THIBER
The cybersecurity think tank

CIBERSEGUROS

la transferencia del **ciberriesgo** en España

Patrocinado por:

AIG

AON
Empower Results®

K2 Intelligence
Investigations · Compliance Solutions · Cyber Defense

MARSH

minsait
by Indra

Telefónica

Partner académico:

ie business school

Copyright y derechos:

THIBER, the Cyber Security Think Tank

Todos los derechos de esta Obra están reservados a THIBER, the Cyber Security Think Tank. Los titulares reconocen el derecho a utilizar la Obra en el ámbito de la propia actividad profesional con las siguientes condiciones:

a) Que se reconozca la propiedad de la Obra indicando expresamente los titulares del Copyright.

b) No se utilice con fines comerciales.

c) No se creen obras derivadas por alteración, trasformación y/o desarrollo de esta Obra.

Los titulares del Copyright no garantizan que la Obra esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores señalados.

Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos citados en la Obra son de propiedad exclusiva de los titulares correspondientes.

Más información:

THIBER, The Cyber Security Think Tank.

Editado en Madrid. Abril de 2016.

ISBN 978-84-608-7693-9

Patrocinado por:

Partner académico:

CIBERSEGUROS

la transferencia del **ciberriesgo** en España

ÍNDICE

1.

Ciberseguros frente al riesgo tecnológico

Ciberseguros frente al riesgo tecnológico

El ciberespacio es un nuevo entorno repleto de oportunidades. Éste ha redefinido la forma de comunicarse y relacionarse de ciudadanos, empresas y gobiernos. También se ha erigido como uno de los principales pilares del mercado digital, sustentando gran parte de las actividades económicas y sociales de una sociedad moderna como la española.

Sin embargo, a medida que el ciberespacio se va integrando en nuestras vidas diarias, también se van planteando nuevos riesgos y amenazas de variable naturaleza e impacto sobre los ciudadanos, empresas y administraciones. Cada día se plantean nuevos peligros cibernéticos que difícilmente se pueden cuantificar mediante ejercicios prospectivos.

Es por ello que las nuevas amenazas asociadas al entorno digital, la interconectividad y la digitalización del tejido empresarial español constatan la necesidad de un cambio de paradigma al gestionar los riesgos cibernéticos. Es necesario replantear las estrategias de gestión de riesgos digitales corporativos y adoptar medidas que permitan mejorar la fiabilidad, seguridad y resiliencia con el fin de que las empresas y los ciudadanos puedan aprovechar plenamente las ventajas de la economía digital.

Hoy en día ya no cuestionamos si las ciberamenazas pueden incidir sobre una empresa. La pregunta que tenemos que plantearnos es, simplemente, cuándo sucederá y si la organización contará con los mecanismos adecuados para hacerles frente.

Es en este contexto donde las pólizas de ciberriesgos se establecen como medidas de defensa de primer orden que, junto con la concienciación de los trabajadores y el incremento de la ciberseguridad corporativa, tendrán beneficiosos efectos sobre el mercado español. Más concretamente, estas pólizas no sólo permitirán gestionar los ciberriesgos corporativos con mayor efectividad que hasta ahora y mejorar el nivel general de la ciberseguridad industrial de nuestro país; sino que también aportarán un conocimiento relevante de las amenazas cibernéticas que atenazan a nuestras empresas.

Para ello, el propio sector asegurador, los proveedores de servicios de ciberseguridad y de asesoramiento en riesgos, la Administración Pública, así como el resto del sector empresarial deben ser los protagonistas de esta nueva gestión integral de los ciberincidentes.

En consecuencia, la mentalidad y el enfoque con el que las aseguradoras deben diseñar y comercializar sus productos en este entorno también debe tener un enfoque global, transversal y multidimensional. No puede limitarse a la actividad que el asegurado realiza en el ciberespacio, sino que debe contemplar todas las interrelaciones que existen hoy – y que serán cada vez más en el futuro inmediato – entre este entorno y dichas actividades.

El presente documento, el primero de su clase focalizado en el mercado nacional, servirá como una herramienta de análisis para el asegurado y como referencia – bajo una lógica propositiva – de nuevas medidas de trabajo común para mejorar la gestión corporativa y la resiliencia general ante incidentes cibernéticos.

Javier Solana
Ex Alto Representante para la Política Exterior y de Seguridad Común (PESC) de la Unión Europea, ex secretario general de la OTAN, ex ministro de Asuntos Exteriores.

2.
Resumen ejecutivo

Resumen ejecutivo

Desde sus inicios en la década de 1990 para gestionar los riesgos corporativos vinculados con la explosión de Internet, el mercado de los ciberseguros ha ido penetrando lenta pero decididamente en el tejido industrial estadounidense y europeo. Con un número creciente de proveedores, una cadena de valor cada vez más madura, un volumen de negocio cada vez mayor y un aumento de la oferta y la competencia en el sector, los ciberseguros se han convertido en un producto cada vez más popular. Precisamente, cada vez son más las empresas que están contratando este tipo de productos como una compra obligatoria y no como una acción discrecional.

En nuestro país, con un volumen de negocio de 500 millones de euros anuales y un crecimiento anual del 12%, el mercado de los ciberseguros se halla en plena expansión. Hasta fechas recientes, éste se había centrado en productos dirigidos a las grandes empresas debido a su mayor exposición a los riesgos cibernéticos. No obstante, actualmente este mercado se está orientando al sector de la pequeña y mediana empresa – con una limitada experiencia en la gestión de estos riesgos, una creciente exposición a los ciberataques y una necesidad de cumplir con un marco regulatorio cada vez más exigente en materia de protección de datos – adaptando su oferta a su realidad específica y necesidades concretas.

En consecuencia, los ciberseguros no sólo permiten transferir el riesgo corporativo a terceros, sino que también promueven la adopción de medidas de ciberprotección más robustas y mejorar la ciberseguridad del mercado, puesto que pueden requerir a sus clientes el cumplimiento de unas cautelas mínimas de ciberseguridad como condición *sine qua non* para la contratación de las pólizas; ofrecer descuentos en las primas a aquellas entidades que demuestren un nivel adecuado de madurez en seguridad; poner en práctica los procedimientos de gestión de ciberincidentes en nombre del asegurado; comprender los patrones de las amenazas y mejorar el intercambio de información entre el gobierno y las empresas aseguradas respecto a ciberincidentes proporcionando una alerta temprana ante este tipo de incidentes.

Un mercado de ciberseguros consolidado desempeñará un papel fundamental en la economía española porque permitirá al asegurado trasladar los riesgos de su actividad a un tercero con capacidad económica para soportar aquéllos; reforzará la posición crediticia del asegurado y fomentará la inversión productiva y el ahorro, puesto que financieramente el tomador de una póliza de seguros se constituye en prestamista del asegurador, quien convierte las primas que recibe en una inversión a largo plazo y, por ende, en ahorro para el asegurado.

Aunque el mercado nacional de los ciberseguros debe ser netamente privado, para incentivar su adopción pueden crearse unas líneas de acción desde los organismos gubernamentales de forma que se reduzca el coste de las primas mediante la asunción de parte de las coberturas de las aseguradoras privadas a través de programas de reaseguro. Igualmente, cuando los riesgos sean considerados como "no asegurables" por el mercado asegurador privado, el Estado debería asumir ciertos riesgos para reemplazar o estabilizar el mercado privado mediante programas específicos de compensación. En

tercer lugar, sería fundamental promover la adopción de marcos de ciberseguridad con un nivel de madurez determinado como una muestra de control debido, siendo de esta forma condiciones atenuantes ante potenciales delitos y limitando por extensión las responsabilidades civiles e, incluso, penales según la legislación nacional. Al mismo tiempo, teniendo en cuenta que la propia Administración Pública española posee un nutrido ecosistema de proveedores de Tecnologías de la Información y las Comunicaciones (TIC), se recomienda que actúe como eje vertebrador para aumentar el nivel de resiliencia de todos sus proveedores en términos de ciberseguridad y, por extensión, de un alto porcentaje del tejido empresarial nacional. Finalmente, el Estado puede favorecer el establecimiento de unos criterios comunes de seguridad a través de un marco de controles de seguridad de referencia cuya observancia y cumplimiento por parte de las empresas facilitase al sector asegurador la suscripción de seguros de ciberriesgos.

El mercado de los ciberseguros en España es un mercado en auge. Es responsabilidad de todos los actores garantizar su consolidación.

3.
Los ciberseguros

3.1. Origen

Aunque es difícil establecer una fecha exacta, las primeras estrategias contemporáneas de transferencia de riesgos tecnológicos vieron la luz en Estados Unidos a mediados de los noventa.

Sin embargo, no fue hasta finales de la década cuando estos seguros comenzaron a comercializarse de una manera más regular al albor de cuatro acontecimientos de especial relevancia:

1. La llegada del **efecto año 2000**, conocido también por el numerónimo Y2K, y los potenciales impactos catastróficos que conllevaría el cambio de milenio sobre los sistemas informáticos que sustentaban un entorno empresarial cada vez más dependiente de las tecnologías de la información.

2. Explosión de las **Puntocom**, empresas que aprovechando la exuberante financiación de fondos de capital riesgo y una corriente especulativa favorable, explotaron el auge de Internet y del comercio electrónico para establecer nuevos modelos de negocio digitales. Empresas como *Amazon, Yahoo, eBay, Altavista* y *Google,* se convirtieron en clientes potenciales de estos productos de seguro que pretendían cubrir su negocio ante un panorama de amenazas digitales creciente.

3. La profesionalización del **cibercrimen**, pasando de una práctica desarrollada por aficionados a una vertiente criminal susceptible de ser enseñada, aprendida y mejorada. En pocos años se ha producido un importante proceso de profesionalización: actualmente los cibercriminales actúan perfectamente coordinados mediante estructuras jerarquizadas y ejecutando campañas de forma descentralizada en distintos países de manera simultánea.

4. La promulgación en California, el 1 de Julio de 2003, de la **SB1386**, la primera ley a nivel mundial que obligaba a que *"cualquier agencia estatal, persona o empresa que lleve a cabo negocios en el estado de California y que posea u opere datos informatizados con información de carácter personal, deba comunicar formalmente cualquier brecha de seguridad que implique una fuga de datos".* Esta norma sentaba las bases del denominado *Data Breach Notification,* es decir, la obligatoriedad de notificar al regulador ciertos incidentes de ciberseguridad asociadas a una fuga de datos digitales.

Este último aspecto es, sin duda alguna, uno de los factores catalizadores decisivos que han supuesto un espaldarazo comercial a la proliferación de las pólizas de ciberriesgos. La SB1386 fue la precursora en Estados Unidos de una oleada legislativa a la que en poco tiempo se sumaron otros cuarenta y cinco estados y que a día de hoy vive un momento muy activo a nivel internacional con el futuro nuevo Reglamento Europeo de Protección de Datos y la Directiva Europea 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Esos primeros productos de transferencia del riesgo tecnológico eran concebidos como productos financieros centrados en cubrir las pérdidas económicas asociadas a un incidente de seguridad. No obstante, dado que estos productos tenían un origen estrechamente vinculado con la normativa relativa a la notificación de fugas de información, sus coberturas eran limitadas y focalizadas en la responsabilidad civil asociada a los gastos de reclamación y responsabilidad ante terceros derivada de un fallo de seguridad de los sistemas informáticos del asegurado.

La propia naturaleza del riesgo a asegurar ha actuado, junto a otros factores, como inhibidores a la hora de favorecer el crecimiento masivo de las ciberpólizas.

A saber: Falta de datos históricos de ciberincidentes, su impacto y el vector de ataque explotado, provocado por el oscurantismo reinante y la reticencia en el sector empresarial a notificar y compartir datos sobre incidentes y amenazas. Ello redundó en la imposibilidad de los departamentos actuariales de las aseguradoras de disponer de datos fiables para elaborar los modelos estadísticos y matemáticos necesarios para la evaluación de los ciberriesgos.

"la propia naturaleza del riesgo a asegurar ha actuado, junto a otros factores, como inhibidor a la hora de favorecer el crecimiento masivo de las ciberpólizas"

Falta de concienciación del nivel de exposición y del impacto asociado a las ciberamenazas entre las empresas como tomadores de seguros. Ello contribuyó a que la demanda de estos productos fuera limitada.

Las entidades interesadas en contratar estas pólizas de seguro debían – y en algunos casos todavía deben hacerlo – someterse a un conjunto de procedimientos de evaluación de su madurez en seguridad informática a menudo invasiva. Ello implicaba revelar el estado de sus infraestructuras tecnológicas y sus políticas o procedimientos de gestión TIC. Al mismo tiempo al complementar los formularios de contratación aportados por las aseguradoras, se suele subestimar el riesgo por parte del asegurado siendo además respondidos por el área de Tecnologías de la Información (IT) y no intervienen las áreas de la empresa que son sensibles a la información como activo.

La naturaleza ubicua del ciberriesgo posibilita que una compañía aseguradora pueda sufrir pérdidas muy elevadas de un gran número de clientes repartidos en diferentes zonas geográficas del mundo como resultado de un mismo incidente. Este efecto, denominado agregación de riesgo, puede provocar que una misma compañía aseguradora o reaseguradora no pueda hacer frente al pago de las reclamaciones resultantes de un evento catastrófico.

De este modo, el mercado de los ciberseguros no logró prosperar a la velocidad esperada en sus etapas iniciales y se mantuvo como un mercado de nicho. Los pronósticos más conservadores en el año 2002 preveían un mercado mundial de ciberseguros de unos 2.500 millones dólares para el año 2005. Sin embargo, el ejercicio prospectivo era demasiado optimista, ya que tan sólo tres años después, en 2008, la previsión del año 2002 seguía siendo cinco veces superior que el tamaño del mercado ese año[1].

[1]Jay Kesan; Rupterto Majuca y William Yurcik: "The Economic Case for Cyberinsurance", *University of Illinois College of Law Working Papers*, Nº 2, 2004, pp. 1-31.

3.2. Panorama actual

Fenómenos como el cibercrimen, el Traiga Su Dispositivo Propio (BYOD), la consumerización de las TIC o la explosión de la economía digital han transformado la vertebración y desarrollo del sector. Hoy en día, el mercado de los ciberseguros es un mercado cada vez más establecido, con un número creciente de proveedores y una cadena de valor cada vez más madura, formado por aseguradoras, reaseguradoras, *brokers* y empresas de servicios. El aumento de oferta y de la competencia en el sector está, a su vez, reduciendo los precios de las pólizas. Además, existe un buen número de mercados primarios disponibles para colocar los grandes riesgos, y empresas de todos los tamaños están contratando cada vez más este tipo de productos como una compra obligatoria y no como una acción discrecional.

Cadena de valor mercado ciberseguro. Fuente: elaboración propia.

Según datos de *Marsh*[2], el mercado de los ciberseguros generó en Estados Unidos 1.000 millones de dólares en 2013, cantidad que se duplicó en 2014. El mercado europeo de ciberseguros es aún pequeño comparado con Estados Unidos, pero crece también a buen ritmo. En cualquier caso, es indiscutible que los ciberseguros son uno de los productos de más rápido crecimiento en el mercado asegurador. A medio plazo, éste alcanzará los 7.500 millones en ventas anuales en 2020, frente a los 2.500 millones de dólares del año pasado[3].

En el caso español, este tipo de productos aseguraticios han sido trasladados desde los mercados norteamericano y británico principalmente. En dicha génesis nacional, los productos presentaban coberturas y estructuración similar a sus homólogos extranjeros para, paulatínamente, ir adaptándose a la realidad de las empresas españolas. Las compañías internacionales de seguros así como los grandes *brokers*, debido al profundo conocimiento de estos productos, están liderando esta adaptación a las necesidades nacionales.

Adicionalmente, la crisis económica en España, ha obligado a muchas empresas a internacionalizarse y a operar en otros mercados para sobrevivir, enfrentándose muchas con la necesidad de adquirir este tipo de seguros a consecuencia de cumplir con las normativas de seguridad exigidas en los mismos.

Hoy en día ya no es una cuestión de si las ciberamenazas pueden o no afectar a una empresa con independencia de su tamaño, sector o ubicación. La pregunta a realizarse es, simplemente, cuándo sucederá y si la organización contará con los mecanismos adecuados para afrontar el incidente.

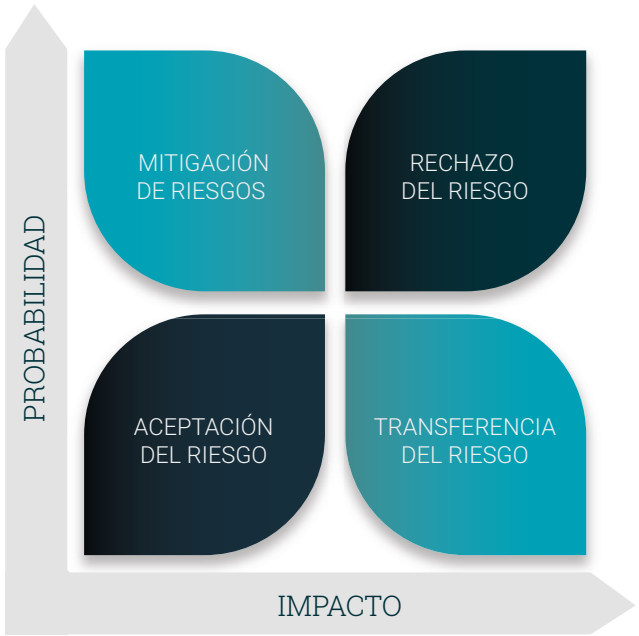
[2] Marsh & McLennan y Cherthoff Group: "*A cybersecurity call to action*", Nueva York: Marsh & McLennan, 2014.

[3] PWC: "Cyber insurance market set to reach $7.5 billion by 2020", *PWC News room* (16 de septiembre de 2015), en: http://press.pwc.com/News-releases/cyber-insurance-market-set-to-reach--7.5-billion-by-2020/s/5CC3FA21-221C-43DF-A133-05435E365342

3.3. Contexto en el mercado de la seguridad y en la gestión de ciberriesgos

A finales de la década de 1990 se comenzaron a abordar los problemas de seguridad desde una forma metodológica y procedimentada mediante técnicas de análisis de riesgos.

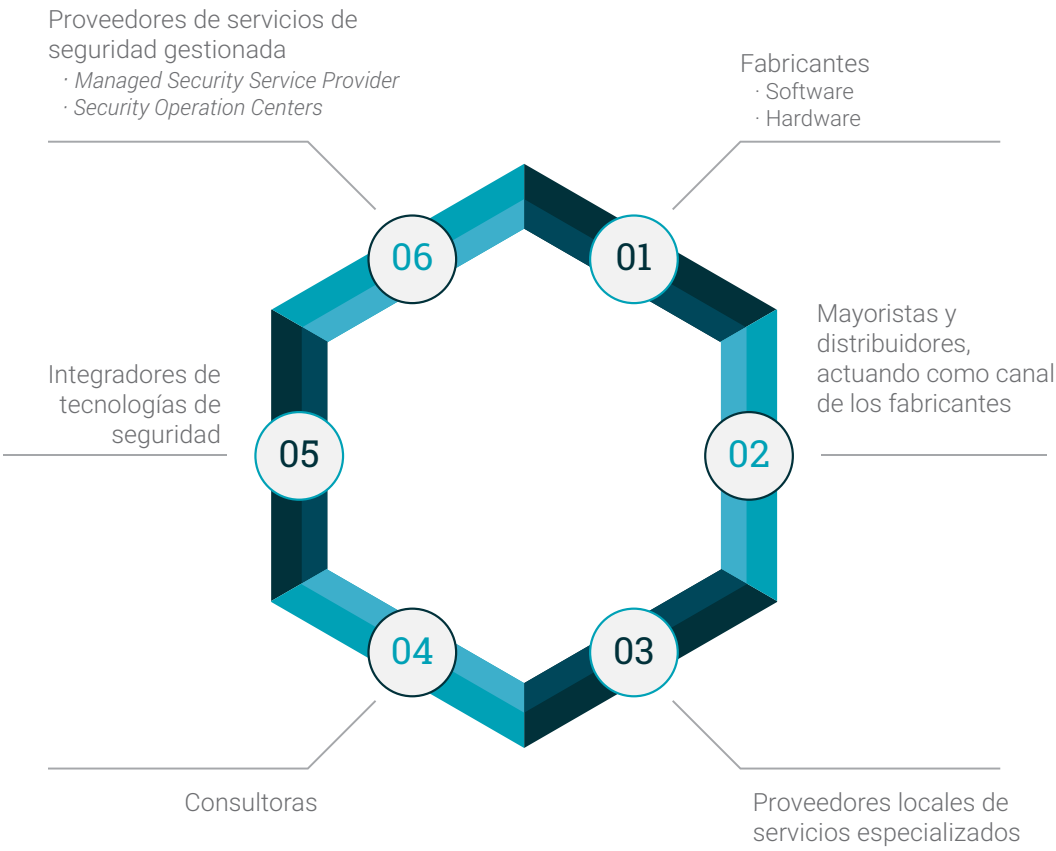
De esta manera, las empresas comenzaron a planificar sus estrategias de seguridad a través de planes directores de seguridad cuyo elemento principal vertebrador era un análisis de riesgos ponderado. Una vez realizado el análisis y definido el apetito de riesgo de la compañía, se tomaba una decisión de gestión: los riesgos de seguridad de la información se aceptaban, se rechazaban, se mitigaban o se transferían.



Estrategias de gestión de ciberriesgo. Fuente: elaboración propia.

Sin embargo, la transferencia del riesgo tendía a ser descartada debido a la incipiente oferta aseguradora existente en el mercado. En consecuencia, muchos riesgos de seguridad y de privacidad eran, simplemente, asumidos o retenidos por parte de las organizaciones. No obstante, a fecha de hoy la transferencia del riesgo parece una opción cada vez más atractiva, entendiéndose como la última línea de defensa, no la única, ni sustitutoria de un marco de control de seguridad que deberá ser adecuado al panorama de riesgos de la organización.

Precisamente la gestión de riesgos tecnológicos, de seguridad de la información o de ciberseguridad ha servido de marco sobre el cual se ha acomodado la definición de portfolios comerciales de servicios de ciberseguridad. Más concretamente, en el mercado privado de la ciberseguridad nacional es posible hallar la siguiente cadena de valor:



Cadena valor del mercado de ciberseguridad. Fuente: elaboración propia.

Dichos proveedores han establecido una carta de servicios y de productos que generalmente se suelen clasificar en soluciones o servicios de tipo de detección, prevención y reacción. Así pues, los ciberseguros quedarían incluidos entre los servicios reactivos, orientados a la gestión directa de incidentes de ciberseguridad, cuyo objetivo es mitigar el impacto.

3.4. Qué son: la última línea de defensa

Para poder definir las pólizas de ciberriesgos es necesario acotar de forma previa qué es un ciberriesgo. Éste puede ser definido como el riesgo de pérdida financiera, de interrupción del negocio u otros daños (como el daño reputacional) de una organización que se deriva del uso de sistemas informáticos y redes de comunicación y operación; de la información almacenada y gestionada por los sistemas de dicha organización y de su presencia en medios digitales. Sin embargo, esta definición no abarca la totalidad de riesgos asociados al ciberespacio, puesto que sus efectos pueden ir más allá de las meras pérdidas financieras – como pueden ser daños materiales o lesiones personales – y afectando no sólo a las organizaciones y empresas, sino también a los usuarios.

Generalmente éstos no están cubiertos en los productos aseguradores clásicos de daños o de responsabilidad general, puesto que estos riesgos solían ser tipificados como una exclusión en las pólizas tradicionales.

Así pues, de forma general, los ciberseguros o pólizas de ciberriesgos son productos aseguradores cuyo objetivo es proveer protección ante una amplia gama de incidentes derivados de los riesgos en el ciberespacio, el uso de infraestructuras tecnológicas y las actividades desarrolladas en este entorno[4].

De forma general, un contrato de seguro (póliza) ante ciberriesgos vincula y obliga legalmente a una compañía aseguradora ante la ocurrencia de determinados eventos ciber definidos contractualmente que conlleven pérdidas, pagando una cantidad especificada (reclamación/siniestro) al asegurado[5]. En contraprestación, el tomador del seguro paga una suma fija (prima) a la compañía aseguradora. El contrato es firmado por ésta y el asegurado e incluye aspectos como los tipos de coberturas, límites y sublímites, exclusiones, definiciones y, en algunos casos, cómo se va a proceder a evaluar el nivel de seguridad del asegurado.

Estructura general de una póliza de ciberriesgos. Fuente: elaboración propia.

Sobre la base de los puntos anteriores se fijará el valor neto de la prima a pagar. Como cabe imaginar, su valor es altamente dependiente fundamentalmente del valor de los activos bajo amenaza del tipo de negocio, tamaño de la compañía, nivel de exposición digital, volumen de datos digitales a salvaguardar y nivel de seguridad de la organización.

Esta falta de consenso en la definición del producto se pone de manifiesto en la heterogeneidad de denominaciones que adquieren estos productos entre la propia industria aseguradora. Así aparecen referencias en lengua inglesa a C*yberrisk, Network Risk, Privacy Protection, Network Liability, Security & Privacy Liability, Professional Liability Privacy, Media Liability, Technology & Privacy Professional Liability* o *Data Privacy & Network Security* con sus respectivas traducciones a nuestro idioma.

Ello pone de manifiesto la gran diversidad de la oferta, ya que cada asegurador ha desarrollado el producto de seguro bajo la premisa de su comprensión de qué es lo que necesitan las empresas para mitigar los ciberriesgos, lo que implica también muy diversa terminología en cuanto a las garantías y al alcance de los riesgos cubiertos. En consecuencia, se pueden hallar seguros enfocados a responsabilidad frente a terceros por vulneración de datos personales o violaciones de seguridad, riesgos regulatorios y gastos diversos, y otros que incorporan coberturas de daños propios (*First Party*) y que, por lo tanto, dan cobertura a pérdida de beneficios o lucro cesante, robo y otros gastos y pérdidas relacionadas.

No obstante, debe señalarse que el fallo de seguridad no es la única causa de riesgo. Existen otros factores, como puede ser el riesgo de errores humanos, fallos técnicos o de programación, riesgos de difamación o usurpación negligente de propiedad intelectual de terceros o fallo en la cadena de suministro, que pueden ocasionar un perjuicio financiero, interrupción del negocio o un daño reputacional. Estas coberturas no suelen ser ofrecidas de forma estándar y hay que negociar normalmente de forma expresa su inclusión en el cuadro del seguro.

Deliberadamente se han excluido otras causas de riesgo como pueden ser los riesgos naturales o el riesgo de incendio y explosión, que también dan lugar a los mismos perjuicios financieros, de interrupción o de daño reputacional. Este conjunto de riesgos suele estar contemplado en seguros tradicionales pero el enfoque frente al riesgo de cada organización es muy distinto y no siempre está asegurado. Y también son muy distintas las necesidades de cobertura de las organizaciones.

Bajo estas líneas se analizan las principales coberturas ante ciberriesgos ofrecidas en el mercado, si bien su redacción y las definiciones y exclusiones variarán entre los diversos productos.

[4] Tridib Bandyopadhyay: "Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management – A Modelling Approach", *Proceedings of the Southern Association for Information Systems Conference,* Atlanta, 2012, pp. 23-29.

[5] The White House: *Cyber-Insurance Metrics and Impact on Cyber Security*, Washington DC: GPO, s.f., en: www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20 on%20Cyber-Security.pdf

3.4.1. Coberturas básicas

- **Responsabilidades frente a terceros *(Third Party Loss)*** por privacidad de datos y seguridad de redes: se da cobertura frente a reclamaciones de terceros (indemnización y gastos de defensa) por perjucios causados a dichos terceros como consecuencia de un fallo en la privacidad de datos de carácter personal o información corporativa de terceros, o por un fallo en la seguridad (como por ejemplo, transmisión de códigos maliciosos, participación en ataques de denegación de servicios o por un impedimiento de acceso a datos y sistemas como consecuencia de un virus o intrusión, entre otros).

- **Procedimientos regulatorios:** se da cobertura de gastos de asesoramiento legal frente a un procedimiento administrativo iniciado por un organismo regulador por un incumplimiento de la normativa de protección de datos de carácter personal y eventualmente – siempre que no exista legislación en contra – se abona asimismo la potencial sanción administrativa.

- **Gastos de gestión de incidentes:** siempre que se incurra en estos gastos mediante contratación de servicios externos:
  a) Gastos forenses para analizar la causa y alcance del incidente/datos comprometidos y eventualmente terminar la causa del incidente.
  b) Gastos de asesoramiento legal para analizar consecuencias legales frente a afectados, reguladores y asesoramiento en actuaciones como notificación, custodia de pruebas, etc.
  c) Gastos de comunicación y/o gestión del riesgo reputacional, que incluye tanto el asesoramiento durante la notificación como a la propia la realización de campañas de comunicación.
  d) Gastos de servicios prestados a los afectados: comprende gastos tales como la contratación de servicios de atención de llamadas *(call centers)*, gastos de servicios de prevención de fraude y robo de identidad, pagos de primas de seguros en caso de robo de identidad, etc.

Garantías opcionales o complementarias (éstas deben estar expresamente indicadas como cubiertas en las condiciones particulares del contrato e implican una prima mayor).

- **Pérdidas pecuniarias propias** (First Party Loss):
  a) la pérdida de ingresos derivada de una interrupción de sistemas o redes por las causas indicadas en póliza (la cobertura estándar se limita a fallo de seguridad) incluyendo los gastos extraordinarios para mitigar la pérdida de beneficios, los costes de reposición de activos ditigitales (costes de reconstrucción de datos y software)
  b) las pérdidas pecuniarias propias por amenazas de extorsión a sistemas (gastos de consultoría, recompensas y eventualmente, rescates).

- **Responsabilidad Civil de Medios Digitales:** da cobertura frente a reclamaciones de terceros (indemnización y gastos de defensa) por perjucios causados por la difusión y publicación de contenidos en los sitios web de la empresa. Estos perjucios pueden ocasionarse por muy diversos motivos, desde invasión de privacidad, calumnia y difamación a la terceros hasta la vulneración de propiedad intelectual o marcas cuando se publican contenidos que pueden estar protegidos por derechos de propiedad intelectual de dichos terceros.

** En función del asegurador / negociación*

Coberturas de un producto típico de ciberriesgos. Fuente: AON

Existen otras posibles garantías que pueden contratarse como parte de la cobertura. Es muy común para empresas que gestionan un volumen elevado de pagos por tarjeta de crédito y almacenan dichos datos. En consecuencia, una quiebra de datos o un fallo de seguridad puede dar lugar a penalizaciones con los medios de pago, cuyo importe puede quedar cubierto bajo la cobertura. También hay aseguradores que otorgan – con sublímites o cantidades limitadas – la pérdida económica del asegurado por transferencia fraudulenta de fondos. En consecuencia, las diferencias entre pólizas son muy diversas. Las principales radican por supuesto, en el alcance de la cobertura que va más allá de la contratación de las garantías opcionales.

Dependiendo de qué cobertura tenga que responder, los desencadenantes o *triggers* pueden ser varios:

a) Por privacidad de datos: una reclamación por la revelación o transmisión no autorizada de datos personales de carácter personal.

b) Por procedimientos regulatorios: una inspección o procedimiento iniciado por un regulador en materia de privacidad de datos por infracción de la normativa de privacidad de datos.

c) Por seguridad de datos: una reclamación por una actuación negligente o fallo del asegurado al proteger sus datos digitales, pérdidas causadas por un empleado, actos de terceros y pérdida derivada del robo o desaparación de soportes donde se encuentra almacenada la información.

Las garantías *First Party* de las pólizas varían entre productos: gastos forenses, gastos de publicidad u otros gastos incurridos para minimizar la pérdida del asegurado o de los afectados. Una mera sospecha de una intrusión no autorizada en los sistemas puede activar la cobertura de gastos forenses. Otros gastos, tales como la monitorización de crédito, van a estar ligados seguramente a una reclamación, un proceso regulatorio o tras activar los gastos asociados a los servicios forenses, si la brecha de seguridad es real e implica una fuga de datos.

En cuanto a pérdida de ingresos, la interrupción de los sistemas está vinculado normalmente a fallo de seguridad en sistemas propios, aunque como se ha mencionado, existen coberturas de pérdida de beneficios contingente (por fallo en la cadena de proveedores de servicios tecnológicos, por ejemplo) o por otras causas (como fallo de sistemas y errores humanos). La interrupción o el fallo debe ocurrir durante el periodo de seguro y la cobertura está sometida a un periodo máximo de indemnización (que varía entre 90 y 120 días), a una franquicia medida en horas de parada.

Por otra parte, en relación a la pérdida de beneficios existe la problemática asociada a las dos aproximaciones predominantes: el enfoque americano (calcular la pérdida de beneficios hasta que se reinician las operaciones) y el enfoque de pólizas de londinenses o europeo (hasta el restablecimiento de la producción al nivel normal), así como las dificultades que normalmente encuentran las empresas para sepa-

rar y cuantificar los factores que inciden en una reducción o aumento de los beneficios esperados que están directamente relacionados con el siniestro.

Pero también hay otras distinciones que son relevantes a la hora de seleccionar un producto frente a otro, como pueden ser la prestación de servicios de consultoria pre-siniestro o los servicios vinculados con la gestión de siniestros.

Los servicios pre-siniestro están muy poco extendidos en España. Ello obedece a varios factores, entre los que se hallan la escasa percepción del valor que pueden aportar estos servicios a las empresas de tamaño medio o grande y, quizá también en vista del escaso interés que suscitan estos servicios, la oferta se limita de forma general a unas horas gratuitas de expertos en materia de seguridad tecnológica y algún dispositivo que combina herramientas de información de amenazas con herramientas de información.

Estos servicios sin embargo, pueden ser de gran valor en el sector de pequeña y mediana empresa. De hecho, los pocos productos aseguradores que están viéndose en el mercado español para este sector presentan una aproximación técnica previa para mitigar el riesgo, además de una asistencia técnica especializada cuando ocurre el siniestro. En cualquier caso la oferta de esta naturaleza es aún muy modesta y el valor de los servicios ofrecidos, lógicamente, muy ajustado.

Ejemplo de servicios y soluciones pre-siniestro o preventivas. Fuente: elaboración propia.

Los servicios de gestión de siniestros son más habituales. Los aseguradores que prestan estos servicios ya han negociado con expertos forenses, legales y de comunicación y crisis (pudiéndose extender al establecimiento de servicios adicionales de respuesta a afectados) con proveedores de prestigio y experiencia tarifas exclusivas y los ofrecen como "paneles" dentro de las pólizas. La principal ventaja – siempre que los proveedores respondan en los plazos establecidos – radica en que una empresa que carezca de planes de contingencia o de gestión crisis ante incidentes de esta naturaleza pueda delegar en estos expertos la gestión de la crisis paso a paso.

No obstante, el asegurado continúa manteniendo el derecho de gestionar el siniestro por si mismo y con sus propios expertos, pero tiene que tener en cuenta que debe solicitar aprobación previa al asegurador – y en teoría antes de incurrir en cualquier gasto – para que el asegurador acepte el reembolso del gasto.

Volviendo al entorno de las pequeñas y medianas empresas, aunque los productos pueden presentar prácticamente las mismas coberturas, su contrapartida radica en que su coste es todavía elevado (cercano a los 1.000/1.500€). Otras pólizas contemplan costes inferiores, pero son más limitadas al cubrir básicamente garantizas responsabilidades frente a terceros por fallo de privacidad (defensa e indemnizaciones) y los gastos se limitan a asistencia forense y reconstrucción de datos.

3.4.2. Exclusiones principales

El apartado de exclusiones merece una atención especial. Un producto con una oferta tan variada también tendrá múltiples exclusiones. No obstante, existen unas exclusiones comunes en todos ellos que se pueden resumir de la siguiente manera:

- Actos deshonestos y fraudulentos y deliberados del asegurado: hay que delimitar claramente cómo afecta esta exclusión a actos de empleados, cuando éstos son asegurados bajo la póliza.
- Daños personales y materiales.
- Responsabilidades asumidas por contrato o acuerdo: las pólizas de responsabilidad civil asumen principalmente responsabilidad extracontractual y sólo responden si existiera responsabilidad en ausencia de dicho contrato o acuerdo.
- Reclamaciones previas y litigios previos e incidentes que hubieran ocurrido (y fueran conocidos) con anterioridad a la fecha de efecto del contrato.
- Infracción de secretos comerciales y patentes.
- Guerra y Terrorismo, a pesar de que a día de hoy existen coberturas afirmativas (o expresas) relacionadas con ataques ciberterroristas.

Existe otra exclusión – que puede estar incluida como tal o formar parte de las condiciones generales del contrato y pasar más desapercibida – y es la relativa a datos no declarados o mantenimiento de datos y seguridad por debajo de lo declarado al asegurador durante el proceso de suscripción. Aunque esta exclusión o condición causa mucha controversia, los asegurados deben tener en cuenta que la información y cuestionarios de riesgo se consideran parte inseparable del contrato, y existen pólizas en las que pueden incluso invalidar la cobertura. En consecuencia, es necesario analizar esta cláusula, proponer medidas que suavicen dicha exclusión otorgando cobertura, pero sobre todo, ser conscientes que cualquier cambio en el riesgo debe ser declarado, ya que el asegurador también tiene derechos contractuales de analizar el riesgo durante el ciclo de vida completo de la póliza, proponiendo cambios que se ajusten al estado de riesgo en cada momento.

Para finalizar, merecen una mención independiente los riesgos asociados a las infraestructuras críticas y sobre todo, los sistemas de control industrial. Determinadas industrias, como la energética y utilities, tienen altamente automatizado la generación y distribución de energía o la producción a través de controladores de lógica programable (PLC), sistemas de control distribuido (DCS) o sistemas de supervisión, control y adquisición de datos (SCADA). Antaño aislados, estos sistemas tienen que interactuar con nuevas soluciones tecnológicas y aplica-

ciones interconectadas y, en algunos casos, con acceso a Internet. Una incidencia en uno de esos sistemas podría conllevar daños físicos, materiales, adicionalmente a los meramente financieros.

La oferta aseguradora para este tipo de riesgo es muy limitada. Existen productos en el mercado que incorporan coberturas de daños materiales y personales, bien con diferentes condiciones respecto a los seguros tradicionales o bien asegurando la pérdida no cubierta. Sin embargo, ninguno de estos productos puede cubrir la pérdida de ingresos por paralización de actividad: asumiendo que la capacidad máxima del mercado asegurador se estima en 150/200 millones de euros por riesgo, esta cantidad puede ser claramente insuficiente en muchos casos donde se produzca la paralización de una infraestructura crítica con el consiguiente corte de suministro afectando a miles de usuarios.

En definitiva, el problema es doble: por un lado, los asegurados no han realizado aún un análisis de riesgos exhaustivo y les es difícil trasladar la información de forma adecuada al mercado asegurador. Y, por otra parte, esta falta de información, junto a la falta de conocimiento de las amenazas, siniestralidad e impactos por parte de las aseguradoras hace que dicho mercado opte por una posición conservadora, otorgando coberturas de daños materiales y responsabilidad civil, siendo reticente a proponer productos y capacidad.

3.5. A quiénes van dirigidos

Hasta ahora el mercado asegurador se había centrado en productos dirigidos a aquellas empresas más expuestas al riesgo cibernético, siendo normalmente grandes corporaciones multinacionales y que, por tanto, necesitan mayores niveles de protección. No obstante, cada vez hay más aseguradoras que dirigen su mirada al sector de la pequeña y mediana empresa y están intentando adaptar su oferta a su realidad y necesidades. La dificultad para asegurados, aseguradores y mediadores radica en la necesidad de adaptar los productos al perfil de riesgo y la cobertura que necesitan, no tanto al tamaño de la compañía.

Una característica diferenciadora que presenta el mercado español es el gran tejido de pequeñas y medianas empresas (PYMES) existente, hecho que las aseguradoras han identificado como una oportunidad de negocio diseñando y adaptando los productos a este sector.

El gran reto para llegar a este mercado es el escepticismo del pequeño empresario, que no encuentra necesario adquirir este tipo de seguros, porque considera que los ciberataques son consustanciales a las grandes empresas.

Sin embargo las PYMES son ahora los objetivos comunes de los ciberdelincuentes, no porque sean lucrativas de forma individual, sino porque la automatización hace que sea fácil de atacar en masa siendo víctimas fáciles *(soft targets)*. Así pues se puede afirmar que:

- **Las PYMES** se enfrentan a las mismas ciberamenazas que las grandes empresas, pero con una fracción del presupuesto para hacerlas frente.
- **La inversión en seguridad** es impulsada por la necesidad de cumplir con el marco regulatorio, como Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS), Ley Orgánica de Protección de Datos (LOPD), etc.
- **Las organizaciones** más pequeñas carecen de la experiencia interna para gestionar sus ciberriesgos.

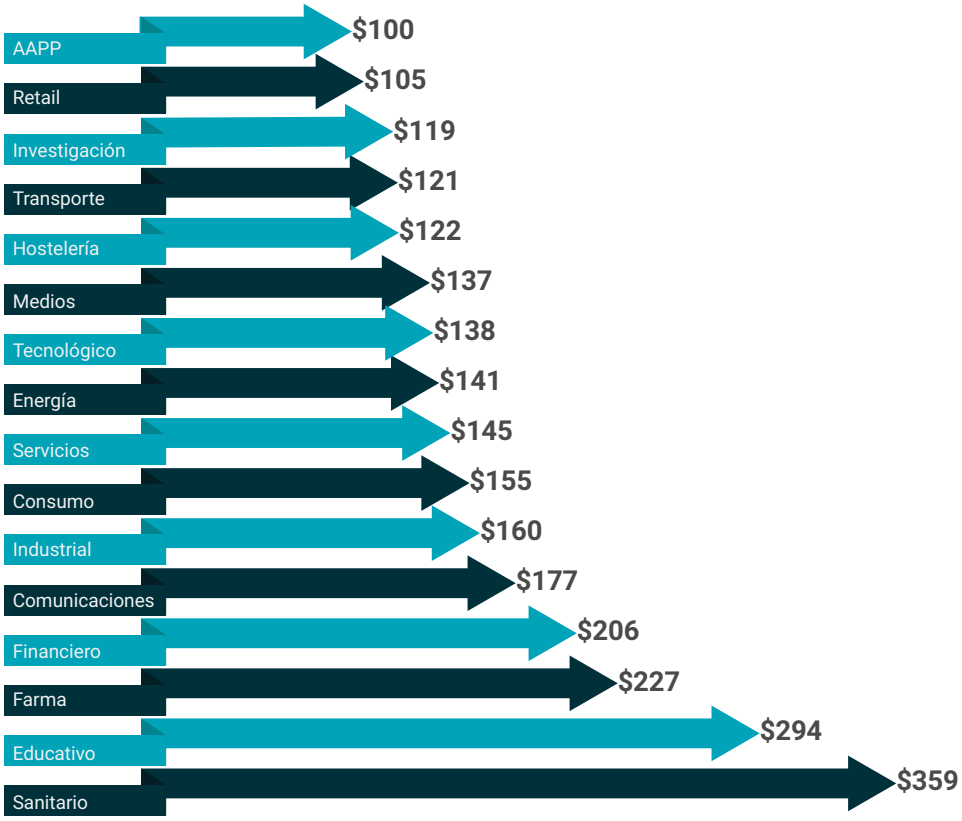
Aunque la seguridad plena no existe, sí es posible reducir la exposición al riesgo digital. Y es que todas las empresas, con independencia de su tamaño o sector de actividad, tienen algún componente de riesgo cibernético ya que:

- Recopilan, mantienen, ceden o almacenan información privada de carácter personal o confidencial.
- Dependen, en mayor o menor grado, de sistemas informáticos o redes que pueden estar interconectados entre ellos o con otras redes o sistemas de terceros.
- Proveen servicios y productos a través de internet u otros medios electrónicos.
- Contratan con proveedores de servicios tecnológicos (desde mantenimiento, seguridad, gestión de infraestructuras u otros servicios) o con otros proveedores y contratistas independientes para el almacenamiento o tratamiento de la información.
- Pueden estar sujetos a normativa sectorial reguladora de su actividad en cuanto a seguridad de datos o comunicaciones electrónica que implique mayores medidas de seguridad adicionales (y por tanto un mayor riesgo de investigaciones y sanciones) a las que establece la LOPD.
- Pueden tener obligaciones que cumplir en materia de seguridad frente a la industria de medios de pago.
- Los empleados constituyen el eslabón más débil de la cadena de seguridad de la información.
- Poseen *know-how* o secretos comerciales en formato digital de los que depende su negocio.
- Proporcionan algún servicio o producto a terceros que pueden, en caso de ataques maliciosos, constituir los verdaderos objetivos de criminales y atacantes.

Aunque cada sector empresarial posee sus propios componentes, riesgos y exposición, existen sectores más sensibles que representan un mayor riesgo desde el punto de vista del análisis asegurador, a saber:

- **Instituciones financieras** (incluyendo las aseguradoras), sector sanitario y sector retail, tanto por el tipo de datos que manejan, así como el volumen de los mismos. No obstante, el sector financiero suele presentar un nivel de madurez de seguridad mayor.
- **Telecomunicaciones y proveedores de servicios tecnológicos,** tanto por la información gestionada así como por los datos de terceros procesados.
- **Sector energético y utilities en general,** por el impacto de una potencial pérdida y quizá los que están en clara desventaja desde el punto de vista de medidas de seguridad preventivas en los sistemas industriales.

COSTE PER CAPITA DE LAS FUGAS DE DATOS POR SECTOR (2014)



Fuente: Ponemon Institute, op. cit., p. 7

Distribución de siniestros y reclamaciones por sector. Fuente: Net Diligence, op. cit., p. 8.

3.6. Necesidades del asegurado

Los gestores de riesgos, los responsables de seguridad de la información y en definitiva los directivos de las compañías, afrontan determinadas necesidades en las que los ciberseguros presentan coberturas de especial utilidad y relevancia :

NECESIDAD NORMATIVA

Las necesidades del asegurado en el ámbito de la ciberseguridad no vienen solo motivadas por el mayor uso de las tecnologías y una mayor conectividad, sino también por las obligaciones legales impuestas por los órganos regulatorios. Un ejemplo de ello son las obligaciones impuestas a todos aquellos proveedores de servicios de comunicaciones o redes electrónicas. Desde la Directiva Marco 2002/21/CE, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, España ha venido transponiendo la misma mediante la Ley 9/2014 General de Telecomunicaciones.

Esta norma exige a los operadores de redes públicas o de servicios de comunicaciones electrónicas a informar a los abonados de todos aquellos riesgos de fuga de datos que puedan existir y de las medidas a adoptar, así como comunicar de eventuales incidente a la Agencia Española de Protección de Datos, al Ministerio de Industria, Energía y Turismo y a los abonados afectados.

El nuevo Reglamento Europeo de Protección de Datos indica también que tan pronto como el responsable del tratamiento de datos tenga conocimiento de que se ha producido una violación de seguridad, debe notificarla a la autoridad de control sin retraso injustificado y, cuando sea posible, en el plazo de 24 horas. Los costes asociados a dichas notificaciones y actuaciones son una de las coberturas básicas ofrecidas en las pólizas.

Adicionalmente, el procesamiento, almacenamiento o transmisión de datos de tarjeta de crédito por parte de las organizaciones obliga al cumplimiento del estándar de seguridad de los datos de tarjeta, PCI-DSS versión 3, entre cuyos requisitos se encuentra la notificación a los titulares de tarjeta en caso de fuga de datos relativos a los mismos.

NECESIDAD DE REDUCIR EL IMPACTO DE LOS CIBERRIESGOS

Los riesgos cibernéticos que pueden cernirse sobre las empresas pueden ser:

• **De carácter directo,** destacando el robo de datos personales, de contraseñas o de *know-how*; la utilización indebida de información privilegiada, el sabotaje a sistemas o programas informáticos de la compañía; abusos en el acceso a correos e internet; accesos no autorizados; redes de equipos infectados remotamente; daños físicos de los equipos; captura de contraseñas; extorsiones; explotación de servidores y navegadores; hurtos y robos de ordenadores o dispositivos móviles[6] entre otros.

• **De carácter indirecto,** incluyendo la paralización de la actividad y/o suspensión de la prestación del servicio a terceros, con el consiguiente incumplimiento contractual; pérdida de beneficios (*loss of profit* – LOP); pérdida de mercado o pérdida de confianza en el sector; imposición de sanciones regulatorias; perjuicios causados a terceros; responsabilidad civil, penal o administrativa; incremento del coste para resolver o minimizar los daños así como el derivado de tener que asumir el pago de las indemnizaciones que se determinen a favor de los posibles afectados.

Como elemento principal, relacionado con los riesgos indirectos a los que puede enfrentarse un potencial asegurado, destaca la responsabilidad derivada del desarrollo de su actividad en el ciberespacio. Un único incidente de ciberseguridad puede provocar varios tipos de responsabilidad de forma que algunas de sus consecuencias queden cubiertas en las pólizas:

- **Responsabilidad civil** frente a terceros, clientes y/o usuarios.
- **Responsabilidad laboral** frente a los trabajadores de la compañía que se han visto afectados por el ciberincidente.
- **Responsabilidad penal** de la compañía y/o sus administradores o directivos surgida, como consecuencia de la actuación en el ciberespacio de un tercero (ajeno a la compañía o no), o de la propia compañía por actuaciones poco diligentes.
- **Responsabilidad administrativa** que pudiera derivarse frente a organismos regulatorios por el incumplimiento de obligaciones legales tendentes a garantizar un determinado nivel de seguridad.
- **Responsabilidad contractual** en caso de que se produzca la paralización de la actividad y la imposibilidad de prestar servicio a los clientes y usuarios.
- **Responsabilidad extracontractual** en caso de que haya terceros, ajenos a la prestación del servicio, afectados por el ciberincidente.

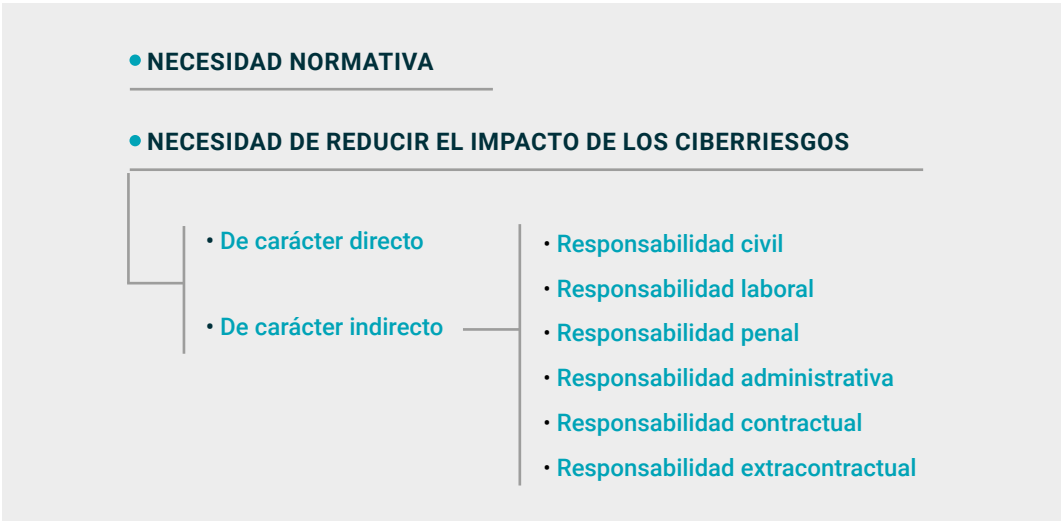
Finalmente, en relación a las medidas a adoptar por los potenciales asegurados, es preciso comentar que, con el objeto de que los proveedores de ciberseguros acepten dar cobertura a las compañías en el ámbito de la ciberseguridad, es imprescindible que los interesados acrediten primero que ejercen un determinado nivel de monitorización, control y supervisión de las herramientas utilizadas para el desarrollo de su actividad (software y hardware) y que im-

[6] José Luis González: "Estrategias legales frente a las ciberamenazas", en: *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.* Cuadernos de Estrategia Nº 149, Madrid: Ministerio de Defensa, 2010, pp. 85-127.

plementan y actualizan los procedimientos de control y fomentan una mayor concienciación de los trabajadores de la compañía en el ámbito de la ciberseguridad, así como demostrar un nivel de cumplimiento determinado ante el marco regulatorio y normativo de aplicación en cada caso (LOPD, PCI-DSS, etc).

Por otro lado, y respecto a la obligación de informar a las autoridades de cualquier vulneración de seguridad sufrida, se consolida la tendencia dirigida a que las autoridades incentiven a las compañías eventualmente afectadas, de manera que éstas no teman represalias o la imposición de sanciones elevadas por haber sufrido una vulneración de sus sistemas de seguridad. Es importante que estén decididas a informar (e informen) a las autoridades sobre cualquier violación de seguridad que sufran. Es conveniente que la colaboración entre el sector privado y público sea continua y transparente, de forma que las compañías favorezcan el intercambio de información sobre incidentes que afronten.

Es conveniente que el asegurado adopte con carácter preventivo y proactivo en el diseño, adopción e implementación de todas esas medidas, antes de suscribir un ciberseguro. De lo contrario, puede encontrarse con que el asegurador o bien no acepte inicialmente suscribirle un seguro específico o bien, una vez suscrito, no otorgue cobertura al incidente en concreto por falta de cumplimentación de lo antes mencionado. El resultado, en cualquiera de los casos, es que el interesado no habrá transferido los ciberriesgos de manera eficiente, y no verá cubiertas sus necesidades en el ámbito de la ciberseguridad en caso de sufrir un ciberincidente. **"El hecho de que se adquiera un seguro, no significa que se pueda ignorar la seguridad tecnológica. Los aspectos tecnológicos, operacionales y del seguro van de la mano"**



[7] Allianz Corporate & Specialty: *A Guide to Cyber Risk. Managing the Impact of Increasing Interconnectivity*, Munich,: Allianz, 2015, p. 25.

3.7. Recomendaciones para realizar la contratación

Las pólizas de ciberriesgos, como cualquier otro producto asegurador, presentan definiciones, coberturas, términos y exclusiones.

Entender de forma adecuada los factores limitantes es el primer paso para contratar la póliza que mejor se adecue a las necesidades de cualquier empresa, evitando tanto el sobredimensionamiento como un alcance insuficiente de las mismas. A continuación, se listan los elementos más relevantes a considerar:

1. • Identificar correctamente el alcance necesario de la cobertura a contratar:
   a) Sujetos asegurados b) Ámbito temporal c) Ámbito territorial
2. • Conocer el negocio, los procesos y sus riesgos.
3. • Entender las coberturas contratadas.
4. • Contratar las coberturas en base a las necesidades del negocio.
5. • Estructuración del panel de proveedores de servicios.
6. • Definir de forma adecuada límites y sublímites.
7. • Atención con las definiciones y las exclusiones.
8. • Definir y comprender los disparadores *(triggers)*.

[8] CISCO: "Sólo el 45% de las organizaciones confían en sus estrategias de seguridad", *Global Newsroom CISCO* (21 de enero de 2016), en: http://globalnewsroom.cisco.com/es/es/release/S%C3%B3lo-el-45-de-las-organizaciones-confi%C3%ADan-en-su-estrategia-de-seguridad-2287959

- **Identificar correctamente el alcance necesario de la cobertura a contratar:**

  a) **Sujetos asegurados:** la propia persona jurídica y si, fuese necesario – en el caso de un grupo empresarial – sus filiales, así como cualquier persona física que sea o haya sido un empleado, Administrador o Directivo, así como cualquier autónomo o persona subcontratada, siempre y cuando trabaje bajo la dirección y supervisión del Tomador. Asimismo, pueden negociarse coberturas específicas para proteger cargos concretos como el responsable de seguridad, el director de cumplimiento normativo o el director de asesoría jurídica.

  También es recomendable que la póliza incluya extensión de cobertura al Proveedor Externos de Servicios Informáticos, de manera que, si se produce una brecha de seguridad en sus sistemas afectando al Asegurado, su póliza actúe como si dicha brecha la hubiese sufrido el propio Asegurado.

  b) **Ámbito temporal:** es necesario verificar la que aplica en el contrato. Es habitual que las pólizas otorguen cobertura a incidentes producidos con anterioridad a la entrada en vigor del seguro. Teniendo en cuenta que el tiempo medio de detección de un incidente oscila entre 100 y 200 días[8] es importante negociar una retroactividad ilimitada en las pólizas para amparar hechos descubiertos, o reclamados por primera vez, por un tercero perjudicado, durante la vigencia del contrato pero sucedidos con anterioridad al mismo. No obstante, es preciso tener en cuenta que todas las pólizas aplican una exclusión específica de hechos conocidos a la fecha de contratación del seguro. Es decir, no podrá asegurarse aquello de lo que ya se tiene conocimiento a la fecha de contratación.

  c) **Ámbito territorial:** en el contexto empresarial es habitual la existencia de servicios TIC en la nube u otros servicios externalizados ubicados en otros territorios; por lo que es importante acotar el ámbito geográfico de aplicación de la póliza a contratar.

- **Conocer el negocio, los procesos y sus riesgos.** Aunque no es necesario disponer de conocimientos avanzados en la gestión de riesgos de ciberseguridad, es importante entender e identificar el tipo de ciberamenazas asociadas al sector de actividad y a la exposición al mundo digital. Los brokers, las aseguradoras y determinadas empresas de ciberseguridad son actores habilitados para asesorar en la priorización y cuantificación de dichos riesgos. La selección de los límites de indemnización, franquicias y coberturas más adecuadas debería estar basada en el análisis de posibles escenarios derivados de la identificación de estas amenazas y sus riesgos.

- **Entender las coberturas contratadas.** Es importante comprender qué tipo de coberturas deben contratarse en función del análisis de riesgo comentado en el punto anterior. Del mismo modo, es recomendable efectuar una auditoría del programa de seguros de la empresa, ya que algunas coberturas ciber podrían estar aseguradas bajo otras pólizas de seguros corporativas contratadas.

- **Contratar las coberturas en base a las necesidades del negocio.** El elenco de coberturas y servicios proporcionados por las pólizas cada vez es mayor, por lo que el análisis de riesgo y

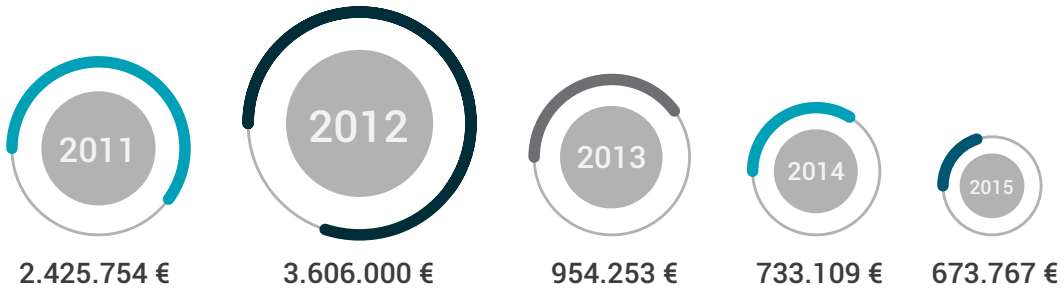
el asesoramiento de los *brokers* especialistas en ciberseguros pueden contribuir a contratar las garantías adecuadas para proteger la empresa y, sobre todo, gestionar el evento cuando suceda.

- **Estructuración del panel de proveedores de servicios.** Cada vez son más las pólizas que ofrecen la garantía de Primera Respuesta. Este servicio permite una actuación urgente para cerrar la brecha cuanto antes y controlar la situación desde el inicio, consiguiendo con ello reducir la pérdida económica derivada del siniestro. Consiste en un panel preaprobado compuesto comúnmente por proveedores expertos en (i) informática forense, (ii) asesoramiento legal especializados en materia de Protección de Datos de Carácter Personal y (iii) especialistas en comunicación, siendo éstos últimos empleados para minimizar el daño ocasionado a la imagen del Asegurado en caso de que tal evento saltase a los medios de comunicación.

  Las pólizas que tienen panel preaprobado también suelen admitir la libre designación de expertos por parte del Asegurado, de manera que éste siempre podrá elegir entre un experto establecido en la póliza, o bien, elegir otro que él estime conveniente. Por otro lado, aquellos productos que no incluyen panel preaprobado asumirán los honorarios de aquellos expertos que designe el Asegurado en el momento de producirse el siniestro. Adicionalmente es interesante comprobar en los paneles preabroados si (i) existen tiempos de respuesta establecidos para cada uno de los servicios (ii) existe la opción de elegir más de un proveedor de cada tipo.

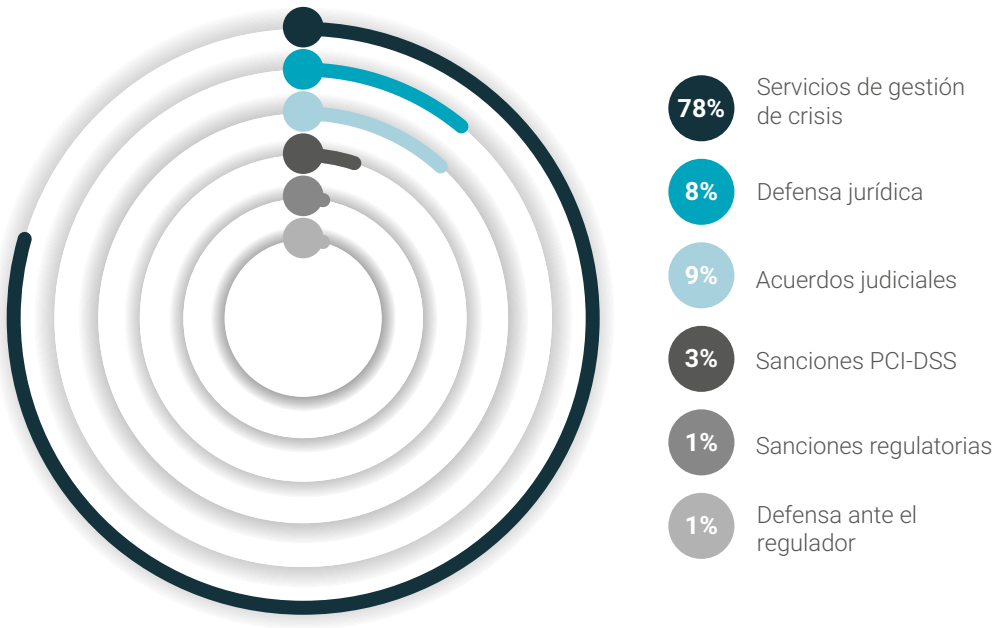
- **Definir de forma adecuada límites y sublímites.** Este punto es, con toda probabilidad, uno de los aspectos más delicados e importantes al contratar la póliza. Incluso ahora, los ejercicios prospectivos para tratar de determinar el impacto económico directo e indirecto de un ciberincidente es un ejercicio arduo y complicado. Ello, unido a la falta de datos históricos detallados, hace especialmente relevante la selección de límites, para no caer en un error de percepción *versus* realidad. Ante estas circunstancias, es aconsejable efectuar un análisis de posibles escenarios derivados de la identificación de las amenazas y los riesgos cibernéticos que permitirá plantear varios escenarios de pérdidas económicas ayudando a elegir el límite de indemnización y franquicia a asumir por el Asegurado más adecuado o conveniente.

  Adicionalmente, la mayoría de las pólizas de ciberseguros sublimitan algunas coberturas. Es importante analizar estos sublímites para que mantengan una coherencia respecto al límite de indemnización general contratado en la póliza. Sublimitando algunas coberturas (como sanciones administrativas, servicio de control e identidad/monitorización del crédito, etc.) se puede evitar quedarse sin límite económico antes de finalizar la gestión total del siniestro en cuestión. Estos aspectos suelen ser negociables y están directamente relacionados con el coste económico de la póliza. Bajo estas líneas se muestran datos referenciales sobre el coste medio por evento o siniestro, así como el coste medio asociado a algunas de las coberturas más habituales.



Coste medio por incidente y año

Fuente: Net Diligence: 2015 Cyber Claims Study, Gladwyne: Network Standard Corporation, 2015, p. 6.



Distribución del coste por servicios de las coberturas. Fuente: Ibíd., p. 7.

- **Atención con las definiciones y las exclusiones.** La amplitud del ámbito de cobertura va a depender también del clausulado de la póliza y en especial, de las definiciones y exclusiones empleadas. En este sentido, es importante contar con el asesoramiento de un *broker* especialista en ciberriesgos que negocie un redactado *ad hoc* o incluya las matizaciones y aclaraciones que sean necesarias, tanto en las definiciones como en las exclusiones, para que el clausulado se ajuste a las necesidades y particularidades del Asegurado.

- **Definir y comprender los disparadores *(triggers)***. Es preciso entender los sucesos que activarían la cobertura de la póliza de ciberriesgos contratada, es decir, las causas del daño, ya que hay pólizas que sólo se activan ante una brecha de seguridad en los sistemas informáticos, y otras más amplias, admiten también causas de índole técnica como la sobrecarga de la tensión eléctrica, daños al sistema derivados de Incendio o Inundación afectando a los ficheros electrónicos, o eventos como el robo o pérdida de un dispositivo móvil cuando éstos contienen datos de carácter personal.

  Igualmente, también debe tenerse en cuenta que algunas pólizas ejecutan la cobertura en la fecha en la que ocurrió el evento *(occurrence)*, mientras que otras se activan en la fecha en la que se recibe una reclamación de terceros contra el Asegurado como consecuencia, por ejemplo, de una fuga de datos *(claims made)*.

3.8. Gestionando un incidente con una póliza de ciberriesgos

***Target* Corporation es una de las mayores cadenas estadounidenses de supermercados que, entre los meses de noviembre y diciembre de 2013, fue víctima de un ciberataque por el cual unos ciber-criminales lograron acceder a sus sistemas informáticos y robar datos financieros y personales de 110 millones de clientes. Estos datos se desviaron a un servidor alojado en Europa del Este desde donde se trasladaron a un mercado negro de venta de tarjetas de crédito (*carding*).**

Se utilizará este caso para ilustrar las coberturas de la póliza de ciberriesgos que se han visto afectadas y conocer el volumen de la pérdida económica sufrida por *Target*.

Se ha seleccionado este caso práctico por dos motivos:

- En Estados Unidos existe la obligación de notificar las brechas de seguridad cuando hay datos de carácter personal comprometidos. Ello ha permitido seguir este caso de cerca y conocer los detalles de la pérdida económica asociada, máxime cuando en este ciberataque se vieron comprometidos los datos personales de más de un tercio de la población estadounidense, lo que provocó que el Gobierno, a través del Comité de Comercio, Ciencia y Transportes del Senado, llevase a cabo un exhaustivo análisis de la secuencia del ataque.

- La compañía tenía contratada una póliza de ciberriesgo.

ANTECEDENTES. ¿QUÉ SUCEDIÓ?

De acuerdo con las conclusiones del análisis efectuado por el Gobierno, los puntos críticos por los que ésta fuga de datos fue exitosa fueron los siguientes:

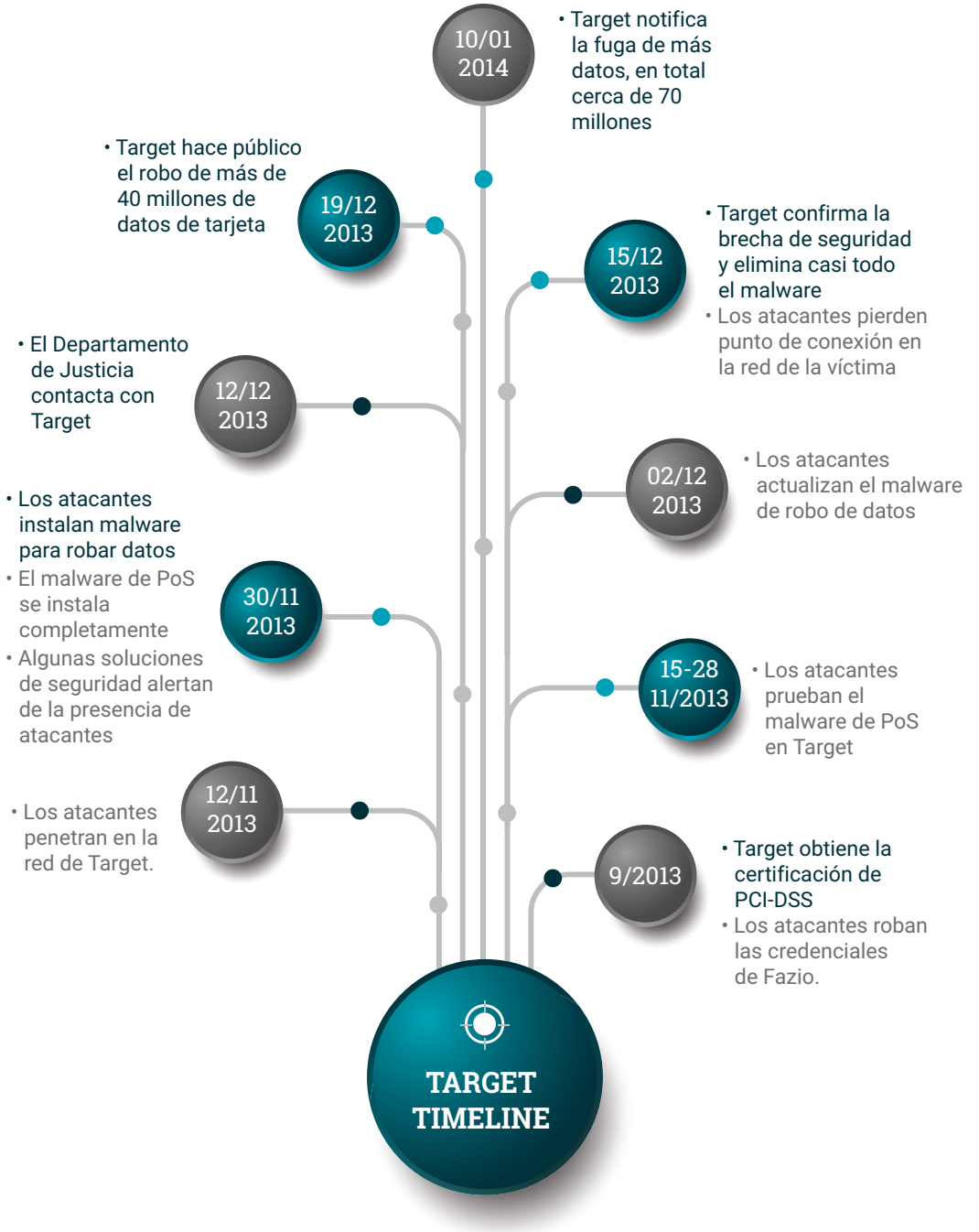
- *Target* dio acceso a un pequeño proveedor de servicios de refrigeración que no tenía suficientes garantías de seguridad en sus sistemas informáticos. Esto es lo que permitió a los criminales acceder a los sistemas de la compañía mediante una plataforma de compras.

- Los criminales infiltrados a través de las credenciales del proveedor se movieron con éxito y rapidez hasta las áreas de almacenamiento de datos, lo que sugiere que *Target* no tenía aislados adecuadamente los activos de información más sensible.

- Hubo al menos dos alertas automáticas de intrusión y de instalación de malware en el software y sistemas informáticos de la organización que no fueron detectados o identificados por la compañía. Asimismo, los sistemas llegaron a alertar sobre las rutas de escape que los criminales habían abierto en el sistema para extraer los datos y enviarlos al exterior, sin que éstas fueran detectadas.

Este proceso duró poco más de dos semanas hasta que el 12 de diciembre el Departamento de Justicia notificó a *Target* la existencia de una fuga de datos tras haberse detectado movimiento en el mercado negro de tarjetas.

El 19 de diciembre, tras las conclusiones de las primeras investigaciones internas, Target anunció públicamente la fuga, inicialmente cuantificada en 40 millones, de las tarjetas de sus clientes desde sus sistemas.



Cronograma del ciberataque contra Target. Fuente: elaboración propia.

GASTOS CUBIERTOS BAJO PÓLIZA CIBERRIESGOS

Target tenía contratada una cobertura de ciberriesgos por un límite de indemnización de 100 millones de dólares en exceso de la franquicia que retenían de 10 millones dólares[9].

• **Fase 1. Gestión del evento**

Bajo su póliza no existía un panel preaprobado de expertos. Justamente, es a raíz de este evento que los aseguradores empiezan a plantearse la importancia de que las pólizas lo establezcan con la finalidad de empezar a gestionar el evento a la mayor brevedad posible ayudando a limitar y reducir la pérdida económica asociada.

Sin embargo, la póliza sí amparaba los honorarios para llevar a cabo la investigación forense. Ello permitió descubrir más detalles de lo sucedido y determinar el alcance de la fuga de datos: 110 millones de registros, tarjetas de crédito y débito con sus números PIN y datos personales vinculados a las tarjetas de fidelización[10].

• **Fase 2. Daños Propios**

Bajo la póliza quedaban amparados los honorarios de un experto en materia de privacidad que asesorara en la notificación a los titulares afectados y a los organismos competentes. En este caso concreto se estima que los gastos de notificación han superado los 60 millones de dólares y probablemente la compañía se enfrente también a sanciones administrativas y regulatorias (como las derivadas por el incumplimiento de PCI-DDS). Igualmente, deberían sumarse también los costes del servicio de monitorización de crédito por un plazo de veinticuatro meses a los titulares afectados[11].

En cuanto a los gastos de recuperación de datos y mejora de la red informática, éstos superaron los 100 millones de dólares. Cabe destacar que la inversión en mejoras de los sistemas no estaba cubierto por la póliza[12].

En tercer lugar, *Target* sufrió un descenso del 46% de sus beneficios tras haberse hecho público el evento.

---

[9] Judy Greenwald: "Target has $100 million of cyber insurance and $65 million of D&O coverage", *Business Insurance* (19 de enero de 2014), en: http://www.businessinsurance.com/article/20140119/NEWS07 /301199973

[10] "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores", *TARGET Corporate* (19 de diciembre de 2013), en: http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores

[11] Nicole Perloth y Elizabeth Harris: "Cyberattack Insurance: a Challenge for Business", *The New York Times* (8 de junio de 2014), en: http://nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html?_r=0

[12] John Vomhof: "Target's data breach fraud could top $1 billion, analyst says", *Charlotte Business Journal* (3 de febrero de 2014), en: http://www.bizjournals.com/charlotte/news/2014/02/03/targets-data-breach-fraud-cost-could-top-1-billion.html

[13] Elizabeth Harris: "Faltering Target Parts Ways With Chief", *The New York Times* (5 de mayo de 2014), en: http://www.nytimes.com/2014/05/06/business/target-chief-executive-resigns.html?ref=technology&_r=0

• **Fase 3. Daños ocasionados a terceros**

Target se enfrenta a más de ciento cuarenta demandas judiciales promovidas por consumidores afectados por la brecha de seguridad, por lo que se enfrenta a importantes gastos de defensa y posibles indemnizaciones.

Los bancos han reclamado a Target los costes de reemisión de tarjetas de crédito y débito, que según la *Consumer Bankers Association* podrían exceder los 200 millones de dólares[14]. De momento, se ha hecho público un acuerdo entre *Target y Mastercard* mediante el cual ésta será indemnizada con 19 millones de dólares para compensar parte de los costes de reemisión de tarjetas así como los cargos fraudulentos que hayan sufrido sus clientes[15].

OTROS GASTOS CUBIERTOS POR OTRAS PÓLIZAS

Asimismo, los administradores, consejeros y directivos de *Target* se enfrentan a reclamaciones por parte de sus accionistas. Se ha publicado un acuerdo de indemnización de 10 Millones de dólares tras una *Class Action* promovida por éstos[16]. Éstas deberán canalizarse por una póliza de Responsabilidad Civil de Administradores y Directivos para cubrir los gastos de defensa y posibles indemnizaciones que se deriven, entre otros gastos, como los daños reputacionales a la propia marca y a sus Administradores y Consejeros. Para algunos, este evento ha tenido un coste personal debiendo renunciar y dimitir de su cargo como ha sido el caso del Director Ejecutivo (CEO) y del Director de Seguridad de la Información (CISO) de la compañía.

[14] Christine DiGangi: "The Target Data Breach Has Cost Banks $240 Million… So Far", *Credit* (21 de febrero de 2014), en: http://blog.credit.com/2014/target-data-breach-cost-banks-240-million-76636

[15] Kavita Kumar: "Banks ask court to block part of $19 million settlement over Target's data breach", *Star Tribune* (22 de abril de 2015), en: http://www.startribune.com/banks-ask-court-to-block-part-of-19-million-settlement-over-target-s-data-breach/300970281/)

[16] Monica Langley: "Inside Target, CEO Gregg Steinhafel Struggles to Contain Giant Cybertheft". *Wall Street Journal* (18 de febrero de 2014), en: http://www.wsj.com/articles/SB10001424052702304703804579382941509180758

4.

Ciberseguros como elemento de mejora de la seguridad

4.1. Por qué permiten mejorar la seguridad

Las aseguradoras suelen preocuparse por la percepción sobre la seguridad de sus asegurados, ya que éstos tienden a relajar la implantación de controles, sabiendo que el riesgo de pérdida se ha transferido a un tercero. Obviamente, ello redunda en una mayor probabilidad de afección ante una ciberamenaza y, por extensión, en un uso potencialmente mayor de las coberturas de una póliza.

En consecuencia, las aseguradoras juegan un papel clave para mejorar la madurez de ciberseguridad del mercado, ya que[17]:

- Pueden requerir a sus clientes el cumplimiento de unas cautelas mínimas de ciberseguridad como condición *sine qua non* para la contratación de las pólizas incluyendo, entre éstas, la adopción demostrada (auditada) de un marco de buenas prácticas de seguridad, ya sea a través de modelos de gestión internacionales como la *ISO 27001* o bien mediante el desarrollo de un modelo de gobierno de seguridad específico desarrollado, por ejemplo, para la industria española.

- Pueden ofrecer descuentos en las primas a aquellas entidades que demuestren un nivel adecuado de madurez en seguridad de forma que reduzcan los riesgos de pérdidas a transferir a la aseguradora. A mayor madurez en seguridad, menor número potencial de incidentes y, por lo tanto, menor coste de la póliza.

- Las aseguradoras pueden poner en práctica los procedimientos de gestión de ciberincidentes en nombre del asegurado de forma inmediatamente posterior al mismo, mejorando la respuesta coordinada al mismo a través de paneles de coberturas preaprobados. La principal ventaja es que, generalmente, en este tipo de aproximaciones, la aseguradora establece tiempos de respuesta contractuales (a través de acuerdos de nivel de servicio) a los proveedores del panel para que respondan en los plazos establecidos, por lo que una empresa que carezca de planes de contingencia o de gestión crisis pueda delegar en estos expertos la gestión de la crisis paso a paso.

- Dado que las aseguradoras necesitan datos fiables para que sus departamentos de suscripción cuantifiquen de manera adecuada las coberturas y las políticas de precios, el crecimiento del mercado de los ciberseguros podría conducir a una mejor comprensión de los patrones de las amenazas y la mejora de intercambio de información entre el gobierno y las empresas aseguradas respecto a ciberincidentes y coste (impactos) derivados de los mismos.

- Las propias aseguradoras desplegarán mecanismos de monitorización del estado de ciberriesgo de los mercados de sus clientes, jugando un papel importante en alerta temprana ante incidentes. Es factible imaginarse, como ya sucede en otras ramas de seguro, como por ejemplo el seguro de automóvil que presenta un coste reducido para aquellos conductores que autoricen la instalación de un GPS en su vehículo, una aproximación en la cual el asegurado autorice la instalación de sondas en

[17] Gianluca D'Antonio; Adolfo Hernández, Enrique Fojón y Manel Medina: *Incentivando la adopción de la ciberseguridad*, Madrid: ISMS y THIBER, 2014.

sus sistemas informáticos de forma que tanto la aseguradora, como el propio asegurado, disponga de una visión del riesgo informático en tiempo real, combinado con estrategias de monitorización de internet y fuentes abiertas para detectar amenazas externas. De este modo, los precios de las pólizas podrán ser totalmente ajustados a lo largo del ciclo de vida del producto al nivel de riesgo del asegurado.

En definitiva, la adopción de este tipo de productos supone una mejora significativa del nivel de seguridad de las compañías bajo dos ópticas temporales diversas:

- **A corto plazo** para los sujetos asegurados, ya que permite una gestión más efectiva de forma directa (transferencia de riesgo) e indirecta (mejora de los controles preventivos) de los impactos asociados a un ciberincidente.

- **A medio/largo plazo**, para toda la industria, gracias a la visión agregada de los ciberriesgos, otorgando una comprensión detallada e incluso sectorial de las amenazas que atenazan el tejido empresarial español.

4.2. El papel de las aseguradoras en España

Los ciberseguros y el sector asegurador en general desempeñan un papel fundamental en la economía de cualquier país, al favorecer e impulsar su desarrollo económico, ya que:

- Permiten al asegurado trasladar los riesgos de su actividad a un tercero (asegurador) con capacidad económica para soportar aquéllos.
- Refuerzan la posición crediticia del Asegurado, sobre todo en aquellas ocasiones en las que contratar un seguro supone algo fundamental y necesario para poder desarrollar determinadas actividades.
- Fomentan la inversión productiva y el ahorro, puesto que financieramente el tomador de una póliza de seguros se constituye en prestamista del asegurador, quien convierte las primas que recibe en una inversión a largo plazo y, por ende, en ahorro para el Asegurado[18].

El papel clásico de las aseguradoras ha consistido en una labor reactiva, más que proactiva, actuando como depositarias de los fondos que sus clientes destinan a la cobertura de ciertas contingencias consustanciales al desarrollo de su actividad, para el caso de que alguna o todas ellas se materialicen.

La traslación del contenido de la mayoría de la vida comercial y profesional de las sociedades modernas desde el papel al ciberespacio ha cambiado radicalmente este escenario. La mentalidad y el enfoque con el que las aseguradoras deben diseñar y comercializar sus productos en este entorno habrá de tener también un enfoque global, transversal y multidimensional, sin limitarse a la actividad que el asegurado realiza en el ciberespacio, sino contemplando todas las interrelaciones que existen hoy (y serán cada vez más en el futuro inmediato) entre este entorno y dicha actividad.

En suma, nuestro país está asistiendo a un verdadero cambio de paradigma en el sector del seguro, donde se ha convenido que el primer supuesto de ciberseguro, considerado y denominado como tal, data del año 2006, con la comercialización por una conocida firma multinacional con presencia en España del primer seguro que cubría los ataques de virus y las actividades dañinas piratas informáticos.

Hasta hace escasos años, la práctica totalidad de las aseguradoras en España, tanto nacionales como extranjeras, sólo protegían los equipos informáticos cuando éstos resultaban dañados por un siniestro con efecto primario y directo sobre el hardware (incendio, inundación, etc.), dejando de lado todos aquellos riesgos derivados de o relacionados con el software y/o, sobre todo, con la conexión de los equipos informáticos a Internet.

[18] Gabriel Tortella (dir.): *Historia del Seguro en España,* Madrid: MAPFRE, 2014.

Es más, en muchos ámbitos aseguraticios específicos, como por ejemplo el del transporte marítimo, ha sido costumbre, en la mayoría de los casos, excluir de cobertura cualquier pérdida, daño o responsabilidad y gasto causado o relacionado, directa o indirectamente, con el uso de equipos o programas informáticos.

Algunos de los principales operadores del mercado nacional del seguro han reaccionado, adaptando sus productos durante los últimos años a los riesgos derivados del ciberespacio, abriendo incluso nuevas líneas de negocio, mediante el diseño de pólizas *ad hoc* para cubrir múltiples ciberriesgos (tanto los derivados de ciberataques, como de la existencia de una arquitectura informática o red obsoleta, o el uso incorrecto de las herramientas informáticas, entre otros).

Este cambio de mentalidad en el mercado del seguro en España es una realidad palpable, pero todavía incipiente, tanto por el lado de las aseguradoras, entre quienes las ciberpólizas constituyen hoy un valor añadido y diferencial (y no una *commodity* como pudiera ser el seguro de daños a terceros), como por el lado de los asegurados, donde aproximadamente el 40% del tejido industrial y empresarial español (y dentro de este porcentaje, sólo las grandes compañías y superficies) se encuentra cubierto, en mayor o menor grado, frente a algún tipo de ciberriesgo.

Lo relativamente reciente del enfoque del seguro cibernético es que éste afecta a un elemento nuclear de la relación aseguraticia: el histórico de ciberincedentes sobre los que se hacen los cálculos actuariales y estadísticos que han de permitir una tarificación con una sólida base técnica. No existe en España, como es lógico, un *track record* o histórico lo suficientemente amplio y variado de ciberriesgos, con el detalle de su periodicidad, alcance e impacto, que permita a los actuarios españoles hacer estimaciones precisas que permitan ajustar las primas de las ciberpólizas, optimizar y rentabilizar sus correlativos procesos de contratación y comercialización.

> "No existe en España un histórico lo suficientemente amplio y variado de ciberriesgos, con el detalle de su periodicidad, alcance e impacto, que permita a los actuarios españoles hacer estimaciones precisas"

En esta línea, el mercado del ciberseguro en España debe dar el siguiente paso en su evolución hacia la madurez, mediante la implementación de cinco elementos básicos:

- La concienciación del cliente respecto del alcance de su propia exposición a los ciberriesgos.
- La gestión integral de todas las fases y sujetos relacionados con este tipo de riesgos y su aseguramiento.
- La colaboración entre agentes: Administración Pública y organismos oficiales, empresas del sector asegurador (asociaciones, aseguradoras, *brokers*, proveedores de servicios) y los asegurados.
- La retroalimentación.
- El aprendizaje continuo.

Hace falta, pues, una importante labor de concienciación y en ello las aseguradoras pueden jugar un importante papel a través de su ejemplo, publicidad, conferencias, programas de formación y relación de contacto continuo entre la aseguradora y su cliente, superando la tradicional relación basada solo en los hitos de contratación, atención al siniestro (si es que se éste produce eventualmente) y renovación (o en su caso cancelación) de la póliza.

Es también vital que las aseguradoras superen su concepción del ciberseguro como algo centrado en reducir la exposición del asegurado y/o la probabilidad de que ocurra o se materialicen las ciberamenazas. Se ha de pasar a una gestión integral de todas las fases y sujetos relacionados con este tipo de riesgos y su aseguramiento en una relación pre y post siniestro.

Esencial es, igualmente, que exista una colaboración fluida entre toda la cadena de valor de los ciberseguros, que ayude a superar en este ámbito las reservas que tradicionalmente existen en España (a diferencia de otros países) por parte de los afectados, a reportar con la deseada asiduidad y detalle los siniestros sufridos.

Una mayor fluidez y transparencia en este tipo de comunicación ayudaría a los ya citados actuarios a realizar mejor su trabajo, contribuyendo con ello a la obtención de un mayor *expertise* en materia de ciberseguros y, a la postre, a la maduración del sector.

De la mano de lo anterior va la conveniencia y/o necesidad de que exista una retroalimentación entre aseguradoras, asegurados, Administración, instituciones o gobiernos.

En este sentido, los condicionados que comienzan a manejarse en las ciberpólizas de las mayores aseguradoras proveedoras de estos productos prevén específicamente coberturas consistentes en servicios especializados de análisis continuo de la situación real del asegu-

rado, de constatación o auditoría casi continua del nivel de actualización de los sistemas del asegurado, de compartición de *know-how* específico de las aseguradoras con los clientes y de un apoyo y asistencia casi en tiempo real tan pronto se detecta una posible incidencia cibernética. No es exagerado identificar una tendencia a que los centros de gestión de incidentes o crisis de las aseguradoras actúen casi como una extensión de los departamentos de IT de los asegurados, en los supuestos de compañías de cierto tamaño.

Según el Instituto Nacional de la Ciberseguridad (INCIBE), el mercado del ciberseguro en España mueve unos 500 millones de euros anuales, con ritmo de crecimiento anual estimado entorno al 12%. Este crecimiento va parejo al de la frecuencia e impacto de los ciberincidentes. El Instituto de Comercio Exterior (ICEX) apunta que las compañías españolas pueden estar perdiendo más de 13.000 millones de euros anuales como consecuencia de ciberincidentes.

La antes comentada transición, desde el tradicional ámbito de relación entre aseguradora y asegurado (contratación, pago de la prima, pago de potencial siniestro y renovación o cancelación de la póliza), a un nuevo escenario en que la aseguradora se convierte en proveedor de servicios técnicos y de auditoría continua de los sistemas del asegurado, supone, obviamente, una ampliación de las posibilidades de oferta de tales aseguradoras.

Evolución del precio del riesgo (risk pricing)

Fuente: Capgeminy-Efma: World Insurance Report 2016, París: Capgemini, 2016, p. 27.

En estrecha relación con la necesaria acumulación de información fáctica de incidencias relevantes a efectos del seguro (el célebre "histórico de siniestralidad") se encuentran los avances tecnológicos en el área de la obtención, tratamiento y correlación de datos.

4.3. Incentivos públicos

Si bien el mercado de los ciberseguros se recomienda que sea netamente privado, para incentivar su adopción pueden crearse unas líneas de acción desde los organismos gubernamentales de forma que[19]:

- Se reduzca el coste de las primas mediante la asunción de parte de las coberturas de las aseguradoras privadas a través de programas de reaseguro.
- Cuando los riesgos sean considerados como "no asegurables" por el mercado asegurador privado, se puede considerar la opción de que sea el Estado el que asuma ciertos riesgos para reemplazar o estabilizar el mercado privado, por ejemplo, a través de programas específicos de compensación. En el caso español se podría vehiculizar a través del Consorcio de Compensación de Seguros.
- Reconocer la adopción de marcos de ciberseguridad con un nivel de madurez determinado como una muestra de control debido, siendo de esta forma condiciones atenuantes ante potenciales y limitando por extensión las responsabilidades civiles e, incluso, penales según la legislación nacional.

Al mismo tiempo, teniendo en cuenta que la propia Administración Pública española posee un nutrido ecosistema de proveedores de TIC, se recomienda que actúe como eje vertebrador para aumentar el nivel de resiliencia de todos sus proveedores en términos de ciberseguridad y, por extensión, de un alto porcentaje del tejido empresarial nacional. Para ello deberá solicitar como criterio básico obligatorio de contratación para con la Administración el disponer de pólizas de seguro de ciberriesgo con un alcance de coberturas relevante para el servicio prestado y cuya cuantía no sea excesiva en relación con el objeto del contrato. Como ya sucediera con los seguros de responsabilidad civil, esta medida supondría un claro habilitador de estos productos aseguradores en el mercado español a la par que una mejora de control financiero de los ciberriesgos asociados a la cadena de suministro (*supply chain risk*).

El Estado puede favorecer el establecimiento de unos criterios comunes de seguridad a través de un marco de controles de seguridad de referencia cuya observancia y cumplimiento por parte de las empresas facilitase al sector asegurador la suscripción de seguros de ciberriesgos.

Las administraciones públicas tienen una doble función, como proveedores de servicios críticos a la sociedad y como reguladores del mercado y de la economía. Esta doble responsabilidad les ofrece también la capacidad de fijar los requisitos mínimos que deben cumplir no solo

[19] D'Antonio; Hernández; Fojón y Medina, *op. cit.*, pp. 33-41.

sus servicios y proveedores TIC; sino también aquellos considerados críticos para la sociedad siguiendo el ejemplo de la Directiva Europea de Servicios de Confianza.

Esta regulación tiene una doble función:

- Definir los límites por encima de los cuales deben situarse los planes de seguridad de las empresas.

- Ayudar a los responsables de seguridad a conseguir los recursos necesarios para implantar los mecanismos mínimos de seguridad requeridos en la regulación.

La acreditación de capacidades de las empresas que optan a ofrecer servicios a la Administración Pública ha sido siempre objeto de polémica, ya que no siempre son uniformes o están armonizados con los de otras administraciones europeas.

Es por esto que la definición de unos criterios de selección basados en normas y buenas prácticas reconocidas internacionalmente incentivaría su aplicación, ya que facilitaría la acreditación de capacidades para optar a la provisión de servicios a cualquier Administración Pública europea.

De hecho, éste es uno de los objetivos de la Comisión Europea para conseguir el mercado único y eliminar las barreras administrativas.

Además, la Administración Española podría mantener un listado de compañías que demostrasen su alineamiento con este marco de control. Mediante la constitución de una lista pública de empresas certificadas, países como el Reino Unido[20] o Australia[21] han dado respuesta a la necesidad de regular un mercado creciente con unas garantías de profesionalidad y calidad. Estas listas centralizadas actuarían como punto de referencia público en el mercado aportando:

- **Un impacto positivo comercial y reputacional** entre las empresas.

- **Un nivel demostrable de seguridad** de los procesos y procedimientos y validación de competencias técnicas de las organizaciones miembros.

- **Orientación, normas y oportunidades** para compartir y mejorar los conocimientos.

- **Medio ágil** de inserción en el mercado de competencias, servicios y tecnologías de ciberseguridad.

- **Herramienta útil** para las aseguradoras ya que contarían con una validación por parte un agente externo a la propia empresa privada sobre el nivel de madurez de sus controles de seguridad alineados con un marco de control definido.

[20] CREST: http://www.crest-approved.org/

[21] CREST Australia: http://www.crestaustralia.org/

5.

Anexo: Los casos de Estados Unidos y Reino Unido

5.1. Estados Unidos

Ha pasado un cuarto de siglo desde que Estados Unidos calificara el ciberespacio como el quinto elemento del entorno donde se desarrollan las operaciones militares (tras la dimensión terrestre, naval, aérea y espacial) y una década desde que considerara que este dominio constituía una prioridad estratégica en materia de seguridad nacional. Desde entonces, Washington ha realizado ingentes avances en la configuración de un entramado de ciberseguridad que integre a los actores públicos y privados del país con un triple objetivo: incrementar la seguridad, protección y resiliencia de su entramado social frente a cualquier ciberataque; mantener el liderazgo estratégico americano en el ciberespacio y consolidar un mercado en expansión que genera ingentes volúmenes de negocio a nivel global.

Una de las principales áreas prioritarias que requiere de la participación público-privada es la ciberprotección de las infraestructuras críticas. Para ello, además de incrementar la colaboración entre departamentos y agencias gubernamentales – Justicia, Comercio, Interior o la Agencia Nacional de Seguridad, por poner algunos ejemplos – para mejorar la seguridad de estos servicios vitales para el normal funcionamiento del país; también se está reforzando la concienciación, capacitación y trasvase de información entre sus propietarios u operadores con el gobierno. Éste es el marco donde se desarrolla la Orden Ejecutiva 13636 *Improving Critical Infrastructure Cybersecurity* que, firmada por el Presidente Barack Obama a principios de 2013, exponía que las ciberamenazas sobre las infraestructuras críticas constituye uno de los principales retos que debe afrontar el país en materia de seguridad nacional e instaba a reforzar su seguridad y resiliencia frente a cualquier ataque de este tipo[22].

Esta norma sentó las bases para la configuración de un marco de ciberseguridad que, elaborado por el Departamento de Comercio y monitorizado por el Departamento de Interior, pudiera ser adoptado voluntariamente por los propietarios y operadores de las infraestructuras críticas del país. Abierto a cualquier organización del sector con independencia de su dimensión física, volumen de negocio o madurez cibernética, este marco pretende:

- Fijar un conjunto de estándares tecnológicos y procedimentales susceptible de ser adoptado por todos los actores del sector.
- Homogeneizar y armonizar – en la medida de lo posible – las prácticas ya existentes entre los actores del sector.
- Incrementar la comunicación entre empresas, y entre éstas y la administración en materia de ciberriesgos.
- Establecer un conjunto de propuestas que permitan reducir la exposición y aumentar la resiliencia de las infraestructuras críticas frente a los ciberriesgos.

[22] Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*, Registro Federal 11737 (19 de Febrero de 2013), en: https://federalregister.gov/a/2013-03915.

Aunque la participación en este marco es libre, el Departamento de Interior ha lanzado la *Critical Infrastructure Cyber Community*, una iniciativa público-privada encaminada a facilitar su implementación entre los propietarios y operadores de las infraestructuras críticas del país apoyándoles en la adopción de los estándares técnicos, el cumplimiento de la normativa vigente, la aceptación de buenas prácticas, el establecimiento de requerimientos específicos a los proveedores y socios o la integración de los ciberriesgos en las actividades de gestión y control del riesgo corporativo. Además, conscientes del coste económico que puede tener para el sector privado la adopción de este marco de actuación en el corto plazo, el Gobierno, el Departamento del Tesoro y el Departamento de Comercio han lanzado un conjunto de estímulos – asistencia financiera, exenciones fiscales, bonificaciones económicas, patentes de productos, participación en proyectos de I+D+i o reconocimiento público – que permitan incentivar su implementación.

Precisamente, Washington ha estimado que, para garantizar la adopción de este nuevo marco de ciberseguridad, es fundamental contar con la colaboración de las empresas aseguradoras. Mediante la provisión de pólizas susceptibles de cubrir – específica o globalmente – toda la gama de ciberriesgos que se ciernen sobre las empresas y que su prima esté condicionada tanto por el grado de cumplimiento del marco federal como por el desarrollo y resiliencia de sus sistemas, las aseguradoras adquieren un papel central en la armonización, homogeneización y mejora de las cibercapacidades de este sector. Por un lado, éstas pueden proporcionar a la administración federal y a las infraestructuras críticas del país ingentes volúmenes de información acerca del estado de madurez de las empresas del sector, los principales vectores de ataque, las mayores vulnerabilidades, el nivel de resiliencia, las prácticas corporativas o la tipología de incidentes. Por otro lado, su colaboración es vital para que las infraestructuras críticas puedan gestionar eficazmente las responsabilidades legales y financieras derivadas de los ciberataques (exceptuando los actos de terrorismo o de guerra), evaluar si éstas pueden participar en el marco de ciberseguridad y proponer los mejores mecanismos – provisionando pólizas capaces de cubrir toda la gama de ciberincidentes o limitando las responsabilidades – para que estas infraestructuras puedan reducir, transferir o limitar el impacto de los ciberriesgos.

"Washington ha estimado que, para garantizar la adopción de este nuevo marco de ciberseguridad, es fundamental contar con la colaboración de las empresas aseguradoras."

Además de la centralidad que poseen los ciberseguros para la promoción, adopción y consolidación de este marco de ciberseguridad, la Casa Blanca pretende fortalecer las relaciones entre la administración federal, las infraestructuras críticas y las compañías aseguradoras para afianzar un marco de colaboración que permita la puesta en común de información sobre ciberincidentes, mejore la ciberconcienciación de las empresas del sector, desarrolle un modelo de buenas prácticas que redunde sobre la prima del ciberseguro y garantice la consolidación de un mercado de ciberseguros maduro y competitivo a nivel global.

Resumiendo, Estados Unidos considera que los ciberseguros son fundamentales para promover la adopción de este nuevo marco de ciberseguridad para reforzar, armonizar y homologar las cibercapacidades de las infraestructuras críticas del país. Además, las interacciones que se están produciendo entre la administración, las infraestructuras y las aseguradoras no sólo redundan en el conocimiento mutuo, sino también en la consolidación de un marco estratégico de colaboración público-privada de inestimable valor. En este sentido, no debe descartarse que Washington proponga aplicar este modelo a otros sectores de la actividad empresarial y promueva la adopción de los ciberseguros para gestionar el impacto de las amenazas procedentes del ciberespacio y consolidar un nuevo mercado en franca expansión.

5.2. Reino Unido

El enfoque británico es sensiblemente distinto al estadounidense. Mientras el segundo se circunscribe a la adopción del marco de ciberseguridad para las infraestructuras críticas del país y la consolidación de un modelo de colaboración público-privada en esta materia, el Reino Unido está integrando los ciberseguros en todos los sectores de la actividad económica del país, regulando este mercado emergente con infinitas posibilidades de negocio y trabajando para que Londres se convierta en un referente mundial en materia de ciberseguros.

En línea con Estados Unidos y muchos países de nuestro entorno, Reino Unido también considera que los riesgos procedentes del ciberespacio son cada vez más importantes para la seguridad nacional y su impacto económico, corporativo, legal o técnico sobre el tejido empresarial del país aumenta día a día. Para intentar encauzar esta situación, el gobierno británico proyectó una amplia batería de medidas enfocadas a incrementar la concienciación pública sobre los ciberriesgos y apoyar a las empresas del país – con independencia del sector de negocio, perfil de riesgo, nivel de madurez o volumen – a gestionar las ciberamenzas. Y es que si bien las grandes corporaciones han tomado conciencia de los ciberriesgos y están invirtiendo importantes sumas de dinero para reducir su exposición a los ciberataques, la mayoría de pequeñas y medianas empresas – muchas de ellas proveedores o clientes de las primeras – no poseen ningún tipo de seguridad.

Los *Cyber Essentials*[23] son la principal iniciativa propuesta por Londres para reforzar la protección corporativa frente a toda la gama de ciberriesgos, especialmente aquellos susceptibles de provocar la pérdida de datos, interrupciones de servicio o robo de propiedad intelectual. Elaborada por el gobierno con el apoyo de la industria, esta guía susceptible de ser adoptada por cualquier organización – desde un negocio familiar a una empresa, centro universitario u ONG – contiene un conjunto de directrices básicas en materia de ciberseguridad para reducir su exposición frente a las ciberamenazas más comunes. Y para facilitar la adopción de este esquema, además de la asistencia técnica y el apoyo económico proporcionado por la administración, el gobierno y las aseguradoras han resuelto emplear los ciberseguros como una forma de incentivar la prevención, mitigación, gestión y transferencia del riesgo corporativo y una estrategia para homogeneizar, simplificar y consolidar el mercado emergente de los ciberseguros.

En efecto, además de concienciar a las empresas del país sobre los riesgos procedentes del ciberespacio y explicar que éstos pueden asegurarse, Londres pretende que éstos se conviertan – junto con la concienciación y tecnología – en una inversión prioritaria en ciberseguridad, puesto que la prima que pagará la industria estará condicionada por la madurez de sus ciberc apacidades[24].

De hecho, es importante destacar que las aseguradoras han comenzado a utilizar – y ofrecer pólizas que sufragan el proceso de acreditación por la reducción del riesgo que ello represen-

[23] HM Government: *Cyber Essentials Scheme*, Londres: Department of Busness, Innovation & Skills, 2014.

[24] HM Government: *Cyber Essentials Scheme: Assurance Framework*, Londres: Department of Business, Innovation & Skills, 2015.

ta – la certificación del cumplimiento de los *Cyber Essentials* como un condicionante de los análisis de riesgo de las pequeñas y medianas empresas. A su vez, esta certificación no sólo redunda sobre la prima del ciberseguro; sino también sirve para informar al resto de actores – socios, proveedores o clientes – sobre el estado de madurez de sus cibercapacidades.

Además de mejorar la seguridad y reducir el impacto corporativo de los ciberataques, la popularización de los ciberseguros también reforzará la conciencia situacional de las empresas y el gobierno sobre los ciberriesgos que se ciernen sobre el sector industrial británico. Conocedoras de los ciberincidentes que se producen entre sus clientes y que no siempre se reportan a los poderes públicos, las aseguradoras pueden proporcionar – bien sea mediante el flamante *Cyber Security Information Sharing Partnership* u otras iniciativas que garanticen la confidencialidad entre la aseguradora y el asegurado – al gobierno una fuente de información adicional sobre los principales riesgos, amenazas, vulnerabilidades y ataques que se ciernen sobre las empresas del país. Estos datos también redundarán sobre las aseguradoras, ya que podrán conocer con mayor detalle las tendencias individuales y sectoriales en materia de ciberataques para así modular las coberturas, pólizas, responsabilidades o primas de riesgo para los distintos sectores empresariales.

Por último, el Reino Unido aspira a que Londres – uno de los principales centros económicos del globo, sede de numerosas corporaciones, con vasta experiencia en materia de servicios financieros, técnicos, legales o de consultoría y que factura importantes sumas de dinero en coberturas de protección de datos estadounidenses – se convierta en un *hub* para el mercado de los ciberseguros a nivel global. Y es que si bien éstos son un producto relativamente novedoso que apenas se ha explotado fuera de Estados Unidos, Londres pretende valerse tanto de sus relaciones con Washington, situación en el continente europeo o presencia en los mercados internacionales como la floreciente legislación acerca de la protección de datos en el seno de Unión Europea y en muchos otros países del planeta para consolidar su posición de mercado.

En resumen, el Reino Unido considera los ciberseguros como algo consustancial para la gestión de los ciberriesgos y la mejora de las cibercapacidades del tejido industrial británico. Además, pretende convertir a Londres en un centro de referencia global en este mercado floreciente con enormes posibilidades de crecimiento. **Muchos países deberían tener en consideración el ejemplo británico para proceder a la configuración de un mercado de ciberseguros eficaz, competitivo y puntero a escala local, regional y global.**

Síguenos en
www.thiber.org