MERCANTIL

¿QUÉ SON LOS SEGUROS DE «CIBERRIESGOS»?

Miguel Ángel Toledano Jiménez
Socio director de Curia Legis Abogados
Profesor del Área Jurídica. CEF.-UDIMA

Extracto

Analizamos en el presente trabajo los denominados seguros de «ciberriesgos»: su encuadre dentro de la Ley de Contrato de Seguro (50/1980 LCS), concepto, garantías más habituales, legislación aplicable, así como la posibilidad de las aseguradoras para operar en este tipo de seguros de conformidad con lo expuesto en la Ley de Ordenación, Supervisión y Solvencia de Entidades Aseguradoras y Reaseguradoras (20/2015 LOSSEAR).

Palabras clave: seguros de ciberriesgos; contrato de seguro; garantías.

Fecha de entrada: 05-07-2017 / Fecha de aceptación: 24-07-2017

WHAT ARE «CYBER-RISK» INSURANCES?

Miguel Ángel Toledano Jiménez

Abstract

We analyze in the present work the insurances called of «cyber-risks»: his setting inside the Law of Contract of Insurance (50/1980 LCS), concept, more habitual were guarantees, applicable legislation, as well as the possibility of the insurance ones to produce in this type of insurances of conformity with exposed in the Law of Arrangement, Supervision and Solvency of insurance and reinsurance Entities (20/2015 LOSSEAR).

Keywords: insurances of cyber-risks; contract of insurance; guarantees.

Sumario

1. CONCEPTO Y UBICACIÓN DE LOS SEGUROS DE «CIBERRIESGOS» EN LA LCS Y EN LA LOSSEAR

El seguro cambia con los tiempos, ¡qué duda cabe! Recordemos que la historia del seguro se remonta a las antiguas civilizaciones que ya efectuaban contratos a la gruesa financiando pérdidas; se trataba de contratos de préstamo en los transportes marítimos, en los que el prestamista entregaba dinero u otros bienes fungibles, obligándose el naviero a pagar el precio del riesgo si el viaje concluía felizmente. Al parecer, fueron los griegos los que inventaron este sistema de préstamo, que en realidad era un tipo de seguro, por la aleatoriedad del mismo, recogiéndolo luego los romanos con el nombre de *nauticum foenus* (navegación + interés del dinero prestado).

En sus orígenes, los seguros siempre han estado relacionados con el transporte de mercancías, bien por mar, bien por tierra; pensemos también en los mercaderes babilónicos cuando las mercancías que transportaban podían ser diezmadas por piratas y se concedían préstamos de alto interés que eran reembolsados si el viaje tenía un final feliz.

Aparecieron, con posterioridad, los seguros sobre la vida, incluso ya en la Edad Media, siempre vinculados a los viajes tanto por mar como por tierra, hasta llegar a la primera manifestación del seguro de daños, aproximadamente en el año 1500, en Hamburgo.

La primera ley que regula con carácter obligatorio el contrato de seguro marítimo data de 1549 y la dictó Carlos V. Las primeras manifestaciones del seguro de incendio se refieren al Londres de 1667, a raíz del famoso incendio que destruyó 13.200 casas y 90 iglesias, creándose entonces las primeras oficinas de seguros llamadas *fire office* y *friendly society*, surgiendo en 1687 Lloyd's como la más poderosa empresa aseguradora.

No vamos a hacer un recorrido histórico, tan solo indicar que la historia del seguro ha estado ligada a la historia de la humanidad, desde la Antigüedad, pasando por la Edad Media y hasta la Edad Moderna.

Hemos oído hablar de seguros de todo tipo, vida y no vida, en sus más diversas facetas: transporte (en sus diferentes ámbitos), daños, incendio, responsabilidad civil (automóviles, profesional, explotación, patrona,etc.), decesos, vida, accidentes, enfermedad, crédito, caución, pérdidas pecuniarias, defensa jurídica, etc. Pero, nunca habíamos oído hablar (hasta hace escaso tiempo) de los seguros de «ciberriesgo». ¿Qué son este tipo de seguros y qué pretenden?

En realidad, la palabra «ciberriesgo» no figura en el diccionario de la Real Academia Española, sin embargo sí aparece la definición de «cibernética», como referencia a lo que es creado y regulado mediante computadora, como la ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; también otras palabras como «ciberespacio» (ámbito artificial creado por medios informáticos), o incluso palabras como «cibernauta» (persona que navega por el espacio).

Sin embargo, sí encontramos definida la palabra «ciber» (ciber-), que significa aquello que tiene relación con redes informáticas. Su origen está en la palabra griega *kibernao* que significa pilotar una nave.

Por otro lado, estaría la palabra «riesgo», sin la cual un seguro no puede existir; recordemos que el riesgo es la proximidad o contingencia de un daño, y en materia aseguradora, sería cada una de las contingencias que pueden ser objeto de un contrato de seguro.

Recordemos que el riesgo, con la prima y la indemnización, constituye uno de los tres soportes básicos en que se asienta la institución aseguradora. No puede concebirse el seguro sin la existencia del riesgo, hasta el punto de que se podría decir que siempre *ab initio*, en el ámbito asegurador, nos encontraremos con la existencia del riesgo.

Ciñéndonos al concepto de «ciberriesgo», lo podríamos definir como la posibilidad de que por azar ocurra un hecho, relacionado con las redes informáticas, que produzca una necesidad patrimonial.

Tiene que existir la posibilidad e incertidumbre de que el hecho llegue a producirse, un elemento de azar o aleatoriedad, y una necesidad patrimonial, siendo estos elementos indispensables para que exista el riesgo.

En sentido genérico, podríamos indicar que los seguros de «ciberriesgos» cubren los daños derivados de la utilización de redes informáticas, en todas las formas posibles.

Desde nuestro punto de vista, es más adecuado hablar de este tipo de seguros como seguros de riesgos cibernéticos, ya que, al fin y al cabo, protegen de riesgos ocasionados por la utilización de computadoras y sistemas informáticos (recordemos que la cibernética es la ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas).

¿Qué pretenden? Evidentemente, cubrir los nuevos riesgos que aparecen en la sociedad, obteniendo por ello beneficios derivados de su comercialización y venta.

Muy ligada a los riesgos informáticos se encuentra la normativa sobre protección de datos. Recordemos que el Reglamento de Protección de Datos de la Unión Europea 2016/679 indica claramente que las empresas están obligadas a informar sobre las brechas de seguridad y a notificar a los terceros las violaciones de sus datos, estableciéndose un régimen sancionador más severo

sobre todo para aquellas empresas que tenga mayor facturación, y que afectarán tanto a los responsables del tratamiento como al encargado del mismo, alcanzando las sanciones hasta los 20 millones de euros o el 4 % del volumen de negocios total anual del ejercicio financiero anterior.

Este Reglamento entró en vigor el 25 de mayo de 2016, y las empresas tienen hasta el 25 de mayo de 2018 para adaptarse. El Gobierno ya trabaja en el anteproyecto de la nueva Ley Orgánica de Protección de Datos para adecuar la normativa española a la norma europea. Precisamente, el Consejo de Ministros, en nota de prensa de 27 de junio de 2017, ha indicado que, a propuesta del ministro de Justicia, ha impulsado un anteproyecto de la LOPD con el fin de mejorar la regulación de este derecho fundamental en los datos de carácter personal, y con el fin de adaptar la legislación española a las disposiciones contenidas en el Reglamento UE 2016/679, del Parlamento Europeo en esa materia antes de su definitiva entrada en vigor fijada, como hemos indicado, para el 25 de mayo de 2018.

El anteproyecto de la LOPD consta de 78 artículos estructurados en 8 títulos, 13 disposiciones adicionales, 5 disposiciones transitorias, 1 disposición derogatoria única (se deroga la LOPD 15/1999, de 13 de diciembre) y 4 disposiciones finales.

Qué duda cabe que las obligaciones impuestas por la normativa de protección de datos tendrán amplia repercusión en los denominados seguros de ciberriesgos, toda vez que los retos planteados por la rápida evolución tecnológica y la globalización han hecho que los datos personales y su regulación sean el recurso fundamental de la sociedad de la información, y su tratamiento hay que protegerlo. Las empresas tendrán que adaptarse, y para el caso de que se produzcan responsabilidades con motivo de negligencia, errores u omisiones involuntarios, los seguros tendrán que hacer su función. Si bien existen productos aseguradores específicos de protección de datos que conllevan coberturas en caso de sanciones administrativas e indemnizaciones por daños y perjuicios, este tipo de riesgos bien pudiera englobarse dentro del conjunto común de los «ciberriesgos», puesto que la mayor parte del tratamiento de datos ya se hace por vías tecnológicas, unidas, muchas veces, al tratamiento del dato en la red de redes, es decir, Internet.

Definidos los seguros de «ciberriesgos» como aquellos que cubren los daños derivados de la utilización de redes informáticas, analicemos ahora su ubicación, tanto dentro de la Ley 50/1980, de 8 de octubre, de Contrato de Seguro (LCS); así como dentro de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras (LOSSEAR).

Evidentemente, no encontramos este seguro como tal, sin embargo, entendemos que se trata de un seguro de daños en sentido estricto, y como tal seguro de daños, de un seguro perteneciente al ramo de no vida.

Por lo tanto, a este tipo de seguros les sería aplicable:

- Título I de la LCS (arts. 1 a 24), reguladores con carácter general de aspectos tan importantes, como el concepto de contrato de seguro, imperatividad de la norma,

condiciones generales, particulares, cláusulas limitativas (art. 3), conclusión, documentación del contrato, deber de declaración del riesgo, obligaciones y deberes de las partes, duración y prescripción.

- Título II, específico de los seguros contra daños, en el que encontramos: disposiciones generales aplicables a los seguros contra daños y las disposiciones específicas sobre los seguros de incendios, robo, transporte terrestre, lucro cesante, caución, crédito, responsabilidad civil y defensa jurídica. No vemos ningún problema en que se aplique a los seguros de «ciberriesgos», en cuanto seguros de daños que son, las disposiciones generales mencionadas y contenidas en los artículos 25 a 44 (suma asegurada e interés asegurado, prohibición del enriquecimiento injusto, valor del interés, infraseguro, regla proporcional, sobreseguro, seguro múltiple y coaseguro, comunicación del siniestro e indemnización del mismo, etc.). Por supuesto, habrá que estar a las garantías concretas que se oferten en este tipo de seguros y que deberán contenerse en la póliza (condiciones generales, particulares, documentos adicionales en su caso).

En cuanto a su ubicación en la LOSSEAR, los situamos dentro de los ramos de seguro distintos del seguro de vida, es decir, seguros de no vida (Anexo LOSSEAR), con toda la normativa aplicable a los mismos, si bien, como decimos, no existe mención específica ya que realidad se trataría de un seguro multirriesgo, que, por definición, sería un contrato de seguro en el que se reúnen garantías o coberturas de distintas pólizas de diferente ramos, cubriendo los diversos riesgos (en este caso cibernéticos) mediante un único documento o póliza.

2. GARANTÍAS MÁS HABITUALES

Los principales asegurados de riesgos cibernéticos son las empresas, y, en menor medida, el particular. En definitiva, se trata de proteger el patrimonio del asegurado (empresa, socio, directivo, empleado o particular) frente a las posibles fugas de seguridad, ataques de *hacker*, virus informáticos, empleados negligentes, suplantación de identidad, fuga de información y robo de identidad, extorsiones cibernéticas, etc.

Hemos llevado a cabo un breve análisis de las coberturas más habituales que ofrecen las compañías de seguros en este campo, y hemos encontrado las siguientes:

- Cobertura de responsabilidad civil frente a reclamaciones por vulneración de privacidad de datos, asistencia en gestión de crisis, pagos en casos de reducción de beneficios, indemnizaciones a terceros afectados por ataques cibernéticos.
- Defensa jurídica y fianzas, como en cualquier otro tipo de seguros.
- Responsabilidad civil y multas derivadas de incumplimiento en materia de protección de datos.

- Coberturas de daños propios a los sistemas informáticos, daños y perjuicios derivados de paralización de la actividad empresarial, gastos realizados para protección de los sistemas informáticos y minoración de las consecuencias derivadas de una extorsión cibernética, gastos para restaurar la imagen de la empresa en caso de que la misma se haya visto afectada por un ciberataque (daño reputacional), robo y pérdida de archivos, etc.
- A nivel particular, dentro de los seguros multirriesgos de hogar, se incluyen algunas figuras de riesgos cibernéticos: suplantación de personalidad, robo de tarjetas, virus informáticos en equipos domésticos, asistencia informática remota, inestabilidad del sistema, ataques en redes sociales, borrado de vida digital, etc. En general, se suelen comercializar bajo la denominación de asistencia informática para el hogar y protección de vida digital.

3. ALGUNOS DATOS

- Recientemente (junio 2017) se ha producido una nueva ola de ciberataques que, empezando en Ucrania, se ha extendido por el resto del mundo; la prensa se ha hecho eco de la noticia:

  – <http://www.elmundo.es/tecnologia/2017/06/27/595269e0ca4741fb3f8b4668.html>

  «Un nuevo ciberataque masivo afecta a empresas de todo el mundo» (Daniel J. Ollero).

  El método elegido por los piratas informáticos es similar al que se empleó con el virus WannaCry a finales del mes de mayo. Europol advierte: se espera una nueva oleada.

  «Mes y medio después del ciberataque WannaCry que puso en jaque a cientos de empresas y multinacionales en todo el mundo, los piratas informáticos han vuelto a actuar a nivel global contra organismos públicos y privados. Se trata de un virus sobre el que no existe unanimidad entre los expertos en seguridad informática. Mientras que según el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia (CNI), se trata de un virus de tipo *ransomware* –que secuestra la información de los equipos y solo la devuelve a cambio de un rescate– variante de Petya (el diminutivo en ruso de Pedro) que ya habría atacado varios sistemas informáticos en todo el mundo en 2016, desde la empresa de ciberseguridad Kaspersky señalan que "se trata de un nuevo *ransomware*, que nunca antes se había visto" al que han bautizado como NotPetya.

Por el momento, la lista de afectados la componen al menos 80 empresas de diversos sectores localizadas en países como Reino Unido, Estados Unidos, Francia, Rusia, España, India y Ucrania. En ella se encuentran algunas como la multinacional alimentaria Mondelez, que es dueña de marcas como Oreo, Tang, Milka o Toblerone, la empresa de publicidad británica WPP, Nivea, Auchan (Alcampo), el laboratorio Merck Sharp & Dohme, la petrolera rusa Rosneft y varias infraestructuras críticas de Ucrania como su Banco Nacional, los sistemas informáticos de sus aeropuertos, la compañía estatal de energía e, incluso, los sistemas de medición de radiación de Chernobil».

– <http://internacional.elpais.com/internacional/2017/06/28/actualidad/1498649539_960151.html>

Algunas empresas ceden y pagan a los *hackers* para liberarse del ciberataque.

La mayoría de compañías todavía trabajan para desbloquear sus ordenadores. Los expertos detectan más de 2.000 ciberataques a empresas de 64 países.

– <http://internacional.elpais.com/internacional/2017/05/31/actualidad/1496241283_691973.htm>

«Este jueves entra en vigor la nueva y polémica ley sobre ciberseguridad en China, entre las quejas de las empresas extranjeras acerca de posibles limitaciones a su capacidad de negocio en el país y promesas de Pekín de que no trata de restringir la libre competencia. La medida, que el Legislativo aprobó el pasado noviembre, busca, según las autoridades del país, proteger la privacidad de los datos y reducir la vulnerabilidad a ataques como el del virus WannaCry, que afectó a centenares de miles de sistemas informáticos en todo el mundo».

– <http://www.abc.es/tecnologia/redes/abci-petya-virus-protagonista-segunda-mundial-ciberataques-201706280129_noticia.html>

Petya, el virus protagonista de la segunda ola mundial de ciberataques.

Los cibersecuestradores pidieron a cambio de la recuperación de los sistemas informáticos un rescate de 300 dólares en *bitcoins*.

España, 15.º país con más intentos de infección de Petya.

El foco de cibersecuestros principales se ha observado en Rusia y Ucrania, pero el impacto se ha percibido también en Polonia, Italia, Reino Unido, Alemania, Francia, Estados Unidos, España y otros países.

España es el 15.º país en el que más se han detectado intentos de infección del *ransomware* Petya, según el mapa en tiempo real establecido por Kaspersky Lab.

- Centrándonos en España:

  – <http://www.elmundo.es/espana/2017/05/15/5918ae9222601d51718b46d7.html>

    España, tercer país del mundo con más ciberataques.

  – <http://tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494585889_857386.html>

  – El Gobierno confirma un ciberataque masivo a empresas españolas.

  – El Instituto Nacional de Ciberseguridad informa que las primeras fases del virus que han afectado a Telefónica y otras compañías han sido mitigadas.

  – <http://tecnologia.elpais.com/tecnologia/2017/05/18/actualidad/1495108825_274656.html>

Los expertos señalan el severo impacto del virus informático que se propagó a gran escala pese al silencio de las numerosas compañías que se han visto afectadas

«El ciberataque que se propagó por medio mundo congelando equipos informáticos y pidiendo un rescate a cambio de la recuperación de los datos comienza a estar controlado gracias a las actualizaciones de Microsoft, al ingenio de los investigadores independientes y al estado de alerta que establecieron la mayoría de empresas e instituciones al conocer la noticia.

Las investigaciones prosiguen, y todavía quedan muchas cuestiones que responder: quién es el «paciente cero», quién está detrás del ataque y cuáles han sido sus motivaciones. Las pistas señalan directamente al grupo de ciberdelincuentes Lazarus Group, vinculado a Corea del Norte y conocido por el ataque a Sony Pictures en el que extrajeron información de carácter confidencial.

España fue uno de los primeros afectados en conocerse gracias al ejercicio de transparencia de la operadora Telefónica, que confirmó haberse visto afectada en la mañana del viernes. Pronto se conocieron más casos como la paralización de varios hospitales del sistema público sanitario de Reino Unido, la infección de numerosos equipos en la compañía estadounidense de transporte FedEx o los problemas en varias cadenas de montaje de los fabricantes de vehículos Nissan y Renault.

China y Rusia fueron los países a los que el ciberataque golpeó más fuerte. Afectando indiscriminadamente al sector público y privado por su gran dependencia del software pirata, señalaron varias empresas especializadas en seguridad informática como la rusa Kaspersky. Una copia pirata de Windows no está registrada y licenciada, por lo que no pueden aplicar los parches de seguridad que se incluyen en las actualizaciones periódicas que ofrece Microsoft».

Cifra baja en España

> «En España, el Instituto Nacional de Ciberseguridad (INCIBE) confirmó el lunes 1.200 equipos afectados por dos variantes del *ransomware* WannaCry, cifra que los expertos consultados por *El País* consideran «muy baja» para el impacto tan grande que han detectado en las empresas españolas».

Es evidente que la mayoría de los ataques cibernéticos están relacionados con los denominados delitos informáticos. En el área jurisprudencial, se ha acuñado ya el concepto de «jurisprudencia informática», que trata cuestiones, todas ellas, relacionadas con la cibernética, uso de redes, suplantación de personalidad, etc.

Algunos ejemplos:

- STS (Penal) de 16 de febrero de 2017, sobre estafa informática.
- STS (Penal), Sección 1.ª, de 20 de abril de 2016. Trata el tema de utilización indebida de cuentas bancarias, operando a través de Internet y ordenando transferencias con suplantación de personalidad.
- ATS (Penal) de 21 de octubre de 2015.

  Resuelve la cuestión de competencia en un supuesto también de transferencias bancarias realizadas por medio de Internet sin autorización del titular de la cuenta. Se trata de un delito de estafa informática mediante el procedimiento conocido como *phishing*, en los que unas personas intermediarias o «mulas», habiendo aceptado de personas desconocidas un supuesto trabajo, reciben en sus cuentas unas transferencias, que después deben remitir a terceras personas.

  > «... en relación con dichos delitos (ver autos de 6.4.11, 23.10.11, 2.11.11, 22.02.12, 16.10.12 cuestión de competencia 20423/12) venimos diciendo: "... que el lugar de emisión de los correos por parte de la empresa contratante y el lugar de residencia del titular de la cuenta bancaria víctima del delito son datos que resultan irrelevantes a los efectos de la instrucción de la causa. Siendo datos trascendentes el lugar de actuación y de residencia del intermediario, al ser donde se reciben las transferencias y se extrae materialmente el dinero del circuito bancario para su envío a destinos en el extranjero; y también el lugar de emisión de la orden de transferencia, que no siempre se puede precisar"».

- STS (Penal) de 12 de junio de 2007, también sobre *phishing*.
- STS (Penal) de 6 de noviembre de 2007, sobre estafa informática y falsedad documental.
- SAP de Burgos (Sección 1.ª, Penal), de 3 de marzo de 2016, que nuevamente trata el tema del *phishing* (en inglés, «ir de pesca»). Se trata de un engaño, a través de

redes sociales y diversos medios de comunicación, en el que personas desconocidas obtienen los datos confidenciales necesarios para operar *on line* en la cuenta de la que otra persona es titular. El término *phishing* se utiliza para referirse a uno de los métodos más utilizados por los delincuentes cibernéticos para estafar y obtener información confidencial de terceros, de forma fraudulenta, generalmente contraseñas o información sobre tarjetas de crédito. Se puede definir como una suplantación de identidad que viene dada por un abuso informático y que se comete mediante el uso de la denominada ingeniería social (redes sociales donde las personas, confiadas, facilitan datos, por ejemplo de la tarjeta de crédito, domicilios, DNI, correo electrónico, etc.).

- SAP de Madrid (Penal) de 23 de junio de 2016 (de nuevo el *phishing*, con utilización indebida de claves bancarias secretas para operaciones bancarias).

La materia relativa a los ataques cibernéticos está íntimamente relacionada con la vulneración de la normativa en materia de protección de datos, secreto de comunicaciones, derecho a la intimidad, y delitos contra la propiedad intelectual, entre otros.

Nuestro Código Penal se adaptó a las nuevas tecnologías, en la reforma operada tras la Ley Orgánica 1/2015, de 30 de marzo; a título de ejemplo: delito de intrusión informática (art. 197 bis 1.º), delito de interceptación de transmisiones de datos informáticos (art. 197 bis, 2.º), delitos informáticos relacionados con la propiedad intelectual e industrial (arts. 270 y ss. CP), fraudes informáticos (art. 248.2 CP), calumnias e injurias vertidas en Internet, etc.

Debemos pensar, no obstante, que el seguro contra riesgos cibernéticos, como cualquier otro tipo de seguro, no cubre los hechos dolosos, si bien es cierto que se trataría de supuestos de dolo de tercero que causan un daño al asegurado, daño que, a su vez, repercute en cientos de personas que están vinculadas al mismo. Pensemos en un ataque informático producido a un banco, siendo el banco asegurado (por lo tanto, no ha cometido el delito) y que a su vez produce daños y perjuicios a los clientes del mismo; no se trata obviamente de cubrir la responsabilidad civil y de pagar la defensa jurídica ni las fianzas del delincuente, pero sí de cubrir las responsabilidades en las que el asegurado (banco) puede incurrir frente a terceras personas por el delito cometido, que ha vulnerado y atacado sus sistemas de seguridad.

No vamos a recoger más ejemplos, es indudable que los ataques informáticos están a la orden del día y seguirán estándolo. Los seguros cibernéticos nacen precisamente para paliar los efectos perjudiciales que estos ataques informáticos puedan tener frente a la propia empresa que los sufre y frente a terceros (generalmente clientes de dicha empresa).

En España, este tipo de seguros todavía se está asentando, aunque cada día el mercado está más desarrollado. Como hemos indicado, no solo el nuevo Reglamento de Protección de Datos incrementa la presión regulatoria en esta área, sino también, por ejemplo, la Ley de Sociedades de Capital ya estableció que la ciberseguridad debe formar parte de la estrategia del negocio y

debe ser tratada en el seno de los consejos de administración de las empresas, formado parte del cumplimiento normativo de las mismas.

Según las previsiones efectuadas por analistas, los seguros cibernéticos serán una de las principales áreas de crecimiento en los denominados seguros de no vida, calculando que este tipo de coberturas aumentará de 7.500 millones de dólares a 20.000 millones en el año 2020.

Dos son las medidas a adoptar: a) protección y prevención, y para el caso de que se materialice el riesgo, b) contratar un seguro, transfiriendo de esta manera el mismo, desde la empresa hasta la aseguradora, que deberá soportarlo conforme a lo indicado en la póliza suscrita. Con la nueva normativa sobre protección de datos, este tipo de seguros aumentará.

Se estima que en España se producen una media de 4.000 ataques al día (<https://blog.sofistic.com/2017/03/13/los-seguros-de-ciberriesgos-llegan-a-espana>). Los seguros harán su función, y los asegurados deben preparar la empresa para que previamente la aseguradora acepte el riesgo y permita la contratación; producido el siniestro, podrán o no surgir problemas legales derivados del rechazo total o parcial por parte de la aseguradora. En este caso conviene recordar que habrá que estar a la regulación general sobre los seguros de daños contenida en la LCS, sin perder de vista las leyes sectoriales que puedan regular si la prevención o no por parte del asegurado era suficiente o insuficiente, si se cumplía o no la normativa específica de seguridad en la materia. A partir de aquí entrará en juego el contenido de la póliza, las cláusulas limitativas, las exclusiones, las condiciones generales, etc., como en cualquier otro tipo de seguros.

Normativa

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 50/1980, de 8 de octubre, de Contrato de Seguro.
- Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de ordenación y supervisión de los seguros privados.
- 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) (Texto pertinente a efectos del EEE).
- STS (Penal) de 16 de febrero de 2017.
- STS (Penal) de 12 de junio de 2007.
- STS de 6 de noviembre de 2007.
- STS (Penal), Sección 1.ª, de 20 de abril de 2016.

- ATS (Penal), de 21 de octubre de 2015.
- SAP de Burgos (Sección 1.ª, Penal) de 3 de marzo de 2016.
- SAP de Madrid (Penal) de 23 de junio de 2016.

Webgrafía

- <http://www.elmundo.es/tecnologia/2017/06/27/595269e0ca4741fb3f8b4668.html>
- <http://internacional.elpais.com/internacional/2017/06/28/actualidad/1498649539_960151.html>
- <http://www.abc.es/tecnologia/redes/abci-petya-virus-protagonista-segunda-mundial-ciberataques-201706280129_noticia.html>
- <http://www.elmundo.es/espana/2017/05/15/5918ae9222601d51718b46d7.html>
- <http://tecnologia.elpais.com/tecnologia/2017/05/18/actualidad/1495108825_27465.html>