# Ciberseguros: la última línea de defensa

**La transferencia de riesgos de ciberseguridad al sector asegurador está empezando a despertar tímidamente y no sin cierta dificultad ante la falta de datos suficientes y de calidad sobre la cibersiniestralidad causada por incidentes asociados con la seguridad de la información. Este hecho va a ir cambiando con la tendencia del panorama normativo global, que estimula la notificación de incidentes –si bien es cierto que con distintas finalidades– y con la asunción plena del riesgo tecnológico como una componente preponderante en la sociedad digital.**

Adolfo Hernández / Enrique Fojón

A finales de la década de los 90 se comenzaron a abordar los problemas de seguridad de la información de una forma metodológica y procedimentada mediante técnicas de análisis de riesgos.

De esta manera, las organizaciones comenzaron a planificar sus estrategias de seguridad a través de planes directores de seguridad, cuyo elemento principal vertebrador era un análisis de riesgos. 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.

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, retenidos por las organizaciones. No obstante, en la actualidad, 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 cada compañía.

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 [1]. 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.

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.

## Cambio de paradigma

El papel clásico de las aseguradoras ha consistido en una labor reactiva (post-siniestro), más que proactiva (pre-siniestro), 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.

Hasta hace pocos años, la práctica totalidad de las aseguradoras en España, tanto nacionales como extranjeras, sólo protegían los equipos informáticos cuando estos 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 (servicios).

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.

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.

## Encajando en el mercado de la seguridad

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 portafolios comerciales de servicios de ciberseguridad en toda la cadena de valor industrial nacional, a saber: MSSP, integradores, fabricantes y consultoras.

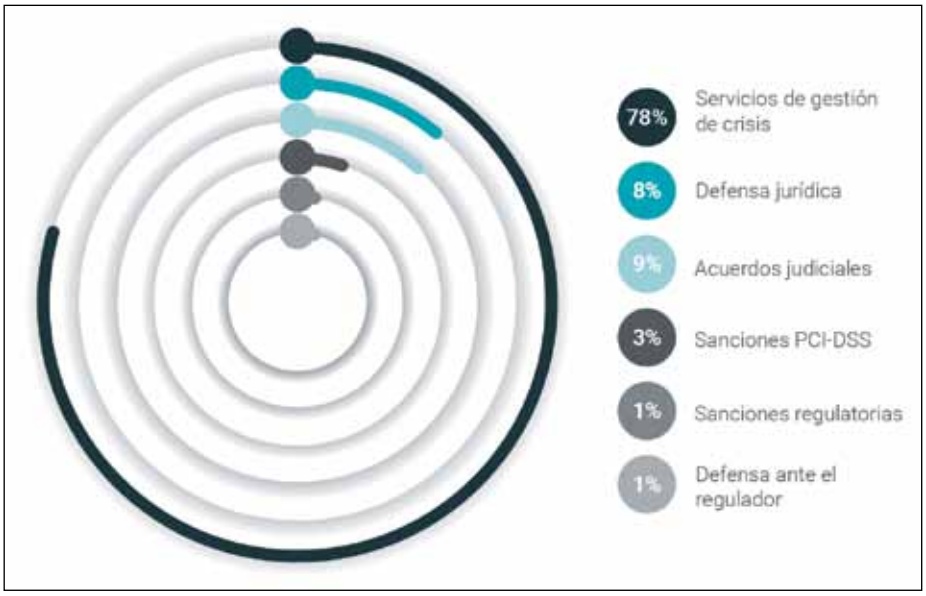


**Figura 1.- Distribución del coste por servicios de las coberturas.**

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

Los servicios pre-siniestro o preventivos 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 la gran empresa y, derivado de lo anterior, la oferta se limita de forma general a unas jornadas gratuitas de expertos en materia de seguridad tecnológica y algún dispositivo que combina herramientas de información de amenazas con soluciones de información de fuentes abiertas.

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, si bien en otros mercados internacionales estos servicios cuentan con un nutrido catálogo de servicios.

Hasta ahora se han cristalizado acuerdos globales y regionales de empresas del sector de seguridad de la información con aseguradoras para ser incluidas las primeras en el panel de proveedores de servicios reactivos, fundamentalmente servicios forenses y de restauración de datos. También se pueden identificar tímidos *partnerships* en los cuales las empresas de seguridad participan en la elaboración de diagnósticos de seguridad esenciales durante la suscripción del seguro o desarrollando servicios y soluciones para tratar de automatizar esta tarea.


**Figura 2.- Coberturas habituales de un ciberseguro.**

Sin embargo, es conveniente recordar la naturaleza financiera del sector seguros y su capacidad de adquirir presencia en todo el ciclo de vida del producto aseguraticio, como ya sucede en el seguro sanitario o de automóvil, en el cual las propias compañías han adquirido clínicas, hospitales, talleres o servicios de asistencia en carretera propios.

Así pues, no sería raro vaticinar una mayor presencia del sector asegurador en el mercado de los servicios reactivos y también preventivos, mediante la adquisición de empresas tecnológicas y de servicios de ciberseguridad, adquiriendo un control mayor sobre la cadena de valor.


**Figura 3.- Recomendaciones al adquirir una ciberpóliza.**

## Por qué mejoran la seguridad

Dicho lo anterior, estos productos aseguraticios suponen una clara línea emergente para promover la adopción de medidas de ciberprotección más robustas.

Las aseguradoras suelen preocuparse por la percepción sobre la seguridad de sus asegurados, ya que los mismos 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, lo cual afectaría de forma directa al modelo económico de las aseguradoras.

En consecuencia, las aseguradoras juegan un papel clave para mejorar la madurez de ciberseguridad del mercado, ya que [2]:

• 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 (tal como ha realizado el gobierno británico a través de los **CyberEssentials**).

• 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 sus sistemas informáticos de forma que tanto la aseguradora, como el propio asegurado, disponga de una visión del riesgo informático en tiempo real, combinada con estrategias de monitorización de fuentes abiertas (OSINT) 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.


**Figura 4.- Ejemplo de servicios y soluciones pre-siniestro o preventivas.**

## Conclusión

La adopción de este tipo de productos puede suponer una mejora significativa del nivel de seguridad de las compañías bajo dos ópticas temporales diversas:

• A corto plazo, 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. ■

*Todos los datos expuestos en el presente artículo se encuentran desarrollados en el informe "**Ciberseguros. La transferencia del ciberriesgo en España**", desarrollado por THIBER con el patrocinio de AIG, AON, K2 Intelligence, Marsh, Minsait y Telefónica.*

**Adolfo Hernández**
Subdirector
adolfo.hernandez@thiber.org

**Enrique Fojón**
Subdirector
enrique.fojon@thiber.org

**THIBER, the cybersecurity think tank**

## REFERENCIAS

[1] 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

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