegal o conflicto laboral de cualquier clase, revuelta o disturbio civil.

- Reacción o radiación nuclear y/o contaminación radiactiva. Armas químicas, biológicas, bioquímicas o electromagnéticas.

- Dolo o culpa grave del asegurado.

- Penalizaciones, multas o sanciones de carácter civil o penal como aquellas no asegurables por ley, a excepción de las sanciones impuestas por la Agencia Española de Protección de Datos.

- Cumplimiento de cualquier ley gubernamental, ordenanza, regulación o reglamento que regule o restrinja el uso del sistema informático del asegurado o del proveedor externo contratado por el propio asegurado, encargado de realizar el mantenimiento o la gestión del sistema informático.

- Uso de software ilegal o sin licencia. Condición totalmente necesaria para la contratación de la póliza por parte del asegurado disponer de un software de protección legal y con la licencia activa. Sino seguramente la compañía aseguradora rechazará su solicitud.

- Error de programación. Entendido como el error ocurrido durante el desarrollo de un software o de un sistema operativo que podría, una vez esté operando, dar lugar a un mal funcionamiento del sistema.

- Desgaste, disminución del rendimiento u obsolescencia de equipos electrónicos utilizados por el asegurado resultante de la operación normal o del deterioro progresivo que por lo habitual deberían estar cubiertas por un contrato de mantenimiento completo.

- Robo, violación o infracción de cualquier propiedad intelectual. Así como el espionaje.

- Rescate o suma económica de extorsión exigida. En España es ilegal pagar por un rescate como consecuencia de una extorsión.

- Fallo o interrupción ocasionada en el acceso a la infraestructura de un tercero o a la del proveedor del servicio, incluidas telecomunicaciones, servicios de internet, satélite, cable, electricidad, gas, agua u otros proveedores públicos.

3.1.4.6. Modificaciones del riesgo

El tomador del seguro o el asegurado deberán, durante el curso del contrato, comunicar a la compañía aseguradora, y tan pronto como le sea posible, todas las circunstancias que pudieran agravar el riesgo.

En el caso de que el tomador del seguro o el asegurado no haya efectuado su declaración y ocurriera un siniestro, el asegurador queda liberado de su prestación si el tomador o el asegurado han actuado con mala fe.

Dentro de este apartado, en pólizas de ámbito internacional, podemos encontrarnos con los siguientes puntos relativos a la adquisición o cese de filiales.

- *Adquisición o constitución de una sociedad filial*: Si durante el período de seguro el tomador del seguro adquiriera o constituyera una sociedad filial, la cobertura de esta póliza aplicará a dicha sociedad filial a partir de la fecha de la mencionada adquisición o constitución, y siempre que acepte y liquide cualquier prima adicional impuesta por el asegurador por dicha inclusión.

- Es importante recalcar que la cobertura para cualquier sociedad filial que se constituyera o fuera adquirida durante el período de seguro, se aplicará únicamente a incidentes que tengan lugar o reclamaciones que se reciban después de la adquisición o constitución de dicha sociedad filial por el tomador del seguro.

- *Cese de cualquier sociedad filial**:*** La cobertura no aplicará a ningún incidente ni ninguna reclamación relacionada con cualquier sociedad filial después de que dejase de ser una sociedad filial.

3.1.4.7. Obligaciones del asegurado

Al contratar la póliza el asegurado adquiere una serie de obligaciones con el asegurador. Las más significativas son:

- Debe adoptar todas las medidas razonables y necesarias para minimizar la pérdida o los daños.

- Debe actuar, contribuir y permitir que se haga todo aquello que pudiera parecer viable para averiguar la causa y el alcance de la pérdida.

- Debe preservar cualquier equipo físico (hardware), software y ponerlos a disposición del asegurador, para su inspección durante el tiempo que se considere necesario.

- Debe proporcionar cualquier información o prueba documental que el asegurador pudiera requerir junto con una declaración jurada sobre la veracidad de la reclamación en el caso de que sea necesario.

- Debe cooperar con el asegurador y sus expertos (ya sean internos o a través de empresas de servicios especializadas).

El incumplimiento de cualquiera de esas obligaciones permitirá al asegurador reducir la prestación haciendo partícipe al asegurado en el siniestro, en la me-

dida en que por su comportamiento haya agravado las consecuencias económicas del siniestro.

3.1.4.8 Duración del seguro

Hace referencia a la duración del contrato firmado entre ambas partes. Las garantías de la póliza entran en vigor en la hora y fecha indicada en las condiciones particulares y finalizarán en la hora y fecha que asimismo se hagan constar, pudiendo ser tácitamente (renovación automática del contrato) o explícitamente (renovación no automática y pendiente de revisión por el equipo de suscripción) prorrogadas.

Las partes podrán oponerse a la prórroga del contrato mediante una notificación escrita a la otra parte, efectuada con un plazo de al menos un mes de anticipación a la conclusión del periodo del seguro en curso cuando quien se oponga a la prorroga sea el tomador, y de dos meses cuando sea el asegurador.

3.1.4.9 Determinación y pago de la prima

En la póliza se tiene que indicar de una manera clara y concisa el importe de las primas devengadas por el seguro.

Respecto al pago el tomador del seguro está obligado al pago de la prima en el momento de la perfección del contrato. Pero si la prima no ha sido pagada antes de que se produzca el siniestro, el asegurador quedará liberado de su obligación de indemnizar.

A su vez, habrá que pactar con la compañía aseguradora si durante la vigencia del contrato y en caso de extinción del mismo se devolverá la parte de prima no consumida o no.

3.1.4.10 Nulidad y pérdida de derechos

Análogo a lo que se exige al resto de pólizas de seguros de no vida, el contrato de seguro será nulo, salvo en los casos previstos por la ley, si en el momento de su conclusión no existía el riesgo o había ocurrido el siniestro, o si no existe un interés del asegurado. Se pierde el derecho a la indemnización:

- En caso de reserva o inexactitud al cumplimentar el cuestionario, si medió dolo o culpa grave. Este hecho resalta la importancia en la correcta cumplimentación del cuestionario por parte del solicitante del seguro.

- En caso de agravación del riesgo, si el tomador del seguro o el asegurado no lo comunican al asegurador, y han actuado con mala fe.

- Si el siniestro sobreviene antes de que se haya pagado la prima.

- Si el tomador del seguro o el asegurado no facilitan al asegurador la información sobre las circunstancias y consecuencias del siniestro, y hubiera concurrido dolo o culpa grave.

- Si el asegurado o el tomador del seguro incumplen su deber de aminorar las consecuencias del siniestro, y lo hacen con manifiesta intención de perjudicar o engañar al asegurador.

- Cuando el siniestro haya sido causado por mala fe del tomador del seguro o del asegurado.

3.2. Notificación, tramitación y resolución de siniestros

Tan importante es la correcta suscripción del riesgo como su posterior tratamiento y resolución del siniestro. Se explicará a continuación los pasos que tiene que dar el asegurado cuando le sobreviene un siniestro, así como los servicios adicionales que prestan las compañías de servicios especializados una vez este se ha producido, y que son de gran ayuda para aminorar la valoración del siniestro tanto para el asegurado como para la aseguradora.

3.2.1. Notificación y gestión de reclamaciones

En caso de una reclamación recibida por parte del asegurado, el tomador del seguro o el asegurado deberán de inmediato y por escrito, notificar al asegurador y/o sus expertos, conforme la existencia de esta reclamación. En caso de que exista un retraso en la comunicación del incidente, el asegurador se puede reservar el derecho de reclamar al asegurado los daños y perjuicios derivados de dicho retraso. La reclamación debe ofrecer pruebas por escrito de cualquier pérdida o daño sufrido. Posteriormente, el gestor de incidentes solicitará al asegurado que dé una explicación con el máximo detalle posible sobre el origen y las consecuencias del evento.

Podríamos decir que, análogamente a lo que ocurre en el momento de contratación de la póliza, el asegurado adquiere también una serie de obligaciones con el asegurador durante la gestión del siniestro.

- Debe cooperar y permitir que se haga todo aquello que pudiera parecer viable para averiguar la causa y el alcance de la pérdida o daño.

- Debe de adoptar todas las medidas razonables y medios a su alcance para minimizar la pérdida o los daños.

- Debe preservar cualquier equipo físico (hardware), software y ponerlos a disposición del asegurador o de sus expertos, para su inspección durante el tiempo que se considere necesario.

- Debe proporcionar cualquier información o prueba documental que el asegurador y/o sus expertos pudieran requerir junto con una declaración jurada sobre la veracidad de la reclamación siempre que sea necesario.

- No podrá tomar ninguna decisión o realizar ninguna acción que perjudique la gestión del incidente o reclamación.

El incumplimiento de cualquiera de esas obligaciones autorizará al asegurador a reducir la prestación en la medida en que por la falta de colaboración del asegurado hayan perjudicado las posibilidades de defensa y/o haya podido agravar las consecuencias económicas del siniestro.

En el caso de que se presente una reclamación de terceros, el asegurado deberá:

- No admitir ninguna responsabilidad y no realizar ningún pago sin el consentimiento previo y por escrito del asegurador.

- Apoyar al asegurador en la investigación, defensa y/o liquidación frente a la reclamación recibida.

- Conceder al asegurador todos los derechos y autoridades necesarias de hacerse cargo de cualquier negociación de liquidación o de procedimientos judiciales con terceros.

3.2.2. Tramitación y resolución del siniestro

A la hora de tramitar siniestros las compañías aseguradoras suelen contar con expertos propios, o en su defecto colaboran con empresas de servicios tecnológicos especializados que les ayudan en el tratamiento y posterior resolución de los siniestros con dos objetivos principalmente. Primero, restaurar lo antes posible los sistemas informáticos del asegurado y así evitar un impacto económico significativo en su cuenta de resultados. Y segundo, colaborar en la gestión de reclamaciones de terceros.

Los servicios más habituales que ofrecen estas empresas de servicios una vez informado el siniestro son:

- Peritación efectiva del siniestro, identificando el tipo de incidente o evento de seguridad que se ha producido, recopilando y analizando la información solicitada al asegurado y emitiendo posteriormente el correspondiente informe de peritación para su valoración e indemnización.

- Puesta en marcha de los sistemas del asegurado. Limpieza del software infectado, revisión y restablecimiento de los sistemas de comunicación, revisión de las políticas de contraseñas, comprobación de las políticas de las copias de seguridad, etc.

- Recuperación de datos. En los casos donde el sistema de almacenamiento quede dañado se procederá a la recogida, proceso de recuperación y puesta en marcha del dispositivo.

- Rescate de datos en el caso de robo de información.

- Certificaciones electrónicas forenses. Informe técnico forense del evento o incidente.

Posteriormente, y en el supuesto de que el siniestro no estuviera cubierto por el seguro, el asegurador comunicará por escrito al asegurado las causas y/o razones para su rechazo.

En caso de rechazo, si el asegurado no está conforme, lo comunicará por escrito al asegurador y podrán ambas partes someter sus diferencias a arbitraje. Si la vía amistosa o extrajudicial no ofreciese resultado positivo aceptable por el asegurado, se procederá a la tramitación por vía judicial. En el supuesto de que exista disconformidad en la tramitación del siniestro, ambas partes podrán acogerse también a arbitraje.

3.2.3 Pago del siniestro

Se determina el plazo máximo de días en que el asegurador, dentro de los límites y condiciones pactadas en la suscripción de la póliza, abonará la indemnización que corresponda por el siniestro al asegurado.

4. El Reaseguro

El papel que juega el Reaseguro en el mercado asegurador, y en particular para esta tipología de ciberseguros, se precisa como fundamental. En este apartado se analiza la importancia que tiene la relación entre el reasegurador y la compañía aseguradora (cedente en términos de reaseguro) en tres diferentes momentos:

- Formalización del contrato de reaseguro entre la reaseguradora y la cedente.
- Ayuda en la suscripción a la aseguradora. Análisis y apetito del riesgo.
- Ayuda en la tramitación de siniestros a la compañía aseguradora.

4.1. Formalización del contrato de reaseguro para el ramo de ciberriesgos entre la reaseguradora y la cedente

Cabe resaltar el valor esencial que tiene el contrato de reaseguros, formalizado por la reaseguradora y la cedente, cuando se lanza un nuevo producto asegurador en el mercado. Y en este caso en particular respecto al seguro de ciberriesgos.

El reasegurador estará interesado en establecer la relación más favorable posible con la cedente, pues ambos tienen un interés asegurador común. Para ello le asesorará, a través de sus expertos, sobre diversos tipos de contratos de reaseguro teniendo en cuenta el equilibrio que debe haber entre la retención propia de la cedente y la cesión al reaseguro. La experiencia que ya posee la reaseguradora en otros países y/o con otras compañías de seguro jugará un papel fundamental a la hora de asesorar a la cedente sobre qué tipos de contratos de reaseguro le puede ofrecer y cual le es más favorable en base a sus necesidades.

Actualmente en el mercado asegurador nos encontramos con dos tipos de contratos de reaseguros muy diferenciados, contrato de reaseguro proporcional y no proporcional:

- *Proporcional:* en los reaseguros proporcionales el reasegurador asume una participación ecuánime de encaje de primas y siniestros con la cedente. Atenderá por lo tanto una proporción de todas las primas suscritas por la cedente, pero también tendrá que hacerse cargo en la misma proporción de todos los siniestros registrados por la cedente, independientemente de su cuantía. Esta opción es más cara para la cedente, ya que hace partícipe a su reaseguradora de una proporción de todos los siniestros informados, independientemente del importe de los mismos.

Entre los contratos más destacados para esta modalidad de seguro nos encontramos:

- *Cuota Parte.* Consiste en la cesión al reasegurador de un porcentaje fijo tanto de primas como de siniestralidad.

- *Contrato de Excedente.* Consiste en la cesión al reasegurador de un porcentaje de riesgos, pero solo de aquellos que excedan un determinado importe. Habrá que determinar que riesgos son los que va a retener la cedente, a los cuales llamamos plenos de retención, y cuales irán a cargo del reasegurador, los cuales llamamos excedentes. La idea es que la cedente tenga plenos de retención más altos cuanto menor sea el riesgo.

Los contratos proporcionales tienen la ventaja para la cedente de que le permite establecer un equilibrio adecuado en la cartera de riesgos que retiene por cuenta propia, ya que le admite fijar retenciones adecuadas en función de la peligrosidad de los riesgos que se quieran suscribir. La dificultad para la cedente es determinar el nivel de retención por cuenta propia.

- *No Proporcional:* en este tipo de contratos el reasegurador solamente soporta aquellos siniestros que sobrepasen la retención previa de la cedente, a la cual llamamos prioridad. El reasegurador en este caso no participa en los siniestros de poca cuantía, sino en los siniestros considerados graves o de cierta magnitud.

La dificultad en este tipo de contratos radica en la determinación de la prioridad por parte de la cedente, ya que si la prioridad es muy elevada puede desequilibrar su capacidad financiera propia asumiendo pérdidas muy importantes para la compañía. Pero por otro lado si determina una prioridad muy baja, al cederle la mayoría de siniestros a su reasegurador, éste le cobrará un precio elevado por ofrecerle dicha cobertura de reaseguro.

Esta opción es más económica para la cedente, ya que en caso de siniestro retiene una cantidad previa (prioridad), y puede que durante toda la vigencia del contrato no le traslade ningún siniestro a su reasegurador, por no pasar dicha prioridad. A su vez la cedente retiene una porción más elevada de todas las primas suscritas, ya que en este caso no las tiene que repartir con su reasegurador.

Entre las modalidades de contrato no proporcionales nos encontramos:

- *Exceso de pérdidas por riesgo (XL por riesgo)* Consiste en la cesión al reasegurador de los siniestros que sobrepase la prioridad que haya fijado previamente.

- *Exceso de siniestralidad (Stop loss)* Consiste en establecer por parte de la cedente el porcentaje máximo de siniestralidad global que estará dispuesta a soportar durante la vigencia del ejercicio. Este tipo de contratos se suele dar más para riesgos de carácter cíclico.

Por mi experiencia, para nuevas modalidades de seguro en fase de introducción en el mercado se suele recomendar la contratación de contratos proporcionales, donde la cedente y la reaseguradora participan tanto en las primas como en los siniestros. Suele ser normal que al principio la cedente retenga menor proporción de riesgos, cediéndole la mayoría de primas y siniestros a su reasegurador para que su capacidad financiera no se vea comprometida. Si después la siniestralidad es buena la cedente irá cediendo menor proporción del riesgo a su reaseguradora con el fin de pagar menos prima y costes de reaseguro al reasegurador.

Una vez satisfecha la vigencia del contrato, los actuarios de la compañía aseguradora apoyándose con el personal de suscripción y siniestros pueden realizar un estudio conjunto sobre cómo ha sido la evolución de la cartera y la siniestralidad soportada. En este punto se valorará si seguir con el contrato de reaseguros actual o por lo contrario se debe volver a negociar con la reaseguradora y cambiar de modalidad o incluso pasar de un contrato proporcional a no proporcional, o viceversa.

La compañía aseguradora, además de concretar qué tipo de contrato de reaseguro fijará con la reaseguradora (proporcional o no proporcional y su modalidad), tiene que tener en cuenta las siguientes especificaciones a la hora de gestionar y documentar las condiciones del contrato:

- *Objeto del contrato*. Recogen las condiciones generales y particulares pactadas entre el reasegurador y la cedente para el ramo de seguros que se esté negociando entre ambas partes.

- *Vigencia del contrato.* Se establece la duración del contrato de reaseguro entre el reasegurador y la cedente. Suele ser de duración anual.

- *Rescisión del contrato*. Se determina la posibilidad de rescindir el contrato ante determinados supuestos que pacten la reaseguradora y la cedente.

- *Confidencialidad de la información.* Ambas partes se deben de comprometer a considerar el acuerdo firmado como estrictamente confidenciales y a no hacer uso indebido respecto a terceros, ni durante su vigencia, ni pasada ésta.

- *Comienzo de la responsabilidad.* Se determinará cuando empieza la responsabilidad del reasegurador para con la cedente. Lo más común es que dicha responsabilidad comience simultáneamente entre el reasegurador y la cedente.

- *Política de suscripción y reparto del riesgo*. Se comentará en el siguiente punto.

- *Peritación e información de siniestros.* Se tratará en el último punto de este apartado.

- *Comunidad de suertes.* El reasegurador deberá seguir la suerte de la cedente en todo lo referente al aspecto técnico del seguro de los riesgos que la cedente haya asumido.

- *Errores y omisiones*. Cualquier error, omisión o defecto cometido en la administración y/o contabilidad efectuadas al reasegurador se acepta como cometido de buena fe y por lo tanto no eximirá al reasegurador de sus responsabilidades.

- *Contribución de gastos*. El reasegurador deberá bonificar a la cedente en cada uno de los negocios que le sean cedidos con las comisiones fijas y variables que se establezcan en el contrato.

- *Cambio de legislación.* La cobertura otorgada en el contrato se corresponderá con la legislación en vigor a la fecha de inicio del mismo. En caso de que existiera cualquier cambio de legislación que incrementará o extendiera la responsabilidad del reasegurador, ambas partes tendrán que acordar emprender de inmediato la revisión adecuada de los términos del contrato.

- *Cláusula de protección de datos*. Tanto el reasegurador como la cedente para los contratos formalizados en España se comprometen a cumplir la Ley Orgánica 15/ 1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- *Ley y jurisdicción.* Se determinará la ley y jurisdicción que rige el contrato ante cualquier disputa o desacuerdo entre el reasegurador y la cedente. En nuestro caso quedará sometido a las leyes y tribunales españoles.

4.2. Ayuda en la suscripción a la Aseguradora: Análisis y apetito del riesgo

La compañía de reaseguros guía y acompaña a la cedente en el análisis y apetito del riesgo a través de una adecuada selección de riesgos para que logre tener una cartera de riesgos equilibrada. Es decir, la reaseguradora ayuda a la cedente en su política de suscripción cuando ésta lanza un nuevo producto asegurador en el mercado y desconoce por insuficiencia de datos técnicos y actuariales que riesgos debe admitir y cuales rechazar, así como la tarifa que se debe de aplicar. En ambos casos y para este seguro de ciberriesgos se analizará el tipo de industria o negocio a asegurar, datos propios y de terceros que almacena y controla el solicitante del seguro, el ámbito geográfico donde se encuentre, y la intensidad y frecuencia de la siniestralidad existente.

Respecto a la tarifa a aplicar sigue siendo una realidad la falta de datos actuariales existentes, pues apenas hay datos de siniestralidad ya que muchas empresas prefieren no revelar que han sufrido un ataque. Por lo tanto, la ley de grandes números que aplica en gran cantidad de seguros no se puede aplicar a los seguros de ciberriesgos. Además, aquellos riesgos de ámbito internacional

con activos en varios países son mucho más complejos y caros de tarificar por las particularidades locales de cada país donde se quiere asegurar el riesgo.

Es interesante precisar que la compañía de reaseguros también participa conjuntamente con la cedente en la elaboración de manuales y cuestionarios para identificar aquellos riesgos que puedan ser de suscripción automática o condicionada. Y respecto a aquellos riesgos que sean considerados de suscripción excluida se estudiará caso a caso la posibilidad de asegurarlos individualmente mediante un reaseguro facultativo y con unas condiciones específicas que fijará la reaseguradora. Para ello es muy importante que la compañía de seguros facilite a la reaseguradora el cuestionario adicional con toda la información que se requiere debidamente cumplimentada por el solicitante del seguro de ciberriesgos.

Por último, y respecto a la política de suscripción y reparto del riesgo que aparece en el contrato de reaseguros, se detallará en una de sus cláusulas cual va a ser la aceptación, evaluación de los riesgos y negocios a asegurar. Quedando reservada exclusivamente a la compañía aseguradora, salvo que se indique lo contrario. No obstante, la aseguradora se tiene que comprometer a no introducir cambios significativos en su política de aceptación y de suscripción en cuanto a los negocios a los que se refiere el contrato, sin previa conformidad del reasegurador.

4.3. Ayuda en la tramitación de siniestros a la Aseguradora

Las reaseguradoras pueden llegar a ser de gran ayuda para las compañías de seguro a la hora de tramitar y gestionar determinados siniestros relacionados con los ciberriesgos, ya que poseen información siniestral precisa, veraz y completa respecto a muchas tipologías de sucesos. Tienen también la capacidad de recoger información de muchos y diferentes siniestros soportados por compañías aseguradoras en todo el mundo para después analizarla y tratar así de adaptar el nivel de primas, coberturas, franquicias y exclusiones que deben aparecer en la póliza.

Podríamos decir que las reaseguradoras ejercen de guía metodológica a las compañías de seguros para el correcto tratamiento y valoración de un siniestro, ya que estas últimas a veces no disponen de los recursos técnicos suficientes para gestionarlo correctamente.

A mi entender este seguro es aún nuevo en el mercado y sigue siendo muy complejo saber tramitar y posteriormente valorar, ya que continuamente se van introduciendo nuevas amenazas cibernéticas como malwares, spywares, troyanos, y virus que hacen cada vez más difícil para las compañías de seguro y reaseguradoras adaptar sus coberturas a las amenazas existentes. Da la sensación de que los hackers y la mafia que opera en internet siempre van un paso por delante de aseguradoras y reaseguradoras. Por lo que implicará un gran reto saber adaptarse a estas nuevas amenazas digitales.

Por otro lado, y respecto al contrato de reaseguro firmado entre la reaseguradora y la cedente existen varias cláusulas que hacen mención a la peritación, notificación y liquidación de siniestros. La cláusula más relevante es la que hace mención a la peritación de siniestros, la cual tiene que indicar cuál de las partes procederá a la peritación, arreglo y/o aceptación de los siniestros. Lo más habitual es que sea la cedente la que proceda a peritar los siniestros por sí sola, y la reaseguradora liquide la indemnización efectuada a la cedente. No obstante, las compañías de seguro suelen contar con la colaboración de empresas de servicios tecnológicos especializadas en la tramitación, ayuda y resolución de siniestros. Será importante negociar quien carga con los gastos especificados causados por el ajuste de los siniestros, como por ejemplo costas judiciales, gastos de peritaje, etc.

Respecto a la cláusula que hace referencia a la notificación de siniestros, la cedente debe indicar claramente la periodicidad con la que notificará a su reasegurador la relación de siniestros pagados y pendientes.

A modo de conclusión, considero importante recalcar que una de las ventajas más importante que satisface una compañía de seguros con su reaseguradora es la confianza que ésta le ofrece. Y con ello me refiero a la ayuda constante que la reaseguradora presta a la aseguradora. Desde la adecuación de la suscripción, al asesoramiento respecto a las garantías, límites, franquicias y exclusiones de la póliza que mejor se adaptan a su portfolio de riesgos y su estrategia. Así como la ayuda y el servicio prestado en la gestión y resolución de siniestros.

Por lo tanto, podemos afirmar que es muy importante para una compañía de seguros acompañarse de buenos reaseguradores, los cuales tengan amplia experiencia aseguradora en el mercado nacional e internacional y una solvencia elevada y demostrable.

5. Conclusiones

Internet junto a las nuevas tecnologías de la información y la comunicación han revolucionado la forma en que ahora hacemos las cosas. Gracias a ello las empresas se han visto enormemente beneficiadas, pero a su vez estas nuevas tecnologías han dado lugar a nuevas amenazas de ámbito cibernético que son complejas de gestionar y tratar en caso de que se produzca un ataque.

El objeto de estudio de esta tesis ha sido determinar el impacto que tienen los ciberriesgos sobre las empresas. Como hemos podido acreditar a través de sus diferentes capítulos, cualquier empresa, independientemente del sector en el que se encuentre y/o su tamaño, puede sufrir en cualquier momento un ataque cibernético que implique una pérdida o bloqueo de datos, una interrupción de negocio severa, pérdidas reputacionales y/o una reclamación por pérdida de información de terceros.

Las empresas para hacer frente a estas nuevas ciberamenazas tendrán que ser capaces de instaurar una nueva cultura de seguridad cibernética, es decir, tendrán que protegerse de forma preventiva implantando medidas concretas de carácter humano y organizativo dentro de la empresa. Es lo que se ha denominado resiliencia cibernética.

No obstante, las empresas actualmente pueden decidir trasferir parte de estos ciberriesgos a través del sector asegurador, pues ya existen soluciones aseguradoras suficientes y adecuadas a través del producto de ciberriesgos. Estos seguros, a diferencia de los seguros tradicionales de daños y responsabilidad civil, contemplan la mayoría de amenazas digitales que pueda sufrir la empresa, ya se trate de un ataque perpetrado desde fuera de la organización por ciberdelincuentes, o también como a consecuencia de actos malintencionados o por descuidos de sus propios empleados o colaboradores.

Será conveniente negociar este seguro con mediadores de seguros especializados y con amplia experiencia, pues se trata de un seguro complejo de entender y saber gestionar. A su vez sería adecuado a la hora de contratar el seguro que este tenga asociado una serie de servicios de carácter preventivo y de tratamiento del siniestro, los cuales suelen ser ofertados por empresas de servicios tecnológicos.

Por último, hay que recalcar la importancia que tiene el reaseguro en los ciberseguros y en particular la ayuda que brinda la reaseguradora a la compañía de seguros en la elaboración del seguro, la suscripción, y la posterior gestión y tratamiento del siniestro si fuera necesario.

En mi opinión, le auguro un gran futuro a esta nueva modalidad de seguros de ciberriesgos dentro del mercado asegurador. Aunque hoy en día sea complicada su comercialización por la falta de concienciación existente entre los empresarios en seguridad informática y cibernética, con la entrada en vigor del nuevo Reglamento Europeo en materia de Protección de Datos Personales

(R.G.P.D.) las empresas se van a ver obligadas a notificar a terceros una violación de seguridad de los datos personales. Este hecho va a obligar a que las empresas se preocupen de tener sus sistemas y equipos informáticos debidamente protegidos.

Por otro lado, ante la aparición de nuevas ciberamenazas, las compañías aseguradoras deberán ser ágiles y dinámicas en la adecuación del seguro, incorporando nuevas garantías que contrarresten los nuevos riesgos existentes, ajustando debidamente las franquicias y ofreciendo un nivel de prima adecuado. La madurez en la seguridad informática y cibernética de las empresas ayudará también a que cada vez sean menos los considerados como riesgos no asegurables. Igualmente, cuando el mercado asegurador privado considere algunos riesgos de no asegurables, el Estado debería asumirlos mediante programas de compensación, como hace en otras pólizas de daños materiales, mediante la Compensación del Consorcio de seguros.

Está por ver si en un futuro próximo la póliza de ciberriesgos se seguirá contratando a través de una póliza a parte como hasta ahora, o por lo contrario sus coberturas se pueden llegar a integrar en las pólizas de seguros de daños materiales y de responsabilidad civil.

Finalmente, habrá que observar con detenimiento como van evolucionando las nuevas tecnologías y en qué medida afectarán al seguro de ciberriesgos. En particular habrá que estar atentos a la interrupción de la nueva tecnología 5G, que según los expertos supondrá una nueva revolución digital. La facilidad con la que la tecnología 5G permitirá transmitir volúmenes masivos de datos a almacenamientos basados en la nube implicará muchas ventajas, pero también una nueva amenaza para empresas y aseguradoras.

Por ello la cooperación de todos los agentes que participan en el mundo de los seguros, tomadores (particulares y empresas), mediadores, empresas de servicios tecnológicos, aseguradoras y reaseguradoras, se precisa fundamental.

6. Bibliografía

Artículos:

Diario El País del 24 de abril de 2019, Facebook y Cambridge Analítica https://elpais.com/economia/2019/04/24/actualidad/1556115002_181533.html

Diario Canarias 7*:* https://www.canarias7.es/siete-islas/gran-canaria/las-palmas-de-gran-canaria/guaguas-municipales-fue-victima-de-la-estafa-del-ceo-CH7090958

Entrevista a actuario Fabián Romo Zamudio, director de Sistemas de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la Universidad Nacional Autónoma de México (UNAM) https://www.laverdad.com.mx/nacional/robo-de-identidad-es-un-ciberdelito-que-va-en-aumento-en-mexico

Noticia del diario El País del 24 de marzo de 2019 *https://elpais.com/politica/2019/03/09/actualidad/1552125807_187332.html?id_externo_promo=enviar_email*

Noticia del diario La Vanguardia del día 13 de junio de 2019 https://www.lavanguardia.com/seguros/20190613/462850840751/ciberataques-ciberdelincuentes-5g-tendencias-ccn-cni-criptojacking-iot.html

Diario Expansión del 27 de febrero de 2019 *"España es el primer país de la UE en desarrollar la Guía de Gestión de Ciberincidentes*" http://www.expansion.com/juridico/opinion/2019/02/27/5c76e366e2704e3e6f8b464c.html

Diario 5 días del 9 marzo de 2019 https://cincodias.elpais.com/cincodias/2019/03/07/companias/1551984662_949974.html

Informes:

Informe sobre amenazas a la seguridad de internet de Symantec (ISTR). 2018

Informe de Deloitte ¿Qué impacto ha tenido el ciberataque de WannaCry en nuestra economía? https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/impacto-economico-wannacry.html

El estudio "Ciberriesgos su impacto en las pymes" realizado por Unespa, Cepime y Cepreven. 2018

Fundación Mapfre: "Guía para proteger tu negocio frente a los ciberriesgos". 2017.

Informe IBM Security and Ponemon Institute: The 2018 Cost of a Data Breach Study: Global Overview

Informe Global de Riesgos 2018 del Foro Económico Mundial

Informe Accenture y Ponemon Institute: The 2017 CostCybercrime

Informe Ponemon e IBM Security: Cyber Resilient Organization. 2018

Ponemon Institute e IBM Resilient

Informe global de infraseguro de 2018 de Lloyd's "Un mundo en riesgo"

Net Diligence: The Cyber Claims Study 2017

Informe Ponemon insitutue: "The Third Annual Study on the Cyber Resilient Organization". 2018

THIBER: la transferencia del ciberriesgo en España

Foro económico mundial: Informe Global de Riesgos 2018 – Resumen Ejecutivo

Jesús Jimeno Muñoz "La responsabilidad civil en el ámbito de los ciberriesgos", editado por la Asociación Española de Gerencia de Riesgos y Seguros (AGERS) y la Fundación Mapfre.

Fuentes de internet:

Enciclopedia de Kaspersky: https://encyclopedia.kaspersky.es/knowledge/year-1988/

INCIBE https://www.incibe.es/

Blog online Kasperky, Ejemplo DDOS: https://www.kaspersky.es/blog/attack-on-dyn-explained/9420/

Fuentes Oficiales:

Cuerpo Nacional de Policía https://www.policia.es/

INCIBE. Glosarios términos de ciberseguridad. https://www.incibe.es/

Ley BOE: Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Ley BOE: Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica https://www.boe.es/eli/es/rd/2010/01/08/3

Ley: Ministerio de Defensa: Cuadernos de estrategia. Número 149. Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio.

Ley BOE: Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). https://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81371

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) https://www.boe.es/doue/2016/119/L00001-00088.pdf

Guillermo García Marcén

Nacido en Zaragoza, el 17 de noviembre de 1983.

A nivel académico, licenciado en Administración y Dirección de Empresas en la Universidad de Economía de Zaragoza, con doble especialidad en Dirección Comercial y Dirección General; realizando parte de los estudios en la prestigiosa Erasmus Universiteit Rotterdam.

A nivel profesional, desarrollando su carrera en la compañía aseguradora Seguros Catalana Occidente desde el año 2009, en el ámbito de Empresas, suscribiendo y gestionando programas internacionales de seguro a través de la red INI.

COLECCIÓN "CUADERNOS DE DIRECCIÓN ASEGURADORA"

Máster en Dirección de Entidades Aseguradoras y Financieras

Facultad de Economía y Empresa. Universidad de Barcelona

PUBLICACIONES

1.- Francisco Abián Rodríguez: "Modelo Global de un Servicio de Prestaciones Vida y su interrelación con Suscripción" 2005/2006

2.- Erika Johanna Aguilar Olaya: "Gobierno Corporativo en las Mutualidades de Seguros" 2005/2006

3.- Alex Aguyé Casademunt: "La Entidad Multicanal. Elementos clave para la implantación de la Estrategia Multicanal en una entidad aseguradora" 2009/2010

4.- José María Alonso-Rodríguez Piedra: "Creación de una plataforma de servicios de siniestros orientada al cliente" 2007/2008

5.- Jorge Alvez Jiménez: "innovación y excelencia en retención de clientes" 2009/2010

6.- Anna Aragonés Palom: "El Cuadro de Mando Integral en el Entorno de los seguros Multirriesgo" 2008/2009

7.- Maribel Avila Ostos: "La tele-suscripción de Riesgos en los Seguros de Vida" 2009/20010

8.- Mercé Bascompte Riquelme: "El Seguro de Hogar en España. Análisis y tendencias" 2005/2006

9.- Aurelio Beltrán Cortés: "Bancaseguros. Canal Estratégico de crecimiento del sector asegurador" 2010/2011

10.- Manuel Blanco Alpuente:"Delimitación temporal de cobertura en el seguro de responsabilidad civil. Las cláusulas claims made" 2008/2009

11.- Eduard Blanxart Raventós: "El Gobierno Corporativo y el Seguro D & O" 2004/2005

12.- Rubén Bouso López: "El Sector Industrial en España y su respuesta aseguradora: el Multirriesgo Industrial. Protección de la empresa frente a las grandes pérdidas patrimoniales"2006/2007

13.- Kevin van den Boom:"El Mercado Reasegurador (Cedentes, Brokers y Reaseguradores). Nuevas Tendencias y Retos Futuros" 2008/2009

14.- Laia Bruno Sazatornil: "L'ètica i la rentabilitat en les companyies asseguradores. Proposta de codi deontològic" 2004/2005

15.- María Dolores Caldés LLopis: "Centro Integral de Operaciones Vida" 2007/2008

16.- Adolfo Calvo Llorca: "Instrumentos legales para el recobro en el marco del seguro de crédito" 2010/2011

17.- Ferran Camprubí Baiges: "La gestión de las inversiones en las entidades aseguradoras. Selección de inversiones" 2010/2011

18.- Joan Antoni Carbonell Aregall: "La Gestió Internacional de Sinistres d'Automòbil amb Resultat de Danys Materials" 2003-2004

19.- Susana Carmona Llevadot: "Viabilidad de la creación de un sistema de Obra Social en una entidad aseguradora" 2007/2008

20.- Sergi Casas del Alcazar: "El PLan de Contingencias en la Empresa de Seguros" 2010/2011

21.- Francisco Javier Cortés Martínez: "Análisis Global del Seguro de Decesos" 2003-2004

22.- María Carmen Ceña Nogué:"El Seguro de Comunidades y su Gestión" 2009/2010

23.- Jordi Cots Paltor: "Control Interno. El auto-control en los Centros de Siniestros de Automóviles" 2007/2008

24.- Montserrat Cunillé Salgado: "Los riesgos operacionales en las Entidades Aseguradoras" 2003-2004

25.- Ricard Doménech Pagés: "La realidad 2.0. La percepción del cliente, más importante que nunca" 2010/2011

26.- Luis Domínguez Martínez: "Formas alternativas para la Cobertura de Riesgos" 2003-2004

27.- Marta Escudero Cutal: "Solvencia II. Aplicación práctica en una entidad de Vida" 2007/2008

28.- Salvador Esteve Casablancas: "La Dirección de Reaseguro. Manual de Reaseguro" 2005/2006

29.- Alvaro de Falguera Gaminde: “Plan Estratégico de una Correduría de Seguros Náuticos” 2004/2005

30.- Isabel Mª Fernández García: “Nuevos aires para las Rentas Vitalicias” 2006/2007

31.- Eduard Fillet Catarina: “Contratación y Gestión de un Programa Internacional de Seguros” 2009/2010

32.- Pablo Follana Murcia: “Métodos de Valoración de una Compañía de Seguros. Modelos Financieros de Proyección y Valoración consistentes” 2004/2005

33.- Juan Fuentes Jassé: “El fraude en el seguro del Automóvil” 2007/2008

34.- Xavier Gabarró Navarro: “"El Seguro de Protección Jurídica. Una oportunidad de Negocio"” 2009/2010

35.- Josep María Galcerá Gombau: “La Responsabilidad Civil del Automóvil y el Daño Corporal. La gestión de siniestros. Adaptación a los cambios legislativos y propuestas de futuro” 2003-2004

36.- Luisa García Martínez: “El Carácter tuitivo de la LCS y los sistemas de Defensa del Asegurado. Perspectiva de un Operador de Banca Seguros” 2006/2007

37.- Fernando García Giralt: “Control de Gestión en las Entidades Aseguradoras” 2006/2007

38.- Jordi García-Muret Ubis: “Dirección de la Sucursal. D. A. F. O.” 2006/2007

39.- David Giménez Rodríguez: “El seguro de Crédito: Evolución y sus Canales de Distribución” 2008/2009

40.- Juan Antonio González Arriete: “Línea de Descuento Asegurada” 2007/2008

41.- Miquel Gotés Grau: “Assegurances Agràries a BancaSeguros. Potencial i Sistema de Comercialització” 2010/2011

42.- Jesús Gracia León: “Los Centros de Siniestros de Seguros Generales. De Centros Operativos a Centros Resolutivos. De la optimización de recursos a la calidad de servicio” 2006/2007

43.- José Antonio Guerra Díez: “Creación de unas Tablas de Mortalidad Dinámicas” 2007/2008

44.- Santiago Guerrero Caballero: “La politización de las pensiones en España” 2010/2011

45.- Francisco J. Herencia Conde: “El Seguro de Dependencia. Estudio comparativo a nivel internacional y posibilidades de desarrollo en España” 2006/2007

46.- Francisco Javier Herrera Ruiz:“Selección de riesgos en el seguro de Salud” 2009/2010

47.- Alicia Hoya Hernández:“Impacto del cambio climático en el reaseguro” 2008/2009

48.- Jordi Jiménez Baena: “Creación de una Red de Agentes Exclusivos” 2007/2008

49.- Oriol Jorba Cartoixà:“La oportunidad aseguradora en el sector de las energías renovables” 2008/2009

50.- Anna Juncá Puig: “Una nueva metodología de fidelización en el sector asegurador” 2003/2004

51.- Ignacio Lacalle Goría: “El artículo 38 Ley Contrato de Seguro en la Gestión de Siniestros. El procedimiento de peritos” 2004/2005

52.- Mª Carmen Lara Ortíz: “Solvencia II. Riesgo de ALM en Vida” 2003/2004

53.- Haydée Noemí Lara Téllez: “El nuevo sistema de Pensiones en México” 2004/2005

54.- Marta Leiva Costa: “La reforma de pensiones públicas y el impacto que esta modificación supone en la previsión social” 2010/2011

55.- Victoria León Rodríguez: “Problemática del aseguramiento de los Jóvenes en la política comercial de las aseguradoras” 2010/2011

56.- Pilar Lindín Soriano: “Gestión eficiente de pólizas colectivas de vida” 2003/2004

57.- Victor Lombardero Guarner: “La Dirección Económico Financiera en el Sector Asegurador” 2010/2011

58.- Maite López Aladros: “Análisis de los Comercios en España. Composición, Evolución y Oportunidades de negocio para el mercado asegurador” 2008/2009

59.- Josep March Arranz: “Los Riesgos Personales de Autónomos y Trabajadores por cuenta propia. Una visión de la oferta aseguradora” 2005/2006

60.- Miquel Maresch Camprubí: “Necesidades de organización en las estructuras de distribución por mediadores” 2010/2011

61.- José Luis Marín de Alcaraz: “El seguro de impago de alquiler de viviendas” 2007/2008

62.- Miguel Ángel Martínez Boix: “Creatividad, innovación y tecnología en la empresa de seguros” 2005/2006

63.- Susana Martínez Corveira: “Propuesta de Reforma del Baremo de Autos” 2009/2010

64.- Inmaculada Martínez Lozano: “La Tributación en el mundo del seguro” 2008/2009

65.- Dolors Melero Montero: “Distribución en bancaseguros: Actuación en productos de empresas y gerencia de riesgos" 2008/2009

66.- Josep Mena Font: “La Internalización de la Empresa Española” 2009/2010

67.- Angela Milla Molina: “La Gestión de la Previsión Social Complementaria en las Compañías de Seguros. Hacia un nuevo modelo de Gestión” 2004/2005

68.- Montserrat Montull Rossón: “Control de entidades aseguradoras” 2004/2005

69.- Eugenio Morales González: “Oferta de licuación de patrimonio inmobiliario en España” 2007/2008

70.- Lluis Morales Navarro: “Plan de Marketing. División de Bancaseguros” 2003/2004

71.- Sonia Moya Fernández: “Creación de un seguro de vida. El éxito de su diseño” 2006/2007

72.- Rocio Moya Morón: “Creación y desarrollo de nuevos Modelos de Facturación Electrónica en el Seguro de Salud y ampliación de los modelos existentes” 2008/2009

73.- María Eugenia Muguerza Goya: “Bancaseguros. La comercialización de Productos de Seguros No Vida a través de redes bancarias” 2005/2006

74.- Ana Isabel Mullor Cabo: “Impacto del Envejecimiento en el Seguro” 2003/2004

75.- Estefanía Nicolás Ramos: “Programas Multinacionales de Seguros” 2003/2004

76.- Santiago de la Nogal Mesa: “Control interno en las Entidades Aseguradoras” 2005/2006

77.- Antonio Nolasco Gutiérrez: “Venta Cruzada. Mediación de Seguros de Riesgo en la Entidad Financiera” 2006/2007

78.- Francesc Ocaña Herrera: “Bonus-Malus en seguros de asistencia sanitaria” 2006/2007

79.- Antonio Olmos Francino: “El Cuadro de Mando Integral: Perspectiva Presente y Futura” 2004/2005

80.- Luis Palacios García: “El Contrato de Prestación de Servicios Logísticos y la Gerencia de Riesgos en Operadores Logísticos” 2004/2005

81.- Jaume Paris Martínez: “Segmento Discapacitados. Una oportunidad de Negocio” 2009/2010

82.- Martín Pascual San Martín: “El incremento de la Longevidad y sus efectos colaterales” 2004/2005

83.- Montserrat Pascual Villacampa: “Proceso de Tarificación en el Seguro del Automóvil. Una perspectiva técnica” 2005/2006

84.- Marco Antonio Payo Aguirre: “La Gerencia de Riesgos. Las Compañías Cautivas como alternativa y tendencia en el Risk Management” 2006/2007

85.- Patricia Pérez Julián: “Impacto de las nuevas tecnologías en el sector asegurador” 2008/2009

86.- María Felicidad Pérez Soro: “La atención telefónica como transmisora de imagen” 2009/2010

87.- Marco José Piccirillo: “Ley de Ordenación de la Edificación y Seguro. Garantía Decenal de Daños” 2006/2007

88.- Irene Plana Güell: “Sistemas d’Informació Geogràfica en el Sector Assegurador” 2010/2011

89.- Sonia Plaza López: “La Ley 15/1999 de Protección de Datos de carácter personal” 2003/2004

90.- Pere Pons Pena: “Identificación de Oportunidades comerciales en la Provincia de Tarragona” 2007/2008

91.- María Luisa Postigo Díaz: “La Responsabilidad Civil Empresarial por accidentes del trabajo. La Prevención de Riesgos Laborales, una asignatura pendiente” 2006/2007

92.- Jordi Pozo Tamarit: “Gerencia de Riesgos de Terminales Marítimas” 2003/2004

93.- Francesc Pujol Niñerola: “La Gerencia de Riesgos en los grupos multisectoriales” 2003-2004

94.- Mª del Carmen Puyol Rodríguez: “Recursos Humanos. Breve mirada en el sector de Seguros” 2003/2004

95.- Antonio Miguel Reina Vidal: “Sistema de Control Interno, Compañía de Vida. Bancaseguros” 2006/2007

96.- Marta Rodríguez Carreiras: “Internet en el Sector Asegurador” 2003/2004

97.- Juan Carlos Rodríguez García: “Seguro de Asistencia Sanitaria. Análisis del proceso de tramitación de Actos Médicos” 2004/2005

98.- Mónica Rodríguez Nogueiras: “La Cobertura de Riesgos Catastróficos en el Mundo y soluciones alternativas en el sector asegurador” 2005/2006

99.- Susana Roquet Palma: “Fusiones y Adquisiciones. La integración y su impacto cultural” 2008/2009

100.- Santiago Rovira Obradors: “El Servei d’Assegurances. Identificació de les variables clau” 2007/2008

101.- Carlos Ruano Espí: “Microseguro. Una oportunidad para todos” 2008/2009

102.- Mireia Rubio Cantisano: “El Comercio Electrónico en el sector asegurador” 2009/2010

103.- María Elena Ruíz Rodríguez: “Análisis del sistema español de Pensiones. Evolución hacia un modelo europeo de Pensiones único y viabilidad del mismo” 2005/2006

104.- Eduardo Ruiz-Cuevas García: “Fases y etapas en el desarrollo de un nuevo producto. El Taller de Productos” 2006/2007

105.- Pablo Martín Sáenz de la Pascua: “Solvencia II y Modelos de Solvencia en Latinoamérica. Sistemas de Seguros de Chile, México y Perú” 2005/2006

106.- Carlos Sala Farré: “Distribución de seguros. Pasado, presente y tendencias de futuro” 2008/2009

107.- Ana Isabel Salguero Matarín: “Quién es quién en el mundo del Plan de Pensiones de Empleo en España” 2006/2007

108.- Jorge Sánchez García: “El Riesgo Operacional en los Procesos de Fusión y Adquisición de Entidades Aseguradoras” 2006/2007

109.- María Angels Serral Floreta: “El lucro cesante derivado de los daños personales en un accidente de circulación” 2010/2011

110.- David Serrano Solano: “Metodología para planificar acciones comerciales mediante el análisis de su impacto en los resultados de una compañía aseguradora de No Vida” 2003/2004

111.- Jaume Siberta Durán: “Calidad. Obtención de la Normativa ISO 9000 en un centro de Atención Telefónica” 2003/2004

112.- María Jesús Suárez González: “Los Poolings Multinacionales” 2005/2006

113.- Miguel Torres Juan: “Los siniestros IBNR y el Seguro de Responsabilidad Civil” 2004/2005

114.- Carlos Travé Babiano: “Provisiones Técnicas en Solvencia II. Valoración de las provisiones de siniestros” 2010/2011

115.- Rosa Viciana García: “Banca-Seguros. Evolución, regulación y nuevos retos” 2007/2008

116.- Ramón Vidal Escobosa: “El baremo de Daños Personales en el Seguro de Automóviles” 2009/2010

117.- Tomás Wong-Kit Ching: “Análisis del Reaseguro como mitigador del capital de riesgo” 2008/2009

118.- Yibo Xiong: “Estudio del mercado chino de Seguros: La actualidad y la tendencia” 2005/2006

119.- Beatriz Bernal Callizo: “Póliza de Servicios Asistenciales” 2003/2004

120.- Marta Bové Badell: “Estudio comparativo de evaluación del Riesgo de Incendio en la Industria Química” 2003/2004

121.- Ernest Castellón Texidó: “La edificación. Fases del proceso, riesgos y seguros” 2004/2005

122.- Sandra Clusella Giménez: “Gestió d’Actius i Passius. Inmunització Financera” 2004/2005

123.- Miquel Crespí Argemí: “El Seguro de Todo Riesgo Construcción” 2005/2006

124.- Yolanda Dengra Martínez: “Modelos para la oferta de seguros de Hogar en una Caja de Ahorros” 2007/2008

125.- Marta Fernández Ayala: “El futuro del Seguro. Bancaseguros” 2003/2004

126.- Antonio Galí Isus: “Inclusión de las Energías Renovables en el sistema Eléctrico Español” 2009/2010

127.- Gloria Gorbea Bretones: “El control interno en una entidad aseguradora” 2006/2007

128.- Marta Jiménez Rubio: “El procedimiento de tramitación de siniestros de daños materiales de automóvil: análisis, ventajas y desventajas” 2008/2009

129.- Lorena Alejandra Libson: “Protección de las víctimas de los accidentes de circulación. Comparación entre el sistema español y el argentino” 2003/2004

130.- Mario Manzano Gómez: “La responsabilidad civil por productos defectuosos. Solución aseguradora” 2005/2006

131.- Àlvar Martín Botí: “El Ahorro Previsión en España y Europa. Retos y Oportunidades de Futuro” 2006/2007

132.- Sergio Martínez Olivé: “Construcción de un modelo de previsión de resultados en una Entidad Aseguradora de Seguros No Vida” 2003/2004

133.- Pilar Miracle Vázquez: “Alternativas de implementación de un Departamento de Gestión Global del Riesgo. Aplicado a empresas industriales de mediana dimensión” 2003/2004

134.- María José Morales Muñoz: “La Gestión de los Servicios de Asistencia en los Multirriesgo de Hogar” 2007/2008

135.- Juan Luis Moreno Pedroso: "El Seguro de Caución. Situación actual y perspectivas" 2003/2004

136.- Rosario Isabel Pastrana Gutiérrez: “Creació d'una empresa de serveis socials d'atenció a la dependència de les persones grans enfocada a productes d'assegurances” 2007/2008

137.- Joan Prat Rifá: "La Previsió Social Complementaria a l'Empresa" 2003/2004

138.- Alberto Sanz Moreno: “Beneficios del Seguro de Protección de Pagos” 2004/2005

139.- Judith Safont González: “Efectes de la contaminació i del estils de vida sobre les assegurances de salut i vida” 2009/2010

140.- Carles Soldevila Mejías: “Models de gestió en companyies d’assegurances. Outsourcing / Insourcing” 2005/2006

141.- Olga Torrente Pascual: “IFRS-19 Retribuciones post-empleo” 2003/2004

142.- Annabel Roig Navarro: “La importancia de las mutualidades de previsión social como complementarias al sistema público” 2009/2010

143.- José Angel Ansón Tortosa: “Gerencia de Riesgos en la Empresa española” 2011/2012

144.- María Mecedes Bernués Burillo: “El permiso por puntos y su solución aseguradora” 2011/2012

145.- Sònia Beulas Boix: “Prevención del blanqueo de capitales en el seguro de vida” 2011/2012

146.- Ana Borràs Pons: “Teletrabajo y Recursos Humanos en el sector Asegurador” 2011/2012

147.- María Asunción Cabezas Bono: “La gestión del cliente en el sector de bancaseguros” 2011/2012

148.- María Carrasco Mora: “Matching Premium. New approach to calculate technical provisions Life insurance companies” 2011/2012

149.- Eduard Huguet Palouzie: “Las redes sociales en el Sector Asegurador. Plan social-media. El Community Manager” 2011/2012

150.- Laura Monedero Ramírez: “Tratamiento del Riesgo Operacional en los 3 pilares de Solvencia II” 2011/2012

151.- Salvador Obregón Gomá: “La Gestión de Intangibles en la Empresa de Seguros” 2011/2012

152.- Elisabet Ordóñez Somolinos: “El sistema de control Interno de la Información Financiera en las Entidades Cotizadas” 2011/2012

153.- Gemma Ortega Vidal: “La Mediación. Técnica de resolución de conflictos aplicada al Sector Asegurador” 2011/2012

154.- Miguel Ángel Pino García: “Seguro de Crédito: Implantación en una aseguradora multirramo” 2011/2012

155.- Genevieve Thibault: “The Costumer Experience as a Sorce of Competitive Advantage” 2011/2012

156.- Francesc Vidal Bueno: “La Mediación como método alternativo de gestión de conflictos y su aplicación en el ámbito asegurador” 2011/2012

157.- Mireia Arenas López: “El Fraude en los Seguros de Asistencia. Asistencia en Carretera, Viaje y Multirriesgo” 2012/2013

158.- Lluis Fernández Rabat: “El proyecto de contratos de Seguro-IFRS4. Expectativas y realidades” 2012/2013

159.- Josep Ferrer Arilla: “El seguro de decesos. Presente y tendencias de futuro” 2012/2013

160.- Alicia García Rodríguez: “El Cuadro de Mando Integral en el Ramo de Defensa Jurídica” 2012/2013

161.- David Jarque Solsona: “Nuevos sistemas de suscripción en el negocio de vida. Aplicación en el canal bancaseguros” 2012/2013

162.- Kamal Mustafá Gondolbeu: “Estrategias de Expansión en el Sector Asegurador. Matriz de Madurez del Mercado de Seguros Mundial” 2012/2013

163.- Jordi Núñez García: “Redes Periciales. Eficacia de la Red y Calidad en el Servicio” 2012/2013

164.- Paula Núñez García: “Benchmarking de Autoevaluación del Control en un Centro de Siniestros Diversos” 2012/2013

165.- Cristina Riera Asensio: “Agregadores. Nuevo modelo de negocio en el Sector Asegurador” 2012/2013

166.- Joan Carles Simón Robles: “Responsabilidad Social Empresarial. Propuesta para el canal de agentes y agencias de una compañía de seguros generalista” 2012/2013

167.- Marc Vilardebó Miró: “La política de inversión de las compañías aseguradoras ¿Influirá Solvencia II en la toma de decisiones?” 2012/2013

168.- Josep María Bertrán Aranés: “Segmentación de la oferta aseguradora para el sector agrícola en la provincia de Lleida” 2013/2014

169.- María Buendía Pérez: “Estrategia: Formulación, implementación, valoración y control” 2013/2014

170.- Gabriella Fernández Andrade: “Oportunidades de mejora en el mercado de seguros de Panamá” 2013/2014

171.- Alejandro Galcerán Rosal: “El Plan Estratégico de la Mediación: cómo una Entidad Aseguradora puede ayudar a un Mediador a implementar el PEM” 2013/2014

172.- Raquel Gómez Fernández: “La Previsión Social Complementaria: una apuesta de futuro” 2013/2014

173.- Xoan Jovaní Guiral: “Combinaciones de negocios en entidades aseguradoras: una aproximación práctica” 2013/2014

174.- Àlex Lansac Font: “Visión 360 de cliente: desarrollo, gestión y fidelización” 2013/2014

175.- Albert Llambrich Moreno: “Distribución: Evolución y retos de futuro: la evolución tecnológica” 2013/2014

176.- Montserrat Pastor Ventura: “Gestión de la Red de Mediadores en una Entidad Aseguradora. Presente y futuro de los agentes exclusivos” 2013/2014

177.- Javier Portalés Pau: “El impacto de Solvencia II en el área de TI” 2013/2014

178.- Jesús Rey Pulido: “El Seguro de Impago de Alquileres: Nuevas Tendencias” 2013/2014

179.- Anna Solé Serra: “Del cliente satisfecho al cliente entusiasmado. La experiencia cliente en los seguros de vida” 2013/2014

180.- Eva Tejedor Escorihuela: “Implantación de un Programa Internacional de Seguro por una compañía española sin sucursales o filiales propias en el extranjero. Caso práctico: Seguro de Daños Materiales y RC” 2013/2014

181.- Vanesa Cid Pijuan: “Los seguros de empresa. La diferenciación de la mediación tradicional“ 2014/2015.

182.- Daniel Ciprés Tiscar: “¿Por qué no arranca el Seguro de Dependencia en España?” 2014/2015.

183.- Pedro Antonio Escalona Cano: “La estafa de Seguro. Creación de un Departamento de Fraude en una entidad aseguradora” 2014/2015.

184.- Eduard Escardó Lleixà: “Análisis actual y enfoque estratégico comercial de la Bancaseguros respecto a la Mediación tradicional” 2014/2015.

185.- Marc Esteve Grau: “Introducción del Ciber Riesgo en el Mundo Asegurador” 2014/2015.

186.- Paula Fernández Díaz: “La Innovación en las Entidades Aseguradoras” 2014/2015.

187.- Alex Lleyda Capell: “Proceso de transformación de una compañía aseguradora enfocada a producto, para orientarse al cliente” 2014/2015.

188.- Oriol Petit Salas: “Creación de Correduría de Seguros y Reaseguros S.L. Gestión Integral de Seguros” 2014/2015.

189.- David Ramos Pastor: “Big Data en sectores Asegurador y Financiero” 2014/2015.

190.- Marta Raso Cardona: Comoditización de los seguros de Autos y Hogar. Diferenciación, fidelización y ahorro a través de la prestación de servicios” 2014/2015.

191.- David Ruiz Carrillo: “Información de clientes como elemento estratégico de un modelo asegurador. Estrategias de Marketing Relacional/CRM/Big Data aplicadas al desarrollo de un modelo de Bancaseguros” 2014/2015.

192.- Maria Torrent Caldas: “Ahorro y planificación financiera en relación al segmento de jóvenes” 2014/2015.

193.- Cristian Torres Ruiz: “El seguro de renta vitalicia. Ventajas e inconvenientes” 2014/2015.

194.- Juan José Trani Moreno: “La comunicación interna. Una herramienta al servicio de las organizaciones” 2014/2015.

195.- Alberto Yebra Yebra: “El seguro, producto refugio de las entidades de crédito en épocas de crisis” 2014/2015.

196.- Jesús García Riera: “Aplicación de la Psicología a la Empresa Aseguradora” 2015/2016

197.- Pilar Martínez Beguería: “La Función de Auditoría Interna en Solvencia II” 2015/2016

198.- Ingrid Nicolás Fargas: “El Contrato de Seguro y su evolución hasta la Ley 20/2015 LOSSEAR. Hacia una regulación más proteccionista del asegurado” 2015/2016

199.- María José Páez Reigosa: “Hacia un nuevo modelo de gestión de siniestros en el ramo de Defensa Jurídica” 2015/2016

200.- Sara Melissa Pinilla Vega: “Auditoría de Marca para el Grupo Integra Seguros Limitada” 2015/2016

201.- Teresa Repollés Llecha: “Optimización del ahorro a través de soluciones integrales. ¿cómo puede la empresa ayudar a sus empleados? 2015/2016

202.- Daniel Rubio de la Torre: “Telematics y el seguro del automóvil. Una nueva póliza basada en los servicios” 2015/2016

203.- Marc Tarragó Diego: “Transformación Digital. Evolución de los modelos de negocio en las compañías tradicionales” 2015/2016

204.- Marc Torrents Fábregas: “Hacia un modelo asegurador peer-to-peer. ¿El modelo asegurador del futuro?” 2015/2016

205.- Inmaculada Vallverdú Coll: “Fórmulas modernas del Seguro de Crédito para el apoyo a la empresa: el caso español” 2015/2016

206.- Cristina Alberch Barrio: “Seguro de Crédito. Gestión y principales indicadores” 2016/2017

207.- Ian Bachs Millet: “Estrategias de expansión geográfica de una entidad aseguradora para un mercado específico” 2016/2017

208.- Marta Campos Comas: “Externalización del servicio de asistencia” 2016/2017

209.- Jordi Casas Pons: “Compromisos por pensiones. Hacia un nuevo modelo de negociación colectiva” 2016/2017

210.- Ignacio Domenech Guillén: “El seguro del automóvil para vehículos sostenibles, autónomos y conectados” 2016/2017

211.- Maria Luisa Fernández Gómez: “Adquisiciones de Carteras de Seguros y Planes de Pensiones” 2016/2017

212.- Diana Heman Hasbach: “¿Podrán los Millennials cobrar pensión?: una aplicación al caso de México” 2016/2017

213.- Sergio López Serrano: “El impacto de los Ciberriesgos en la Gerencia de Riesgos Tradicional” 2016/2017

214.- Jordi Martí Bernaus: “Dolencias preexistentes en el seguro de Salud: exclusiones o sobreprimas” 2016/2017

215.- Jésica Martínez Ordóñez: “Derecho al honor de las personas jurídicas y reputación online” 2016/2017

216.- Raúl Monjo Zapata: “La Función de Cumplimiento en las Entidades Aseguradoras” 2016/2017

217.- Francisco José Muñoz Guerrero: “Adaptación de los Productos de Previsión al Ciclo de Vida” 2016/2017

218.- Mireia Orenes Esteban: “Crear valor mediante la gestión de siniestros de vida” 2016/2017

219.- Oscar Pallisa Gabriel: “Big Data y el sector asegurador” 2016/2017

220.- Marc Parada Ricart: “Gerencia de Riesgos en el Sector del Transporte de Mercancías” 2016/2017

221.- Xavier Pérez Prado: “Análisis de la mediación en tiempos de cambio. Debilidades y fortalezas. Una visión de futuro” 2016/2017

222.- Carles Pons Garulo: “Solvencia II: Riesgo Catastrófico. Riesgo Antropógeno y Reaseguro en el Seguro de Daños Materiales” 2016/2017

223.- Javier Pulpillo López: “El Cuadro de Mando Integral como herramienta de gestión estratégica y retributiva” 2016/2017

224.- Alba Ballester Portero: “El cambio demográfico y tecnológico: su impacto en las necesidades de aseguramiento” 2017/2018

225.- Luis del Blanco Páez: “Aportación de valor al cliente desde una agencia exclusiva de seguros” 2017/2018

226.- Beatriz Cases Martín: “¿Blockchain en Seguros?” 2017/2018

227.- Adrià Díez Ruiz: **“**La inteligencia Artificial y su aplicación en la suscripción del seguro muiltirriesgo de hogar” 2017/2018

228.- Samantha Abigail Elster Alonso: "Soluciones aseguradoras de acción social (público-privada) para personas en situación de vulnerabilidad. Exclusión Social / Residencial y Pobreza Energética” 2017/2018

229.- Cristina Mallón López: “IFRS 17: Cómo afectará a los balances y cuenta de resultados de las aseguradoras” 2017/2018

230.- Carlos Matilla Pueyo: “Modelos de tarificación, transparencia y comercialización en los Seguros de Decesos” 2017/2018

231.- Alex Muñoz Pardo: “Aplicación de las nuevas tecnologías a la gestión de siniestros multirriesgos” 2017/2018

232.- Silvia Navarro García: “Marketing digital y RGDP” 2017/2018

233.- Agustí Ortega Lozano: “La planificación de las pensiones en los autónomos. Nueva reglamentación” 2017/2018

234.- Pablo Talisse Díaz: “El acoso escolar y el ciberbullying: como combatirlos” 2017/2018

235.- Jordi Torres Gonfaus: “Cómo llevar a cabo una estrategia de fidelización con herramientas de relación de clientes” 2017/2018

236.- Anna Valverde Velasco: “Nudging en el ahorro en la empresa. Aplicación de la Economía del Comportamiento a los instrumentos de Pensiones de Empleo” 2017/2018

237.- José Manuel Veiga Couso: “Análisis competitivo del mercado de bancaseguros en España. Una perspectiva de futuro para el periodo 2019-2021” 2017/2018

238.- Laura Villasevil Miranda: “Ecosistemas conectados en seguros. Análisis de seguros en el marco de la economía colaborativa y las nuevas tecnologías” 2017/2018

239.- María del Pilar Álvarez Benedicto: “Los seguros de Asistencia en Viaje. Análisis de caso: estudiantes universitarios desplazados” 2018/2019

240.- Jaume Campos Díaz: “La educación financiera como base de la cultura del ahorro y la previsión social" 2018/2019

241.- David Elías Monclús: "El agente de seguros exclusivo, más allá de la digitalización" 2018/2019

242.- Daniel Fraile García: “El seguro de impago de alquiler: contextualización en España y perspectivas” 2018/2019

243.- Guillermo García Marcén: “Contratación de la póliza de Ciberriesgos, tratamiento del siniestro y la importancia del reaseguro” 2018/2019

244.- Esther Grau Alonso: “Las quejas de los clientes y cómo estas nos brindan una oportunidad para crecer y mejorar” 2018/2019

245.- Ester Guerrero Labanda: “Compliance y ética empresarial. La cultura ética como motor del cambio de la actividad aseguradora” 2018/2019

246.- Sergio Hernández Chico: “El riesgo de mercado en Solvencia II y su optimización” 2018/2019

247.- Silvia Martínez López: “El papel de la Salud en los Planes de Retribución Flexible en las empresas” 2018/2019

248.- Marta Nadal Cervera: “El seguro bajo demanda” 2018/2019

249.- Carla Palà Riera: “Función Actuarial y Reaseguro” 2018/2019

250.- Silvia Paniagua Alcañiz: “Seguro Trienal de la Edificación” 2018/2019

251.- Agustí Pascual Bergua: “Solución integral para las Pymes: un nuevo concepto de Seguro” 2018/2019

252.- Eduardo Pérez Hurtado: “Estrategias de desarrollo para una mutua aseguradora de tamaño medio” 2018/2019

253.- Paquita Puig Pujols: “Inversiones socialmente responsables. Análisis del impacto de una cartera de inversiones en la sociedad y en los ODS” 2018/2019

254.- Maria Puig Pericas: “El seguro de Defensa Jurídica para la explotación comercial de Drones” 2018/2019

255.- Paula Rubio Borrallo: “Soluciones al actual sistema de pensiones individuales privadas. Con una visión internacional” 2018/2019

256.- Sara Sánchez Rámiz: “Implementación de IFRS17: principales fases” 2018/2019