FACULTAD DE DERECHO

EL CONTRATO DE SEGURO DE RIESGOS CIBERNÉTICOS

Autor: Pedro Álvarez-Canal Bravo

5º E-3 A

Tutor: Ignacio Temiño Ceniceros

Madrid

Abril de 2024

RESUMEN.

El seguro de riesgos cibernéticos es un tipo de seguro cuyo objeto es asegurar a los contratantes de esta clase de pólizas ante el riesgo existente en la red cibernética, cubriendo los eventuales daños que estos puedan sufrir en el marco de la utilización de elementos cibernéticos. Esta clase de contrato de seguros tiene una gran importancia en el contexto actual debido a la gran dependencia en las empresas de las redes cibernéticas en este momento de la historia y la gran cantidad de riesgos que existen en ellas. El objetivo de este Trabajo de Fin de Grado es el estudio de esta clase de contrato de seguros partiendo de su evolución histórica hasta llegar a su contexto actual, siguiendo con un análisis de su marco legal centrado en el estudio del entorno normativo europeo y español, para posteriormente analizar el contrato típico de esta clase de seguros, comenzando por un estudio general, seguido de un análisis concreto al contrato de seguro de riesgos cibernéticos y finalizando con un estudio más profundo focalizando en algunas cláusulas de este que son conflictivas en su aplicación actual.

PALABRAS CLAVE.

Seguro, cláusula, cibernético, riesgo, contrato.

ABSTRACT.

Cyber risk insurance is a type of insurance whose purpose is to insure the contracting parties of this type of policy against the risk existing in the cybernetic network, covering the eventual damages that they may suffer in the framework of the use of cybernetic elements. This type of insurance contract is of great importance in the current context due to the great dependence of companies on cybernetic networks at this moment in history and the large number of risks that exist in them. The aim of this Final Degree Project is to study this type of insurance contract starting from its historical evolution until reaching its current context, continuing with an analysis of its legal framework focused on the study of the European and Spanish regulatory environment, to subsequently analyse the typical contract of this type of insurance, starting with a general study, followed by a specific analysis of the insurance contract for cyber risks and ending with a more in-depth study focusing on some of its clauses that are conflicting in their current application.

KEY WORDS.

Insurance, clause, cyber, risk, contract.

ÍNDICE

LISTADO DE ABREVIATURAS.

Pp.	Páginas
Op. Cit.	Obra citada
Art.	Artículo
LCS	Ley del Contrato de Seguro
LOSSEAR	Ley de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras
CC	Código Civil
CCom	Código de Comercio
LOPDPGDD	Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
LGDCU	Ley General para la Defensa de los Consumidores y Usuarios
CBGC	Código de Buen Gobierno de la Ciberseguridad
UE	Unión Europea
OCDE	Organización para la Cooperación y el Desarrollo Económico
CNMV	Comisión Nacional del Mercado de Valores
AEPD	Agencia Española de Protección de Datos
MITM	Man In The Middle
DoS	Denegación de servicios
DDoS	Denegación de servicios distribuido
IoT	Internet de las cosas
2FA	Doble Factor de Autenticación

1. INTRODUCCIÓN

El seguro de riesgos cibernéticos o ciber riesgos es el instrumento mediante el cual los contratantes de este tipo de pólizas cubren los posibles daños que puedan sufrir ante un ciber ataque o ataque sufrido mediante el uso de elementos cibernéticos.

La transmisión del riesgo es la última línea de defensa elegida por los asegurados para cubrirse ante el riesgo inminente del mundo ciber, pero no la única, ya que igualmente estos asegurados deben tomar una protección activa de sus sistemas ante este riesgo.

Este tipo de seguro está dirigido principalmente a las empresas, ya que mediante las pólizas de riesgos cibernéticos las empresas aseguradas se vinculan con las empresas aseguradoras, pagando una cantidad fija llamada prima, normalmente de forma anual o semestral, a cambio de cubrir el impacto que pueda tener un ataque cibernético hacia sus sistemas[1].

El importe de la prima previamente mencionada depende del riesgo a asegurar, lo cual varía según la política en ciberseguridad del asegurado, del sector en el que se encuentre su actividad económica y del tamaño de la empresa asegurada; y según las coberturas que se incluyan en el contrato.

Normalmente, bajo este seguro se suelen cubrir tanto la gestión del siniestro, con un equipo técnico forense y un equipo especialista en protección de datos que analicen el incidente y den una serie de medidas a tomar al asegurado, así como los posibles daños generados a terceros por el siniestro, y también los daños propios que haya sufrido el asegurado a causa del siniestro, como puede ser la paralización del negocio o una transferencia de fondos, por ejemplo[2].

[1] Jiménez Naharro, F., Sánchez Montañés, C. y Sánchez Barrios, M. (2018). *La transferencia de los riesgos cibernéticos en empresas internacionales con alto nivel de capitalización bursátil.* Revista de Pensamiento Estratégico y Seguridad CISDE, 3(1), 67-90. (www.cisdejournal.com)

[2] García Villarrubia, M., Sánchez Bleda, P., Touriño Peña, A., Rodríguez Ayuso, J.F., Serrano Acitores, A., Muñoz Rodríguez, J., Díaz Bizkarguenaga, K., Estévez Sanz, M. y Ortega Burgos, E. (2023). XIV. Cómo gestionar un ciberataque desde un punto de vista jurídico en Eceiza Zubieta, L., *Nuevas Tecnologías 2023.* Tirant Lo Blanch.

1.1. Historia y actualidad del seguro de riesgos cibernéticos

El seguro de riesgos cibernéticos nace en Estados Unidos, dónde en la década de los 90 ya se alcanzan a ver ejemplos de empresas que se aseguran ante este riesgo.

A pesar de esto, no es hasta finales de esa década – principios de los 2000, cuando empieza a proliferar la contratación de pólizas de ciber riesgos, dinamitado por cuatro factores clave:

- La llegada del efecto 2000, con el enorme incremento de la dependencia del mundo empresarial de los sistemas y las redes informáticas, y la mayor exposición ante el riesgo cibernético que ello conlleva.
- La explosión de las empresas cibernéticas, como Yahoo o Google, que se apresuraron en contratar este tipo de pólizas para asegurar su negocio.
- La profesionalización del crimen cibernético, con atacantes cada vez más especializados y perfectamente organizados, convirtiéndose en una vertiente criminal más.
- La SB1386, de California en Julio de 2003, la primera ley en el mundo que obligaba a las empresas o personas que sufriesen una brecha a comunicarlo si había datos informatizados de carácter personal involucrados en la brecha.

Sin embargo, el crecimiento del mercado del seguro de riesgo cibernético fue menor del esperado debido al oscurantismo del sector del crimen cibernético en esos momentos, con pocas noticias y datos al respecto y a la resistencia del sector empresarial de revelar y notificar datos sobre los incidentes o las amenazas que sufrían[3].

El seguro de riesgo cibernético se expandió internacionalmente, llegando a España utilizando como modelo las pólizas estadounidenses y gradualmente adaptándose a las empresas de nuestro país.

El sector cibernético fue creciendo exponencialmente en pocos años, afianzándose en el día a día de cualquier empresa. A medida que este crecía y se establecía, mayor era la preocupación por los riesgos que este podía entrañar, con el consecuente crecimiento del seguro de ciber riesgo para proteger a las empresas de este riesgo creciente.

[3] THIBER, (2016) *la transferencia del ciberriesgo en España*. https://thiber.org/ciberseguros.pdf

El riesgo del mundo cibernético fue subiendo puestos en la importancia mundial muy rápidamente, hasta ser uno de los principales riesgos a nivel global para las empresas, destacando en estudios en los que se alza como el principal riesgo global para las empresas, por encima de otros riesgos como la desaceleración económica, los cambios normativos o los riesgos de pandemia y crisis sanitaria.[4]

Consecuentemente, ha ido aumentando el mercado del seguro de ciberriesgos, rondando los 13.500 millones de dólares en volumen de primas en el mercado mundial en 2022, pero el mercado estadounidense representa más del 50% de este volumen mundial.

A finales de 2022, más de 220 grupos aseguradores ofrecían pólizas de ciberseguro suscribiendo riesgos cibernéticos de forma directa. Sin embargo, los 20 primeros grupos acaparan el 70,3 % del mercado, entre los que están grupos como Munich Re, Chubb, Beazley o Axa.[5]

La OCDE recomienda la suscripción de este tipo de seguros ya que subraya la importancia del papel de estos en la protección de las empresas en la actualidad, identificando que las cifras de mercado son demasiado bajas para el riesgo existente en el mundo cibernético[6].

Las cifras en España mantienen un crecimiento enorme año a año, sobrepasando en 2023 los 100 millones de euros en volumen de primas, con un crecimiento de más de un 50% respecto del año anterior. Los sectores en los que más pólizas de ciber riesgo se suscriben en España son el industrial, los servicios profesionales, las infraestructuras críticas, la salud y las administraciones públicas.

El riesgo cibernético tiene una evolución rápida y continua, con incesantes amenazas e incertidumbres, pero el aumento de la concienciación general y de la inversión en contrarrestarlo favorecen a una cada vez mayor estabilidad del mercado.

Aun así, los asegurados siguen experimentando cambios realizados por las aseguradoras para mantener el riesgo en un punto en el que pueda ser beneficioso para ambos, por lo que más del 60% de los asegurados experimentaron un aumento de las franquicias,

[4] AON. (2021). *Encuesta anual de gestión de riesgos 2021* https://www.aon.com/2021-global-risk-management-survey/latam/es.jsp

[5] Leonor, D. (2023). *Estados Unidos representa más de la mitad de las primas cibernéticas en 2022.* Inese. https://future.inese.es/estados-unidos-representa-mas-de-la-mitad-de-las-primas-ciberneticas-en-2022/

[6] Ministerio de Asuntos Económicos y Transformación Digital. Vicepresidencia Primera del Gobierno. (2022). *Informe 2022 Seguros y Fondos de Pensiones.* Pp. 390-397. dgsfp.mineco.gob.es/es/Publicaciones/DocumentosPublicaciones/Informe del sector 2022.pdf

entiendo por franquicia la cantidad de dinero que un asegurado debe pagar por su cuenta en caso de existir un siniestro cubierto por la póliza suscrita.[7]

En el 2021, a partir de los datos del Ministerio del Interior, el cibercrimen alcanzaba el 1,5% del PIB mundial, superando al tráfico de armas, de drogas y trata de personas juntos.[8]

A nivel mundial, el cibercrimen ha costado al mundo más de 8 billones de dólares y se espera que en 2024 esta cifra aumente hasta los 9,5 billones de dólares. Estas cifras colocarían al cibercrimen como la tercera economía mundial, solo por detrás de Estados Unidos y China[9].

España está en el top 10 mundial de los países que más ciberataques han sufrido en este 2023 y según algunos informes en el top 3 tan solo por detrás de Estados Unidos y Rusia, que posicionan a España como el tercer país que más ciberataques sufrió en el segundo cuarto del año 2023 con más de 3,7 millones de ciberataques[10].

La mediana de la cifra que le ha costado a las empresas españolas estos ciberataques es de 11.400 euros[11], casi el 50% de los siniestros indemnizados han sido por menos de 20.000 euros, pero el 10% de los siniestros que se han indemnizado superando los 2 millones de euros, existiendo este año indemnizaciones de 8 cifras.

Los segmentos de mercado que más sufren esta siniestralidad son el mercado medio, las grandes cuentas y los clientes multinacionales globales, que han sufrido cerca del 30% de los siniestros de este año cada uno. Por línea de mercado, el sector al que pertenecen las empresas que realizan un mayor número de notificaciones sobre siniestros relacionados

---

[7] AON. (2023). *IV Estudio Anual de Aon sobre Ciberseguridad y Gestión del Riesgo Ciber en España*. Pp. 5-8. https://noa.aon.es/wp-content/uploads/2023/09/Informe-Ciber-2023VFD.pdf

[8] González Cerredelo, S. (2022) *Así han evolucionado los ciberataques*. El Mundo. https://historiasdeprogreso.elmundo.es/asi-han-evolucionado-los ciberataques.html#:~:text=Hoy%20en%20d%C3%ADa%2C%20el%20cibercrimen,para%20adelantarse%20a%20los%20ataques.

[9] Morgan, S. (2023). *2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics.* Cybersecurity Ventures. https://cybersecurityventures.com/cybersecurity-almanac-2023/

[10] Surfshark. (2023). *Data breaches ramped up globally as 2023 reaches midpoint.* https://surfshark.com/research/study/data-breach-statistics-q2-2023. Fernández, M. (2023). *España, en el podio mundial de ciberataques: es el tercer país con más cuentas hackeadas en 2023.* https://www.elespanol.com/omicrono/software/20230816/espana-podio-mundial-ciberataques-tercer-pais-cuentas-hackeadas/785921544_0.html

[11] Lamb, E. (2023). *Informe de Ciberpreparación de Hiscox 2023.* Pp 14-16. https://www.hiscox.es/sites/spain/files/2023-10/22594%20-%20Cyber%20Readiness%20Report%202023%20-%20Spanish.pdf

con ciberataques son las instituciones financieras, la industria y los servicios informáticos, datos relacionados con el perfil de clientes más habitual que contratan pólizas de este tipo[12].

Se espera que para 2025 el volumen de primas brutas mundiales del seguro de ciber riesgos pueda superar los 20.000 millones de dólares, incluso se cree que en el 2030 este mercado supere los 50.000 millones de dólares, reflejando la creciente necesidad de este tipo de seguro para las empresas que cada vez son más conscientes del peligro que supone el cibercrimen[13].

1.2. **Incidentes principales.**

Tras el contexto histórico y actual del seguro de ciber riesgos es necesario detenerse en una explicación extensiva de los principales tipos de ciberataques.

Para ello, primero hay que explicar en qué consiste el concepto de malware. Este concepto proviene de las palabras "malicious" y "software" y describe a los programas maliciosos que han sido diseñados para dañar los equipos informáticos con el objetivo de obtener algún beneficio o simplemente perjudicar al usuario de estos[14].

1.2.1. Ransomware

La palabra "ransomware" proviene de los términos en inglés "ransom" que se traduce como rescate y "ware" que significa en español mercancía o producto.

El ransomware es un tipo de malware que consiste en el cifrado del contenido de sistemas informáticos impidiendo así el acceso a estos. Este cifrado produce la paralización de los sistemas informáticos infectados, además de la amenaza de que el contenido se haga público o se venda, con el consecuente daño reputacional y posibles consecuencias legales.

---

[12] Op. Cit. AON. (2023). Pp. 59-63.

[13] Howden. (2023). *Las primas de seguros cibernéticos podrían superar los 50 mil millones de dólares para el año 2030.* https://www.howdengroup.com/es-es/informe-cyber González, P. (2023). *La economía mundial se enfrenta a un riesgo de ciberataque de 3,5 billones de dólares en cinco años.* Inese. https://future.inese.es/la-economia-mundial-se-enfrenta-a-un-riesgo-de-ciberataque-de-35-billones-de-dolares-en-cinco-anos/

[14] IBM. *¿Qué es el malware?.* https://www.ibm.com/es-es/topics/malware

Los atacantes dejan una carta o nota de rescate, que suele aparecer en la pantalla de los dispositivos infectados y solicita una cantidad de dinero, a menudo en Bitcoin u otra criptomoneda para evitar el rastreo del pago, a cambio de desbloquear los equipos y en alguna ocasión amenazan con hacer los datos cifrados públicos o venderlos sino se procede al pago del rescate.

La peligrosidad de este tipo de ciberataque reside en el daño empresarial que es capaz de producir, ya que la encriptación puede llegar a producir la paralización total de los sistemas informáticos de una empresa, lo cual conlleva en muchos casos a la paralización total del negocio, además del daño reputacional que puede infringir este incidente a la empresa e incluso eventuales consecuencias legales por los datos personales que puedan revelarse y por los que la empresa afectada sea responsable.

Son varias las vías de entrada de los ciber atacantes para infectar los sistemas informáticos con un ransomware, las más habituales son consiguiendo las credenciales de acceso a los equipos a través de engaños en la red, como el phishing del que se hablará más adelante, aprovechando agujeros de seguridad presentes en el software, o aprovechando servicios expuestos a internet que no cuenten con las medidas de seguridad necesarias. Una vez se ha dado el acceso a los sistemas el ciberdelincuente procede al desarrollo de su ataque[15].

En 2021 el coste global por este tipo de ataques fue de 18.000 millones de euros. Importantes organizaciones mundiales destacan el peligro del ransomware en nuestra sociedad, como el Parlamento Europeo que considera que es la amenaza más importante de la actualidad. Se estima que el impacto económico global de los ataques ransomware en 2031 alcanzará los 265.000 millones de euros anuales[16].

El ransomware es el ciberataque más habitual en España, junto con el phishing ya que suelen estar muy relacionados, ya que el 15% de los incidentes cibernéticos sufridos en España este último año fueron ransomwares[17]. El 57% de las empresas españolas que sufrieron un ransomware en 2023 pagaron el rescate que solicitaban, lo cual no es

[15] Incibe. (2020). *Ransomware, una guía de aproximación para el empresario.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware.pdf
[16] Op. Cit. AON. (2023) Pp. 51. .Agencia de la Unión Europea para la Ciberseguridad (ENISA). (2022). *Ciberseguridad: amenanzas principales y emergentes.* https://www.europarl.europa.eu/topics/es/article/20220120STO21428/ciberseguridad-amenanzas-principales-y-emergentes
[17] Deloitte. (2023). *El estado de la ciberseguridad en España Cyber Strategy, Transformation and Assessments. https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad-2024.html*

recomendable ya que pagar no te asegura que el atacante cumpla su parte y libere los datos y además se ha encontrado una fuerte relación entre el pago del rescate y el sufrir otro ataque ransomware posterior[18].

1.2.2. Phishing

El concepto de phishing engloba un conjunto de técnicas de ingeniería social utilizadas por los ciber atacantes para engañar y manipular personas y así conseguir sus objetivos.

Para ello, suelen hacerse pasar por personas en las que la víctima confía, como compañeros de trabajo, clientes o proveedores. También se caracteriza porque suelen tener un revestimiento de urgencia para presionar más a la persona que lo recibe y así facilitar que caiga en el engaño.

La forma más habitual de phishing es mediante correo electrónico, pero también se puede dar a través de redes sociales, servicios de mensajería móvil, mensajes dentro de aplicaciones y hasta por llamadas telefónicas.

Dentro de los phishing por correo electrónico hay diferentes tipos, el más frecuente es a través de correos masivos, que generan los atacantes haciendo creer a los receptores que son grandes empresas o instituciones, pero también es habitual el phishing por suplantación de identidad en los que se hacen pasar por entidades o personas en las que se confía utilizando dominios muy parecidos e incluso idénticos al original[19].

En las comunicaciones engañosas contiene algún tipo de enlace en el que se pide una serie de datos que luego el atacante utilizará para cumplir sus pretensiones o simplemente documentos en los que al entrar sin saberlo se permite el acceso de este a los sistemas. Se suelen identificar por no ser el dominio exacto de la persona o entidad que pretenden suplantar, por presentar lenguaje urgente y enlaces sospechosos, por contener peticiones de información confidencial u otras que no son habituales en el emisor y por presentar fallos de estructura y de escritura en el cuerpo del mensaje, pero no siempre es así[20].

[18] Op. Cit. Lamb, E. (2023). Pp. 8-17
[19] IBM. (S.F.). *¿Qué es el phishing?* https://www.ibm.com/es-es/topics/phishing
[20] Rashid, S. (2024). *Reconocer los ataques de phishing en 2024.* https://www.metacompliance.com/es/blog/cyber-security-awareness/recognising-phishing-attacks

El mejor método para evitarlos es, si existe la posibilidad, comprobar mediante una segunda vía quién es el emisor real del mensaje, por ejemplo, con una llamada telefónica a la persona o entidad que se pretende suplantar.

El phishing es utilizado por los ciber criminales para conseguir acceso a datos y sistemas. Está muy relacionado con ataques de ransomware y de otros tipos de malware, como virus informáticos o adware, por ejemplo, ya que a través de este consiguen el acceso a los sistemas de la víctima y así realizar el ataque que pretendían.

El phishing es la segunda causa más costosa de filtración de datos, se estima que en 2021 el coste medio por filtración debida a phishing fue de 4,65 millones de dólares[21], mientras que en 2023 la cifra ascendió hasta los 4,76 millones de dólares de media[22]. Aproximadamente el 91% de las organizaciones en 2023 tenían un alto riesgo de sufrir algún intento de ataque phishing, dato que exhibe la masificación que este tipo de ciber ataque supone en la actualidad y la importancia de protegerse ante el phishing[23].

1.2.3. Man in the middle y ataque de denegación de servicio

Por último, es necesario explicar dos tipos de ciberataque más, que si bien no se dan tan frecuentemente en la actualidad como lo hacen el ransomware y el phishing, son muy dañinos para las empresas que lo sufren y difíciles de evitar.

Primero, los ataques "Man in the middle" o MITM, en español "hombre en el medio". Este tipo de ataques consiste en que un tercero intercepta las comunicaciones entre dos o más individuos y se coloca en el medio de estas sin ser detectado.

Una vez está en el medio puede decidir si los mensajes continúan hacia los receptores y con que contenido, por lo que puede modificar la información de este a su beneficio.

Un ejemplo de un ataque "Man in the middle" sería la intercepción de las comunicaciones entre un cliente y una empresa, interceptando las comunicaciones entre ellos y cambiando el contenido de un mensaje que contenga la petición de un pago por los servicios prestados o bienes vendidos con el número de cuenta real de la empresa por el número de cuenta del atacante, recibiendo así el dinero correspondiente.

---

[21] Op. Cit. IBM. (S.F.)
[22] Op. Cit. Rashid, S.
[23] Forbes. (2023). *El 91% de las empresas corre riesgo de sufrir un ataque de 'phishing' en 2023, según BDO.* https://forbes.es/ultima-hora/231482/el-91-de-las-empresas-corre-riesgo-de-sufrir-un-ataque-de-phishing-en-2023-segun-bdo/

Estos ataques son muy difíciles de detectar. Los métodos de acceso de los atacantes para realizar este tipo de ataques son variados, algunos ejemplos son a través de redes públicas abiertas, redes locales con bajo nivel de seguridad o por la utilización de softwares de navegación anticuados[24].

El otro tipo de ataque cibernético a tener en cuenta son los ataques de denegación de servicios, que pueden ser ataques DOS o ataques DDOS o ataque de denegación de servicios distribuido.

La definición de un ataque de denegación de servicios es: "la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso"[25]

Por lo tanto, este tipo de ataques produce la inutilización de un servicio o sistema, con la consecuente paralización de parte o total del negocio para la empresa que lo sufre. Este tipo de ataque se caracteriza por ser muy dañino y difícil de evitar.

La diferencia entre los ataques DOS y DDOS es que en el primero el ataque se realiza desde un único foco y el segundo cuentan con múltiples focos sincronizados que centran su ataque en un único destino.

Para realizar estos ataques, los ciber delincuentes utilizan cualquier dispositivo IoT[26] que sea vulnerable para saturar los servicios de la empresa objetivo. Al día, más de 7 millones de dispositivos IoT nuevos se conectan a internet y la mayoría no cuenta con la seguridad suficiente, lo que provoca una gran cantidad de nuevas oportunidades para los atacantes para hacer daño a sus objetivos[27].

[24] INCIBE. (2020). *El ataque del "Man in the middle" en la empresa, riesgos y formas de evitarlo*. https://www.incibe.es/empresas/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo
[25] Verdejo Álvarez, G. (S.F.). *SEGURIDAD EN REDES IP: DOS/DDOS.* https://www.cs.upc.edu/~gabriel/files/DEA-es-2DOS-DDOS.pdf Pp. 37.
[26] La IoT (Internet de las cosas) es un sistema de dispositivos electrónicos interconectados que puede recopilar y transferir datos a través de una red inalámbrica sin intervención de personas.
[27] Netscout. (2019). *INFORME GLOBAL DE AMENAZAS DDoS.* https://pro-cdo-web-resources.s3.eu-west-1.amazonaws.com/elevenpaths/uploads/2020/12/elevenpaths-informe-global-amenazas-ddos.pdf Pp. 7-14.

2. MARCO LEGAL APLICABLE AL SEGURO DE RIESGOS CIBERNÉTICOS

Para continuar con este estudio sobre el seguro de riesgos cibernéticos es necesario analizar en detalle el marco legal al que este tipo de seguro está sometido.

Con el propósito de comenzar este análisis es imprescindible iniciar por la ley principal para cualquier contrato de seguro, ya que se trata de una ley específica para regular este tipo de contratos, la Ley del Contrato de Seguro o LCS[28].

A pesar de que, en la Ley del Contrato de Seguro, de ahora en adelante "LCS", no se menciona específicamente el seguro de riesgos cibernéticos, al ser la ley que regula cualquier contrato de seguro también regula el seguro de ciberriesgos.

En primer lugar, las disposiciones generales ubicadas en el Título I de la LCS son de aplicación para el seguro de riesgos cibernéticos. Estas disposiciones engloban desde el artículo 1 hasta el artículo 24 de esta ley, en los que se regulan aspectos de una enorme importancia, tales como la definición de contrato de seguro[29], la nulidad[30], los requisitos formales de las cláusulas limitativas[31], aspectos formales de la póliza[32], los deberes de comunicación del siniestro[33] y de aminorar las consecuencias en caso de este[34] o disposiciones sobre la conclusión o la prórroga del contrato[35], entre otras[36].

Además de este Título I, entendiendo que el seguro de riesgos cibernéticos es un seguro contra daños, ya que se trata como se ha explicado anteriormente de un seguro que cubre

---

[28] Ley 50 de 1980. Contrato de Seguro. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[29] Ley 50 de 1980. Contrato de Seguro. Artículo 1. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[30] Ley 50 de 1980. Contrato de Seguro. Artículo 4. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[31] Ley 50 de 1980. Contrato de Seguro. Artículo 3. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[32] Ley 50 de 1980. Contrato de Seguro. Artículo 5. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[33] Ley 50 de 1980. Contrato de Seguro. Artículo 16. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[34] Ley 50 de 1980. Contrato de Seguro. Artículo 17. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[35] Ley 50 de 1980. Contrato de Seguro. Artículo 22. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[36] Arslanián Baggini, J.M. (2022). *LA LEGISLACIÓN DEL CONTRATO DE SEGURO EN ESPAÑA Y EN ALEMANIA. ANÁLISIS A LA LUZ DEL DERECHO COMPARADO.* http://dspace.umh.es/bitstream/11000/28392/1/TFG%20DERECHO-Arslani%c3%a1n%20Baggini%2c%20Juan%20Manuel.pdf Pp. 15-17.

los daños producidos por la utilización de redes informáticas[37], le será también de aplicación el Título II de la LCS, que regula el seguro contra daños. A modo de ejemplo, el enriquecimiento injusto[38], la suma asegurada como límite indemnizatorio por siniestro[39] o el sobreseguro[40] son materias de gran relevancia que se regulan en esta parte de la LCS.

Por consiguiente, la LCS es un cuerpo normativo de suma relevancia en el marco legal del contrato de seguro de ciberriesgos.

Asimismo, la ley de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras[41], de ahora en adelante "LOSSEAR", forma parte del marco normativo del seguro de riesgos cibernéticos, ubicándolo dentro de las ramos de seguros de no vida, o seguro distinto del seguro de vida en toda la normativa aplicable a estos, al cubrir dentro de la misma póliza riesgos sobre el mundo cibernético que abarcan distintas ramos de seguros[42], ya que como se explica en este mismo cuerpo normativo, cualquier aseguradora o reaseguradora con domicilio social en España queda sometida a esta ley[43].

En esta ley se regulan aspectos de gran importancia para cualquier tipo de seguro, como pueden ser las competencias de la Administración General del Estado, en su capítulo I[44], las condiciones de acceso a la actividad aseguradora y reaseguradora[45] o el capital de

[37] Toledano Jiménez, M.A. (2017). *¿Qué son los seguros de "ciberriesgos"?* https://doi.org/10.51302/ceflegal.2017.10543 Pp. 63-65.
[38] Ley 50 de 1980. Contrato de Seguro. Artículo 26. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[39] Ley 50 de 1980. Contrato de Seguro. Artículo 27. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[40] Ley 50 de 1980. Contrato de Seguro. Artículo 31. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[41] Ley 20 de 2015. de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. 15 de julio de 2015. España. https://www.boe.es/eli/es/l/2015/07/14/20/con
[42] Op. Cit. Toledano Jiménez, M.A.
[43] [43] Ley 20 de 2015. de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. Artículo 2. 15 de julio de 2015. España. https://www.boe.es/eli/es/l/2015/07/14/20/con
[44] [44] Ley 20 de 2015. de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. Artículos 16-18. 15 de julio de 2015. España. https://www.boe.es/eli/es/l/2015/07/14/20/con
[45] [45] Ley 20 de 2015. de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. Artículos 20 y 21. 15 de julio de 2015. España. https://www.boe.es/eli/es/l/2015/07/14/20/con

solvencia obligatorio[46] ,por mencionar algunos. La LOSSEAR es una ley fundamental para cualquier entidad aseguradora o reaseguradora con domicilio en España o que pretenda operar en España.

Adicionalmente, es necesario remarcar dentro del marco legal del contrato de seguro de riesgos cibernéticos el Código Civil Español[47], regulando de forma supletoria a las leyes específicas sobre el contrato de seguro en lo relacionado con obligaciones y contratos. A modo de ejemplo la buena fe[48], la fuerza de las obligaciones que nacen por los contratos[49] o la extinción de las obligaciones[50] se regulan en el Código Civil Español.

Por otra parte, es también fundamental mencionar el Reglamento General de Protección de Datos[51], cuerpo normativo que supone una revisión de las normas de protección de datos añadiendo nuevos requisitos a la seguridad de los datos personales y que impone sanciones elevadas a las empresas que lo incumplan, pudiendo alcanzar los 20 millones de euros, además del posible daño reputacional[52]. Este cuerpo normativo es realmente importante para el seguro de riesgos cibernéticos ya que este contiene coberturas que cubren el riesgo ante una posible filtración de datos o eventualmente el incumplimiento de esta normativa[53]. De igual manera que este reglamento europeo es importante la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales[54], o

---

[46] [46] Ley 20 de 2015. de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. Artículo 74. 15 de julio de 2015. España. https://www.boe.es/eli/es/l/2015/07/14/20/con

[47] Código Civil (CC). 25 de julio de 1889. España. https://www.boe.es/eli/es/rd/1889/07/24/(1)/con

[48] Código Civil (CC). Artículo 7. 25 de julio de 1889. España. https://www.boe.es/eli/es/rd/1889/07/24/(1)/con

[49] Código Civil (CC). Artículo 1091. 25 de julio de 1889. España. https://www.boe.es/eli/es/rd/1889/07/24/(1)/con

[50] Código Civil (CC). Artículo 1156. 25 de julio de 1889. España. https://www.boe.es/eli/es/rd/1889/07/24/(1)/con

[51] Reglamento 679 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. De 27 de abril de 2016. Unión Europea. https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[52] Agra Viforcos, B., Alonso Suárez, L., Álvarez Cuesta, H., Benlloch Domenech, C., Coelho Moreira, T., Durán Santomil, P., Fernández Domínguez, J.J., Fernández, J.J., Fernández López, S., Gallego Córcoles, I., Garrido Juncal, A., Gimeno Presa, M.C., Gomes Ramos, M.E., Hernández Rodríguez, F., Lado-Sestayo, R., Marongiu, D., Martínez Castaño, R., Martínez Pérez, M., Meléndez Alonso, G., … y Zapata Huamaní, G.M. García Novoa, C. y Santiago Iglesias, D. (Ed.). (2018). *4º REVOLUCÓN INDUSTRIAL: IMPACTO DE LA AUTOMATIZACIÓN Y LA INTELIGENCIA ARTIFICIAL EN LA SOCIEDAD Y LA ECONOMÍA DIGITAL.* Thomson Reuters. Pp. 165.

[53] INCIBE. (2023). *El riesgo ciber, máxima prioridad para pymes y autónomos.* https://www.incibe.es/empresas/blog/el-riesgo-ciber-maxima-prioridad-pymes-y-autonomos

[54] Ley Orgánica 3 de 2018. Protección de Datos Personales y garantía de los derechos digitales. De 6 de diciembre de 2018. España. https://www.boe.es/eli/es/lo/2018/12/05/3

LOPDPGDD, que adapta el ordenamiento jurídico español a la norma anteriormente citada.

En este mismo sentido, es necesario comentar la Directiva de la Unión Europea NIS2[55], que deroga a su vez la Directiva de la Unión Europea NIS, ya que se constató que no había sido eficaz para su propósito y que era necesario cambiarla por otra Directiva nueva. El objetivo de estas Directivas era imponer un estado común de ciberseguridad dentro de la Unión Europea en los operadores de determinados servicios esenciales y en los proveedores de servicios digitales. Ya que la primera Directiva no consiguió de manera suficiente este objetivo, la NIS2 realizó cambios significativos basándose en tres pilares fundamentales, i) la ampliación del ámbito de aplicación a otras entidades tanto públicas como privadas que desempeñen funciones importantes para la sociedad, ii) una mayor armonización en el ámbito de aplicación, en los requisitos de seguridad y en la notificación de incidentes, además de la ejecución por parte de los Estados Miembros de la Unión Europea del cumplimiento de esta normativa, ya que en la anterior Directiva se optó por dejar un alto grado de discrecionalidad a los Estados Miembros para la trasposición de la directiva y ese fue uno de los motivos de su fracaso. Y iii) aumentar la colaboración entre los diferentes Estados Miembros en cuanto a la ciberseguridad, asimismo como establecer un buen marco de gobernanza ante posibles incidentes o crisis relacionadas con el mundo cibernético. Esta Directiva tiene como límite para su trasposición por parte de los Estados Miembros el 17 de octubre de 2024[56].

Es relevante también dentro de este marco legal del seguro de riesgos cibernéticos el Código de Comercio de España[57], ya que a pesar de que la LCS deroga la sección dedicada exclusivamente al contrato de seguro de este código, tiene importancia como legislación supletoria además de tener tipificadas en él cuestiones relevantes como el

[55] Directiva de la Unión Europea 2555 de 2022. Medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. De 14 de diciembre de 2022. Unión Europea. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

[56] Barrio Andrés, M. (2024). *La ciberseguridad en el Derecho digital europeo: novedades de la Directiva NIS2.* InDret. https://indret.com/wp-content/uploads/2024/01/1838.pdf Pp. 509-512.

[57] Código de Comercio (C.Com). 22 de agosto de 1885. España. https://www.boe.es/eli/es/rd/1885/08/22/(1)/con

registro de las entidades de seguros en el registro mercantil[58] o cuestiones formales de las pólizas sobre su contenido[59].

De igual manera, es necesario nombrar la Ley General para la Defensa de los Consumidores y Usuarios o LGDCU[60] a la que quedan sometidas para su regulación las cláusulas del contrato de seguros, en especial las cláusulas generales que no se negocian individualmente, en el Título II de esta ley que trata sobre las condiciones generales y las cláusulas abusivas de los contratos. Este sometimiento está reflejado en la LCS[61].

Finalmente, para cerrar el análisis del marco legal de este tipo de seguro, se tienen que mencionar tanto el Reglamento DORA[62], que pretende unificar las directrices relativas a la ciberseguridad en el sector financiero y asegurador, ya que estaban dispersos por diferentes cuerpos normativos[63], como el Código de Buen Gobierno de la Ciberseguridad (CBGC)[64] de la Comisión Nacional del Mercado de Valores (CNMV).

3. ESTUDIO JURÍDICO DEL CONTRATO TÍPICO DEL SEGURO DE RIESGOS CIBERNÉTICOS

Una vez realizada ya la introducción general al mundo de los ciberataques y el seguro de riesgos cibernéticos y ya realizado el análisis del marco legal de este tipo de seguro, se va a realizar un estudio primero de las características típicas del contrato de seguro en general, para después centrarse en las especialidades del seguro de riesgos cibernéticos y finalmente analizar y discutir sobre dos de estas características especiales que crean controversia en la actualidad.

---

[58] Código de Comercio (C.Com). Artículo 16. 22 de agosto de 1885. España. https://www.boe.es/eli/es/rd/1885/08/22/(1)/con

[59] Código de Comercio (C.Com). Artículo 107. 22 de agosto de 1885. España. https://www.boe.es/eli/es/rd/1885/08/22/(1)/con

[60] Real Decreto Legislativo 1 de 2007. Aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. De 30 de noviembre de 2007. https://www.boe.es/eli/es/rdlg/2007/11/16/1/con

[61] Op. Cit. LCS Artículo 3.

[62] Reglamento de la Unión Europea 2554 de 2022. La resiliencia operativa digital del sector financiero. 27 de diciembre de 2022. Unión Europea. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962

[63] Op. Cit. AON (2023) Pp. 5.

[64] Almigorena Eguiluz, R., Baratta Martínez, R., Benido Gómez, M.J., Cornago Baratech, J.F., Domínguez Fernández-Burgos, A., García Quiniela, J., Largacha Lamela, D., Mateo Murillo, I., del Olmo Fons, F., Paredes Hernández, L., Perea Velasco, J., Ramírez Sánchez, O., Ramos García, A., Sánchez López, J., Viana Lara, A. y Vivancos Cerezo, M.E. (2023). D´Antonio, G. y Ruiz Vázquez, A.J. (Ed.) *CÓDIGO DE BUEN GOBIERNO DE LA CIBERSEGURIDAD.* https://www.cnmv.es/DocPortal/Ciberseguridad/CBG_Ciberseguridad.pdf

3.1. Características típicas del contrato de seguro

La definición del contrato de seguros es: "El contrato de seguro es aquel por el que el asegurador se obliga, mediante el cobro de una prima y para el caso de que se produzca el evento cuyo riesgo es objeto de cobertura a indemnizar, dentro de los límites pactados, el daño producido al asegurado o a satisfacer un capital, una renta u otras prestaciones convenidas."[65]

Para comenzar con el análisis de las características del contrato de seguro, es primordial realizar previamente un inciso en los diferentes componentes del seguro, explicando tanto las partes presentes en este tipo de contratos como los elementos del seguro.

Por un lado, las partes del contrato de seguros son;

i) el tomador del seguro, que es quién realiza el pago de la prima y a través de este desplaza el riesgo asegurado a la esfera patrimonial del asegurador, es quién firma el contrato, a quién le corresponden las obligaciones derivadas del contrato (el pago de la prima) y quién posee el derecho de rescisión según lo acordado.
ii) El asegurador, es quién recibe el pago de la prima y a su vez quién asume el riesgo por el que se realiza el contrato, teniendo que asumir este la indemnización correspondiente establecida en el contrato en caso de que el riesgo se materialice y también tiene el derecho de rescisión según lo acordado en el contrato.
iii) El asegurado, que es la parte titular del interés asegurado objeto del contrato de seguro.
iv) El beneficiario, que es la parte a la que le corresponde el derecho a la indemnización o prestación pactada en el contrato en caso de que se consuma el riesgo asegurado[66].

Por otro lado, algunos elementos del contrato de seguro son:

i) La prima, es la prestación que realiza el tomador del seguro al asegurador a cambio de la asunción del riesgo. Se suele pagar periódicamente, el período se

[65] Op. Cit. LCS Artículo 1.
[66] Fundación Area XXI. (S.F.). *ELEMENTOS DEL CONTRATO DE SEGURO.* https://fundacionarea-xxi.com/6-elementos-del-contrato-de-seguro/

acuerda en el contrato. El importe de esta depende del riesgo que asume el asegurador con el contrato de seguro[67]

ii) La franquicia, es la suma que le corresponde pagar al beneficiario en caso de que un siniestro ocurra, es decir, una vez ocurre el siniestro y se calcula la indemnización, es la cantidad que no corre a cuenta del asegurador y por lo tanto se resta de la indemnización total que recibirá el beneficiario. El importe de la franquicia se acuerda en la perfección del contrato de seguro y esta puede ser 0. El sentido de la franquicia se entiende en el marco de la colaboración entre las distintas partes del contrato de seguro para cuidar el bien[68].

iii) El interés asegurable y el interés asegurado: el interés asegurable es el interés de quién pretende contratar una póliza en cubrir ese riesgo como objeto del contrato[69], mientras que el interés asegurado es el interés económico entre la parte que contrata el seguro y el objeto o persona asegurada[70].

iv) Suma asegurada, es el alcance de la cobertura, es decir, el límite máximo de indemnización si se llega a producir el siniestro sobre lo asegurado[71].

v) El siniestro, es la materialización del evento o circunstancia que se había asegurado mediante el contrato de seguros y que da lugar, según lo acordado y atendiendo a las circunstancias que lo rodeen, a la indemnización correspondiente[72].

vi) El riesgo, es la probabilidad de que ocurra el suceso cuya aparición real está cubierta por la póliza mediante el contrato de seguro[73].

vii) La póliza, es el documento por el cual se formalizan los contratos de seguro, en ella se encuentran las diferentes coberturas, condiciones, exclusiones y obligaciones que se acuerdan mediante el contrato de seguro[74].

---

[67] Martínez, D. (s.f.) *La Prima del Seguro: Todo lo que debes saber sobre este factor clave en tus finanzas.* iNEF. https://inef.es/seguros-y-proteccion-financiera/la-prima-del-seguro

[68] Allianz. (s.f) *¿Qué es una franquicia en un seguro?.* https://www.allianz.com.ar/blog-allianz/franquicia.html

[69] Diccionario Panhispánico del Español Jurídico. (2023). *Interés asegurable.* https://dpej.rae.es/lema/inter%C3%A9s-asegurable

[70] Diccionario Panhispánico del Español Jurídico. (2023). *Interés asegurado.* https://dpej.rae.es/lema/inter%C3%A9s-asegurado

[71] Ley 50 de 1980. Contrato de Seguro. Artículo 8. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

[72] Veiga Copo, A.B. (2010). *La temporalidad en el contrato de seguro. Riesgo y siniestro: una ecuación interesadamente compleja.* Pp. 35-37.

[73] Fundación Mapfre. (s.f.) *Diccionario de seguros. Riesgo.* https://www.fundacionmapfre.org/publicaciones/diccionario-mapfre-seguros/riesgo/

[74] Gomis Palau, A. (2021). *Póliza.* https://www.autorizadored.es/finanzas/poliza/

viii) La fecha de efecto, que es una parte de suma relevancia del contrato de seguro, ya que muestra el momento en el que se despliegan los efectos de este contrato, se encuentra en la póliza[75]

Una vez ya presentados estos elementos básicos del seguro, procede analizar las características típicas del contrato de seguro.

El seguro es un contrato consensual debido a que para su perfeccionamiento es necesario el consentimiento de ambas partes, pero a su vez tiene partes de contrato de adhesión, ya que el tomador se adhiere a las condiciones generales de los contratos de seguros[76], exceptuando algunos tipos de contratos de seguro como el seguro de grandes riesgos que tienen una mayor capacidad negociadora y autonomía de la voluntad y no esta característica de adhesión[77].

Además, la bilateralidad es una característica básica del contrato de seguros ya que crea obligaciones para las partes del contrato como puede ser por ejemplo por parte del tomador la obligatoriedad del pago de la prima y por parte del asegurador el pago de la indemnización correspondiente en el caso de que ocurra un siniestro bajo el bien o la persona asegurada[78]

También se caracteriza por ser un contrato oneroso, como se puede deducir de las obligaciones mencionadas *up supra,* ya que el pago de la prima o el de la indemnización suponen una onerosidad. Es así ya que de no existir esta onerosidad el seguro carecería de sentido ya que no es lógico exponerte a un riesgo en tu esfera patrimonial sin contraprestación, como tampoco lo es realizar el pago de la prima sin la existencia del pago de una eventual indemnización.

---

[75] Reale Seguros. (2019). *Fecha de efecto.* https://blog.reale.es/diccionario-de-seguros/fecha-efecto/

[76] Martínez Ortiz, P.J. (2021). *BUENA FE Y CONSENSUALIDAD CONTRACTUAL. ANTECEDENTES EN DERECHO ROMANO E IRRADIACIÓN EN DERECHO VIGENTE RESPECTO DEL CONTRATO DE SEGURO. ANÁLISIS LEGISLATIVO, DOCTRINAL Y JURISPRUDENCIAL.* http://espacio.uned.es/fez/eserv/bibliuned:grado-Derecho-DR-Pjmartinez/Martinez_Ortiz_Pedro_Jose_TFG.pdf

[77] Burguera Abogados. (2019). *Contrato de seguro de grandes riesgos y principio de autonomía de la voluntad*. https://www.burgueraabogados.com/contrato-seguro-grandes-riesgos-principio-autonomia-voluntad/ Hispacolex. (2014). *No se puede considerar al contrato de seguro de grandes riesgos como contrato de adhesión.* https://www.hispacolex.com/biblioteca/articulos-doctrinales/contrato-de-seguro-grandes-riesgos/

[78] Ibarra, M.B. (2017). *La peculiaridad de la adhesión en el contrato de seguro.* https://doi.org/10.18272/lr.v4i1.986 Pp.90-94.

El contrato de seguro de manera imperativa debe de realizarse por escrito, como se especifica en la LCS[79].

Asimismo, el contrato de seguro se trata de un contrato aleatorio, ya que en el momento de la celebración del contrato las partes no saben el importe que finalmente van a recibir o pagar a raíz de este, ya que depende de una cuestión de azar que ocurran o no siniestros que den lugar al pago de indemnizaciones[80].

Por último, el contrato de seguro es un contrato de tracto sucesivo en el que rige la buena fe. Es de tracto sucesivo ya que los efectos del contrato hacen efecto a lo largo de toda la duración del contrato, debido a que de haber varios siniestros en el periodo de vigencia de la póliza se tendrán que ir indemnizando correspondientemente[81]. Se rige por la buena fe como establece el código civil para cualquier tipo de contrato[82]. Este principio de buena fe es imprescindible en el seguro, como se refleja en la jurisprudencia, por ejemplo, "dadas las peculiaridades del contrato de seguro, que exige al máximo la concurrencia de la buena fe"[83] o "Se trata de una nulidad imperativa que priva a la relación de su propia eficacia, ya que la misma se formalizó basándose en la manifestación de los recurrentes de que no había habido siniestro alguno en el período contratado de retroacción, con lo que se vino a faltar a la buena fe, que resulta máxima en los contratos de seguro y obliga al tomador a informar del modo más exacto y veraz de la situación del riesgo amparado, es decir debe participar todo y cuanto sabe."[84]

[79] Op. Cit. LCS artículo 5.
[80] Álvarez Vigaray, R. (1968). *Los contratos aleatorios.* *https://dialnet.unirioja.es/servlet/articulo?codigo=2048496* Pp. 611-614
[81] Aguirre y Baeza. (2018). *El Contrato de Seguro y sus Características Esenciales.* https://www.aguirrebaeza.com/blog/el-contrato-de-seguro-y-sus-caracteristicas-esenciales/
[82] Código Civil (CC). Artículo 1258. 25 de julio de 1889. España. https://www.boe.es/eli/es/rd/1889/07/24/(1)/con
[83] STS de 14 de junio de 2002 (RJ 3847/1996)
[84] STS de 22 de diciembre de 2001 (RJ 2679/1996)

3.2. Especialidades del contrato de seguro de riesgos cibernéticos.

El objeto del seguro de riesgos cibernéticos es cubrir el riesgo de los daños eventuales causados en el marco de la utilización de las redes cibernéticas.

Dado las especialidades de este campo, que ya se han comentado a lo largo de este estudio, el seguro de riesgos cibernéticos presenta una serie de especialidades que se van a analizar a continuación.

En el seguro de riesgos cibernéticos están presentes todos los elementos generales del seguro que se exponen *up supra*, en este caso el seguro está orientado mayoritariamente a empresas y muy rara vez no coinciden en la empresa tomadora las figuras del beneficiario y el asegurado.

Asimismo, este contrato es oneroso, consensual con su parte de adhesión, bilateral, por escrito, aleatorio, de tracto sucesivo y regido por la buena fe cumpliendo con las características principales del contrato de seguro.

Las principales especialidades que encontramos en este seguro se materializan en las coberturas y las exclusiones que las pólizas de seguro de ciberriesgos contienen.

Por un lado, es necesario profundizar en las coberturas que más frecuentemente se ofrecen mediante este seguro, que se pueden dividir en cuatro grupos; a) coberturas de daños propios, b) coberturas de responsabilidad civil y c) servicios adicionales[85].

a) Dentro de las coberturas de daños propios, se encuentran las coberturas cuya finalidad es cubrir los daños sufridos en la empresa en caso de un incidente cibernético. Algunas coberturas de este tipo son:

i) La cobertura por daños en los sistemas informáticos del asegurado, que suele incluir; los costes de reparación de los equipos informáticos y de recuperación de los datos del asegurado, lo cual consiste en los costes derivados de limpiar los dispositivos infectados de las consecuencias del incidente cibernético y la búsqueda, recuperación o restauración de los datos dañados por este. Asimismo, también suelen entrar bajo esta cobertura los costes de restauración del control de acceso.

[85] García Marcén, G. (2019). *Contratación de la póliza de Ciberriesgos, tratamiento del siniestro y la importancia del reaseguro*. http://hdl.handle.net/2445/144759 Pp. 50-58.

ii) La cobertura por la interrupción del negocio, que consiste en la indemnización por el lucro cesante que el asegurado ha experimentado a causa del incidente, es decir, lo que el asegurado ha perdido debido a la eventual paralización parcial o global de su actividad a consecuencia de un incidente cubierto por la póliza.

iii) La cobertura por extorsión cibernética, mediante la cual se cubren los gastos y costes derivados de una extorsión cibernética con el fin de proteger los sistemas informáticos del asegurado.

iv) Cobertura por fraude cibernético, bajo la cual estarían cubiertos los daños financieros sufridos por el asegurado debido a, por ejemplo, una suplantación de identidad debido a un incidente cibernético, o un robo de dinero mediante un ataque cibernético.

v) Las coberturas que cubren eventuales infracciones o sanciones a las normativas de protección de datos, recibidas por parte de la Agencia Española de Protección de Datos o AEPD, o cualquier autoridad de control equivalente. Suelen estar bajo esta cobertura tanto la multa o infracción impuesta como los gastos de restitución de imagen por la sanción impuesta.

b) Las coberturas de responsabilidad civil; estas cubren los daños producidos a otros que sean responsabilidad del asegurado a causa de un incidente cibernético. El ejemplo más claro de estos son los daños producidos a otros a causa de un robo pérdida o revelación de información confidencial o personal que custodiaba el asegurado y por lo tanto estaba bajo su responsabilidad. En estos casos, estarían cubiertos tanto los daños producidos como las indemnizaciones correspondientes a terceros. Además, también es posible que se encuentren bajo esta cobertura los daños ocasionados a terceros debido a la seguridad de la red que sean responsabilidad legal del asegurado, como puede ser la paralización de negocio a terceros.

c) Servicios adicionales. Es muy común que en las pólizas de riesgos cibernéticos se encuentren coberturas dedicadas a cubrir los gastos de diferentes especialistas derivados de un ataque cibernético, algunos ejemplos de estos son:

i) Los gastos de defensa, que están incluidos normalmente bajo los seguros e incluyen los gastos derivados de la defensa del asegurado debido al siniestro cubierto bajo la póliza.

ii) Los gastos derivados de la gestión del incidente. Estos son los gastos derivados de un equipo de respuesta para la gestión del incidente que actúe desde el momento en el que se notifica el incidente sufrido, con los equipos técnicos tanto

forenses para analizar el posible incidente e intentar aminorar el impacto de este, como legales en cuánto a la activación o no de la cobertura y las posibles implicaciones de protección de datos derivadas del incidente.

iii) Los gastos de profesionales derivados al análisis del cumplimiento de la Ley de Protección de Datos también pueden estar cubiertos bajo este seguro.

iv) Los gastos por la realización de comunicaciones y notificación del siniestro, tanto a la AEPD o organismo rector correspondiente como a los posibles afectados por el incidente.

v) Los gastos por la contratación de técnicos que analicen el estado de la infraestructura del asegurado a fin de detectar posibles vulnerabilidades en la red del asegurado que hayan podido desencadenar el incidente y para que realicen recomendaciones a este para evitar posibles futuros incidentes.

vi) Los gastos de peritaje para evaluar los daños producidos por el incidente también suelen estar cubiertos por el seguro.

vii) Los gastos por la contratación de profesionales que analicen posibles infracciones de la propiedad intelectual derivado de un incidente cibernético.

Todas estas coberturas expuestas pueden incluirse o no en la póliza de ciberriesgo, además de tener un límite específico por cobertura o atenerse al límite de la suma asegurada, todas estas cuestiones dependen de cada póliza y de la negociación entre el asegurado y el asegurador[86].

Por otro lado, para completar este análisis es obligatorio hablar sobre algunas de las exclusiones que se incluyen de manera más frecuente en el seguro de riesgos cibernéticos y que son especiales de este.

[86] Mapfre. (s.f.) *CIBERRIESGOS PYME Y AUTÓNOMOS.* https://www.ciberseguros.com/condiciones/CondicionesGeneralesCiberseguroMapfre.pdf Chubb. (2018). *Póliza para la Gestión de Riesgos Cibernéticos*. https://www.chubb.com/content/dam/chubb-sites/chubb-com/latam-microsites/factsheet-cyber.pdf Instituto de Crédito Oficial. (2021). *PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SEGURO DE RIESGOS CIBERNETICOS DEL INSTITUTO DE CRÉDITO OFICIAL, ENTIDAD PÚBLICA EMPRESARIAL EN PROCEDIMIENTO ABIERTO SIMPLIFICADO.* https://contrataciondelestado.es/wps/wcm/connect/c315d0fb-36d2-4b24-84ce-84aa05011428/DOC20210907101335PPT+Plataforma.pdf?MOD=AJPERES BLB Asociados. (s.f.) *Seguro de Ciberriesgos*. https://www.blbcorreduria.com/wp-content/uploads/2021/02/BLB-DOSSIER-Seguro-de-Ciberriesgos.pdf Op. Cit. García Marcén, G. Op. Cit. Toledano Jiménez, M.A.

Las pólizas de seguro de ciberriesgos contienen exclusiones que son comunes a muchos otros tipos de seguro, pero existen algunas específicas a este debido a su relación con el mundo cibernético y con el riesgo asegurado bajo estas pólizas.

Una de ellas es la exclusión de guerra cibernética, la cual solo se menciona en este apartado debido a que se va a realizar un análisis más profundo en los próximos.

Además, una exclusión que se puede encontrar en este tipo de seguros es la exclusión de reclamaciones derivadas del uso de aplicaciones o software sin licencia, de forma ilegal o en periodo de prueba o de desarrollo, esta exclusión suele abarcar tanto las reclamaciones relacionadas con sanciones por el uso de estas aplicaciones o softwares, como los incidentes cibernéticos sufridos por el asegurado a causa de estas. El motivo de esta exclusión es, además del incumplimiento de normas legales en su utilización, que aumentan exponencialmente la exposición de la infraestructura cibernética a virus y malwares que puedan infectar los sistemas cibernéticos y dar lugar a un siniestro[87].

También es muy común la exclusión de daños materiales o personales de cualquier tipo, aunque estos daños materiales sean sobre elementos de la red que puedan producir daños a la infraestructura cibernética del asegurado y eventualmente deriven a la paralización del negocio. Esto es debido a que el objeto del seguro de riesgos cibernéticos es cubrir el riesgo ante posibles amenazas en la utilización de las redes cibernéticas, no el cubrir la infraestructura cibernética del asegurado de cualquier daño, por lo tanto, los daños de este tipo no entran dentro del objeto de este seguro[88].

Igualmente, la exclusión por falta de diligencia de los sistemas cibernéticos es una exclusión especial del seguro de ciberriesgos. Esta excluye la cobertura de los incidentes cibernéticos que se hayan producido por la falta de diligencia al no actualizar, corregir o adaptar los sistemas defectuosos, siempre y cuando la falta de diligencia sea manifiesta por el conocimiento y el tiempo suficientes como para evitarlo[89]

Para finalizar, habitualmente las reclamaciones derivadas de incidentes cibernéticos causados por un fallo de programación del software están excluidas también. Esto abarca

[87] Vadillo Asesores. (2021). *¿Cuáles son los riesgos al usar un software sin licencia o software pirata?.* https://www.grupovadillo.com/cuales-son-los-riesgos-al-usar-un-software-sin-licencia-o-software-pirata/
[88] Op. Cit. Mapfre. *CIBERRIESGOS PYME Y AUTÓNOMOS.*
[89] Op. Cit. Instituto de Crédito Oficial. (2021).

únicamente fallos del sistema debidos a que en la programación del software que se utilice han existido fallos y consecuentemente de esto el sistema cibernético falle[90].

De igual manera que con las coberturas, estas exclusiones pueden estar presentes o no en las diferentes pólizas de riesgo cibernético, no es imperativo que aparezcan todas, depende de la voluntad de las partes y de la negociación entre asegurador y aseguradora, pero suelen estar presentes por los motivos mencionados en su análisis.

3.3. Exclusión por guerra cibernética o "ciberguerra"

La exclusión por guerra cibernética o "ciberguerra" es una exclusión especial del seguro de riesgos cibernéticos que actualmente plantea discusiones en el sector del seguro debido a su ámbito de aplicación.

La exclusión por guerra es una cláusula común de los seguros, tipificada en la misma LCS[91], debido al riesgo inesperado y desmesurado que esta supone. En la cláusula de exclusión por guerra no cabe lugar a dudas en cuanto a su ámbito de aplicación, ya que media un conflicto armado en el lugar donde se encuentra el bien asegurado, pero en la guerra cibernética esta claridad no está presente.

Los ataques Estado-Nación han constituido los ciberataques más dañinos en los últimos tiempos. Estos ciberataques consisten en grupos militares de los estados o en grupos de hackers mercenarios privados que contratan las agencias militares para atacar las infraestructuras básicas de otros países con fines políticos o económicos principalmente.

Los Estados más relacionados con este tipo de ataques son: i) China, que se caracteriza por ciberataques masivos para el robo de información con secretos comerciales y de propiedad intelectual. Además, es popularmente conocido el control del acceso a internet que ejerce el gobierno chino a su población, lo cual le sirve de defensa ante estos ataques. ii) Rusia, en este caso se caracterizan más por la contratación de grupos privados para la realización de estos ataques. El estado ruso se ha especializado mucho en este ámbito ya que sospecha que la clave de las guerras del futuro van a ser estos medios y con la guerra de Ucrania los ataques de este tipo se han incrementado enormemente en occidente. iii) Otros países como Irán y Corea del Norte también se caracterizan por utilizar este tipo

[90] Op. Cit. García Marcén, G.
[91] Ley 50 de 1980. Contrato de Seguro. Artículo 44. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

de ataques para debilitar a sus principales enemigos, en el caso de Corea del Norte se centran en Corea del Sur y Estados Unidos y en el caso de Irán sus ataques más conocidos son contra Arabia Saudí. Asimismo, en estos países el acceso a internet es muy limitado, por lo que también están muy protegidos en este sentido[92].

Estos ataques no solo van dirigidos a los gobiernos de los estados o a las instituciones públicas, sino que también pueden ir dirigidos a cualquier empresa privada, ya que el fin principal de estos ataques es desestabilizar a los países enemigos y el robo de información para el beneficio de los estados atacantes y sus empresas, como se puede evidenciar en lo expuesto sobre China sobre los robos de información comercial y propiedad intelectual.

Por lo que el verdadero conflicto en cuanto al seguro de riesgos cibernéticos se refiere, es la identificación del ámbito de aplicación de la póliza que en este apartado se analiza, puesto que, cuando un ciberataque de estas características es realizado por los cuerpos oficiales o en nombre de un Estado concreto es más obvia la aplicación de esta exclusión, pero cuando el ataque es perpetrado por un grupo privado de individuos la duda de si se puede aplicar o no crece exponencialmente.

La cuestión relevante en este punto es expresar de manera clara ante que circunstancias se puede aplicar esta cláusula de exclusión que produciría la no cobertura del siniestro ocurrido por parte de la aseguradora.

Además, estos son los ataques más frecuentes, ya que rara vez un Estado realiza estos ataques con sus grupos militares públicos y reivindica el ataque, por lo que es necesario delimitar cuando se puede aplicar esta exclusión y cuando no.

El mayor problema es caer en la generalización, ya que si se aplica la solución de que cualquier ataque realizado por un grupo de hackers proveniente de determinados países será siempre un ataque de "ciberguerra" que dé lugar a la aplicación de esta cláusula de exclusión, el ámbito de aplicación de esta sería demasiado amplio, pero si únicamente se limita a los ataques perpetrados por los servicios públicos de un país y a nombre de este se estaría limitando demasiado y dejando fuera del ámbito de esta cláusula siniestros producidos por grupos privados que se han realizado con los propósitos cuyo riesgo

[92] Puyol Montero, J. y Delgado Caravilla, E. (2018) *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea*. Epígrafe 4: *Los riesgos, las amenazas y las medidas técnicas con relación a los tratamientos de datos de carácter personal*. Tirant Lo Blanch.

pretende dejar de cubrir esta cláusula de exclusión, es imprescindible encontrar una solución en un punto medio.

Y en este sentido se ha posicionado la jefa de ciberseguridad de Reino Unido, que en unas declaraciones del año pasado expresaba su preocupación por la situación actual del seguro y la necesidad de proporcionar un marco diseñado específicamente para el riesgo único de la ciberseguridad, con unos límites de cobertura bien definidos en este aspecto para ofrecer una estabilidad para los potenciales clientes y para los asegurados de estas pólizas y así proporcionar una sostenibilidad necesaria al mercado del seguro cibernético[93].

Esta falta de claridad en la delimitación del ámbito de aplicación de la cláusula de exclusión por guerra cibernética está provocando que las grandes aseguradoras abusen de la utilización de esta exclusión, dejando de cubrir numerosos siniestros por estar relacionados con grupos de ciertos países y por creer que por las características el siniestro puede tratarse de un ataque de este tipo, lo cual está conllevando una gran cantidad de reclamaciones judiciales y desestabilidad en el seguro de riesgos cibernéticos, más aun teniendo en cuenta la situación de alta tensión geopolítica mundial[94].

Bajo este contexto, el mercado de seguros y reaseguros de Lloyd´s, se ha visto en la obligación de redactar cuatro modelos diferentes de cláusulas de exclusión por guerra cibernética, delimitando más concretamente el ámbito de aplicación de esta y especificando en todas ellas que el encargado de probar que es conveniente la aplicación de esta exclusión para cada siniestro en concreto es del asegurador, es decir, pone la carga de la prueba en el asegurador[95].

En mi opinión, mientras las aseguradoras no definan bien la aplicación de esta exclusión en sus pólizas deberá siempre interpretarse en favor del asegurado, seguido el principio general de *in dubio pro asegurado*, el cual rige que en el caso de que debido al contenido de la cláusula de una póliza de seguros esta permita varias interpretaciones se optará por la más beneficiosa para el asegurado. Este principio se basa en el artículo 1288 del CC que tipifica que la interpretación de cláusulas oscuras de un contrato no deberá favorecer

[93] Howden. (2023). *Las primas de seguros cibernéticos podrían superar los 50 mil millones de dólares para el año 2030*. https://www.howdengroup.com/es-es/informe-cyber

[94] Satariano, A. & Perlroth, N. (2019) *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.* New York Times. https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html

[95] Davidson, P. (2021). *Cyber War and Cyber Operation Exclusion Clauses.* Lloyd´s Market Association Bulletin. https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx

a la parte que ha provocado la oscuridad[96], por lo tanto, si el asegurador es la parte que provoca la oscuridad ya que es la parte que redacta la póliza, la interpretación deberá favorecer al asegurado. Este es un principio frecuentemente utilizado en la jurisprudencia, por ejemplo: "falta de inclusión en el contrato del supuesto de invalidez permanente y parcial: «in dubio pro asegurado»: indemnización por el baremo más elevado aplicando el porcentaje del 60%."[97] o "llega a esta conclusión a través de determinados documentos, en consonancia con la abundante doctrina jurisprudencial de que las dudas que puedan surgir en las relaciones dimanantes del contrato de seguro deben ser resueltas aplicando el principio « in dubio pro asegurado"[98].

Este principio es clave para la situación actual del conflicto en cuánto al ámbito de aplicación de esta exclusión del seguro de riesgos cibernéticos, ya que al ser el asegurador el encargado de redactar la cláusula concreta en las pólizas que ofrece a sus aseguradores, si no deja especificado y claro los sujetos ante los que pretende que se aplique produciendo oscuridad ante determinadas circunstancias, es responsabilidad suya y es la parte que debería probar que estos determinados supuestos estarían dentro de lo especificado en la definición de la cláusula en la póliza sin dejar lugar a dudas interpretativas o, en caso contrario, asumir las consecuencias del siniestro.

Por consiguiente y atendiendo a lo expuesto *up supra*, hasta que no se defina bien esta cláusula de exclusión, proporcionando claridad en cuanto a la descripción de los supuestos que se pretenden excluir los eventuales siniestros de la cobertura bajo la póliza, delimitando de esta manera la interpretación de esta y eliminando la oscuridad presente, la cuestión de si se aplica o no en los casos en los que existan dudas sobre su aplicación debería interpretarse siempre en favor del asegurado.

[96] Código Civil (CC). Artículo 1288. 25 de julio de 1889. España. https://www.boe.es/eli/es/rd/1889/07/24/(1)/con
[97] STS de 4 de diciembre de 2000 (RJ 2000/9327)
[98] STS de 8 de febrero de 1999 (RJ 1999/337)

3.4. Obligación de implementar las medidas de mitigación

La obligación de implementar las medidas de mitigación recomendadas por el asegurador es una obligación común para los diferentes tipos de seguros. Se justifica por la obligación que tiene el asegurado de reducir el riesgo de que ocurra un siniestro siguiendo los principios de la buena fe que ya se han expuesto en este estudio. En concreto este análisis se va a centrar en la aplicación de esta obligación en los seguros de riesgos cibernéticos y en la posibilidad de los aseguradores de rechazar la cobertura de un eventual siniestro por el incumplimiento de esta obligación por parte del asegurado.

El art. 17 párrafo primero LCS establece la obligación del asegurado o del tomador de adoptar las medidas necesarias para aminorar las consecuencias del siniestro o disminuir el daño que éste pueda producir[99].

En el seguro de riesgos cibernéticos, estas medidas de mitigación suelen ser propuestas por el equipo técnico forense tras un siniestro, que posteriormente de analizar las posibles causas de este y vulnerabilidades existentes en los sistemas informáticos del asegurado, propone las medidas que considere pertinentes.

Por lo tanto, el conflicto a tratar en este estudio es si los aseguradores tienen la posibilidad de no cubrir un eventual siniestro justificándose en el incumplimiento del asegurado de la obligación de implementar las medidas de mitigación, y en caso afirmativo cuando sería esto posible y en qué proporción.

Algunas de las medidas más comunes en el seguro de ciberriesgos son: i) el cambio de todas las contraseñas de las cuentas que pertenezcan al dominio que ha sufrido el siniestro, con el fin de que, si el atacante que ha producido el siniestro ha obtenido las contraseñas en su acceso a los sistemas filtrando estos datos, proteger al asegurando evitando que puedan seguir accediendo a los sistemas a través de las contraseñas que corren peligro de haber sido filtradas. ii) la implementación del doble factor de autenticación o 2FA, que protege los sistemas del asegurado blindando el acceso a estos como medida de seguridad adicional a la contraseña, dificultando exponencialmente a los posibles atacantes el acceso a las cuentas. iii) La implementación de una confirmación por una segunda vía antes de realizar un pago, para así evitar las suplantaciones de identidad, un claro ejemplo

[99] Ley 50 de 1980. Contrato de Seguro. Artículo 17. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

de esto sería la llegada de un correo con la dirección legítima de un proveedor cambiando la cuenta a la que quiere que el asegurado le haga la transferencia por sus servicios, en caso de ser una suplantación de identidad si se implementa una segunda vía de confirmación como una llamada telefónica con un número de contacto se evitaría el siniestro[100].

Este deber de salvamento surge una vez se ha producido el siniestro. Por lo tanto, no lo podemos relacionar con la prevención del mismo. Las medidas de prevención, que no obligan al asegurado a un deber específico, aunque indirectamente si le exigen un determinado comportamiento, se originan antes de la producción del siniestro e incluso antes del aseguramiento del riesgo:

"por otra parte, en dicha sentencia recurrida se hace mención de la obligación del asegurado de aminorar las consecuencias del siniestro, que establece el artículo 17 de la misma ley, que igualmente ha infringido, pues éste contempla el deber de disminuir las consecuencias del siniestro, que no se debe confundir con el de prevención del mismo, que implica una conducta pasiva no constitutiva de actividad específica de evitar el riesgo, que no existe como deber concreto impuesto por ley al asegurado"[101]

No hay que olvidar que el contrato de seguro se desarrolla en la órbita del principio de buena fe contractual entre las partes. Por eso, con base en el mismo, se podría argumentar que el asegurado tiene la obligación de adoptar las medidas necesarias para mantener el riesgo en buen estado, más aun teniendo en cuenta que los aseguradores indican las concretas medidas que debes adoptar para reducir el riesgo y luego exigen la confirmación de la implementación.

Según la doctrina, debemos distinguir entre siniestro y daño, siendo el segundo una consecuencia del primero, ya que el deber de aminorar las consecuencias del siniestro se despliega respecto del daño, una vez que se ha producido el siniestro. Es decir, estamos a un deber claramente *ex post* y no *ex ante*.

Ahora bien, en el eventual supuesto de que quedase acreditada la unidad de siniestro entre ambos incidentes, cabrían más posibilidades por parte del asegurador de rechazar la cobertura del siniestro o aminorar sustancialmente la prestación económica, ya que se

[100] Incibe. (s.f.) *Autenticación de dos factores (2FA).* *https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores*
[101] STS de 2 de abril de 2009 (RJ 2009/1754)

estaría produciendo un claro incumplimiento por parte del asegurado de la obligación *ex post* a la que se encuentra vinculado por el art. 17 LCS.

A modo de ejemplo, se va a analizar un asunto relacionado con esta problemática con una conclusión muy relevante para esta discusión.

En un asunto industrial, el perito del asegurador, tras un incendio, tasó los daños en 100.000 euros aproximadamente y advirtió al asegurador sobre la necesidad de *"efectuar una estructura ligera para evitar que las lluvias o posibles nieves afecten al resto de viviendas"* y, pasados unos meses, se acabó hundiendo la nave, ascendiendo los daños a cerca de 400.000 euros, lo cual acabó iniciando un proceso judicial debido a que el asegurador solo cubrió los primeros 100.000 euros. Finalmente, el tribunal supremo esgrimió la siguiente postura:

"También ha señalado la doctrina científica que el deber impuesto al asegurado en el art. 17 LCS es una exigencia del principio de buena fe que domina el contrato de seguro, como asimismo razona la sentencia impugnada. De esto se sigue, en relación con lo antedicho sobre las facultades del asegurador de dar instrucciones al asegurado, que ambos deben colaborar lealmente en evitar que los daños aumenten tras el siniestro por causas que no sean el siniestro mismo.

De aplicar las anteriores consideraciones a los hechos que la sentencia recurrida declara probados resulta que no fue el asegurado, sino la aseguradora ahora recurrente, quien faltó a ese principio de leal colaboración impuesto por la buena fe y , además, por su propia dedicación profesional: primero, porque nadie advirtió al asegurado sobre la necesidad de dotar al edificio de una estructura provisional para evitar su deterioro por las inclemencias del tiempo, pese a que la aseguradora, por medio de su perito, era consciente, o debió serlo, de esa necesidad; y segundo, porque la sentencia recurrida declara probado que la ejecución de esa obra no estaba "al alcance" del asegurado, expresión que debe entenderse como comprensiva también de las posibilidades económicas del asegurado, y en el motivo nada se razona sobre este punto ni se precisa cuál era el coste de la obra. En suma, la finalidad del seguro para el asegurado es protegerse contra un evento perjudicial, y si la aseguradora le obliga a adelantar un desembolso extraordinario que se encuentre dentro de la cobertura pactada, so pena de tener que soportar las consecuencias, el seguro dejará de tener la utilidad que le es

inherente o, dicho de otra forma, de cumplir la función jurídica que tiene para el asegurado"[102].

En este sentido, podríamos entender, *a sensu contrario*, que si se produce una advertencia por parte del asegurador sobre la necesidad de adoptar unas medidas concretas y la implementación de las mismas está al alcance del asegurado, ya que las medidas de mitigación a implementar en el caso del seguro de riesgos cibernéticos no requieren de un gasto económico excesivo ni inoportuno para el asegurado, podría argumentarse el rechazo de cobertura del eventual siniestro por parte del asegurador con base en esos postulados.

Ahora bien, mientras que el deber de mantener el estado del riesgo impone al asegurado, en general, una conducta pasiva que tiende hacia la prohibición de cualquier conducta que afecte al riesgo, el deber de salvamento exige del asegurado la adopción de medidas concretas activas para reducir las consecuencias del sinestro.

La pregunta aquí reside en el hecho de si la implementación de las medidas de seguridad indicadas por los técnicos forenses se incardina en el deber activo de aminorar las consecuencias del siniestro o en el pasivo de evitar una alteración del riesgo, en mi opinión se encuentra en el activo por lo siguiente:

En primer lugar, que la implementación de las medidas de mitigación se integra como deber pasivo que busca no actuar agravando el riesgo; este supuesto es contradictorio en sí mismo ya que la implementación de las medidas de mitigación propuestas tras un siniestro representa en si misma una conducta activa concreta a la que te compele el asegurador, por lo que este planteamiento de la no actuación por evitar la alteración del riesgo a mi parecer carece de sentido y no se puede relacionar con la obligación de implementar las medidas de mitigación correspondientes.

Segundo, que la implementación de medidas representa un deber activo. Esta es la opción con más sentido ya que la obligación de implementar las medidas de mitigación conlleva una respuesta activa del asegurado.

Por lo tanto, asumiendo tras lo expuesto anteriormente que la obligación de implementar las medidas de mitigación es un deber activo del asegurado, ahora es necesario delimitar

[102] STS de 21 de noviembre de 2011 (RJ 2012/1112)

cuando la no realización de este deber activo podría dar lugar a la no cobertura de un eventual siniestro.

Para ello es imprescindible recordar que, como se ha expuesto a lo largo de este análisis, esta obligación de implementar las medidas de motivación es una obligación *ex post* a la producción del siniestro, ya que estas medidas se proponen, en el caso del seguro de ciberriesgos, por el equipo técnico forense en su actuación tras un siniestro, por lo que en mi opinión la no implementación de estas medidas no pueden comprometer la cobertura de los daños producidos por el siniestro, en el sentido de que este ya se produjo en el momento en el que nace la obligación comentada.

No obstante, en cuanto a un eventual siniestro posterior, la no cobertura de este por incumplir dicha obligación si debería de ser posible, ya que en este caso la obligación ya habría nacido antes de la producción del nuevo siniestro y por tanto de los daños producidos por este. Sin embargo, la no implementación de las medidas de mitigación propuestas por los técnicos forenses en el primer siniestro debe tener relación causal con el eventual segundo siniestro cuya cobertura se pretende excluir, ya que no el mero incumplimiento de esta obligación por parte del asegurado debería permitir al asegurador rechazar cualquier siniestro sin existir relación alguna.

Además, es relevante analizar que proporción del daño ocurrido se puede no cubrir por parte del asegurador en el caso de que esto sea posible. Ateniéndose al supuesto de un segundo siniestro cuya producción guarda relación con la no implementación de las medidas de mitigación recomendadas en un anterior siniestro, único caso en el que como se ha expuesto con anterioridad es posible para el asegurador rechazar la cobertura, hay que atender a la intención del asegurado en el incumplimiento. Esto es porque siguiendo lo tipificado en el art. 17 de la LCS, en caso de que medie culpa se podría disminuir la indemnización que le corresponde al asegurado por los daños consecuencia del siniestro, pero en caso de que mediase dolo el asegurador podría rechazar íntegramente la cobertura del siniestro por el incumplimiento.

En conclusión, el incumplimiento por parte del asegurado de la obligación de implementar las medidas de mitigación recomendadas por el equipo técnico forense no permite por si sola que el asegurador rechace la cobertura del siniestro, sino que debe existir una relación entre la medida de mitigación no implementada por el asegurado y el siniestro sufrido posteriormente a esta, en cuyo caso si podría darse la posibilidad de que

el asegurador rechace la cobertura del siniestro, más aún en el caso concreto del seguro de riesgos cibernéticos ya que la implementación de estas medidas no supone una excesiva onerosidad, con base en el artículo 17 LCS y la jurisprudencia citada.

4. CONCLUSIONES

Para finalizar este Trabajo de Fin de Grado es necesario centrarse en las conclusiones que derivan del profundo estudio realizado del contrato de seguro de riesgos cibernéticos.

El seguro de ciberriesgos es una figura con una gran importancia en la actualidad, relevancia que no puede encaminarse hacia ningún otro camino que difiera del aumento. Esto es debido a la digitalización constante de nuestro entorno, la cual además de las ventajas que nos aporta, también esta plena de riesgos y peligros de los que cada vez es más necesario cubrirse, objetivo hacia el que está dirigido este tipo de seguros.

A pesar de estar expuestos a ellos, estos riesgos son bastante desconocidos por la gran mayoría de la población, por ello es importante concienciarse y comprender la necesidad de protegerse de ellos con instrumentos como el contrato de seguro de riesgos cibernéticos.

Este tipo de contrato de seguro posee un marco legal muy amplio, lo cual es debido a la gran cantidad y novedad de los diferentes riesgos que se agrupan dentro de las redes cibernéticas y su utilización, por lo que las normativas sobre las cuestiones relacionadas con la ciberseguridad son todas de creación muy reciente y se encuentran muy dispersas, produciendo una falta de armonización debido a la inmadurez del sector.

Para el análisis de esta clase de contrato de seguro tan desconocida y relevante a la vez se ha comenzado por exponer las características típicas del contrato de seguro para ir focalizándose en las cuestiones especiales del contrato de seguro de riesgos cibernéticos y finalizar con un estudio sobre cuestiones conflictivas que le rodean en la actualidad.

En cuánto a las especialidades de este tipo de seguro, como se ve reflejado en este Trabajo de Fin de Grado, ofrece una serie de coberturas para asegurar los riesgos presentes en el mundo cibernético.

En mi opinión, es un instrumento al que le falta un gran desarrollo en este sentido, posiblemente justificado por su reciente creación. Esto es porque los riesgos que se pretenden asegurar bajo este contrato de seguros son demasiado amplios como para encontrar una estabilidad en el mercado asegurador.

El seguro de riesgos cibernéticos debe evolucionar hacia varios seguros diferentes que aseguren los dispares riesgos presentes en las redes cibernéticas, ya que en la actualidad como se ha expuesto este instrumento cubre a los asegurados desde una filtración de datos hasta un robo de dinero por suplantación de identidad, supuestos totalmente diferentes con consecuencias diversas y que únicamente tienen en común el alto daño potencial que pueden producir, su producción en las redes cibernéticas y la desprotección que existe actualmente de las personas en este marco, desencadenada seguramente por el desconocimiento. Otro claro ejemplo de la amplitud de la cobertura de este tipo de contrato de seguros es que cubre tanto los daños propios como la responsabilidad civil.

Es razonable que se pretendiese en un primer momento crear una única figura de seguro que englobe todos los riesgos presentes en las redes cibernéticas para conformar una oferta sólida que atraiga a los potenciales asegurados bajo estas pólizas, pero esto debe cambiar hacia una ramificación que diferencie entre los diversos riesgos o, de lo contrario, un gran crecimiento del importe de las primas, para estabilizar el mercado del seguro de ciberriesgos y la dualidad existente entre el riesgo asegurado y el retorno para los aseguradores, ya que en la actualidad la balanza entre las obligaciones asumidas por los aseguradores y las obligaciones asumidas por los asegurados en este contrato de seguro de riesgos cibernéticos esta descompensada, con una siniestralidad tan alta que hace insostenible a largo plazo el modelo seguido hasta ahora.

Además, en este tipo de contrato de seguros las medidas de mitigación que proponen los técnicos forenses tras la producción de un siniestro son un aspecto muy importante en la reducción del riesgo de un eventual siniestro posterior.

Como se ha analizado en este estudio, para que el asegurador pueda rechazar la cobertura por el incumplimiento de la obligación del asegurado de implementar estas medidas es necesario que estén relacionadas causalmente con la producción de un eventual segundo siniestro. En el seguro de ciberriesgos probar esta relación causal es de una muy alta dificultad, ya que confirmar con total seguridad el origen de los siniestros en el marco de las redes cibernéticas es en muchos casos imposible, por lo que en mi opinión es necesario un instrumento que regule este asunto, ya que el aumento del riesgo producido por la evidente falta de buena fe del asegurado, componente imprescindible en el seguro, de no implementar las medidas de mitigación debe de tener consecuencias para este.

Asimismo, como se ha expuesto anteriormente, según se están redactando actualmente las cláusulas de exclusión por guerra en el seguro de riesgos cibernéticos es necesario que el asegurador pruebe la procedencia de su aplicación en determinados supuestos, lo cual también es de una enorme dificultad debido a lo arduo, por no decir imposible, que supone no sólo encontrar al ciber atacante concreto que ha producido el siniestro sino que también confirmar su vinculación con algún gobierno que le haya contratado para realizar el ciberataque que produjo el siniestro. Por consiguiente, es necesario que los aseguradores realicen nuevas redacciones para este tipo de cláusulas en las que claramente y de manera expresa este tipo de supuestos entren bajo su ámbito de aplicación, de lo contrario, seguirán expuestos a este riesgo.

El seguro de riesgos cibernéticos es una figura con una importancia muy grande en el presente y en el futuro, pero que debido a su reciente nacimiento aún necesita evolucionar profundamente en muchos aspectos para estabilizarse en el mercado del seguro y servir de la forma más eficiente posible a su objeto.

5. BIBLIOGRAFÍA

Legislación

Código de Comercio (C.Com). 22 de agosto de 1885. España. https://www.boe.es/eli/es/rd/1885/08/22/(1)/con

Código Civil (CC). 25 de julio de 1889. España. https://www.boe.es/eli/es/rd/1889/07/24/(1)/con

Ley 50 de 1980. Contrato de Seguro. 17 de octubre de 1980. España. https://www.boe.es/eli/es/l/1980/10/08/50

Ley 20 de 2015. de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. 15 de julio de 2015. España. https://www.boe.es/eli/es/l/2015/07/14/20/con

Real Decreto Legislativo 1 de 2007. Aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. De 30 de noviembre de 2007. https://www.boe.es/eli/es/rdlg/2007/11/16/1/con

Reglamento 679 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. De 27 de abril de 2016. Unión Europea. https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Ley Orgánica 3 de 2018. Protección de Datos Personales y garantía de los derechos digitales. De 6 de diciembre de 2018. España. https://www.boe.es/eli/es/lo/2018/12/05/3

Directiva de la Unión Europea 2555 de 2022. Medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. De 14 de diciembre de 2022. Unión Europea. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

Reglamento de la Unión Europea 2554 de 2022. La resiliencia operativa digital del sector financiero. 27 de diciembre de 2022. Unión Europea. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962

Jurisprudencia

Sentencia del Tribunal Supremo de 8 de febrero de 1999 (RJ 1999/337)

Sentencia del Tribunal Supremo de 4 de diciembre de 2000 (RJ 2000/9327)

Sentencia del Tribunal Supremo de 14 de junio de 2002 (RJ 3847/1996)

Sentencia del Tribunal Supremo de 22 de diciembre de 2001 (RJ 2679/1996)

Sentencia del Tribunal Supremo de 2 de abril de 2009 (RJ 2009/1754)

Sentencia del Tribunal Supremo de 21 de noviembre de 2011 (RJ 2012/1112)

Otros

Agencia de la Unión Europea para la Ciberseguridad (ENISA). (2022). *Ciberseguridad: amenanzas principales y emergentes.* https://www.europarl.europa.eu/topics/es/article/20220120STO21428/ciberseguridad-amenanzas-principales-y-emergentes

Agra Viforcos, B., Alonso Suárez, L., Álvarez Cuesta, H., Benlloch Domenech, C., Coelho Moreira, T., Durán Santomil, P., Fernández Domínguez, J.J., Fernández, J.J., Fernández López, S., Gallego Córcoles, I., Garrido Juncal, A., Gimeno Presa, M.C., Gomes Ramos, M.E., Hernández Rodríguez, F., Lado-Sestayo, R., Marongiu, D., Martínez Castaño, R., Martínez Pérez, M., Meléndez Alonso, G., … y Zapata Huamaní, G.M. García Novoa, C. y Santiago Iglesias, D. (Ed.). (2018). *4º REVOLUCÓN INDUSTRIAL: IMPACTO DE LA AUTOMATIZACIÓN Y LA INTELIGENCIA ARTIFICIAL EN LA SOCIEDAD Y LA ECONOMÍA DIGITAL.* Thomson Reuters. Pp. 165.

Aguirre y Baeza. (2018). *El Contrato de Seguro y sus Características Esenciales.* https://www.aguirrebaeza.com/blog/el-contrato-de-seguro-y-sus-caracteristicas-esenciales/

Allianz. (s.f) *¿Qué es una franquicia en un seguro?.* https://www.allianz.com.ar/blog-allianz/franquicia.html

Almigorena Eguiluz, R., Baratta Martínez, R., Benido Gómez, M.J., Cornago Baratech, J.F., Domínguez Fernández-Burgos, A., García Quiniela, J., Largacha Lamela, D., Mateo Murillo, I., del Olmo Fons, F., Paredes Hernández, L., Perea Velasco, J., Ramírez Sánchez, O., Ramos García, A., Sánchez López, J., Viana Lara, A. y Vivancos Cerezo,

M.E. (2023). D´Antonio, G. y Ruiz Vázquez, A.J. (Ed.) *CÓDIGO DE BUEN GOBIERNO DE LA CIBERSEGURIDAD.* https://www.cnmv.es/DocPortal/Ciberseguridad/CBG_Ciberseguridad.pdf

Álvarez Vigaray, R. (1968). *Los contratos aleatorios.* *https://dialnet.unirioja.es/servlet/articulo?codigo=2048496* Pp. 611-614

AON. (2021). Encuesta anual de gestión de riesgos 2021. https://www.aon.com/2021-global-risk-management-survey/latam/es.jsp

AON. (2023). *IV Estudio Anual de Aon sobre Ciberseguridad y Gestión del Riesgo Ciber en España.* Pp. 5-8. https://noa.aon.es/wp-content/uploads/2023/09/Informe-Ciber-2023VFD.pdf

Arslanián Baggini, J.M. (2022). *LA LEGISLACIÓN DEL CONTRATO DE SEGURO EN ESPAÑA Y EN ALEMANIA. ANÁLISIS A LA LUZ DEL DERECHO COMPARADO.* http://dspace.umh.es/bitstream/11000/28392/1/TFG%20DERECHO-Arslani%c3%a1n%20Baggini%2c%20Juan%20Manuel.pdf Pp. 15-17.

Barrio Andrés, M. (2024). *La ciberseguridad en el Derecho digital europeo: novedades de la Directiva NIS2.* InDret. https://indret.com/wp-content/uploads/2024/01/1838.pdf Pp. 509-512.

BLB Asociados. (s.f.) *Seguro de Ciberriesgos*. https://www.blbcorreduria.com/wp-content/uploads/2021/02/BLB-DOSSIER-Seguro-de-Ciberriesgos.pdf

Burguera Abogados. (2019). *Contrato de seguro de grandes riesgos y principio de autonomía de la voluntad*. https://www.burgueraabogados.com/contrato-seguro-grandes-riesgos-principio-autonomia-voluntad/

Chubb. (2018). *Póliza para la Gestión de Riesgos Cibernéticos.* https://www.chubb.com/content/dam/chubb-sites/chubb-com/latam-microsites/factsheet-cyber.pdf

Davidson, P. (2021). *Cyber War and Cyber Operation Exclusion Clauses.* Lloyd´s Market Association Bulletin. https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx

Deloitte. (2023). *El estado de la ciberseguridad en España Cyber Strategy, Transformation and Assessments.* https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad-2024.html

Diccionario Panhispánico del Español Jurídico. (2023). *Interés asegurable.* https://dpej.rae.es/lema/inter%C3%A9s-asegurable

Diccionario Panhispánico del Español Jurídico. (2023). *Interés asegurado.* https://dpej.rae.es/lema/inter%C3%A9s-asegurado

Fernández, M. (2023). *España, en el podio mundial de ciberataques: es el tercer país con más cuentas hackeadas en 2023.* https://www.elespanol.com/omicrono/software/20230816/espana-podio-mundial-ciberataques-tercer-pais-cuentas-hackeadas/785921544_0.html

Forbes. (2023). *El 91% de las empresas corre riesgo de sufrir un ataque de 'phishing' en 2023, según BDO.* https://forbes.es/ultima-hora/231482/el-91-de-las-empresas-corre-riesgo-de-sufrir-un-ataque-de-phishing-en-2023-segun-bdo/

Fundación Area XXI. (S.F.). *ELEMENTOS DEL CONTRATO DE SEGURO.* https://fundacionarea-xxi.com/6-elementos-del-contrato-de-seguro/

Fundación Mapfre. (s.f.) *Diccionario de seguros. Riesgo.* https://www.fundacionmapfre.org/publicaciones/diccionario-mapfre-seguros/riesgo/

García Marcén, G. (2019). *Contratación de la póliza de Ciberriesgos, tratamiento del siniestro y la importancia del reaseguro*. http://hdl.handle.net/2445/144759 Pp. 50-58.

García Villarrubia, M., Sánchez Bleda, P., Touriño Peña, A., Rodríguez Ayuso, J.F., Serrano Acitores, A., Muñoz Rodríguez, J., Díaz Bizkarguenaga, K., Estévez Sanz, M. y Ortega Burgos, E. (2023). XIV. Cómo gestionar un ciberataque desde un punto de vista jurídico en Eceiza Zubieta, L., Nuevas Tecnologías 2023. Tirant Lo Blanch.

Gomis Palau, A. (2021). *Póliza.* https://www.autorizadored.es/finanzas/poliza/

González Cerredelo, S. (2022) *Así han evolucionado los ciberataques*. El Mundo. https://historiasdeprogreso.elmundo.es/asi-han-evolucionado-los ciberataques.html#:~:text=Hoy%20en%20d%C3%ADa%2C%20el%20cibercrimen,para%20adelantarse%20a%20los%20ataques.

González, P. (2023). *La economía mundial se enfrenta a un riesgo de ciberataque de 3,5 billones de dólares en cinco años.* Inese. https://future.inese.es/la-economia-mundial-se-enfrenta-a-un-riesgo-de-ciberataque-de-35-billones-de-dolares-en-cinco-anos/

Hispacolex. (2014). *No se puede considerar al contrato de seguro de grandes riesgos como contrato de adhesión.* https://www.hispacolex.com/biblioteca/articulos-doctrinales/contrato-de-seguro-grandes-riesgos/

Howden. (2023). *Las primas de seguros cibernéticos podrían superar los 50 mil millones de dólares para el año 2030.* https://www.howdengroup.com/es-es/informe-cyber

Ibarra, M.B. (2017). *La peculiaridad de la adhesión en el contrato de seguro.* https://doi.org/10.18272/lr.v4i1.986 Pp.90-94.

IBM. (S.F.) *¿Qué es el malware?*. https://www.ibm.com/es-es/topics/malware

IBM. (S.F.). *¿Qué es el phishing?* https://www.ibm.com/es-es/topics/phishing

INCIBE. (2020). *El ataque del "Man in the middle" en la empresa, riesgos y formas de evitarlo*. https://www.incibe.es/empresas/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo

Incibe. (2020). *Ransomware, una guía de aproximación para el empresario.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware.pdf

INCIBE. (2023). *El riesgo ciber, máxima prioridad para pymes y autónomos.* https://www.incibe.es/empresas/blog/el-riesgo-ciber-maxima-prioridad-pymes-y-autonomos

Incibe. (s.f.) *Autenticación de dos factores (2FA).* https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores

Instituto de Crédito Oficial. (2021). *PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SEGURO DE RIESGOS CIBERNETICOS DEL INSTITUTO DE CRÉDITO OFICIAL, ENTIDAD PÚBLICA EMPRESARIAL EN PROCEDIMIENTO ABIERTO SIMPLIFICADO.* https://contrataciondelestado.es/wps/wcm/connect/c315d0fb-36d2-4b24-84ce-84aa05011428/DOC20210907101335PPT+Plataforma.pdf?MOD=AJPERES

Jiménez Naharro, F.; Sánchez Montañés, C.; Sánchez Barrios, M. (2018). La transferencia de los riesgos cibernéticos en empresas internacionales con alto nivel de capitalización bursátil. Revista de Pensamiento Estratégico y Seguridad CISDE, 3(1), 67-90. (www.cisdejournal.com)

Lamb, E. (2023). *Informe de Ciberpreparación de Hiscox 2023.* Pp 14-16. https://www.hiscox.es/sites/spain/files/2023-10/22594%20-%20Cyber%20Readiness%20Report%202023%20-%20Spanish.pdf

Leonor, D. (2023). Estados Unidos representa más de la mitad de las primas cibernéticas en 2022. Inese. https://future.inese.es/estados-unidos-representa-mas-de-la-mitad-de-las-primas-ciberneticas-en-2022/

Mapfre. (s.f.) *CIBERRIESGOS PYME Y AUTÓNOMOS.* https://www.ciberseguros.com/condiciones/CondicionesGeneralesCiberseguroMapfre.pdf

Martínez, D. (s.f.) *La Prima del Seguro: Todo lo que debes saber sobre este factor clave en tus finanzas.* iNEF. https://inef.es/seguros-y-proteccion-financiera/la-prima-del-seguro

Martínez Ortiz, P.J. (2021). *BUENA FE Y CONSENSUALIDAD CONTRACTUAL. ANTECEDENTES EN DERECHO ROMANO E IRRADIACIÓN EN DERECHO VIGENTE RESPECTO DEL CONTRATO DE SEGURO. ANÁLISIS LEGISLATIVO, DOCTRINAL Y JURISPRUDENCIAL.* http://espacio.uned.es/fez/eserv/bibliuned:grado-Derecho-DR-Pjmartinez/Martinez_Ortiz_Pedro_Jose_TFG.pdf

Ministerio de Asuntos Económicos y Transformación Digital. Vicepresidencia Primera del Gobierno. (2022). Informe 2022 Seguros y Fondos de Pensiones. Pp. 390-397. dgsfp.mineco.gob.es/es/Publicaciones/DocumentosPublicaciones/Informe del sector 2022.pdf

Morgan, S. (2023). *2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics.* Cybersecurity Ventures. https://cybersecurityventures.com/cybersecurity-almanac-2023/

Netscout. (2019). *INFORME GLOBAL DE AMENAZAS DDoS.* https://pro-cdo-web-resources.s3.eu-west-1.amazonaws.com/elevenpaths/uploads/2020/12/elevenpaths-informe-global-amenazas-ddos.pdf Pp. 7-14.

Puyol Montero, J. y Delgado Caravilla, E. (2018) *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea.* Epígrafe 4: *Los riesgos, las amenazas y las medidas técnicas con relación a los tratamientos de datos de carácter personal*. Tirant Lo Blanch.

Rashid, S. (2024). *Reconocer los ataques de phishing en 2024.* https://www.metacompliance.com/es/blog/cyber-security-awareness/recognising-phishing-attacks

Reale Seguros. (2019). *Fecha de efecto.* https://blog.reale.es/diccionario-de-seguros/fecha-efecto/

Satariano, A. & Perlroth, N. (2019) *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.* New York Times. https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html

Surfshark. (2023). *Data breaches ramped up globally as 2023 reaches midpoint.* https://surfshark.com/research/study/data-breach-statistics-q2-2023.

THIBER, (2016) la transferencia del ciberriesgo en España. https://thiber.org/ciberseguros.pdf

Toledano Jiménez, M.A. (2017). *¿Qué son los seguros de "ciberriesgos"?* https://doi.org/10.51302/ceflegal.2017.10543 Pp. 63-65.

Vadillo Asesores. (2021). *¿Cuáles son los riesgos al usar un software sin licencia o software pirata?.* https://www.grupovadillo.com/cuales-son-los-riesgos-al-usar-un-software-sin-licencia-o-software-pirata/

Veiga Copo, A.B. (2010). *La temporalidad en el contrato de seguro. Riesgo y siniestro: una ecuación interesadamente compleja.* Pp. 35-37.

Verdejo Álvarez, G. (S.F.). *SEGURIDAD EN REDES IP: DOS/DDOS.* https://www.cs.upc.edu/~gabriel/files/DEA-es-2DOS-DDOS.pdf Pp. 37.

6. ANEXO

PÓLIZA DE CIBERRIESGOS; PYME Y AUTÓNOMOS, MAPFRE[103]:

CONDICIONES GENERALES

PREÁMBULO

El presente Contrato de Seguro se rige por lo dispuesto en las Condiciones Generales, Particulares y, salvo pacto en contrario que resulte más beneficioso para el Asegurado, por la Ley de Contrato de Seguro (Ley 50/1980, de 8 de octubre), la Ley de Ordenación, Supervisión y Solvencia de las Entidades Aseguradoras y Reaseguradoras, (Ley 20/2015, de 14 de julio), sus normas reglamentarias de desarrollo y demás legislación que resulte aplicable. Si el contenido de la póliza difiere de la proposición de seguro o de las cláusulas acordadas, el Tomador del Seguro podrá reclamar a la Entidad Aseguradora en el plazo de un mes a contar desde la entrega de la póliza para que subsane la divergencia existente. Mediante la firma de las Condiciones Particulares de la póliza, el Tomador del Seguro acepta específicamente las cláusulas limitativas de los derechos del Asegurado que se resaltan en letra «negrita» en estas Condiciones Generales.

1. DEFINICIONES. A efectos de esta póliza:

1.1. AMENAZA DE EXTORSIÓN CIBERNÉTICA Significa una amenaza o conjunto de éstas creíbles, incluyendo la petición de una cantidad de dinero, dirigidas contra el Asegurado para evitar un Daño o Pérdida de Datos o introducción de un Código Malicioso Informático, en los Sistemas Informáticos del Asegurado, o cualquier amenaza o serie de amenazas relacionadas con revelar o dar a conocer Información Confidencial o Datos de Carácter Personal alojada en los Sistemas Informáticos del Asegurado o la interferencia no autorizada o inesperada, que limite o impida el acceso a dichos sistemas a personas o entidades autorizadas por el propio Asegurado para dicho acceso, o la realización de comunicaciones falsas a clientes o proveedores del

[103] Mapfre. (s.f.) *CIBERRIESGOS PYME Y AUTÓNOMOS.* https://www.ciberseguros.com/condiciones/CondicionesGeneralesCiberseguroMapfre.pdf

Asegurado simulando ser el Asegurado, , o amenaza de daño o de destrucción de los Sistemas Informáticos del Asegurado.

1.2. ARCHIVOS DIGITALES Significa cualquier almacenamiento digital controlado y fiable que utilice determinados procesos, políticas, Medios Electrónicos y software para el almacenamiento y la conservación de Datos y que ofrezca protección, seguridad, autenticidad y disponibilidad de los Datos y defina y controle el acceso a los Datos.

1.3. ASEGURADO Significa la persona titular del interés expuesto al riesgo a quien corresponden, en su caso, los derechos derivados del contrato. El Asegurado podrá asumir las obligaciones y deberes del Tomador. Cuando el Asegurado sea persona jurídica, y únicamente a efectos de la c obertura de Responsabilidad Civil, tendrán también la condición de Asegurados sus Directivos en el ejercicio del cargo y los Empleados vinculados con el mismo en virtud de una relación laboral mientras actúen en el ámbito de su dependencia.

1.4. ASEGURADOR O ASEGURADORA Significa MAPFRE ESPAÑA, COMPAÑÍA DE SEGUROS y REASEGUROS, S.A., entidad emisora de esta Póliza que, en su condición de Asegurador y mediante el cobro de la Prima, asume la cobertura de los riesgos objeto de este contrato con arreglo a las condiciones establecidas en el mismo. La entidad se halla sometida en su actividad aseguradora a la supervisión del Ministerio de Economía, Industria y Competitividad del Reino de España, a través de la Dirección General de Seguros y Fondos de Pensiones.

1.5. BENEFICIO NETO Significa la diferencia entre el Volumen de Negocio y los costes de explotación del Asegurado, después de realizada la debida provisión para todos los gastos, permanentes o no, y antes de la deducción de impuestos que recaen sobre los beneficios del mismo período. No entran en el cálculo los beneficios o pérdidas resultantes de operaciones financieras ni, en general, las operaciones atípicas o no propias de la actividad del Asegurado.

1.6. DAÑO O PÉRDIDA DE DATOS Significa cualquier introducción, corrupción, creación, modificación, alteración o eliminación de Datos, que, al procesarlos en el Sistema Informático del Asegurado, podrían conducir a un funcionamiento deteriorado, degradado o anómalo de los Sistemas Informáticos y/o a la interrupción o alteración de las operaciones de proceso de Datos.

1.7. DATOS Significa cualquier información legible, independientemente del modo de uso o presentación (texto, cifras, voz o imágenes), software incluido, transmitida o almacenada en formato digital fuera de la memoria de acceso aleatorio (RAM) propiedad del Asegurado u operada por éste. El término Datos abarcará también Archivos Digitales.

1.8. DATOS DE CARÁCTER PERSONAL Significa cualquier información personal utilizable directa o indirectamente, por sí misma o en conexión con otra información, para identificar, contactar o localizar a una sola persona o para identificar a un individuo en un contexto, incluidos pero no limitados a los apellidos, número de seguridad social, información médica o información protegida relativa a la seguridad, el permiso de conducir, número de identificación fiscal, número de tarjeta de crédito o de débito, dirección o número de teléfono, referencia de la cuenta individual o contraseña y cualquier otra identificación personal, conforme a lo especificado en la Legislación de Protección de Datos de Carácter Personal, cualquiera que sea el formato y el medio de la misma.

1.9. DIRECTIVOS Significa cualquier persona física que ostente en la empresa asegurada la condición de administrador, consejero, alto cargo, director general, administrador de hecho, gerente o cualquier posición equivalente.

1.10. EMPLEADO Significa cualquier persona física que preste servicios o aporte trabajo al servicio y en las instalaciones del Asegurado en virtud de un contrato de trabajo, con independencia de la temporalidad del mismo, así como el personal subcontratado o externo que preste sus servicios en las instalaciones del asegurado y tenga por razón de su empleo acceso a los sistemas informáticos del asegurado, sin perjuicio de la acción de repetición frente a la empresa contratante del mismo, por el cual el Asegurado o sus representantes legales tengan derecho a controlar los detalles de su prestación laboral. El término “Empleado” no incluirá a los representantes legales del Asegurado.

1.11. ERROR HUMANO Significa cualquier error de operación informática cometido por negligencia o involuntariamente, incluido un error en la elección del software a emplear, un error de configuración o cualquier otra operación informática indebida llevada a cabo por un Empleado del Asegurado.

1.12. EVENTO NO FÍSICO Significa cualquiera de los siguientes eventos perpetrados por un Tercero en los Sistemas Informáticos del Asegurado: ACTO INFORMATICO DOLOSO: todo acto indebido llevado a cabo con la intención de causar daño o conseguir acceso ilegítimo a Datos, Sistemas Informáticos o redes informáticas mediante el uso de cualquier Sistema Informático o red informática. CODIGO MALICIOSO INFORMÁTICO: cualquier software hostil o intruso, incluidos Virus Informáticos, programas espía, gusanos, troyanos, rootkits, ransomware, keyloggers, dialers, programas espía, adware, objetos maliciosos de ayuda del explorador (BHO, por sus siglas en inglés) y software de seguridad fraudulento, diseñados para infiltrarse e interrumpir operaciones de ordenadores, recopilar información sensible o acceder a Sistemas Informáticos sin autorización. ROBO DE DATOS: cualquier Acto Informático Doloso de copia ilegítima o para extraer Datos de Sistemas Informáticos. DENEGACIÓN DE SERVICIO: cualquier Acto Informático Doloso del que resulte la privación total o parcial, la alteración y/o la falta de disponibilidad de Sistemas Informáticos o instalaciones de redes, incluida la alteración o la destrucción del software correspondiente, por medio de un aluvión de Datos que sobrecargan Sistemas Informáticos con un flujo entrante de solicitudes, incluidos ataques por Denegación Repartida de Servicios (DdoS, por sus siglas en inglés), utilizando una multitud de sistemas involucrados para coordinar un ataque simultáneo.

1.13. FRANQUICIA Significa la cantidad o procedimiento para su deducción establecido en las Condiciones Particulares de esta Póliza, que no será de cuenta del Asegurador y que asume directamente el Asegurado. Por tanto, el Asegurador sólo indemnizará los Siniestros hasta el límite de la suma asegurada en exceso de las cantidades resultantes como Franquicias.

1.14. GASTOS PERMANENTES Significa los gastos que no varían en función directa de las actividades de la empresa asegurada y que, en consecuencia, deberán ser mantenidos a pesar de la interrupción total o parcial de la operación de negocio provocada por el Evento No Físico.

1.15. INFORMACIÓN CONFIDENCIAL Significa toda actividad sensible y secretos de comercio de cualquier naturaleza y cualquier forma que no sea de dominio público.

1.16. INTERRUPCIÓN DE NEGOCIO Significa la pérdida de Margen Bruto indemnizable derivada de la paralización, suspensión o reducción de los procesos productivos o de negocio de conformidad con las coberturas contratadas.

1.17. LÍMITE POR ANUALIDAD Significa la cantidad máxima a cargo del Asegurador por cada período de Seguro, con independencia de que sea consumida en uno o varios Siniestros, entendiendo por período de Seguro el comprendido entre la fecha de efecto y de vencimiento, expresadas en las Condiciones Particulares o en el período anual establecido en el último recibo de Primas.

1.18. MARGEN BRUTO La suma que resulta de añadir al Beneficio Neto el importe de los Gastos Permanente asegurados. En caso de pérdidas, se considerará como Margen Bruto el importe de los Gastos Permanentes asegurados, menos la proporción de la pérdida que corresponda a dichos Gastos Permanentes asegurados en relación con los Gastos Permanentes totales.

1.19. LÍMITE DE INDEMNIZACIÓN POR SINIESTRO Significa la cantidad máxima que, en cualquier caso, se verá obligado a indemnizar el Asegurador por cada Siniestro amparado por la Póliza, sea cual fuese el número de coberturas afectadas y el número de víctimas o perjudicados.

1.20. MEDIOS DE INFORMACIÓN Significa cualesquiera medios impresos, tal como diarios, cartas de información, revistas, libros y obras literarias de cualquier formato, folletos y publicaciones de todas clases, medios publicitarios, incluidos envolturas, fotos e impresiones digitales.

1.21. MEDIOS ELECTRÓNICOS Significa cualesquiera dispositivos TI (incluidos pero no limitados a discos duros externos, CD ROM, DVD-ROM, cintas magnéticas, discos magnéticos, lápices USB) utilizados para el proceso de registrar y almacenar Datos.

1.22. PERIODO DE CARENCIA Significa el número de horas que deben transcurrir desde que se produce el fallo de los Sistemas Informáticos del Asegurado para que surta efecto la cobertura de INTERRUPCIÓN DE NEGOCIO. En tanto no se supere este periodo no se produce obligación alguna para el Asegurador ni se generan derechos para el Asegurado.

1.23. PERIODO DE INDEMNIZACIÓN Significa el período que se inicia el día del Evento No Físico y finaliza dentro del periodo especificado como Periodo de

Indemnización en las Condiciones Particulares, Generales o Especiales de la Póliza o cuando se haya restaurado el Sistema Informático del Asegurado, si esto último ocurre antes de que finalice el citado Periodo de Indemnización.

1.24. PERÍODO DE VIGENCIA Significa: el período entre la Fecha de Efecto y la Fecha de Vencimiento designadas en las Condiciones Particulares de la Póliza, o el período entre la Fecha de Efecto indicada en las Condiciones Particulares de la Póliza y la fecha en la cual la Póliza sea rescindida.

1.25. PERJUICIOS Significa los daños amparados por la cobertura de la Póliza causados por el Asegurado en el patrimonio de un Tercero y que el Asegurado está legalmente obligado a pagar por razón de una Reclamación cubierta y de conformidad con una sentencia, o una transacción acordada con el previo consentimiento por escrito del Asegurador o aquellos causados por Terceros al Asegurado.

1.26. PÓLIZA Significa el documento múltiple que contiene las condiciones reguladoras del Contrato de Seguro. Forman parte integrante de la Póliza las siguientes condiciones reguladoras: Las Condiciones Generales: documento que recoge el conjunto de cláusulas generales reguladoras del contrato. Las Condiciones Particulares: documento que contiene los datos personales, las condiciones económicas y las garantías cubiertas, individualiza el riesgo y complementa las Condiciones Generales. Los Suplementos y apéndices que se emitan de la Póliza para complementarla o modificarla durante la vigencia del seguro. El Certificado Individual del Seguro: documento emitido por la Entidad Aseguradora, que acredita como tal al Asegurado.

1.27. PORCENTAJE DE INDEMNIZACIÓN Significa el porcentaje que representa el Margen Bruto o los Gastos Permanentes asegurados, según corresponda, respecto al Volumen de Negocio del ejercicio económico inmediatamente anterior a aquel en que ocurra el siniestro.

1.28. PRIMA Significa el precio del Seguro, en cuyo recibo se incluirán también los impuestos y recargos repercutibles legalmente al Tomador.

1.29. RECLAMACIÓN Significa: La notificación escrita comunicada por primera vez por parte del Tercero perjudicado al Asegurado o Asegurador de su intención de reclamar, o de la interposición de cualquier acción susceptible de ejercitarse ante los Tribunales de cualquier orden, Reclamación administrativa o investigación oficial con

origen o fundamento en la realización por parte del Asegurado de una acción u omisión que haya producido un daño indemnizable bajo la presente Póliza, Cualquier notificación escrita al Asegurador de la intención del Asegurado de exigirle responsabilidad, respecto de la cual las coberturas de esta Póliza sean de aplicación. Todas las reclamaciones derivadas de una misma causa de origen, serán consideradas como una sola y única Reclamación, y esta Reclamación se considerará que ha sido realizada dentro de la anualidad de Seguro en que se hizo la primera Reclamación.

1.30. SANCIÓN Significa cualquier sanción impuesta en el ejercicio de su potestad sancionadora por la Agencia Española de Protección de Datos por vulneración de normas relativas a la protección de Datos de Carácter Personal de conformidad con las disposiciones legales vigentes en la materia.

1.31. SINIESTRO Significa todo acontecimiento o hecho cuyas consecuencias económicas dañosas estén cubiertas dentro de los términos y condiciones pactados en la Póliza. El conjunto de los daños derivados de un mismo evento constituye un solo Siniestro.

1.32. SISTEMA DE CONTROL DE ACCESO Significa todo conjunto de reglas, derechos y privilegios requeridos para el acceso legítimo a los Sistemas Informáticos del Asegurado.

1.33. SISTEMAS INFORMÁTICOS DEL ASEGURADO Significa todos los Sistemas Informáticos y redes controlados y gestionados por el Asegurado, incluyendo sistemas operativos, software, hardware, , equipos de enrutamiento, cableados, redes de comunicación, redes del sistema y Datos, así como teléfonos, tablets y otros dispositivos móviles que el Asegurado facilite a sus Empleados; siempre que sean requeridos y se empleen para las operaciones del negocio Asegurado. A efectos de esta Póliza no se incluyen en los Sistemas Informáticos del Asegurado, en ningún caso, los sistemas, entornos, aplicaciones, Datos o redes en fase de desarrollo, pruebas o pre- producción.

1.34. SUBLÍMITES Significa las cantidades indicadas en las Condiciones Particulares que representan los límites máximos asumidos por el Asegurador para cada una de las coberturas especificadas en dichas Condiciones.

1.35. TERCERO Significa cualquier persona física o jurídica distinta de: El Tomador del Seguro y el Asegurado. El representante legal del Tomador del Seguro y el

Asegurado. Cualquier Empleado del Tomador del Seguro y el Asegurado. Directivos del Tomador del Seguro y el Asegurado.

1.36. TOMADOR DEL SEGURO Significa la persona que suscribe el presente contrato con el Asegurador, y a quien corresponden las obligaciones que se deriven del mismo, salvo aquellas que, por su naturaleza, deban ser cumplidas por el Asegurado.

1.37. VOLUMEN ANUAL DE NEGOCIO Significa el volumen de negocio correspondiente a los doce meses inmediatamente anteriores a la fecha en que ocurre el siniestro.

1.38. VOLUMEN DE NEGOCIO Significa el conjunto de ingresos que percibe el Asegurado en contrapartida de operaciones que constituyen la actividad típica de la empresa y cuya facturación ha sido efectuada en el curso del ejercicio o del período considerado, así como los trabajos realizados para el inmovilizado de la empresa en idéntico período.

1.39. VOLUMEN NORMAL DE NEGOCIO Significa el volumen de negocio correspondiente a los doce meses inmediatamente anteriores a cada uno de los días del Período de Indemnización.

1.40. UNIDAD DE SINIESTRO Significa que la sucesión de hechos o circunstancias que se deriven de un mismo origen o igual causa, con independencia del número de perjudicados y reclamaciones formuladas, se considerará como un sólo y único Siniestro. Se considerará como fecha de ocurrencia del Siniestro la del primer hecho o circunstancia siniestral.

COBERTURAS Y GARANTÍAS

2. OBJETO Y ALCANCE DEL SEGURO

El Asegurador garantiza al Asegurado en relación con la actividad asegurada que figura en las Condiciones Particulares, la cobertura de las garantías y prestaciones que a continuación se especifican, en los términos y condiciones establecidos en estas Condiciones Generales y en las Condiciones Particulares:

3. COBERTURA DE RESPONSABILIDAD CIVIL Por la Cobertura de Responsabilidad Civil, el Asegurador asumirá, en los términos establecidos en estas Condiciones Generales, hasta el límite establecido en la Póliza, el pago de las

indemnizaciones de las que el Asegurado pudiera resultar, conforme a derecho, civilmente responsable por perjuicios ocasionados a Terceros, así como las costas judiciales y gastos que le pudieran ser impuestos, siempre y cuando tales responsabilidades deriven de los supuestos previstos en esta cobertura y sean consecuencia de actos u omisiones de carácter culposo o negligente, que le pudieran ser imputables en base a los mismos, en relación con la actividad asegurada. En ningún caso amparará la Responsabilidad Civil directa de los subcontratistas y los empleados de estos y/o sus dependientes. Quedan cubiertas, en los términos pactados, las reclamaciones por Perjuicios presentadas por escrito y por primera vez contra el Asegurado o contra el Asegurador durante la vigencia de la Póliza respecto a los actos y omisiones amparados en las coberturas de la Póliza y conocidas por primera vez por el Asegurado con posterioridad al efecto de la Póliza establecido en Condiciones Particulares y notificadas al Asegurador durante los 12 meses siguientes a la fecha de cancelación de la póliza. Esta delimitación temporal de la cobertura ha sido acordada por las partes en razón al equilibrio contractual entre el alcance de la cobertura y la Prima correspondiente. Si las partes hubieran pretendido establecer un alcance distinto de la cobertura, se hubieran pactado condiciones económicas diferentes. Esta cobertura amparará, exclusivamente, las responsabilidades derivadas de hechos ocurridos en la Unión Europea, que sean exigidas ante los Tribunales que resulten competentes de acuerdo en las Leyes Españolas y los Tratados Internacionales de los que España forma parte, con excepción de las dictadas por los Tribunales de EEUU y Canadá". La cobertura ampara únicamente la responsabilidad civil del Asegurado derivada de:

3.1. RESPONSABILIDAD CIVIL POR VIOLACIÓN DE LA PRIVACIDAD El Asegurador garantiza, con el límite de la suma asegurada establecida en las Condiciones Particulares para la Cobertura de Responsabilidad Civil, el pago de las indemnizaciones en que pueda incurrir el Asegurado por perjuicios económicos ocasionados a Terceros en el ejercicio del desarrollo de su actividad descrita en Condiciones Particulares, de los que deba responder conforme a derecho, y que tengan como consecuencia una Reclamación debida a: Daño o pérdida de Información Confidencial o de Datos de Carácter Personal confiados al cuidado, custodia y control del Asegurado, causado directamente por: Un Acto Informático Doloso perpetrado en el Sistema Informático del Asegurado, o Un Código Malicioso Informático (Malware) activo en el Sistema Informático del Asegurado, Robo de Información Confidencial o de Datos de Carácter

personal, confiados al cuidado, custodia y control del Asegurado, en Medios Electrónicos, Medios de Información o en el Sistema Informático del Asegurado. Revelación de Información Confidencial o de Datos de Carácter Personal confiados al cuidado, custodia y control del Asegurado, en Medios electrónicos, Medios de información o en el Sistema Informático del Asegurado a Terceros no autorizados. Esta cobertura ampara, exclusivamente, la responsabilidad exigible al Asegurado por perjuicios que se hayan producido a consecuencia de los hechos descritos, siempre que en los mismos no hayan intervenido, en modo alguno, sus Empleados, y sean imputables a la acción de Terceros y agentes externos a la empresa Asegurada. A efectos únicamente de esta cobertura de Responsabilidad Civil por Violación de la Privacidad tendrán la consideración de perjudicados los Empleados, tal y como estos se describen en estas Condiciones Generales.

3.2. RESPONSABILIDAD CIVIL MULTIMEDIA Y PUBLICIDAD El Asegurador garantiza, con el límite de la suma asegurada establecida en las Condiciones Particulares para la Cobertura de Responsabilidad Civil, el pago de las indemnizaciones en que pueda incurrir el Asegurado por perjuicios económicos ocasionados a Terceros en el ejercicio del desarrollo de su actividad descrita en Condiciones Particulares, de los que deba responder conforme a derecho, y que tengan como consecuencia una Reclamación debida a la publicación de cualquier contenido en formato electrónico o físico, incluyendo Datos electrónicos, internet, periódicos, revistas, newsletters, libros, folletos o cualquier otro tipo de publicación y material publicitario, presentaciones, imágenes digitales y fotografías, cuando este contenido trascienda y repercuta en la esfera patrimonial del perjudicado y sean causados directamente por: Un Acto Informático Doloso perpetrado en el Sistema Informático del Asegurado, o Un Código Malicioso Informático (Malware) activo en el Sistema Informático del Asegurado, No está cubierta, en ningún caso, la responsabilidad que le sea exigida al Asegurado como autor de hechos calificados como calumnia o cualquier otro delito o por cualquier daño intencionado o malicioso.

3.3. GASTOS DE DEFENSA, FIANZAS Y CONFLICTO DE INTERESES Con el Límite de la Suma asegurada estipulado en las Condiciones Particulares para la Cobertura de Responsabilidad Civil y de conformidad con las Condiciones establecidas en el presente Seguro, siempre que el objeto de la Reclamación esté incluido en las coberturas de la Póliza, quedan también garantizadas: Las fianzas que sean exigidas al

Asegurado para garantizar las responsabilidades pecuniarias civiles, en virtud de resolución judicial dictada en el procedimiento seguido contra el mismo. El Asegurado vendrá obligado a reintegrar al Asegurador el importe de las fianzas prestadas en su favor para garantizar las resultas civiles del procedimiento, siempre que de la resolución judicial que finalmente se dicte resulte que la Reclamación no queda cubierta por este contrato. Las costas judiciales, que serán abonadas en la misma proporción existente entre la indemnización que deba satisfacer el Asegurador, de acuerdo con lo previsto en la Póliza y el importe total de responsabilidad del Asegurado en el Siniestro. Salvo pacto en contrario, en cualquier procedimiento judicial que se derive de un Siniestro amparado por la Póliza, el Asegurador asumirá a sus expensas, la dirección jurídica frente a la Reclamación del perjudicado, designando los letrados y procuradores que defenderán y representarán al Asegurado en las actuaciones judiciales que se siguiesen en Reclamación de responsabilidades civiles cubiertas por esta Póliza, y ello aun cuando dichas Reclamaciones fuesen infundadas. Cuando el Asegurado designe su propia defensa, los gastos judiciales que se originen serán de su exclusiva cuenta, salvo pacto expreso en contrario. Si la cantidad reclamada supera la suma asegurada pactada en las Condiciones Particulares de la Póliza para la cobertura afectada, la Aseguradora asumirá los gastos derivados de la defensa del Asegurado en la misma proporción que corresponda a la cuantía de la indemnización que, de acuerdo con lo convenido en la póliza, deba satisfacer, respecto del importe total en que se fije la indemnización por el Siniestro. El Asegurado deberá prestar la colaboración necesaria a dicha defensa, comprometiéndose a otorgar los poderes y la asistencia personal que fuesen precisos. La Aseguradora tomará la dirección de todas las gestiones relacionadas con el Siniestro, actuando en nombre del Asegurado para tratar con los perjudicados, sus derechohabientes o reclamantes, comprometiéndose el Asegurado a prestar su colaboración. Si por falta de esta colaboración se perjudicaren o disminuyeren las posibilidades de defensa del Siniestro, la Aseguradora podrá reclamar al Asegurado Daños y Perjuicios en proporción a la culpa del Asegurado y al Perjuicio sufrido. Si el incumplimiento se produjera con la manifiesta intención de perjudicar o de engañar al Asegurador o si obrase dolosamente en connivencia con los reclamantes o con los damnificados, el Asegurador quedará liberado de toda prestación derivada del Siniestro. En cualquier caso, no podrá negociar, admitir ni rechazar reclamaciones de Terceros perjudicados relativas al Siniestro, salvo con autorización expresa de la Aseguradora. La prestación de defensa y representación en causas criminales será potestativa del

Asegurador, y siempre con consentimiento del defendido. Sea cual fuere el fallo o resultado del procedimiento judicial, el Asegurador se reserva la decisión de ejercitar los recursos legales que procedieren contra dicho fallo o resultado, o a conformarse con el mismo. Si el Asegurador estima improcedente el recurso, lo comunicará al Asegurado, quedando éste en libertad para interponerlo por su exclusiva cuenta y aquél obligado a reembolsarle los gastos de abogado y procurador causados, en el supuesto de que dicho recurso prosperase, hasta el límite del importe en que se minore la indemnización a cargo del Asegurador. Cuando se produjere algún conflicto entre el Asegurado y el Asegurador motivado por tener que sustentar éste en el Siniestro intereses contrarios a la defensa del Asegurado, el Asegurador lo pondrá en conocimiento del Asegurado, sin perjuicio de realizar aquellas diligencias que, por su carácter urgente, sean necesarias para la defensa. En este caso, el Asegurado podrá optar entre el mantenimiento de la dirección jurídica por el Asegurador o confiar su propia defensa a otra persona. En este último caso, el Asegurador quedará obligado a abonar los gastos de tal dirección jurídica hasta el límite de 6.000,00 Euros. La Suma asegurada en Condiciones Particulares para la Cobertura de Responsabilidad Civil es la máxima responsabilidad económica exigible del Asegurador por todos los conceptos (indemnización, gastos de representación y defensa y costas procesales, así como otros gastos necesarios tales como peritaciones o similares). No obstante, en el caso de que el litigio se solvente ante los Juzgados y Tribunales españoles y además la dirección jurídica de la reclamación sea asumida por el Asegurador, la Suma asegurada se entenderá liberada de tales gastos, que se satisfarán en exceso de la misma.

4. COBERTURA DE DAÑOS PROPIOS Por la Cobertura de Daños Propios, el Asegurador asumirá, en los términos establecidos en estas Condiciones Generales, el pago de las indemnizaciones o la realización de las prestaciones que correspondan para la reparación de los Daños que sufra el Asegurado ocasionados por los riesgos que a continuación se especifican. Esta cobertura ampara únicamente bienes que se encuentren en España, donde deben tener su domicilio el Tomador y el Asegurado, y hechos ocurridos durante el periodo de vigencia de la Póliza. La presente cobertura incluye únicamente las siguientes garantías:

4.1. GARANTÍA DE DAÑOS A LOS SISTEMAS INFORMÁTICOS DEL ASEGURADO Cuando los Sistemas Informáticos del Asegurado sufran un Daño o Pérdida de Datos a consecuencia de un Evento no Físico cubierto por la Póliza, el

Asegurador garantiza al Asegurado, con el límite de la Suma asegurada establecida en las Condiciones Particulares para la Cobertura de Daños, la prestación, a su cargo, de los Servicios que a continuación se especifican para su reparación. Los servicios serán prestados por profesionales especializados que, en todo caso, designará el Asegurador y no podrán sustituirse por el abono de cantidades al Asegurado en concepto de indemnización, salvo pacto expreso en otro sentido para el caso concreto. Esta garantía ampara también el coste de adquisición de las licencias de sustitución de software cuyo sistema físico de protección haya resultado dañado, perdido o destruido, siempre que el Asegurado dispusiera de estas licencias antes de producirse el siniestro, que sean necesarias y que no fuera posible su recuperación, y que deberá realizar el Asegurado directamente, indemnizando la Aseguradora al Asegurado en la cantidad que corresponda. Los servicios cuyo coste asume el Asegurador por esta garantía son únicamente los siguientes: COSTES DE RESTAURACIÓN Y RECREACIÓN DE DATOS, que incluye únicamente: Coste de recuperación, restauración o recreación de software dañado, perdido o destruido Coste de búsqueda y recopilación de Datos, restauración o recreación de los Datos dañados, perdidos o destruidos disponibles en copias de seguridad (backup), Medios Electrónicos u otros Medios de Información, incluyendo la fuente o la documentación original en la que se basaban los Datos. Se hace constar expresamente que la Compañía se compromete a analizar el Daño y siempre que ello fuera posible, recuperar los Datos. Para poder realizar la reinstalación del software e intentar la recuperación de datos en caso de siniestro, será imprescindible que el asegurado disponga del software original y facilite al proveedor la licencia, así como de copias de seguridad. El servicio se prestará sobre los soportes internos de almacenamiento de datos utilizados en los equipos de procesamiento de datos informático propiedad del Asegurado, y en concreto sobre discos duros, ficheros, sistemas operativos, dispositivos extraíbles, tarjetas de memoria y periféricos, no estando cubierta la recuperación de datos cuando estos se contengan en cualquier otro dispositivo de almacenamiento. La compañía no se hace responsable de la no recuperación de la información o datos. En ningún caso estará cubierto: Las recuperaciones sobre soportes de almacenamiento que hayan sido manipulados antes de la entrega al Asegurador. El coste de las licencias de software cuando estás se estuvieran utilizando de forma ilegal así como el enriquecimiento injusto por parte del Asegurado derivado de este concepto. El abono de indemnizaciones cuando la recuperación resultara imposible, y en concreto, en los casos de desaparición del soporte, de daños

con ácidos o productos similares, en los casos de sobre-escritura del soporte o el conocido como Head-Crash. La recuperación de originales como películas, CD, JUEGOS, software sin su licencia original. Cuando la realización de los servicios antes descritos requiera la intervención de los Empleados del Asegurado, o puedan únicamente ser realizadas por éstos, el Asegurador garantiza con el previo acuerdo por escrito, sin que dicho acuerdo pueda ser denegado injustificadamente al Asegurado, el pago de los gastos necesarios y razonablemente incurridos en la contratación de plantilla y/o horas extras de los Empleados al objeto de restaurar y recrear los Datos del Asegurado, de acuerdo con lo establecido en los puntos anteriores. En ningún caso se asumirá por el Asegurador el pago de cantidades sin previa justificación de las contrataciones o del abono de las horas extraordinarias para esta concreta actividad. COSTES DE DESCONTAMINACIÓN DE CÓDIGO MALICIOSO INFORMÁTICO (MALWARE), que incluye únicamente: Gastos de descontaminación, limpieza y restauración de Datos, copias informáticas de seguridad y Medios Electrónicos, incluyendo los costes de restauración de los Sistemas Informáticos del Asegurado afectados por Código Malicioso Informático (Malware). COSTES DE RESTAURACIÓN DEL SISTEMA DE CONTROL DE ACCESO, que incluye únicamente: Costes de restauración del Sistema De Control De Acceso al Sistema Informático del Asegurado afectado; o Costes de restauración del perímetro de seguridad alrededor del Sistema Informático del Asegurado al estado anterior al Evento No Físico. La restauración será posible si el cliente tiene una copia de seguridad actualizada. En ningún caso estará cubierta por el servicio de restauración: -Cuando el método de acceso se encuentre en todo o en parte localizado en una base de datos o también llamados servicios de directorio (tipo LDAP). -Los servicios que sean propietarios, no estándares, entendiendo por aquellos los servicios de software que funcionan con una licencia de pago, con desarrollos a medida y/o en los que su instalación o configuración se puede efectuar únicamente por la empresa externa que lo desarrolló. HONORARIOS DE EXPERTOS en los siguientes casos: i. ii. iii. para determinar el origen de un Evento No Físico; o para limitar el impacto de un Evento No Físico; o para evaluar la cuantía de costes y gastos sostenidos con respecto a un Evento No Físico. Esta garantía de Daños a los Sistemas Informáticos del asegurado no cubre, en ningún caso: −Sustitución, reemplazo o reparación de equipos de hardware y/o periféricos. Datos cuya fuente original no exista. Cualquier mejora, rediseño o reconfiguración de los Sistemas Informáticos o Datos del Asegurado para ponerlos en

una condición superior de la existente con anterioridad al Evento no Físico. Abono de indemnizaciones cuando no sea posible la descontaminación, restauración o recreación cubiertas por la Póliza.

4.2. GARANTÍA DE INTERRUPCIÓN DEL NEGOCIO El Asegurador garantiza al Asegurado con el sublímite establecido en las Condiciones Particulares para esta garantía, el abono de indemnización por la pérdida efectiva del Margen Bruto debido a la disminución del Volumen de Negocio y/o al aumento en los costes de explotación durante el Período de Indemnización, que se produzca como resultado directo de una interrupción parcial o total de las operaciones de negocio a consecuencia del fallo completo o parcial de los Sistemas Informáticos del Asegurado como consecuencia de un Evento No Físico, cubiertos por la garantía de daños a los Sistemas Informáticos, que afecten negativamente a la disponibilidad de los Sistemas Informáticos del Asegurado. Criterio de Indemnización, se establece un periodo de carencia de 12 horas desde la fecha efectiva del fallo en los sistemas informáticos del asegurado. El Período de Indemnización máximo será de 90 días desde dicha fecha efectiva del fallo, en los términos definidos en el alcance de la presente cobertura. El cálculo de la indemnización se efectuará conforme a los siguientes parámetros: Respecto a la disminución del Volumen de Negocio: La cantidad que resulte de multiplicar el Porcentaje de Indemnización por la cifra en que el Volumen de Negocio se reduzca con relación al Volumen Normal de Negocio, a consecuencia del Evento no físico, durante el período en que se vea afectado (con el límite máximo del Periodo de Indemnización). Si durante el Periodo de Indemnización se vendieran mercancías o se prestaran servicios en cualquier otra parte fuera de los locales asegurados, a cuenta del negocio, sea por el Asegurado o por cualquier otra persona en su nombre, el importe de tales operaciones o servicios se tendrá en cuenta al determinar el Volumen de Negocio habido durante el Periodo de Indemnización. Cualquier tipo de pérdida de Volumen de Negocio que no se derive directamente de la falta de capacidad de suministro de productos y/o servicios del Asegurado a sus clientes provocada por el propio Evento No Físico, no queda amparada por esta Póliza. Del mismo modo, tampoco queda amparada la suspensión o cancelación de pedidos, licencias o contratos que se produzcan con posterioridad a la recuperación de la capacidad operativa tras un Siniestro. b) Respecto al aumento en el coste de explotación: Se indemnizarán los gastos adicionales que se realicen necesaria y razonablemente por parte del Asegurado con el único fin de evitar o aminorar la

disminución del Volumen de Negocio que, a no ser por tales gastos, habría tenido lugar durante el Período de Indemnización. Los gastos adicionales de este apartado serán indemnizados en su totalidad siempre que: No lleven el Margen Bruto a un nivel superior al que se hubiese alcanzado de no ocurrir el Siniestro, en cuyo caso se descontarían los sobrecostes correspondientes al Margen Bruto obtenido de más por el Asegurado sobre el esperado. Su importe no sea superior a la disminución de la indemnización que con los mismos se ha tratado de conseguir. Si transcurrido el Período de Indemnización pactado no se hubiese logrado la recuperación de las existencias de productos terminados al nivel necesario para la actividad normal del negocio, o al existente antes del Siniestro, caso de ser inferior, y siempre que éstas hayan sido utilizadas en el salvamento de pérdidas de ventas, el Asegurador indemnizará los costes extraordinarios a los que el Asegurado tenga que hacer frente para recuperar las citadas existencias. Si las existencias de productos terminados se hubiesen utilizado para evitar pérdidas de ventas durante el período de la Franquicia temporal deducible, la indemnización antes señalada se reducirá en la proporción existente entre el Margen Bruto salvado en dicho período y el total de Margen Bruto salvado. Idéntico criterio se aplicará en el caso de que los productos terminados hayan sido utilizados para salvaguardar la fidelidad de clientes que, caso de haberse perdido, hubiesen provocado pérdidas más allá del Período de Indemnización. Del importe total de la indemnización, calculada en la forma anteriormente indicada, serán deducidos los costes de explotación asegurados que puedan ser economizados o reducidos durante el Período de Indemnización. No están cubiertos, en ningún caso: Reclamaciones de Personas o entidades que hubieran tenido con el Asegurado relación contractual con acceso a sus operaciones de negocio. Daños indirectos, tales como falta de alquiler o uso, rescisión de contrato, pérdida de mercado, suspensión de trabajo o cualquier otro perjuicio análogo. Los Perjuicios que resulten de la interrupción total o parcial del proceso productivo, sin que se incurra en pérdida del Volumen de Negocio y/o el incremento en los costes de explotación. Igualmente no serán indemnizables las pérdidas objeto del seguro si la empresa asegurada no reanuda su actividad. Si el cese definitivo de la misma se debe a una causa de fuerza mayor o a la intervención de cualquier Organismo o Autoridad Pública, se indemnizarán los Gastos Permanentes incurridos hasta el momento en que haya tenido conocimiento de la imposibilidad de reanudar la explotación, y siempre con el límite máximo del Periodo de Indemnización pactado. Los Siniestros que sean consecuencia de la retirada o trabajo lento de los empleados,

cierre patronal y en general, cualquier cese de trabajo que sea causado por un Siniestro no amparado en la Garantía de Daños a los Sistemas Informáticos del Asegurado. En caso de que el negocio asegurado se halle en liquidación o fuera declarado en concurso y se inicie la fase de liquidación, o sea embargado o intervenido judicialmente, esta cobertura quedará automáticamente rescindida desde el momento en que, de acuerdo con la legislación vigente, se declaren tales estados. El Asegurador restituirá la parte de Prima que corresponda al período de seguro, por el que no haya soportado el riesgo como consecuencia de la rescisión anticipada.

4.3. GARANTÍA DE AMENAZA DE EXTORSIÓN CIBERNÉTICA: El Asegurador garantiza el pago al Asegurado, con el sublímite establecido en las Condiciones Particulares para esta Garantía, de los costes y gastos razonables en los que fuera necesario incurrir, con la previa autorización escrita del Asegurador, 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. Salvo pacto expreso en otro sentido para el caso concreto, el Asegurador no asumirá el pago de costes o gastos que no haya autorizado previamente. Obligaciones del Asegurado El Asegurador sólo estará obligado a indemnizar al Asegurado bajo esta garantía cuando el Asegurado cumpla con las siguientes condiciones acumuladas: Notificación: El Asegurado autorizará al Asegurador (o a los representantes nombrados por el Asegurador) a comunicar cualquier Amenaza de Extorsión Cibernética a la policía o a otras autoridades responsables del cumplimiento de la ley. A instancias del Asegurador, el Asegurado deberá ponerlo en conocimiento de la policía o de otras autoridades responsables del cumplimiento de la ley. Confidencialidad: Bajo cualquier circunstancia, en todo lugar y en todo momento el Asegurado garantizará que se mantiene la confidencialidad con respecto a la existencia del seguro contra Amenaza de Extorsión Cibernética cubierto por la presente garantía. En caso de que la existencia del seguro contra Amenaza de Extorsión Cibernética cubierto por esta garantía se hiciera de dominio público o se revelase a un Tercero sin el consentimiento del Asegurador, el Asegurador podrá denegar la cobertura y dar por terminado el seguro cubierto por esta garantía con efecto inmediato, efectivo desde la fecha en que se haya hecho de dominio público o se haya revelado a ese Tercero. No están cubiertos, en ningún caso: Amenazas

de Extorsión por personas o entidades que sean o hayan ostentando para el Asegurado la condición de auditor o consultor externo. Amenazas de Extorsión por Empleados o Directivos en plantilla, o por aquellos que hubieran formado parte de la misma ostentando dicha condición. El importe exigido en concepto de rescate o cualquier otro importe que no sea asegurable de conformidad con la Legislación vigente.

4.4. GARANTÍA DE PROTECCIÓN DE DATOS

4.4.1. MULTAS Y SANCIONES POR VULNERACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS Por la presente garantía, con el sublímite establecido en las Condiciones Particulares para la misma, quedan amparadas, en los términos establecidos en estas Condiciones Generales, las multas o Sanciones impuestas al Asegurado por la Agencia Española de Protección de Datos o autoridad de control equivalente estatal como consecuencia de la vulneración de normas relativas a la protección de Datos de Carácter Personal, por el ejercicio de la actividad objeto del Seguro, como consecuencia de una investigación o inspección iniciada y notificada al Asegurador durante el periodo de vigencia de la Póliza. No está cubierto, en ningún caso: Multas o sanciones de carácter civil o penal, o cualquier otra no asegurable por ley. Multas o Sanciones impuesta al Asegurado cuando éste no haya llevado a cabo con carácter previo a la contratación del Seguro un proceso de adaptación interna acreditable para el cumplimiento de las leyes y disposiciones materiales sobre Protección de Datos de Carácter Personal. Multas o Sanciones impuestas por incumplimientos deliberados o reiterados de la normativa reguladora de la Protección de Datos de Carácter Personal. La responsabilidad civil del Asegurado por daños y Perjuicios de cualquier tipo frente a Empleados en nómina del mismo. La responsabilidad que derive del ejercicio de actividades distintas a las contempladas en las disposiciones legales que regulen la actividad objeto del Seguro.

4.4.2. GASTOS DERIVADOS DE NOTIFICACIÓN POR VIOLACIÓN DE PRIVACIDAD Por la presente garantía, con el sublímite establecido en las Condiciones Particulares para la misma , y en los términos de actividad asegurada, el Asegurador garantiza al Asegurado el pago de los gastos necesarios y razonablemente incurridos para cumplir con cualquier supuesto contenido en la legislación española o europea, de notificar al interesado, la existencia de: a) Daño o pérdida de Datos de Carácter Personal, confiados al cuidado, custodia y control del Asegurado, causado directamente por: Un Acto Informático Doloso perpetrado en el Sistema Informático del Asegurado, o

Un Código Malicioso Informático (malware) activo en el Sistema Informático del Asegurado, o Robo de Datos de Carácter Personal, confiados al cuidado, custodia y control del Asegurado, en Medios Electrónicos, Medios de Información o en el Sistema Informático del Asegurado. Revelación de Datos de Carácter Personal confiados al cuidado, custodia y control del Asegurado, en Medios Electrónicos, Medios de Información o en el Sistema Informático del Asegurado a Terceros no autorizados. Quedarán expresamente amparados los gastos derivados de: Gastos de asesoramiento legal de Terceros para evaluar la violación y asesorar sobre las medidas más apropiadas. Redacción por un asesor legal de notificación a cualquier Tercero o Empleado afectado por la violación de Datos real o supuesta, y los gastos de envío y/o correo para emitir y/o enviar dichas notificaciones o emitir notificaciones sucesivas. El establecimiento de un servicio de atención telefónica (call center) para gestionar las llamadas entrantes y/o salientes en relación con la violación de Datos. La realización de una investigación forense de los Sistemas Informáticos del Asegurado, si fuere requerida por ley u organismo oficial. La investigación y la emisión del oportuno informe serán efectuados por un especialista contratado por la propia Aseguradora, pudiendo ésta autorizar al Asegurado excepcionalmente la contratación de servicios externos. Diseño y puesta en marcha de una campaña de publicidad, por una firma tercera de relaciones públicas, dirigida a mitigar el potencial impacto mediático de la violación de Datos en la marca y reputación del Asegurado durante el periodo inmediato tras una violación. Los gastos derivados del cumplimiento de obligaciones contractuales referentes a notificación por violación de la privacidad asumidas por el Asegurado en favor de Terceros cuando se produzca alguno de los eventos arriba indicados que den lugar a la aplicación de esta garantía.

4.4.3. GASTOS DERIVADOS DE RESTITUCIÓN DE LA IMAGEN POR SANCIONES IMPUESTAS POR LA AGENCIA DE PROTECCIÓN DE DATOS El Asegurador garantiza al Asegurado, con el previo acuerdo por escrito y sin que dicho acuerdo pueda ser denegado injustificadamente, con el sublímite establecido en Condiciones Particulares por Siniestro y anualidad para esta Garantía, aquellos gastos en los que razonablemente deba incurrir el Asegurado para restituir su imagen comercial o marca mediante el asesoramiento por parte de profesionales independientes en el ámbito de la comunicación, marketing de relaciones públicas o la publicidad y con el propósito de mitigar o restituir el Daño a su reputación como consecuencia de una

Sanción impuesta por la Agencia Estatal De Protección De Datos. Esta garantía amparará los referidos gastos únicamente cuando se trate de una Sanción cubierta por la Póliza.

5. RIESGOS NO CUBIERTOS RIESGOS NO CUBIERTOS POR NINGUNA DE LAS COBERTURAS Y GARANTÍAS DE LA PÓLIZA El Asegurador no garantiza en ningún caso las Reclamaciones derivadas de: Actos intencionados, maliciosos o ilegales realizados por el Asegurado o persona por la que deba responder, o bien derivados de la infracción o incumplimiento deliberado de las normas legales o por haberse desviado a sabiendas de la ley, disposiciones, instrucciones o condiciones de los clientes o de personas autorizadas por ellos. Por hechos o circunstancias que, a la entrada en vigor de la Póliza, fueran conocidos de forma fehaciente por el Tomador o por el Asegurado. Por responsabilidades y obligaciones que el Asegurado haya asumido bajo cualquier forma de garantía, acuerdo o convenio contractual y que no serían legalmente exigibles en caso de no existir, salvo que el Asegurado hubiere estado sujeto a la misma responsabilidad civil en ausencia de dicha garantía, acuerdo o convenio contractual. Daños materiales y personales de cualquier tipo. Multas o Sanciones de carácter civil o penal así como aquellas no asegurables por ley a excepción de las Sanciones impuestas por la Agencia de Protección de Datos. Daños por hechos de guerra civil o internacional, motín o tumulto popular, terrorismo, terremotos e inundaciones y otros eventos extraordinarios de análoga naturaleza. Por interrupciones, sobretensiones, cortes u oscilaciones del suministro eléctrico y fallos de los sistemas de ADSL, infraestructuras GPS, sistemas de supervisión, control y adquisición de datos (SCADA), estructura básica de Internet o proveedores de servicios de telecomunicación, que no estén bajo la dirección operativa del Asegurado. Por discriminación de cualquier tipo, real o supuesta, incluyendo pero no limitando las referidas a la edad, color, raza, género, credo, nacionalidad de origen, estado civil, preferencias sexuales, discapacidad o embarazo. Derivadas de juegos de azar, pornografía, premios, cupones, o la venta o suministro de artículos prohibidos, restringidos o regulados, incluyendo, pero no limitándose a, bebidas alcohólicas, tabaco o drogas. Derivadas de propiedad intelectual o industrial, incluyendo “copyright”, derechos de marca, o la apropiación indebida, robo, copia, exhibición o publicación de cualquier secreto industrial La violación de patentes y modelos de utilidad industriales. Por el uso de software y/o aplicaciones utilizado de forma ilegal, sin licencia, o en fase de desarrollo, experimental o prueba.

Consecuencia directa o indirecta de la suspensión, cancelación, revocación o fallo al renovar cualquiera de los nombres de dominio o URL del Asegurado. Daños producidos por fusión o fisión nuclear, radiación y contaminación radioactiva o química. Aquellas partes de las Reclamaciones que supongan una mejora respecto a la posición financiera para el perjudicado o que excedan de la obligación legal de reparar el Daño. Consecuencia directa de cualquier período planificado de no funcionamiento de los sistemas del Asegurado, incluyendo cualquier falta de funcionamiento que sea el resultado de un apagón planificado que dure más de lo que se había planificado o esperado inicialmente. Consecuencia directa de la falta de previsión o de capacidad del Asegurado para atender demandas a nivel normal, o por encima de lo normal, de los Sistemas Informáticos del Asegurado, excepto cuando esta demanda sea resultado de un Acto Informático Doloso o Denegación de Servicio. Al respecto de cualquier espionaje real o supuesto, escucha ilegal, pinchazo telefónico, o grabación de audio o video no autorizada, cometida por el Asegurado o por un Tercero en su nombre con el conocimiento y consentimiento del Asegurado. De equipos hardware y/o periféricos. Derivados directamente de un asesoramiento negligente del Asegurado o de unos servicios profesionales prestados negligentemente por el Asegurado a un Cliente a cambio de una retribución. Consecuencia directa de un Error Humano, tal y como se define en estas Condiciones Generales. Derivados de daños causados por personal subcontratado o externo que no preste sus servicios en las instalaciones del Asegurado y/o tenga acceso a los Sistemas Informáticos del Asegurado por razón distinta a la de su empleo.

NORMAS GENERALES

1. LÍMITE DE INDEMNIZACIÓN El límite de indemnización establecido en las Condiciones Particulares se aplica por periodo de Seguro y constituye la cantidad máxima a pagar por el Asegurador por todas las pérdidas de los Asegurados y bajo todas las coberturas contempladas en la Póliza. Las coberturas de RESPONSABILIDAD CIVIL, y DAÑOS PROPIOS, presentan límites de indemnización independientes cuyo sumatorio constituye el límite de indemnización total de la póliza. Asimismo, los Sublímites de Indemnización establecidos en las Condiciones Particulares constituyen las cantidades máximas a pagar por cada uno de los conceptos establecidos y forman parte integrante del límite de indemnización, no siendo en adición al mismo. Si una Reclamación comportara cuestiones cubiertas y no cubiertas bajo esta Póliza, el

Asegurado y la Entidad harán todo lo posible por asignar, de modo justo y adecuado, entre el Asegurado y la Entidad, la parte de la pérdida cubierta y la no cubierta, tomando en consideración las implicaciones legales y financieras atribuibles a eventos cubiertos y no cubiertos bajo esta Póliza, así como los posibles beneficios obtenidos por las partes.

2. BASES DEL CONTRATO La solicitud de seguro y el cuestionario cumplimentados por el Tomador del Seguro, así como la proposición del Asegurador, en su caso, en unión de esta Póliza, constituyen un todo unitario, fundamento del seguro, que sólo alcanza, dentro de los límites pactados, a los riesgos especificados en la misma.

3. CONSENTIMIENTO Sin el consentimiento escrito del Asegurador, el Asegurado no podrá:

Revelar a persona alguna la naturaleza de los términos de este Seguro (salvo en lo referente al Artículo 76 de la Ley 50/80 de 8 de octubre, de Contrato de Seguro); excepto a requerimiento judicial o administrativo. Reconocer responsabilidad alguna; Realizar ninguna transacción, oferta, promesa o pago.

4. DECLARACIONES SOBRE EL RIESGO AL EFECTUAR EL SEGURO Y DURANTE SU VIGENCIA La presente Póliza ha sido concertada sobre la base de las declaraciones formuladas por el Tomador del Seguro en el cuestionario que le ha sometido el Asegurador, que han motivado la aceptación del riesgo por el Asegurador, la asunción por su parte de las obligaciones derivadas del contrato y la fijación de la Prima. Si el Tomador del Seguro, al formular las declaraciones del cuestionario, incurriera en reserva o inexactitud sobre las circunstancias por él conocidas que puedan influir en la valoración del riesgo, se aplicarán las reglas siguientes: a) b) El Asegurador podrá rescindir el contrato, mediante declaración dirigida al Tomador del Seguro en el plazo de un mes, a contar desde el conocimiento de la reserva o inexactitud. Corresponderán al Asegurador, salvo que concurra dolo o culpa grave por su parte, las primas relativas al período de seguro en curso en el momento en que se haga la declaración. Si el siniestro sobreviene antes de que el Asegurador efectúe dicha declaración, la indemnización se reducirá proporcionalmente a la diferencia entre la prima convenida y la que se hubiese aplicado de haberse conocido la verdadera entidad del riesgo. Si medió dolo o culpa grave del Tomador del Seguro, el Asegurador quedará liberado del pago de la indemnización.

5. DEBER DE COMUNICAR LA EXISTENCIA DE OTRAS PÓLIZAS El Tomador del Seguro o el Asegurado quedan obligados a comunicar al Asegurador la existencia de otras Pólizas, contratadas con distintos Aseguradores, cubriendo los efectos que un mismo riesgo puede producir sobre el mismo interés y durante idéntico tiempo.

6. MODIFICACIONES DEL RIESGO AGRAVACIÓN DEL RIESGO El Tomador del Seguro o el Asegurado deberán durante la vigencia del contrato comunicar al Asegurador, tan pronto como le sea posible, la alteración de los factores y las circunstancias declaradas en el cuestionario que agraven el riesgo y sean de tal naturaleza que si hubieran sido conocidas por éste en el momento de la perfección del contrato no lo habría celebrado o lo habría concluido en condiciones más gravosas. La agravación del riesgo podrá ser aceptada o no por el Asegurador y se aplicarán las normas siguientes: 1. 2. En caso de aceptación, el Asegurador propondrá al Tomador del Seguro la modificación correspondiente del contrato, en el plazo de dos meses a contar desde el día en que la agravación le haya sido declarada. El Tomador del Seguro dispone de quince días, desde la recepción de esa proposición, para aceptarla o rechazarla. En caso de rechazo, o de silencio por parte del Tomador, el Asegurador puede, transcurrido dicho plazo, rescindir el contrato previa advertencia al Tomador del Seguro, dándole, para que conteste, un nuevo plazo de quince días, transcurridos los cuales y dentro de los ocho siguientes, comunicará al Tomador del Seguro la rescisión definitiva. Si el Asegurador no acepta la modificación del riesgo, podrá, rescindir el contrato, comunicándolo por escrito al Asegurado dentro de un mes, a partir del día en que tuvo conocimiento de la agravación del riesgo. En el caso de que el Tomador del Seguro o Asegurado no haya efectuado su declaración y sobreviniera un Siniestro, el Asegurador queda liberado de su prestación, si el Tomador o el Asegurado han actuado con mala fe. En otro caso, la prestación del Asegurador se reducirá proporcionalmente a la diferencia entre la Prima convenida y la que se hubiera aplicado de haberse conocido la verdadera entidad del riesgo. En el caso de agravación del riesgo durante la duración del seguro que dé lugar a un aumento de Prima, cuando por esta causa quede rescindido el contrato, si la agravación es imputable al Asegurado, el Asegurador hará suya en su totalidad la Prima cobrada. Siempre que dicha agravación se hubiera producido por causas ajenas a la voluntad del Asegurado, éste tendrá derecho a ser reembolsado por la parte de la Prima satisfecha correspondiente al período que falte por transcurrir de la anualidad en curso si el Asegurador no acepta la modificación del riesgo.

DISMINUCIÓN DEL RIESGO El Tomador del Seguro o el Asegurado podrá, durante el curso del contrato, poner en conocimiento del Asegurador todas las circunstancias que disminuyan el riesgo y sean de tal naturaleza que si hubieran sido conocidas por éste en el momento de la perfección del contrato, lo habría concluido en condiciones más favorables para el Tomador del Seguro. En tal caso, al finalizar el período en curso cubierto por la Prima, el Asegurador deberá reducir el importe de la Prima futura en la proporción correspondiente, teniendo derecho el Tomador del Seguro, en caso contrario, a la resolución del contrato y a la devolución de la diferencia entre la Prima satisfecha y la que le hubiera correspondido pagar, desde el momento de la puesta en conocimiento de la disminución del riesgo.

7. EFECTO Y DURACIÓN DEL CONTRATO El Seguro se estipula por el período señalado en las Condiciones Particulares de la Póliza y entrará en vigor el día y hora señalados en las mismas, siempre que estén firmadas y la Compañía haya cobrado la Prima del primer recibo. Si se contrata por períodos renovables, cuando la duración inicial del seguro sea inferior a un año, el seguro se prorrogará automáticamente por periodos sucesivos de igual duración; si el periodo inicial es superior a un año, se prorrogará automáticamente por períodos sucesivos de un año cada vez, salvo que alguna de las partes se oponga a la prórroga mediante notificación escrita a la otra, efectuada con un plazo de, al menos, un mes de antelación a la conclusión del período en curso cuando quien se oponga a la prórroga sea el Tomador, y de dos meses cuando sea el Asegurador.

8. IMPORTE Y PAGO DE LA PRIMA Y EFECTOS DE SU IMPAGO NORMA GENERAL El Tomador del Seguro está obligado al pago de la Prima de acuerdo con las Condiciones Generales y Particulares de la Póliza. En ausencia de pacto, respecto al lugar de pago, el Asegurador presentará los recibos en el último domicilio que el Tomador del Seguro le haya notificado. La Prima es indivisible y se debe y corresponde al Asegurador por entero durante todo el periodo de duración del contrato pactado, aun en el caso de que se haya acordado el fraccionamiento del pago. En caso de extinción del contrato antes de la fecha de vencimiento pactada, o de cualquiera de sus prórrogas, el Asegurador no está obligado a reintegrar al Tomador cantidad alguna correspondiente a la Prima que haya sido satisfecha íntegramente, salvo en los supuestos legalmente previstos. PRIMA INICIAL La Prima inicial es la que se fija en las Condiciones Particulares y corresponde al período inicial de cobertura señalado en las mismas. Si por

culpa del Tomador del Seguro la Prima no ha sido pagada una vez firmado el contrato o la Prima única no lo ha sido a su vencimiento, el Asegurador tiene derecho a resolver el contrato o a exigir el pago de la Prima debida en vía ejecutiva. Salvo pacto expreso en contrario, si la Prima no ha sido pagada antes de que se produzca el Siniestro, el Asegurador quedará liberado de su obligación. PRIMAS SUCESIVAS Para el caso de prórroga tácita del contrato, la Prima de los períodos sucesivos será la que resulte de aplicar las tarifas de Prima que tenga establecidas el Asegurador en cada momento, fundadas en criterios técnico-actuariales, teniendo en cuenta, además, las modificaciones de garantías o las causas de agravación o disminución del riesgo que se hubieran producido, conforme a lo previsto en estas Condiciones Generales y el historial de siniestralidad de la Póliza registrado en los períodos de seguro precedentes. Si la prima fijada para el nuevo periodo de cobertura implicase un incremento respecto a la del periodo precedente, el Asegurador, al menos dos meses antes del vencimiento del contrato, comunicará al Tomador del Seguro el importe de la Prima para el nuevo período de cobertura, mediante envío de un aviso de cobro del recibo correspondiente conforme a lo establecido en el apartado 14 de estas Condiciones Generales para las comunicaciones. La falta de pago de una de las Primas sucesivas dará lugar a que la cobertura quede suspendida un mes después del día de su vencimiento. Si se produjera un Siniestro durante el transcurso de ese mes, el Asegurador podrá deducir del importe a indemnizar el de la Prima adeudada para el periodo en curso. Si el Asegurador no reclama el pago pendiente de la Prima dentro de los seis meses siguientes a su vencimiento, el contrato quedará extinguido de forma automática. PAGO A TRAVÉS DE ENTIDAD FINANCIERA O DE CRÉDITO Si se pacta, como forma de pago, la domiciliación bancaria de los recibos de Prima, el Tomador del Seguro entregará al Asegurador carta dirigida al Banco o Entidad de Crédito, dando la orden correspondiente, y serán de aplicación, además de las contenidas en este capítulo, las normas siguientes: a) Primera Prima La Prima se supondrá satisfecha desde el día del efecto de la Póliza salvo que, intentado el cobro dentro del plazo de un mes a partir de dicho efecto, la Entidad Financiera o de Crédito designada devolviera el recibo impagado. En tal caso, el Asegurador notificará por escrito al Tomador de Seguro el impago producido y que tiene el recibo en el domicilio del Asegurador durante 15 días para su pago. Transcurrido este plazo sin que la Prima hubiera sido satisfecha, el contrato quedará resuelto. b) Primas sucesivas Si la Entidad Financiera o de Crédito devolviera el recibo impagado, el Asegurador notificará el impago al Tomador del

Seguro indicándole que tiene el recibo en el domicilio de ésta para su pago. El Seguro quedará en suspenso si no se realiza el pago dentro del mes siguiente al día de vencimiento del Seguro o dentro del plazo de 15 días desde la citada notificación del impago al Tomador, si hubiese transcurrido dicho mes. PAGO DURANTE LA SUSPENSIÓN DE LA COBERTURA DEL SEGURO Sí el contrato no hubiera sido resuelto o extinguido conforme a los artículos anteriores, la cobertura volverá a tener efecto a las 24 horas del día en que el Tomador del Seguro pague la Prima. FRACCIONAMIENTO DEL PAGO Podrá pactarse el fraccionamiento del pago de la Prima, en los plazos y de acuerdo con las estipulaciones que se establezcan en las Condiciones Particulares de la Póliza. Si el Tomador del Seguro no pagase uno de los recibos en que se hubiese fraccionado el pago de la Prima, el Asegurador puede exigir al Tomador el pago de todos los recibos pendientes de vencimiento, pago que habrá de hacerse efectivo en el plazo máximo de los treinta días siguientes a aquél en el que el Tomador recibió la notificación del Asegurador por medios fehacientes; de no producirse el pago, el Seguro quedará en suspenso un mes después del día del vencimiento de la primera fracción de Prima impagada. Sin perjuicio de lo dispuesto en el apartado precedente y en tanto no se haya producido la suspensión de la cobertura, en caso de Siniestro el Asegurador podrá deducir de la indemnización el importe de las fracciones de Prima vencidas y no satisfechas por el Tomador del Seguro. Si se produjera la pérdida total de los bienes asegurados, se deducirá también el importe de las fracciones de Prima no vencidas correspondientes a la anualidad del Seguro en curso

9. ACTUACIÓN EN CASO DE SINIESTRO OBLIGACIÓN DE COMUNICAR EL SINIESTRO El Tomador del Seguro o el Asegurado deberán comunicar al Asegurador el acaecimiento del Siniestro dentro del plazo máximo de siete días de haberlo conocido, salvo que se haya fijado en la Póliza un plazo más amplio. En caso de incumplimiento, el Asegurador podrá reclamar los daños y Perjuicios causados por la falta o retraso de la declaración. En caso de existir varios Aseguradores, esta comunicación deberá hacerse a cada uno de ellos, con indicación del nombre de los demás. DEBER DE INFORMACIÓN El Tomador del Seguro o el Asegurado deberán, además, dar al Asegurador toda clase de informaciones sobre las circunstancias y consecuencias del Siniestro. En caso de violación de este deber la pérdida del derecho a la indemnización sólo se producirá en el supuesto de que hubiese concurrido dolo o culpa grave. DEBER DE COLABORACIÓN El Tomador del Seguro y el Asegurado

habrán de colaborar en la más correcta tramitación del Siniestro, comunicando a la Compañía en el plazo más breve posible cualquier notificación judicial, extrajudicial o administrativa que llegue a su conocimiento y esté relacionada con el Siniestro. En cualquier caso, no deberán negociar, admitir ni rechazar reclamaciones de Terceros perjudicados relativas al Siniestro, salvo con autorización expresa de la Compañía.

10. CONCURRENCIA DE SEGUROS Si existen varios Seguros el Asegurador contribuirá al abono de la indemnización en proporción a la propia suma asegurada, sin que pueda superarse la cuantía del Daño. Dentro de este límite el Asegurado puede pedir a cada Asegurador la indemnización debida, según el respectivo contrato. Si por dolo se hubiera omitido esta declaración, el Asegurador no está obligado al pago de la indemnización.

11. SUBROGACIÓN DEL ASEGURADOR El Asegurador, una vez pagada la indemnización, podrá ejercitar los derechos y las acciones que por razón del Siniestro correspondieran al Asegurado frente a las personas responsables del mismo, hasta el Límite de la Indemnización. El Asegurador no podrá ejercitar en perjuicio del Asegurado los derechos en que se haya subrogado. El Asegurado será responsable de los Perjuicios que, con sus actos u omisiones, pueda causar al Asegurador en su derecho a subrogarse. El Asegurador no tendrá derecho a la subrogación contra ninguna de las personas cuyos actos u omisiones den origen a responsabilidad del Asegurado, de acuerdo con la Ley, ni contra el causante del Siniestro que sea, respecto del Asegurado, pariente en línea directa o colateral dentro del tercer grado civil de consanguinidad, padre adoptante o hijo adoptivo que convivan con el Asegurado. Pero esta norma no tendrá efecto si la responsabilidad proviene de dolo o si la responsabilidad de los mismos está amparada por un contrato de Seguro. En este último supuesto, la subrogación estará limitada en su alcance de acuerdo con los términos de dicho contrato. En caso de concurrencia del Asegurador y Asegurado frente a tercer responsable, el recobro obtenido se repartirá entre ambos, en proporción a su respectivo interés.

12. REPETICIÓN DEL ASEGURADOR CONTRA EL ASEGURADO El Asegurador podrá repetir contra el Asegurado por el importe de las indemnizaciones que haya debido satisfacer como consecuencia del ejercicio de la acción directa por el perjudicado o sus derechohabientes, con fundamento en causas excluidas de cobertura o falta de vigencia de la Póliza que no fueran oponibles al Tercero perjudicado.

13. PRESCRIPCIÓN, JURISDICCIÓN E INSTANCIAS DE RECLAMACIÓN Las acciones que se deriven de este contrato prescribirán en el término de dos años, a contar desde la fecha en que puedan ejercitarse. El presente contrato queda sometido a la jurisdicción española y, dentro de ella, será juez competente para el conocimiento de las acciones derivadas del mismo el del domicilio del Asegurado, a cuyo efecto éste designará uno en España si estuviese domiciliado en el extranjero. Conforme a la normativa establecida para la protección de los usuarios de los servicios financieros, en el caso de que se suscite controversia en la interpretación o ejecución del presente contrato de seguro, el Tomador del seguro, el Asegurado, los beneficiarios y los terceros perjudicados o sus derechohabientes, podrán formular reclamación o queja mediante escrito dirigido a la Dirección de Reclamaciones de MAPFRE por escrito (Apartado de correos 281- 28220 Majadahonda (Madrid), o por correo electrónico (reclamaciones@mapfre.com) de conformidad con el Reglamento para la Solución de Conflictos entre las Sociedades del Grupo MAPFRE y los Usuarios de sus Servicios Financieros, que puede consultarse en la página Web "mapfre.es", y las normas de actuación que lo resumen y que se facilitan al Tomador junto con este contrato. Asimismo, podrán formular reclamaciones y quejas los clientes de la Aseguradora, así como sus derechohabientes, en relación con la actuación de sus agentes de seguros y operadores de bancaseguros, de conformidad con el Reglamento y el procedimiento antes citado. La Reclamación podrá realizarse en soporte papel o por medios informáticos, electrónicos o telemáticos, conforme a lo previsto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y en el teléfono 900205009. Desestimada dicha reclamación o queja o transcurrido el plazo de dos meses desde su presentación, e l usuario podrá éste formular reclamación o queja ante el Servicio de Reclamaciones de la Dirección General de Seguros y Fondos de Pensiones (Paseo de la Castellana, 44, 28046 Madrid; correo electrónico: reclamaciones.Seguros@mineco.es, Oficina virtual: oficinavirtual.dgsfp@mineco.es.), a cuyo efecto, si lo solicita, pondremos a su disposición el formulario correspondiente. Sólo con la expresa conformidad de las partes, podrán someterse las diferencias derivadas de la interpretación y cumplimiento de este contrato al juicio de mediadores o árbitros, de acuerdo con la legislación vigente.

14. COMUNICACIONES Las comunicaciones del Tomador del Seguro, del Asegurado o del Beneficiario sólo se considerarán válidas si han sido dirigidas por escrito al Asegurador. En caso de contratación a distancia, cuando el contrato se haya

perfeccionado por el consentimiento de las partes manifestado de forma verbal, las comunicaciones relativas a las declaraciones de los factores de riesgo y demás datos necesarios para la suscripción y emisión de la Póliza o sus suplementos se harán verbalmente. Las partes se autorizan mutuamente a grabar las conversiones telefónicas que se mantengan. Todas las comunicaciones entre el Tomador, Asegurado o Beneficiario y la Aseguradora que puedan efectuarse por razón de esta Póliza, podrán realizarse y serán válidas, además de por carta, por cualquier otro medio escrito, incluido correo electrónico, SMS o FAX, en la dirección que tanto la Aseguradora como el Tomador hubieran facilitado, ya sea al contratar la Póliza o en un momento posterior, debiendo el Tomador comunicar a la Aseguradora, tan pronto como sea posible, cualquier cambio de domicilio, teléfono, fax o dirección de correo electrónico facilitado. Las comunicaciones efectuadas a la Aseguradora por un Corredor de Seguros, en nombre del Tomador del Seguro, surtirán los mismos efectos que si las realizara éste, salvo expresa indicación en contrario por su parte. En todo caso, se precisará el consentimiento expreso del Tomador del Seguro para modificar o rescindir el contrato del seguro en vigor.

15. ACEPTACIÓN EXPRESA La presente Póliza está formada por la solicitud, las Condiciones Particulares y las presentes Condiciones Generales, así como por cualquier suplemento emitido a la misma. El Tomador de la Póliza reconoce expresamente haber recibido dicha documentación, manifestando su conocimiento y conformidad con las mismas. El Tomador de la Póliza manifiesta que ha leído, examinado y entendido el contenido y alcance de todas las cláusulas de la presente Póliza y, especialmente, aquellas que, debidamente resaltadas en letra negrita, pudieran ser limitativas de sus derechos. El Tomador de la Póliza asume el deber de informar a los Asegurados sobre sus derechos y obligaciones, y para que conste su conocimiento, expresa conformidad y aceptación de las mismas, firma al pie de cada una de las páginas.

En _____ a, _____ POR EL TOMADOR

(firma y sello) POR MAPFRE ESPAÑA, COMPAÑÍA DE SEGUROS Y REASEGUROS, S. A. (firma y sello)