Swiss Re Institute

N.º 1/2017

sigma

Cibernética: cómo enfrentarse a un riesgo complejo

Resumen

Los costes de las violaciones de la seguridad cibernética están creciendo significativamente.

Las amenazas cibernéticas evolucionan rápidamente debido a la creciente transformación digital de la sociedad, al uso generalizado de procesos y dispositivos con conexión a Internet y al perfil cambiante de los *hackers*. Recientemente se han producido ataques cibernéticos de alto perfil que demuestran que también se está ampliando el alcance de las posibles pérdidas asociadas, abarcando más daños físicos y económicos relacionados con la violación de la privacidad de datos y con los activos tangibles e intangibles de las empresas, además de los costes por interrupción del negocio. Como resultado, la cuestión de la protección cibernética se sitúa en el centro de la agenda corporativa, tanto en grandes como en pequeñas empresas.

Pese a la creciente concienciación todavía quedan muchas empresas por institucionalizar la gestión del riesgo cibernético.

A pesar de la mayor concienciación, las corporaciones no están por lo general bien preparadas para hacer frente a los riesgos cibernéticos. Han sido relativamente pocas las empresas que han integrado la ciberseguridad en su sistema de gestión de riesgos. Esta es una situación insostenible. En muchas jurisdicciones se está comenzando a aplicar legislación que obliga a las empresas a introducir medidas de seguridad reforzadas sobre la información privada de sus clientes, y se enfrentan a fuertes multas en caso de no llegar a cumplir las normas requeridas.

Se está desarrollando seguro cibernético especializado, pero la magnitud y el alcance de la cobertura en relación con la exposición son modestos.

La primera línea de defensa de las empresas contra las amenazas cibernéticas es invertir más en tecnología de seguridad y prácticas de gestión de riesgos sólidas y exhaustivas. Hay muchas que buscan soluciones externas para gestionar sus exposiciones cibernéticas, incluida la transferencia de riesgos a terceros en mejores condiciones para absorberlos. Se está desarrollando rápidamente un mercado especializado en seguro cibernético y cada vez hay más aseguradoras que desean ampliar el negocio en este ramo especializado. Pero algunos riesgos cibernéticos importantes siguen estando sin asegurar en gran parte y la escala de cobertura es modesta respecto a las exposiciones globales de las empresas.

Las aseguradoras y las empresas están creando modelos que a la larga deberían ser la base de otras soluciones de transferencia de riesgo.

Es difícil comprender y calibrar los riesgos cibernéticos, especialmente dado el gran potencial de exposiciones correlacionadas. La vertiginosa evolución del entorno tecnológico y la carencia de historial de datos de siniestros que serviría para extrapolar información sobre futuras pérdidas constituyen todo un desafío. Sin embargo, las aseguradoras y sus clientes están trabajando arduamente con diferentes enfoques de modelización del riesgo cibernético. Aunque los modelos probabilísticos completos se encuentran todavía en una fase inicial, la experiencia con otros peligros ofrece la esperanza de que finalmente surjan modelos de riesgo cibernético más ricos y mejores a medida que evolucione la comprensión de los factores de riesgo fundamentales y se disponga de más datos sobre pérdidas cibernéticas.

La innovación de productos y procesos puede ayudar a hacer más asegurables los riesgos cibernéticos, pero también es esencial la colaboración entre empresas y aseguradoras.

Sin embargo, el progreso a la hora de abordar el riesgo cibernético no debe estar regido por los avances en la modelización del riesgo. La innovación de productos y procesos en el sector del seguro ayudará a hacer más asegurables los riesgos cibernéticos y a ampliar la cobertura disponible para un número mayor de asegurados. Esto incluye normas comunes para obtener, compartir y comunicar datos sobre incidentes cibernéticos, y un mayor uso de analíticas inteligentes para mejorar la detección de amenazas y la evaluación de riesgos. El futuro desarrollo de nuevos títulos vinculados con el seguro puede también facilitar que, en su momento, se transfieran ciertos riesgos cibernéticos a inversores del mercado de capitales. Para ampliar los límites de la asegurabilidad, las empresas deberán trabajar con sus aseguradoras para crear un mercado que sea sostenible.

Rápida evolución del panorama del riesgo cibernético

Coste de las violaciones cibernéticas

Las violaciones de ciberseguridad constituyen una amenaza creciente y un alto riesgo global.

En los últimos años ha aumentado la preocupación sobre los riesgos cibernéticos luego de varios casos de violaciones de seguridad y datos de gran repercusión mediática, entre los que se incluyen ataques cibernéticos promovidos por estados. Organizaciones como el Foro Económico Mundial consideran que los ataques cibernéticos son uno de los principales riesgos a los que se enfrenta el mundo en la actualidad[1]. En cuanto a los negocios, el alcance de las posibles pérdidas físicas y económicas, tanto de primeras como de terceras partes, ocasionadas por un incidente cibernético es muy amplio, siendo necesario subrayar el carácter generalizado de los riesgos asociados[2].

Las amenazas van más allá de la pérdida/corrupción de datos e incluyen pérdidas ocasionadas por daños materiales, reputación e interrupción del negocio.

Las preocupaciones sobre los costes de un ciberataque o una violación de seguridad no solo se limitan a hacer frente a la pérdida, el robo o la corrupción de datos, sino que cada vez más incluyen daños potenciales a las propiedades y la reputación de una empresa, y también los costes asociados a la interrupción del negocio (LC) o a la alteración grave de infraestructuras críticas. Las pérdidas pueden surgir como consecuencia de un ataque malicioso desde dentro o desde fuera de una organización o pueden estar vinculadas al fallo fortuito de una máquina o a un error humano. La Tabla 1 muestra algunos ejemplos de los tipos de pérdidas que pueden producirse a raíz de peligros cibernéticos.

Tabla 1 :
Tipo de daños relacionados con la cibernética

Tipo de incidente	Ejemplos
Problema/error del sistema	Error del propio sistema o sistema afectado por *malware*, error de comunicación de la red, alteración accidental de sistema de terceros, alteración de infraestructura digital externa.
Confidencialidad de datos	Exposición de datos propios; robo de datos de terceros.
Disponibilidad/ integridad de datos	Borrado, cifrado o corrupción de datos propios o de terceros.
Actividad maliciosa	Mal uso del sistema, comunicación maliciosa, robo/fraude cibernético.

Nota: *malware* es una abreviatura de «*software* malicioso», un tipo de programa creado para infectar un ordenador y causarle daños.

Fuente: anexo de *CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk*, CRO Forum, junio de 2016.

Los costes económicos generales de una violación cibernética pueden ser significativos.

Un estudio realizado en 2016 estimó que el coste promedio de una violación de datos se situaba en torno a 200 000 USD por empresa[3]. Sin embargo, las pérdidas resultantes de algunos incidentes pueden ser muchas veces superiores a esa cifra, provocando la subida de los costes promedios totales (véase la Tabla 2). Otros estudios han tratado de cuantificar el impacto económico general de los incidentes cibernéticos incluyendo costes LC, daño a la reputación y pérdida de futuros

[1] *Informe de Riesgos Globales 2016*, Foro Económico Mundial, 2016.
[2] Las pérdidas de primeras partes están relacionadas con gastos como resultado directo del incidente (p. ej., coste de investigación forense para determinar la causa, notificación a consumidores afectados, campañas de relaciones públicas). Las pérdidas de terceras partes están relacionadas con costes de litigios privados o multas/honorarios de organismos gubernamentales.
[3] S. Romanosky, «Examining the costs and causes of cyber incidents», *Journal of Cybersecurity*, agosto de 2016.

clientes, costes de daños físicos, etc.,[4,5]. Por ejemplo, Lloyd's of London estima que los ataques cibernéticos cuestan al conjunto de las empresas al menos 400 000 millones de USD al año, incluyendo el propio daño y la subsiguiente alteración del curso normal del negocio[6]. Un estudio realizado por McAfee muestra estimaciones de pérdidas agregadas similares[7]. Además, cuando se trata de incidentes cibernéticos hay costes de oportunidad de tiempo y recursos, y también pérdida de beneficios por el desaliento de la inversión. Las empresas deberían ser extremadamente precavidas antes de asignar más recursos para crear sus capacidades digitales y prestar mucha atención a los posibles nuevos riesgos cibernéticos que conlleve el hacerlo.

Tabla 2:
Estimaciones de los costes económicos, por incidente cibernético seleccionado

Tipo de evento	N.º de eventos	Promedio (millones de USD)	Mediana (millones de USD)	Máx. (millones de USD)
Violación de datos(1)	602	5,87	0,17	572
Sistemas afectados(2)	36	9,17	0,33	100
Violación de privacidad(3)	234	10,14	1,34	750
Acceso ilícito(4)	49	19,99	0,15	710
Total	**921**	**7,84**	**0,25**	**750**

Notas:
(1) Revelación involuntaria de información personal de identificación (IPI) derivada de pérdida o robo (p. ej., robo de ordenadores que contienen información personal de empleados o clientes, por un *hacker* o empleado malicioso).
(2) Compromiso o disrupción de sistemas TI corporativos o propiedad intelectual (p. ej., ataque de denegación de servicio, robo, infiltración maliciosa y posterior ciberextorsión).
(3) Recopilación, uso y/o intercambio no autorizados de IPI. A diferencia de (1) y (2), que hacen referencia a incidentes «sufridos por» una empresa, esta categoría se refiere a eventos «causados por» una empresa (p. ej., una empresa que recopila o vende IPI de forma inadecuada).
(4) Delitos informáticos o electrónicos directamente contra otros individuos o empresas incluyendo ataques de suplantación de identidad, robo de identidad o ataques de *skimming*.

Los datos de la Tabla 2 comprenden un periodo de 10 años entre 2005 y 2014 de una muestra de incidentes donde los costos estimados están disponibles públicamente.

Fuente: S. Romanosky, «Examining the costs and causes of cyber incidents», *Journal of Cybersecurity,* agosto de 2016.

[4] Un estudio realizado en 2016 por Ponemon Institute reveló que la pérdida de información es la consecuencia más costosa de un ataque cibernético (39 % del coste), seguida por la interrupción del negocio (36 %), que incluye la disminución de la productividad de los empleados y fallos en el proceso empresarial después de un ataque. Le siguen la pérdida de ingresos y los daños al equipo con un 20 % y un 4 %, respectivamente. *2016 Cost of Cyber Crime Study & the Risk of Business Innovation,* Ponemon Institute, octubre de 2016.

[5] La empresa de telecomunicaciones de Reino Unido TalkTalk perdió 101 000 clientes, no alcanzó su objetivo de adquisición de clientes a corto plazo e incurrió en costes de 60 millones de GBP después de un ataque cibernético en octubre de 2015. S. Farrell, «TalkTalk counts costs of cyber-attack», *The Guardian,* 2 de febrero de 2016, https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave

[6] S. Gandel, «Lloyd's CEO: Cyber attacks cost companies $400 billion every year», *Fortune,* 23 de enero de 2015, http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

[7] *Net Losses: Estimating the Global Cost of Cybercrime,* McAfee, Centro de Estudios Estratégicos e Internacionales, junio de 2014. El estudio de McAfee asumió el coste del delito cibernético como una proporción constante de la renta nacional, ajustada a niveles de desarrollo. Utilizó estimaciones nacionales disponibles para extrapolar un rango de estimaciones de costes del delito cibernético de 375 000 a 575 000 millones de USD. Esto incluye costes directos e indirectos, pérdida de propiedad intelectual, robo de activos financieros e información comercial sensible, costes de oportunidad, costes adicionales para proteger redes, y el coste de recuperación de ataques cibernéticos, incluyendo daños a la reputación.

La ciberseguridad se está convirtiendo en una cuestión seria para las empresas…

El riesgo cibernético ha tomado relevancia en la agenda corporativa a medida que se han hecho más visibles las consecuencias de una violación de seguridad. Una encuesta reciente realizada por Swiss Re-IBM reveló que un 40 % de empresas se vieron afectadas por un incidente cibernético en los últimos tres años, y que un 60 % de todas las empresas creen que el riesgo se va a incrementar en los próximos años[8]. Esto se cumple en todas las regiones e industrias, y no solo en aquellas áreas o sectores donde los ataques han sido recientemente más notorios (p. ej., sector minorista y sanitario).

… y no solo para las más grandes.

Sea cual sea su tamaño, las empresas son cada vez más conscientes del impacto potencial de ciberataques y violaciones de seguridad sobre sus operaciones[9]. Según un informe de septiembre de 2015, seis de cada 10 pequeñas empresas de Reino Unido encuestadas previamente sufrieron una violación, y más de la mitad de estas ocurrieron en el año anterior (63 %)[10]. Los términos y condiciones de los contratos que firman los proveedores pequeños y medianos con socios comerciales más grandes a veces les hacen responsables de pérdidas ilimitadas en caso de evento cibernético[11]. Si se produce una violación seria de ciberseguridad, la recuperación de las pequeñas empresas puede resultar difícil, y muchas salen del mercado en los seis meses siguientes a un incidente[12].

Un riesgo que se transforma rápidamente

Los riesgos cibernéticos evolucionarán inevitablemente a medida que aparezcan nuevos factores de amenaza.

Los riesgos cibernéticos están en continua evolución. Tres características principales subrayan la naturaleza dinámica del riesgo cibernético: la creciente velocidad y alcance de la transformación digital, las fuentes cada vez más amplias de vulnerabilidad como consecuencia de la hiperconectividad y la evolución de los actores de las amenazas.

El acelerado ritmo de la transformación digital es un desafío para la seguridad TI de las empresas.

Vertiginoso ritmo y alcance de la transformación digital

La tecnología digital está calando cada vez más en los procesos internos de las empresas y en su interacción con los clientes, y en muchos casos está creando nuevos modelos de negocio. Los protocolos de seguridad tradicionales para proteger sistemas heredados a menudo están mal preparados para abordar el brusco cambio creado por nuevas aplicaciones digitales. Por otro lado, puede que los nuevos servicios sean dirigidos por unidades de negocio diferentes de la empresa sin implicación directa de sus equipos de gestión de riesgos, lo que dificulta que los controles internos se mantengan al día[13]. Además, gana terreno la cultura «trae tu propio dispositivo» (BYOD, por sus siglas en inglés) ya que las empresas permiten a empleados, socios comerciales y otros usuarios utilizar dispositivos personales para ejecutar aplicaciones de empresa y acceder a datos. Gartner predice que en 2017, el 90 % de las organizaciones apoyará alguna forma de BYOD, dificultando aún más el reto de mantener la seguridad TI[14].

8 *Cyber: in search of resilience in an interconnected world,* Swiss Re/IBM, octubre de 2016.
9 *Key risks for small and medium enterprises (SMEs) in 2016 Global survey report,* Zurich Financial Services, septiembre de 2016.
10 *Small business Reputation & the cyber risk,* KPMG/Be Cyberstreetwise.com, septiembre de 2015.
11 *Cyber/Privacy Insurance Market Survey – 2016,* The Betterley Report, junio de 2016.
12 «Most Small Businesses Don't Recover From Cybercrime», *wsj.com,* 22 de marzo de 2013, http://www.wsj.com/articles/SB10001424127887324557804578376291878413744
13 *The Four Steps to Manage Risk and Security in Bimodal IT,* Gartner, 7 de marzo de 2016.
14 *Gartner Predicts,* Gartner, enero de 2016.

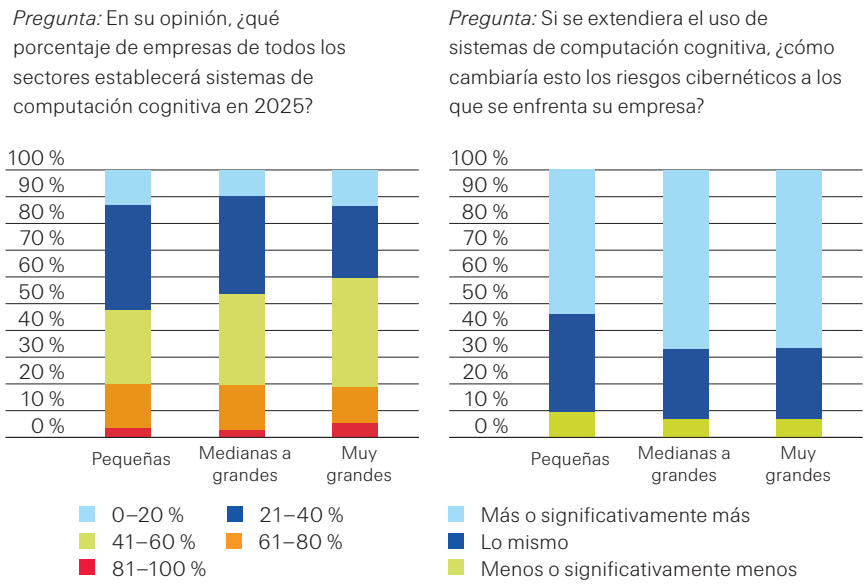
Es posible que las empresas estén subestimando la complejidad que crea la tecnología digital en sus modelos de negocio.

La filosofía del negocio digital también es muy diferente a la del negocio tradicional y crea complicaciones de seguridad adicionales. En el mundo digital, las empresas mueven rápidamente un producto desde el diseño, pasando por la distribución, hasta los clientes, y lo mejoran continuamente tras recibir la respuesta de los clientes. Los directores ejecutivos a menudo dirigen sus organizaciones para que avancen más rápidamente en cuestiones de transformación digital e innovación, y esto puede llevar a la infravaloración de riesgos operativos y de seguridad implícitos[15]. Una encuesta reciente indicó que el 95 % de las empresas reconocía que el panorama de riesgo está cambiando debido a la tecnología digital. Aun así, muchas empresas clasifican sus sistemas como simples cuando en realidad son complejos[16] .

Se pueden usar tecnologías regidas por algoritmos para lanzar nuevos tipos de ataques a gran escala.

Utilizando sofisticados algoritmos de inteligencia artificial (IA), los ordenadores pueden buscar automáticamente entre millones de líneas de código de *software* para encontrar debilidades que explotar. Los investigadores ya han demostrado cómo pueden robarse y manipularse mediante ingeniería inversa modelos de aprendizaje computacional para atacar sistemas[17]. De manera más general, en una encuesta reciente, el 62 % de los encuestados dijo que a medida que se extienda la IA aumentará el riesgo cibernético y de seguridad de la información[18], reflejando resultados similares a los hallazgos de la reciente encuesta de Swiss Re-IBM (véase la Figura 1).

Figura 1 :
Encuesta de opinión de las empresas sobre la adopción y los riesgos de la computación cognitiva, por tamaño de empresa



Pequeñas = hasta 500 empleados
Medianas a grandes = de 500 a 10 000 empleados
Muy grandes = más de 10 000 empleados

Fuente: *Cyber: in search of resilience in an interconnected world,* Swiss Re/IBM, 2016.

[15] *Kick-Start Bimodal IT by Launching Mode 2,* Gartner, 29 de abril de 2016.
[16] *The Risk of Complexity in a Digital Economy,* MIT e Infosys, junio de 2016.
[17] F. Tramèr, F. Zhang, A. Juels y T. Ristenpart, *Stealing Machine Learning Models via Prediction APIs,* Asociación USENIX, agosto de 2016.
[18] *State of Cybersecurity: Implications for 2016,* encuesta realizada por ISACA y RSA, 2016.

Ampliación de las fuentes de vulnerabilidad

El IoT incrementa el rango de vulnerabilidades...

La rápida propagación de los dispositivos con conexión a Internet, el denominado Internet de las Cosas (IoT, por sus siglas en inglés), está posibilitando nuevas formas de comunicación, intercambio de información y dirección/orientación del negocio (p. ej., operaciones remotas). Pero también incrementa la gama de vulnerabilidades. Con el tiempo, el IoT creará todo un mundo de dispositivos interconectados digitalmente, desde electrodomésticos para el día a día como pequeñas tostadoras hasta vehículos aéreos no tripulados (VANT) o drones y vehículos totalmente autónomos.

... ya que los dispositivos conectados pueden tener normas de seguridad débiles.

Algunos de estos dispositivos podrían tener poca seguridad, o incluso ninguna, y pueden estar abiertos a *hackers* maliciosos, especialmente si están expuestos a vulnerabilidades para las que no se dispone de ningún parche o solución. Por ejemplo, pueden utilizarse redes conectadas en ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés), que emplean dispositivos IoT poco protegidos para echar abajo otros servicios conectados a la web[19]. Es especialmente preocupante la debilidad de la seguridad de red porque una de las aplicaciones dominantes del IoT se dará en procesos industriales e infraestructura gubernamental, y no solamente en dispositivos de consumo[20]. La constante interacción entre dispositivos remotos y su entorno proporciona muchas superficies de ataque posibles para el aspirante a *hacker*.

El creciente uso de la nube reduce la transparencia y genera nuevas amenazas.

La adopción generalizada de la computación en nube complica aún más el problema de la ciberseguridad[21]. En un entorno descentralizado la falta de transparencia supone un desafío, y las empresas tratan de dilucidar qué servicios en nube están en uso, quién es responsable y cómo un proveedor protege datos de su propia plantilla TI[22]. Los sistemas con alojamiento en nube también son vulnerables a nuevos tipos de *malware* que pueden buscar entornos virtuales para infectarlos[23]. Y las aplicaciones de intercambio de archivos son susceptibles de ser hackeadas incluso con fuertes normas de seguridad porque los usuarios pueden introducir inadvertidamente sus propias vulnerabilidades, como contraseñas compartidas.

[19] H. Kuchler, «Connected devices create millions of cyber security weak spots», *Financial Times*, 23 de octubre de 2016, https://www.ft.com/content/a63b2de8-992c-11e6-8f9b-70e3cabccfae

[20] Las empresas invertirán una suma considerable en *hardware* IoT en 2017 (964 000 millones de USD), y los consumidores (725 000 millones de USD). Véase *Gartner Says 8.4 Billion Connected «Things» Will Be in Use in 2017, Up 31 Percent From 2016*, Gartner, 7 de febrero de 2017, http://www.gartner.com/newsroom/id/3598917

[21] Gartner predice que en 2020 las pólizas corporativas «sin nube» quedarán obsoletas. Véase *Gartner Says By 2020, a Corporate «No-Cloud» Policy Will Be as Rare as a «No-Internet» Policy Is Today*, Gartner, 22 de junio de 2016, http://www.gartner.com/newsroom/id/3354117

[22] El término «TI en la sombra» a veces se utiliza para describir una situación donde las unidades de negocio procuran nuevo *software*/arquitectura sin control de la TI interna. Véase C. Pettey, *Don't Let Shadow IT Put Your Business at Risk*, Gartner, 3 de mayo de 2016, http://www.gartner.com/smarterwithgartner/dont-let-shadow-it-put-your-business-at-risk/

[23] D. Shackleford, «Malware analysis: How some strains 'adapt' to virtual machines», TechTarget, junio de 2015, http://searchsecurity.techtarget.com/feature/Malware-analysis-How-some-strains-adapt-to-virtual-machines

Evolución del perfil de los *hackers*

La llegada de herramientas de hackeo de bajo coste y la colaboración están ampliando el grupo de *hackers*.

El perfil de los *hackers* también está cambiando (véase la Figura 2). Las herramientas de hackeo de precio reducido disminuyen el coste de los ataques y eliminan las barreras de entrada para una clase más amplia de *hackers*, no solo aquellos con capacidades TI altamente especializadas[24]. Los ataques DDoS constituyen un buen ejemplo: son relativamente baratos de llevar a cabo, aunque suele ser costoso prevenirlos y resolverlos. Por ejemplo, en 2016 el *malware* Mirai utilizó una multitud de dispositivos domésticos conectados a Internet para lanzar ataques DDoS[25]. Además, la colaboración entre *hackers* está aumentando y los *malware* se comparten de forma anónima en foros basados en web.

Figura 2:
Expansión de los tipos de atacantes, recursos y motivaciones

	Aficionados	Hacktivistas	Crimen organizado	Patrocinados por estados
Recursos	Recursos técnicos limitados	Amplias redes Fuerte compromiso emocional	Recursos técnicos significativos	Solo limitados por el presupuesto gubernamental
Motivaciones	Fama y notoriedad	Se pronuncian, causan situaciones embarazosas	Beneficio económico	Fomentar la innovación Mayor poder en las negociaciones
Sofisticación	No profesional Utiliza vulnerabilidades conocidas	A veces poco sofisticado, constante y selectivo	Mafias profesionales consolidadas	Altamente sofisticado, paciente, creativo, persistente

Fuente: Swiss Re Economic Research and Consulting.

El beneficio económico derivado de los delitos cibernéticos es cada vez mayor.

Antes motivados en gran parte por la fama y la atención, los *hackers* valoran cada vez en mayor medida el beneficio económico derivado de ataques cibernéticos exitosos. Mafias consolidadas con acceso a importantes recursos técnicos y capacidades encuentran en el delito cibernético una actividad lucrativa. *Hackers* patrocinados por el estado participan en la perturbación cibernética y el espionaje corporativo para acceder a información secreta u obtener una ventaja competitiva desleal. Por ejemplo, presentando ofertas a licitaciones internacionales o desarrollando innovación «de salto» reduciendo los costes de I+D a través del robo de propiedad intelectual.

[24] Al parecer, los *hackers* técnicamente competentes invierten una media de 1367 USD en herramientas especializadas para ejecutar ataques. Véase *Flipping the Economics of Attacks*, Ponemon Institute, enero de 2016.

[25] Estos nuevos tipos de *malware* a menudo se construyen como plataformas de *software* de actualización a las que los *hackers* pueden añadir más funcionalidad con el tiempo. Véase L.H. Newman, «The Web-Shaking Mirai Botnet Is Splintering — But Also Evolving», *Wired*, 15 de noviembre de 2016, https://www.wired.com/2016/11/web-shaking-mirai-botnet-splintering-also-evolving/

Los *hackers* están utilizando técnicas muy sofisticadas para obtener información confidencial.

Los *hackers* también se están volviendo más sofisticados y toman como objetivo a los empleados de una empresa utilizando métodos innovadores de manipulación. Los empleados de las empresas a menudo contribuyen decisivamente a la hora de propagar ataques, ya sea de forma maliciosa o accidental. En 2015, el *phising* o suplantación de identidad y las técnicas de ingeniería social se situaron entre los métodos de ataque más exitosos para explotar redes empresariales[26]. Con el tiempo, los usuarios pueden llegar a ser conscientes de notorios fraudes de suplantación de identidad y aprender a reconocer correos electrónicos dudosos, pero resulta difícil mantenerse al día de nuevas formas de estafar a la gente asaltando procedimientos de seguridad normales[27]. Las plataformas públicas de uso generalizado también pueden verse afectadas con acciones innovadoras. Por ejemplo, en 2016 unos *hackers* demostraron cómo puede utilizarse la IA para crear tuits personalizados y persuadir al objetivo para que haga clic en enlaces maliciosos[28].

El *ransomware* también es una amenaza que está creciendo rápidamente.

La ciberextorsión también se está convirtiendo en una técnica popular utilizada por delincuentes, junto con otros métodos más convencionales como robar y vender información privada en el mercado negro[29]. *Ransomware* es un tipo de *malware* diseñado para bloquear el acceso a un sistema informático o datos hasta que se paga una suma de dinero, a menudo en *bitcoins*. Los ecosistemas industriales IoT son especialmente vulnerables porque las amenazas de los *hackers* de interrumpir las operaciones podrían provocar el pago del rescate si la pérdida de productividad es sustancial y/o si resulta fundamental mantener un funcionamiento continuado[30]. Según el FBI, en 2015 se produjeron en EE. UU. 2400 incidentes de *ransomware* (1800 en 2014), que ocasionaron unas pérdidas estimadas de 24 millones de USD[31]. En otras partes, datos de AIG Europe revelan que el *ransomware* y la extorsión representan el mayor número de reclamaciones en las pólizas de ciberseguro en Europa, por encima de los incidentes de violación de datos[32]. Aunque las pérdidas individuales por tales ataques continúan siendo relativamente pequeñas, el desarrollo del modelo de negocio «*ransomware* como servicio» mediante el cual los creadores del *malware* venden su código a múltiples usuarios y reciben una parte de los beneficios obtenidos, aumenta significativamente la escala y el alcance de cualquier ataque[33].

[26] *Phishing* o suplantación de identidad es el intento de obtener información sensible haciéndose pasar por una entidad de confianza en una comunicación electrónica. Ingeniería social es la manipulación psicológica de personas al divulgar información confidencial. Véase encuesta de ISACA y RSA Conference, *op. cit*.

[27] Un ejemplo de ingeniería social sofisticada es un caso recientemente publicado de transferencia de fondos engañosa donde los empleados fueron manipulados sin saberlo para transferir fondos de la empresa a cuentas fraudulentas tras recibir correos electrónicos de delincuentes haciéndose pasar por un ejecutivo autorizado. Véase «Central banks seek global standards in wake of Bangladesh heist», *Reuters*, 15 de septiembre de 2016, http://www.reuters.com/article/us-cyber-heist-basel-taskforce-idUSKCN11L269

[28] T. Simonite, «This AI Will Craft Tweets That You'll Never Know Are Spam», *MIT Technology Review,* 4 de agosto de 2016, https://www.technologyreview.com/s/602109/this-ai-will-craft-tweets-that-youll-never-know-are-spam/

[29] N. Elliott, «Ransomware Is Booming and Companies Are Paying Up», *WSJ Risk & Compliance Journal*, 27 de octubre de 2016, http://blogs.wsj.com/riskandcompliance/2016/10/27/ransomware-is-booming-and-companies-are-paying-up/

[30] B. Dickson, «What makes IoT ransomware a different and more dangerous threat?», *Tech Crunch,* 2 de octubre de 2016, https://techcrunch.com/2016/10/02/what-makes-iot-ransomware-a-different-and-more-dangerous-threat/

[31] V.D. Anderson, «Ransomware: Latest Cyber Extortion Tool», *FBI Cleveland,* 26 de abril de 2016, https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/ransomware-latest-cyber-extortion-tool

[32] P. Lucas, «Top cyber claim causes revealed by AIG» , *Insurance Business*, 29 de noviembre de 2016, http://www.insurancebusinessmag.com/uk/news/breaking-news/top-cyber-claim-causes-revealed-by-aig-41109.aspx

[33] Véase, por ejemplo, «Ransomware-as-a-Service: Ransomware Operators Find Ways to Bring in Business», *Trend Micro,* 2 de septiembre de 2016, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-ransomware-operators-find-ways-to-bring-in-business

Gestión del riesgo cibernético en la práctica

Inacción

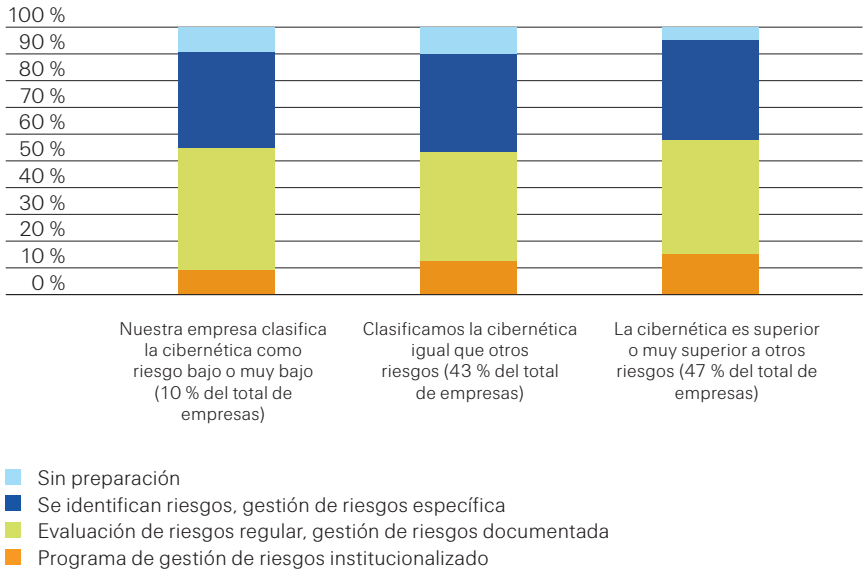
A pesar de la creciente concienciación, las empresas todavía no han institucionalizado la gestión del riesgo cibernético.

Aunque las empresas cada vez son más conscientes de los riesgos cibernéticos parece que esto no se ha traducido en planes de acción concretos y exhaustivos. En consonancia con otros estudios recientes, la encuesta de Swiss Re-IBM de 2016 mostró que un número relativamente bajo de empresas había institucionalizado la gestión del riesgo cibernético, incluso entre aquellas que veían la cibernética como una importante amenaza (véase la Figura 3). Son relativamente pocas las empresas que disponen de una estrategia formal de gestión del riesgo cibernético que perfile su apetito de riesgo global y de procedimientos detallados para controlar vulnerabilidades[34].

Figura 3:
Encuesta de opinión de las empresas sobre su preparación ante riesgos

Pregunta para las respuestas del eje horizontal: ¿Dónde situaría actualmente sus riesgos de interconexión digital como amenaza respecto a cualquier otro tipo de riesgo que afecta a su empresa? (menor/igual/mayor);

Pregunta para las respuestas del eje vertical: ¿Hasta qué punto está preparado para riesgos de incidentes de interconexión digital? (agrupación de empresas en % de acuerdo con la clasificación del riesgo cibernético respecto a otros: menor/igual/mayor).



Fuente: *Cyber: in search of resilience in an interconnected world,* Swiss Re/IBM, 2016.

Las empresas podrían estar subestimando la posibilidad de ser objetivo de repetidos ataques cibernéticos.

Una razón para la inacción podría ser el exceso de confianza: las empresas podrían subestimar la probabilidad de verse atacadas repetidamente. Una encuesta reciente realizada por Lloyd's of London reveló que del 92 % de las empresas que sufrieron una violación de ciberseguridad en los últimos cinco años, solo un 42 % estaban preocupadas porque se produjera otro ataque en el futuro[35]. En líneas generales, según la empresa de analítica de seguridad Advisen, el escaso progreso de los esfuerzos de mitigación de riesgo está causado por una combinación de factores entre los que se incluyen recursos, compromiso y conocimiento limitados[36]. Esto, a su vez, podría estar vinculado a la ciberseguridad, que en muchas organizaciones se sigue considerando más una cuestión técnica que una cuestión estratégica más

[34] Para más información sobre la gestión institucionalizada del riesgo cibernético, véase *Enhanced Cyber Risk Management Standards* publicado por el Departamento del Tesoro, el Sistema de Reserva Federal y la Corporación Federal de Seguro de Depósitos, octubre de 2016, https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf

[35] *Facing the cyber risk challenge,* Lloyd's of London, septiembre de 2016.

[36] J. Bradford, «Public-private partnership is key to combating cybercrime», *Advisen,* http://www.advisen.com/tools/fpnproc/fpns/articles_new_23/P/263440646.html?rid=263440646&list_id=23

amplia[37]. Aunque actualmente suele formar parte de la comunicación regular al personal directivo, el control de la ciberseguridad normalmente todavía sigue estando dirigido por la Tecnología de la Información (TI).

En algunos mercados emergentes las empresas podrían estar especialmente mal preparadas.

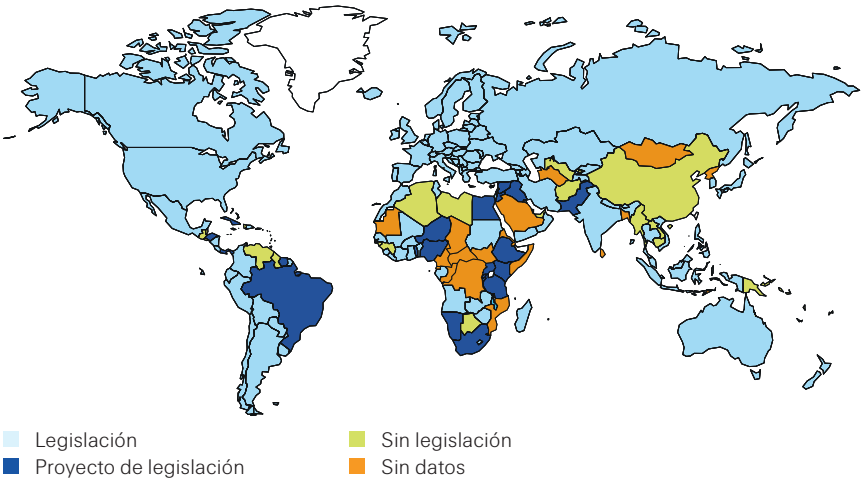
Existen disparidades regionales, con mercados emergentes aparentemente menos preparados. Un informe sobre la región de Asia-Pacífico reveló que las empresas no eran capaces de detectar *hackers* en sus entornos durante una media de 520 días, que es muy superior a la media global de 146 días[38]. Otro problema es que en estos mercados las empresas utilizan *software* personalizado que no siempre está sometido al tipo de control que las grandes empresas de *software* aplican a sus productos. Al mismo tiempo, es difícil evaluar la verdadera extensión de la escasa preparación en muchos mercados emergentes, ya que a menudo no se exige a las empresas ni a los gobiernos que informen de los ataques[39].

Aumento de la supervisión normativa en cuestiones cibernéticas

Los reguladores están exigiendo globalmente a instituciones y empresas más esfuerzos para proteger los datos del consumidor.

Reguladores y legisladores están impulsando el cambio para garantizar que las violaciones de ciberseguridad no son una fuente de inestabilidad sistémica ni van en detrimento de consumidores que confían en organizaciones para proteger su información privada. En todo el mundo, 107 países (de los cuales 66 son economías en desarrollo) han promulgado leyes que exigen la protección de datos y privacidad (véase la Figura 4). En Asia y África, menos del 40 % de países cuenta con una legislación, aunque por lo general se están elaborando propuestas legislativas en estas regiones.

Figura 4:
Leyes de protección de datos y privacidad en el mundo



Fuente: UNCTAD Global Cyberlaw Tracker. Información extraída el 1 de diciembre de 2016.

[37] Gartner revisó más de 400 presentaciones a la dirección sobre riesgo cibernético y encontró que la mayoría no repercutían en el negocio porque se centraban en medidas técnicas y métricas operativas. Véase J. Wheatman, P.E. Proctor, R. McMillan, *The Comprehensive Guide to Presenting Risk and Information Security to Your Board of Directors*, Gartner, 3 de marzo de 2016.

[38] B. Boland, «M-Trends Asia Pacific», *FireEye*, 24 de agosto de 2016, https://www.fireeye.com/blog/threat-research/2016/08/m-trends_asia_pacifi.html

[39] L. Lewis, D. Weinland, M. Peel, «Asia hacking: Cashing in on cyber crime», *Financial Times*, 19 de septiembre de 2016, https://www.ft.com/content/38e49534-57bb-11e6-9f70-badea1b336d4

Nuevos reglamentos de protección de datos imponen estrictos requisitos de gran alcance, aunque con inciertas consecuencias.

Con arreglo al nuevo Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) que entrará en vigor en 2018, las empresas europeas se enfrentarán a importantes multas si no protegen adecuadamente los datos[40]. Las empresas también deberán ser capaces de eliminar los datos de un individuo de sus sistemas si esa información ya no es relevante o necesaria, lo que puede ser difícil si los datos están fragmentados entre organizaciones y/o hay visibilidad limitada sobre la información mantenida externamente. Sin embargo, no parece que las empresas hayan asimilado todavía las graves consecuencias financieras y jurídicas del no cumplimiento. Una encuesta reciente de Lloyd's of London reveló que el conocimiento de las implicaciones del RGPD de la UE es bajo: el 57 % dijo que sabía «poco» o «nada» del nuevo reglamento[41]. Otra encuesta mostró que de los encuestados de Europa, Oriente Medio y África (EMEA, por sus siglas en inglés), una quinta parte no había comenzado a prepararse para el RGPD, y solo una cuarta parte estaba completamente preparada para su introducción. Asimismo, en Australia apenas un tercio de los responsables de TI encuestados se sentía totalmente preparado para gestionar notificaciones obligatorias de violaciones como parte de enmiendas a la Ley de Protección de la Intimidad (Privacy Act) de Australia, que entrará en vigor en 2017[42].

La evolución de las interpretaciones jurídicas también complica los esfuerzos de las empresas para estimar los costes de violaciones cibernéticas.

Los cambios en la jurisprudencia cibernética también podrían acarrear litigios y aumentar los costes de liquidación, aunque los fragmentados y todavía incipientes precedentes jurídicos hacen difícil calibrar el impacto futuro. Por ejemplo, los tribunales de EE. UU. permiten llevar adelante demandas judiciales en algunos casos en que la mera posibilidad de robo de identidad tras una violación de seguridad cuenta como un daño que puede merecer una indemnización. Anteriormente, los tribunales podían desestimar demandas de violación de datos si los demandantes no eran capaces de demostrar daños sufridos[43]. Aunque estos casos normalmente se han resuelto fuera de los tribunales, en el futuro solo será necesario demostrar que los datos fueron divulgados para que las empresas se enfrenten a una sanción legal.

Y los requisitos de cumplimiento tienen implicaciones para todas las partes de una cadena de suministro.

Las presiones regulatorias afectarán al modo en que todas las partes de la cadena de suministro de una empresa piensen sobre el riesgo cibernético, ya que cada vez son mayores los requisitos de cumplimiento y la responsabilidad por daños para todos. Por ejemplo, el Pentágono en EE. UU. debe ser notificado si alguno de sus contratistas o subcontratistas sufre un ciberataque. Pero, en términos más amplios, no todas las empresas o instituciones son totalmente conscientes de los riesgos presentes en su cadena de suministro. Por ejemplo, en Europa, el 80 % de las empresas no evalúa el perfil de riesgo cibernético de sus proveedores[44] .

[40] Las multas dependerán del incidente y tipo de violaciones. Pero, en general, las infracciones de disposiciones clave del RGPD están sujetas a multas administrativas de hasta 20 millones de EUR o hasta el 4 % del volumen de negocio global, lo que sea mayor. Las infracciones menores están sujetas a multas administrativas de hasta 10 millones de EUR o hasta el 2 % del volumen de negocio global, lo que sea mayor.

[41] Lloyd's of London, *op. cit.*

[42] *Global Advanced Threat Landscape Survey 2016*, CyberArk, 2016.

[43] N. Hong, «For Consumers, Injury is Hard to Prove in Data-Breach Cases», *WSJ*, 26 de junio de 2016, http://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988

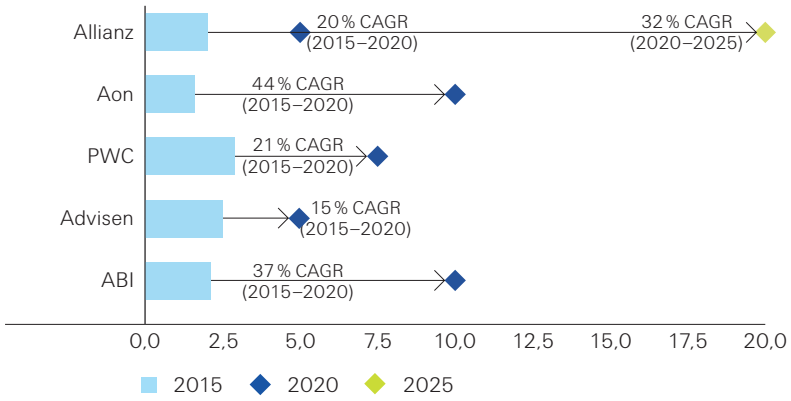
[44] *Continental European Cyber Risk Survey: 2016 Report*, Marsh, octubre de 2016.

Crecimiento del mercado de seguros cibernéticos

La demanda de seguro cibernético está creciendo y contribuye al rápido aumento de las primas agregadas.

En un contexto de aumento de los riesgos cibernéticos, ampliación de fuentes de vulnerabilidad y mayor presión regulatoria, la demanda de seguro de protección contra riesgos cibernéticos está creciendo. Según Zurich/Advisen, la proporción de empresas que afirma comprar seguro de responsabilidad cibernética prácticamente se ha duplicado desde 2011[45]. Y una encuesta de Swiss Re-IBM reveló que las empresas cada vez están considerando más comprar cobertura específica para protegerse contra pérdidas relacionadas con la cibernética. El mercado del seguro cibernético independiente está creciendo rápidamente: las estimaciones de diferentes entidades aseguradoras varían (véase la Figura 5), pero sugieren un crecimiento interanual de las primas de seguro cibernético de al menos un 15 % en los próximos 5 a 10 años.

Figura 5:
Estimaciones de primas de seguro cibernético en todo el mundo (2015–2025) en miles de millones de USD, por participantes de mercado seleccionados



Fuente: Allianz, Aon, PWC, Advisen, ABI, Swiss Re Economic Research and Consulting.

Los límites de las pólizas de riesgos cibernéticos normalmente van de 5 a 100 millones de USD.

El seguro cibernético especializado ofrece normalmente protección básica contra violaciones de seguridad de redes y datos y pérdidas asociadas, con límites de capacidad que van de unos 5 millones de USD a 100 millones de USD. La mayoría de pólizas se suscriben en base a los «siniestros presentados y notificados», lo que significa que es necesario notificar los siniestros a la compañía aseguradora durante el periodo de la póliza, o como mucho en un plazo de 30 a 60 días desde el vencimiento de la póliza.

El mercado del ciberseguro está bastante concentrado aunque hay más aseguradoras que quieren entrar.

El mercado del seguro cibernético todavía está relativamente concentrado. Según se informa, en EE. UU. tres aseguradoras (AIG, Chubb y XL Group) tienen alrededor del 45 % del mercado[46]. Sin embargo, es probable que esto cambie debido a que hay muchas aseguradoras que desean ampliar sus capacidades de protección contra riesgos cibernéticos. La mitad de las aseguradoras encuestadas en el sondeo de Swiss Re-IBM que actualmente no ofrecen planes de ciberseguro pretenden hacerlo en los próximo años.

[45] *Information security and Cyber risk management*, Advisen/Zurich, octubre de 2016.
[46] «AIG, Chubb, XL Group Lead in U.S. Cyber Coverage Market Share: Fitch Ratings», *Insurance Journal*, 6 de septiembre de 2016, http://www.insurancejournal.com/magazines/features/2016/09/06/424904.htm

El ciberseguro es un ramo de negocio relativamente nuevo. Estados Unidos es el mayor mercado.

Evolución del ciberseguro

El seguro de riesgos cibernéticos es un negocio relativamente nuevo y está evolucionando rápidamente. Las primeras pólizas especializadas aparecieron en EE. UU. a finales de la década de 1990 y estaban orientadas a cuestiones de responsabilidad de seguridad/privacidad que surgían con el uso cada vez mayor de Internet (véase la Figura 6). EE. UU. sigue siendo el mayor mercado de ciberseguro, representando la mayor parte de los 2000-3000 millones de USD en primas en 2015 en todo el mundo, aunque mucha de la cobertura de EE. UU. está suscrita por aseguradoras internacionales (p. ej., a través del mercado de Londres).

Figura 6:
Hitos en décadas recientes del desarrollo del seguro cibernético independiente

Década de 1990

- El producto independiente aparece en EE. UU. a mediados/finales de la década de 1990. Evoluciona a partir de pólizas de responsabilidad civil profesional (p. ej., E&O, D&O).
- Primeras pólizas suscritas para abordar la exposición a *software* o contenido en línea.
- Estas pólizas de «seguro de Internet»:
  - están limitadas a fallos de seguridad informática;
  - no ofrecen cobertura para costes de primeras partes por violación de datos;
  - no incluyen divulgación accidental o registros no electrónicos.

Década de 2000

- Las pólizas de soportes en línea comienzan a incluir pérdidas por «acceso no autorizado», «seguridad de red» y «virus». Pero hay significativas exclusiones (p. ej., acciones de empleados deshonestos y multas regulatorias) y no ofrecen cobertura para primeras partes.
- A mediados de la década de 2000, se introduce la cobertura para algunas pérdidas de primeras partes (p. ej., interrupción cibernética del negocio, ciberextorsión) y daños por violación accidental de datos.
- Los reglamentos de privacidad de datos de EE. UU. catalizan la innovación de productos, incluyendo protección contra costes incurridos por TI forense, relaciones públicas y notificación al cliente.

Década de 2010

- Crecimiento del número de compañías de seguros con productos independientes, no solo en EE. UU.
- La mayor incidencia de escándalos de hackeo de gran repercusión fomenta la demanda de ciberseguro a nivel mundial (tanto de cobertura específica como de suplementos a pólizas tradicionales de daños/accidentes).
- Las autoridades de la UE llegan a un acuerdo sobre la reforma de protección de datos; la legislación se implementará en 2018.
- Introducción de legislación de protección de datos en otras jurisdicciones que aumenta la conciencia de la amenaza cibernética y la necesidad de protección.
- Las aseguradoras se asocian con expertos informáticos externos para profundizar su conocimiento sobre riesgos cibernéticos.

Fuente: Swiss Re Economic Research & Consulting.

Las pólizas independientes de riesgos cibernéticos difieren entre sí, pero la mayoría combinan protección de pérdidas de diversos datos y violaciones de seguridad en red.

Las diferentes aseguradoras utilizan diferentes terminologías, pero en la actualidad la cobertura cibernética independiente suele ser una combinación de los siguientes componentes:

- *Red, fallo de seguridad informática:* seguro de interrupción de negocios (LC), que cubre la pérdida de ingresos del asegurado, los gastos operativos y a menudo los costes de restauración de datos cuando se interrumpen o suspenden las operaciones del negocio debido a un fallo de seguridad informática en casos de ataque malicioso, incluyendo ataques DDoS.
- *Red, fallo del sistema informático:* seguro de interrupción de negocios, con cobertura similar al *fallo de seguridad* (arriba) pero cuando las operaciones del negocio se interrumpen o suspenden debido a un fallo de los sistemas informáticos (eventos cibernéticos no maliciosos) y a veces también a un percance/error humano.
- *Interrupción de negocios accidental (INA):* cubre la pérdida de ingresos del asegurado y los gastos operativos en caso de que un proveedor digital (p. ej., un proveedor en nube) sufra una interrupción y, en algunos casos, también si la sufre un proveedor de servicios públicos convencionales (p. ej., electricidad).
- *Violaciones de privacidad:* cubre siniestros relacionados con gastos incurridos como respuesta a una violación de datos, incluyendo costes de gestión de crisis (p. ej., costes de TI forense, costes de notificación y, en algunos casos, multas por incumplimiento de regulaciones).
- *Responsabilidad de red:* cubre daños a proveedores externos como resultado de un evento perturbador procedente o que se transmite a través del sistema del asegurado.
- *Errores y omisiones:* cubre siniestros derivados de errores en la ejecución de servicios ofrecidos, incluyendo *software* y consultoría.
- *Responsabilidad multimedia:* cubre siniestros como violación de la propiedad intelectual, violación de derechos de autor/marca comercial y difamación y calumnias.
- *Ciberextorsión:* cubre siniestros relacionados con los costes adicionales incurridos al tratar una infección procedente de *ransomware* y, cuando esté permitido por ley, el rescate si se estima necesario pagarlo.

El ciberseguro, en un principio destinado a cubrir los costes de responsabilidad relativa a la privacidad/seguridad, se ha ampliado para incluir otro tipo de siniestros.

Las ciberpólizas se diseñaron originalmente para cubrir riesgos y daños no físicos a activos intangibles. Estos incluyen el coste de notificar a personas, supervisión de crédito, TI forense, relaciones públicas y gestión de crisis y comunicación. Pero poco a poco la cobertura se ha ampliado. Ahora algunos ciberproductos se han combinado con otros tipos de póliza de seguros, como el seguro de responsabilidad civil por errores y omisiones en servicios tecnológicos.

No obstante, algunos riesgos cibernéticos importantes siguen sin estar asegurados…

Con el tiempo, el ciberseguro ha evolucionado para incluir más riesgos, pero muchas empresas todavía subrayan una falta de disponibilidad de cobertura para algunos riesgos cibernéticos (véase la Figura 7). Según una encuesta de 2016 entre compradores de seguro corporativo, dos de las principales razones para no comprar cobertura cibernética eran la cobertura inadecuada y la escasez de soluciones de seguro relevantes[47]. Por ejemplo, muchas aseguradoras ofrecen cobertura LC en sus pólizas de riesgos cibernéticos, pero algunas empresas dicen que los límites son demasiado bajos para cubrir las potencialmente enormes pérdidas que podría causar un evento cibernético, aunque la situación está mejorando porque los límites se han incrementado progresivamente.

… incluyendo tanto daños físicos como no físicos.

Además de LC, otra área de cobertura con carencias es la de daños físicos. Pocas aseguradoras incluyen en su seguro cibernético independiente protección de daños materiales y lesiones corporales, aunque algunas pérdidas relacionadas podrían estar cubiertas por el seguro de daños y responsabilidad civil tradicional[48]. Las ciberpólizas normalmente tienen exclusiones de guerra e incluso las que cubren ciberterrorismo suelen excluir daños no cubiertos en pólizas de riesgos cibernéticos tradicionales (como pérdida de propiedad y daños a activos físicos)[49]. Por ejemplo, una importante causa de discusión entre aseguradoras y sus asegurados refleja la falta de claridad sobre lo que se consideraría un ciberataque y un acto de ciberterrorismo[50]. De modo similar, el riesgo de reputación raramente está cubierto por el ciberseguro[51]. Las aseguradoras también tienden a ofrecer cobertura mínima para robo de propiedad intelectual (PI) y daños por espionaje industrial. Y cuando se ofrece, algunas empresas consideran que los límites del seguro de PI son demasiado bajos[52].

47 En líneas generales, más de la mitad de participantes en la encuesta anual de 2016 entre miembros de la Association of Insurance and Risk Managers in Industry and Commerce (Airmic) citan una falta de ciberseguro. Véase *The top priority risks are also among the most difficult to insure,* Airmic, 7 de junio de 2016, https://www.airmic.com/news/press/top-priority-risks-are-also-among-most-difficult-insure

48 El producto CyberEdge PC de AIG introdujo cobertura que proporciona protección contra daños materiales y lesiones corporales resultantes de un ciberataque. La cobertura se proporciona sobre una base de exceso y diferencia de condiciones (lo que significa que las otras pólizas de responsabilidad civil del asegurado pagarán primero y CyberEdge intervendrá en lo que estas pólizas no cubran, sujeto por supuesto a sus propias condiciones de cobertura). Véase «AIG Launches Primary Cyber Coverage for Property and Liability Exposures», 19 de julio de 2016, *businesswire.com,* http://www.businesswire.com/news/home/20160719005867/en/AIG-Launches-Primary-Cyber-Coverage-Property-Liability

49 M. Aguirre, A. Bansal, E. Douglas, et. al. *Can Cyber-Insurance Coverage Keep Apace With Cyber-Exposure?* Towers Watson, septiembre de 2015. https://www.towerswatson.com/en/Insights/Newsletters/Global/emphasis/2015/emphasis-2015-3-can-cyber-insurance-coverage-keep-apace-with-cyber-exposure

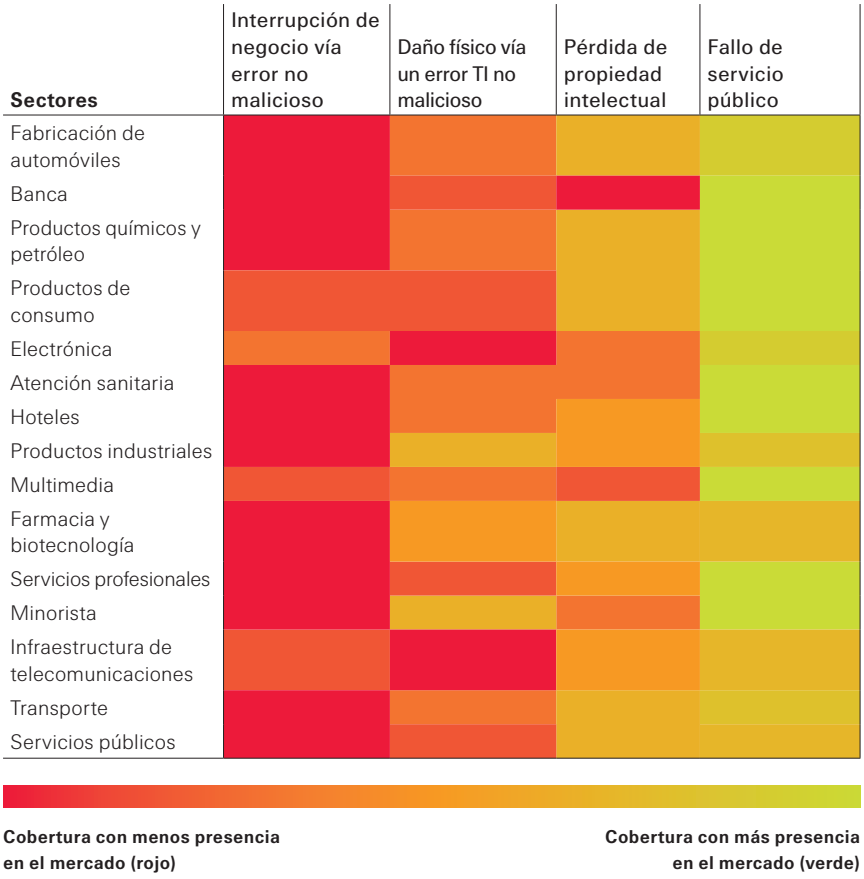
50 *Ibíd.*

51 Los compradores de ciberseguro antes se quejaban de que las pólizas que se ofertaban eran muy limitadas porque no cubrían los daños que podría causar un ataque a la reputación o marca de una empresa. Véase «Lloyd's chief urges UK to share cyber attack data», *Financial Times,* 28 de noviembre de 2016. https://www.ft.com/content/acac3a5e-b255-11e6-a37c-f4a01f1b0fa1

52 *Intellectual Property and Media Liability Insurance Market Survey* – 2016, The Betterley Report, abril de 2016.

Figura 7 :
Encuesta sobre riesgos cibernéticos cuya cobertura de seguro las empresas piensan que no está disponible inmediatamente, por sector

Pregunta: ¿Contra qué riesgos de interconexión digital le gustaría asegurar su empresa para los que actualmente no hay soluciones de seguro disponibles?



Fuente: *Cyber: in search of resilience in an interconnected world,* Swiss Re/IBM, 2016.

El coste y la falta de cobertura estándar pueden disuadir a algunos compradores.

El coste del ciberseguro puede ser otra razón para no comprar cobertura de riesgos cibernéticos. La baja penetración del ciberseguro y la cantidad limitada asociada de datos perdidos se traduce en que muchas aseguradoras adoptan una estructura de precios fijos, por la cual se cobra a las empresas tarifas generalmente similares independientemente de su riesgo subyacente[53]. Además, cuando en una encuesta realizada en 2016 se preguntó a corredores de seguros si los precios del ciberseguro se habían vuelto más coherentes con el tiempo, alrededor de un tercio contestó que los precios todavía eran muy inconexos entre aseguradoras, solo ligeramente menos que en la misma encuesta en años anteriores[54]. En parte, esto podría reflejar las diferentes herramientas de calificación de las aseguradoras y el historial limitado de datos perdidos. La ausencia de lenguaje normalizado en las pólizas de riesgos cibernéticos dificulta a las empresas la compra de la cobertura de seguro deseada comparando entre múltiples aseguradoras, aunque se están desplegando iniciativas del sector para introducir normas comunes[55].

[53] *UK cyber security: the role of insurance in managing and mitigating the risk,* HM Government/Marsh, marzo de 2015.
[54] *2016 Survey of Cyber Insurance Market Trends,* PartnerRe/Advisen, octubre de 2016.
[55] En un análisis de 427 pólizas de seguro de riesgos cibernéticos, incluyendo formularios y suplementos, riskgenius.com reveló que había 78 cláusulas singulares entre las 140 definiciones de Código Malicioso. De las 67 compañías de seguros representadas en el conjunto de datos, 20 utilizaron más de una definición de Código Malicioso. Véase «Evaluating Insurance Policies with Machine Learning», *riskgenius.com,* http://blog.riskgenius.com/insurtechebookform-0

Incluso en las pólizas tradicionales existe mucha incertidumbre sobre el alcance de la cobertura cibernética proporcionada.

Además, persiste la ambigüedad en torno al alcance de la cobertura de seguro existente para siniestros relacionados con la cibernética. La Prudential Regulatory Authority de Reino Unido reveló que la exposición «silenciosa» de las aseguradoras al riesgo cibernético —implícita en pólizas de seguro «a todo riesgo» y otras pólizas de responsabilidad civil— es material y es posible que crezca, especialmente en los ramos de accidentes y especialización[56]. La presión que ejercen los reguladores de seguros sobre las aseguradoras para reconocer y abordar la exposición cibernética silenciosa podría alentar más exclusiones relacionadas con los riesgos cibernéticos en el seguro tradicional de daños y responsabilidad civil.

A pesar del rápido crecimiento de los riesgos cibernéticos, el tamaño del mercado del ciberseguro todavía es pequeño.

En resumen, el mercado del ciberseguro está creciendo fuertemente, pero las primas y los límites de las pólizas son todavía pequeños respecto al valor de los activos tangibles e intangibles que podrían verse afectados por un evento de riesgo cibernético. Según un estudio de Aon/Ponemon, solo en torno al 12 % de los activos de información están cubiertos por seguro, comparado con el 51 % de propiedad, planta y equipo[57]. Para ampliar y profundizar el mercado sería necesaria una estrecha colaboración entre asegurados y aseguradoras. Desde el punto de vista del negocio, la demanda es alta y crece en transferencia de riesgos cibernéticos, pero para las aseguradoras todavía sigue siendo un desafío mejorar la comprensión y la cuantificación del potencial de pérdidas cibernéticas significativas.

[56] «Riesgo silencioso» se refiere a la potencial exposición de las aseguradoras a riesgos cibernéticos dentro de la amplia cobertura que ofrecen que no están considerados explícitamente en las pólizas de ciberseguro. Véase «PRA concerned about 'silent' cyber risk underwriting», *out-law.com,* 17 de noviembre de 2016, http://www.out-law.com/en/articles/2016/november/pra-concerned-about-silent-cyber-risk-underwriting/

[57] *2015 Global Cyber Impact Report,* Aon/Ponemon Institute, abril de 2015.

El desafío de cuantificar el riesgo cibernético

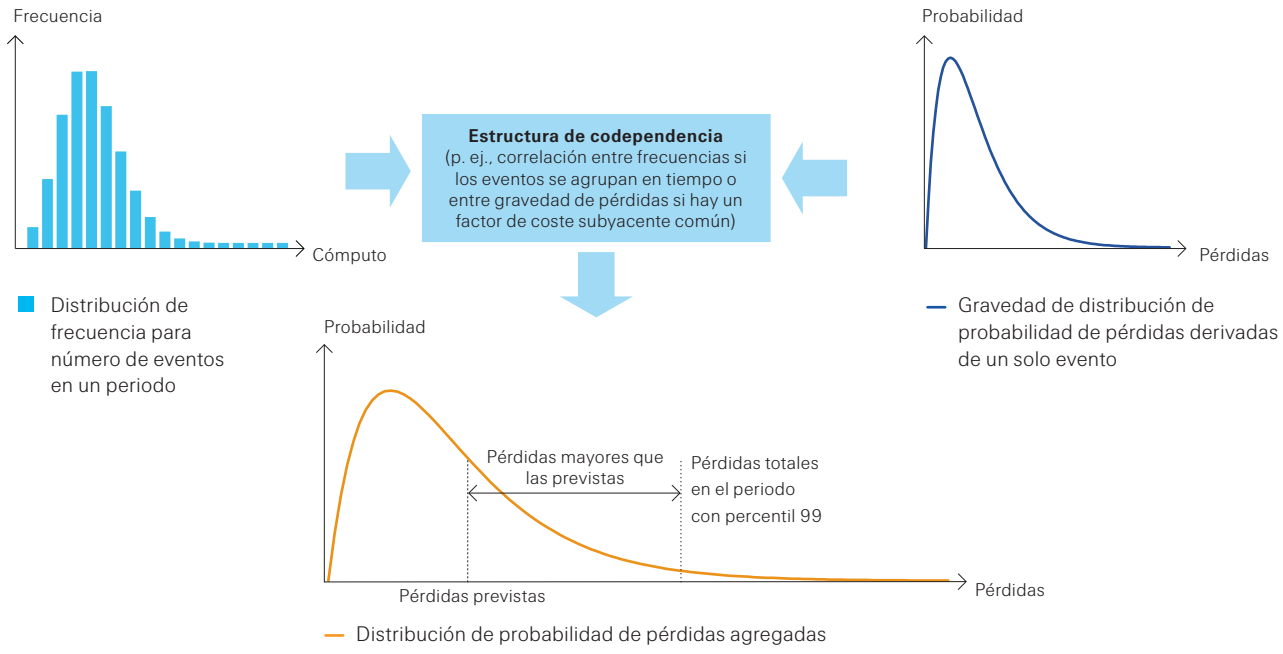
Cualquier análisis de riesgos considerará la probabilidad de que se produzca un evento y su impacto potencial.

En esencia, cualquier cuantificación formal de riesgos debe intentar captar la frecuencia de un evento particular junto con la gravedad de cualquier pérdida futura asociada. Esto significa, en el caso de un evento adverso, con qué frecuencia es probable que se produzca y cómo de adverso será cuando suceda. Debe tenerse en cuenta tanto la frecuencia como la gravedad porque los eventos de pérdidas pueden ser infrecuentes pero muy graves (p. ej., daños catastróficos en activos físicos), o producirse con elevada frecuencia pero ser de poca gravedad (p. ej. accidentes menores).

Normalmente se utilizan datos del pasado sobre frecuencia y gravedad de pérdidas para informar sobre la probable distribución de futuras pérdidas.

El enfoque actuarial tradicional para medir el riesgo consiste en utilizar información tanto del número como de la magnitud de pérdidas pasadas para inferir distribuciones de probabilidad para la frecuencia y gravedad de pérdidas futuras sobre un horizonte particular. La combinación de estas dos distribuciones da una distribución de pérdidas agregadas que ofrece una visión futura de todo el rango de posibles pérdidas que pueden surgir en relación con un peligro particular y la probabilidad asociada de que ocurra ese peligro (véase la Figura 8)[58]. Una empresa puede evaluar desde una perspectiva probabilística a cuántos daños relacionados con ese peligro se enfrenta y compararlo con su disposición y capacidad para soportar el riesgo de que las pérdidas puedan resultar mucho mayores de lo esperado.

Figura 8:
Representación esquemática del enfoque actuarial tradicional sobre la cuantificación del riesgo



Fuente: Swiss Re Economic Research & Consulting.

[58] Obtener una distribución de pérdidas agregadas (compuestas) a partir de distribuciones empíricas de frecuencia y gravedad puede conseguirse por lo general de dos formas: puede utilizarse una solución analítica cerrada para calcular la distribución compuesta o, de forma alternativa, pueden utilizarse técnicas Monte Carlo para simular las muchas posibles combinaciones diferentes de frecuencias y magnitudes de pérdidas. Véase, por ejemplo, P. Shevchenko, «Calculation of aggregate loss distributions», *The Journal of Operational Risk* 5(2), 2010.

Obstáculos para la modelización del riesgo cibernético

La modelización del riesgo cibernético es todo un desafío.

Sin embargo, aunque este enfoque inductivo sobre la modelización del riesgo es sencillo para muchos peligros, la naturaleza de los riesgos cibernéticos presenta un nuevo conjunto de retos. La frecuencia y gravedad de los eventos cibernéticos, así como su codependencia, no son fáciles de establecer, lo que dificulta la evaluación de posibles pérdidas agregadas.

Existen datos empíricos limitados sobre pérdidas relacionadas con la cibernética…

Información limitada sobre pérdidas actuales y futuras

Hay una carencia de datos históricos sobre incidentes cibernéticos a partir de los cuales extrapolar información sobre pérdidas futuras (tanto frecuencia, incluyendo ataques no exitosos, como gravedad). Puede que las empresas ni siquiera sepan cuándo han sido atacadas, al menos mientras sucede, sin hablar de recopilar datos sistemáticamente sobre los daños causados. Esta situación se agrava por la ausencia de un marco comúnmente aceptado para obtener información sobre incidentes cibernéticos[59]. Las amenazas cibernéticas no son tan fácilmente identificables como las amenazas físicas y las capacidades de los delitos cibernéticos pueden ser más fáciles de esconder. Las empresas podrían ser reacias a dar a conocer violaciones por la vergüenza que supone admitir fallos de seguridad, el posible impacto que tenga la pérdida de reputación sobre las ventas futuras y también por el deseo de no atraer más ataques.

… especialmente sobre eventos catastróficos extremos.

Además, aunque las empresas están comenzando cada vez más a hacer un seguimiento de la información sobre su exposición cibernética y a implementar protocolos de higiene cibernética rutinarios para evitar violaciones de seguridad TI/privacidad de datos, las pérdidas extremas por eventos cibernéticos hasta la fecha han sido pocas. Desde una perspectiva estadística, el historial real solo da una idea de lo que podría haber pasado. En el caso de eventos que suceden rutinariamente como la violación de datos, el historial real de pérdidas es a menudo lo suficientemente grande como para englobar posibilidades más realistas. Pero en el caso de riesgos graves y menos frecuentes puede ser engañoso fiarse de datos históricos porque podría fomentar sesgos de percepción sobre este tipo de eventos de cola[60].

Las amenazas cibernéticas están en constante evolución y transformación.

Ambigüedad sobre los factores de riesgo subyacentes

Incluso con información detallada sobre pérdidas relacionadas con la cibernética y los factores subyacentes que las causaron, los eventos pasados no son necesariamente una buena guía para el futuro. El riesgo está en constante evolución con nuevos actores, métodos de ataque y tecnologías en juego, por lo que a las empresas les resulta sumamente difícil comprender y controlar su exposición. El potencial de amenazas cibernéticas «unknown-unknown» (desconocidas que desconocemos) crea mucha ambigüedad en torno a las fuentes de exposición subyacentes, especialmente porque pueden ser diferentes para violaciones de seguridad TI/datos normales en comparación con eventos cibernéticos catastróficos.

Un pequeño cambio en el equilibrio entre las capacidades de los *hackers* y las defensas cibernéticas de las empresas podría provocar un importante cambio en la frecuencia y gravedad de los ataques.

El factor humano añade un enorme elemento de complejidad a la modelización de riesgos cibernéticos, especialmente el potencial de perturbación accidental y maliciosa tanto desde ataques internos como externos. Las motivaciones de los *hackers* y su eficacia responderán a las más recientes medidas de seguridad. Del mismo modo, las acciones realizadas por empresas para detectar y combatir amenazas pretenden reducir sus vulnerabilidades, restando relevancia a la información sobre ataques pasados a la hora de predecir eventos futuros. Los ataques de nivel bajo normalmente no son aislados, sino continuos. Incluso un

[59] Por ejemplo, en 2014 Yahoo sufrió un ataque que solo salió a la luz unos dos años más tarde cuando la empresa estaba investigando informes sobre una violación particular. Véase D. Volz, «Yahoo says hackers stole data from 500 million accounts in 2014», *reuters.com*, 23 de septiembre de 2016, http://www.reuters.com/article/us-yahoo-cyber-idUSKCN11S16P

[60] Véase G. Woo, «Counterfactual Disaster Risk Analysis», *variancejournal.org*, 29 de febrero de 2016, http://www.variancejournal.org/issues/articlesinpress/Counterfactual-Woo.pdf

pequeño cambio en el equilibrio entre las capacidades de los *hackers* y las defensas cibernéticas podría provocar un cambio importante en la frecuencia y gravedad de los ciberataques[61].

Potencial de pérdidas acumuladas significativas

Los riesgos cibernéticos suelen ser altamente interdependientes...

Los riesgos cibernéticos suelen ser altamente interdependientes: un sistema afectado puede incrementar la vulnerabilidad de otros sistemas en una única empresa. En grandes empresas multinacionales, los incidentes de ciberseguridad pueden abrir y atacar todo el *software*, sistemas TI e infraestructuras. Además, normalmente existe una monocultura TI: muchas organizaciones tienden a utilizar *software*, programas de seguridad y otras infraestructuras informáticas similares. Como resultado, el ataque con éxito a una empresa implica que otras son vulnerables al mismo ataque[62]. La migración de servicios TI de las empresas a la nube incrementa el potencial de problemas correlacionados entre empresas si se producen perturbaciones en productos clave de «*software* como servicio» o proveedores de red.

... tanto dentro de las empresas como entre empresas...

El grado de dependencia variará de acuerdo con el tipo de amenaza cibernética (véase la Figura 9). En particular, el fallo de un solo ordenador debido a un problema de *hardware* causaría probablemente daños limitados en la misma empresa o, de un modo más general, en otra parte. El hecho de que un trabajador abuse de sus privilegios de acceso podría afectar a casi todos los ordenadores dentro de la red interna, causando una importante perturbación en una empresa, pero el potencial para afectar a los sistemas de otras empresas es limitado. En cambio, los ataques que implican interacción del usuario como el *phishing* o *spyware/malware,* pueden provocar vulnerabilidades correlacionadas entre empresas si el objetivo son unos pocos empleados en muchas empresas diferentes. Normalmente, otros tipos de *malware* como gusanos, virus y troyanos provocan daños correlacionados tanto dentro como entre empresas porque pocas veces están limitados a una única red[63].

Figura 9:
Ejemplos de diferentes tipos de correlación de riesgo cibernético

Correlación dentro de empresa	Correlación entre empresas	
	Baja	Alta
Baja	*Fallos de hardware*	*Spyware/phishing*
Alta	*Ataque desde dentro*	*Gusanos, virus y troyanos*

Fuente: basado en R. Böhme y G. Kataria, «Models and Meaures for Correlation in Cyber Insurance», *documento de trabajo*, University of Cambridge, junio de 2006.

... lo que puede dar lugar a una importante acumulación de pérdidas.

Esta interdependencia supone que las pérdidas originadas por incidentes cibernéticos individuales a menudo se pueden acumular significativamente, en especial si la causa correlacionada tarda en revelarse. Este potencial de acumulación de pérdidas es particularmente problemático para las aseguradoras que asumen riesgos relacionados con la cibernética de sus clientes, ya sea como parte de pólizas de seguro normales o a través de cibercobertura independiente (véase Cuadro: *Riesgo de acumulación*).

[61] T. Harvey, «Prudential Regulation Authority on the Challenges Facing Cyber Insurers», *rms.com,* 22 de noviembre de 2016, http://www.rms.com/blog/tag/cyber-risk/

[62] *Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance*, Z/Yen Group y Long Finance, julio de 2015.

[63] Un virus es un tipo de *malware* que se propaga insertando una copia de sí mismo en otro programa y se extiende de un ordenador a otro, dejando infecciones en su recorrido. En cambio, los gusanos son *software* independiente y no necesitan un programa anfitrión o ayuda humana para propagarse. Los troyanos no se reproducen infectando otros archivos, y no se autorreplican, a diferencia de los virus y gusanos, pero se propagan a través de la interacción del usuario, como al abrir un adjunto de un correo electrónico o al descargar y ejecutar un archivo de Internet. Para más información, véase http://www.cisco.com/c/en/us/about/security-center/virus-differences.html

Riesgo de acumulación

Las aseguradoras que asumen riesgos cibernéticos de sus clientes esperan ser capaces de diversificar su exposición.

Por definición, las aseguradoras aceptan riesgos de asegurados a cambio de primas. Lo hacen con la esperanza de que agrupando una cantidad suficientemente grande de riesgos independientes, las probabilidades de pago simultáneo a muchos tomadores sean limitadas y que las pérdidas acumuladas de la cartera sean predecibles. Esta diversificación es uno de los principios en que se funda el modelo de negocio de toda compañía re/aseguradora.

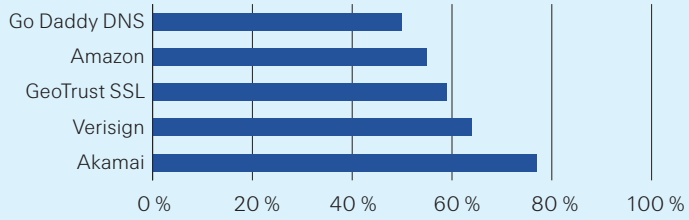
Pero podrían enfrentarse a importantes pérdidas acumuladas derivadas del mismo incidente subyacente...

La naturaleza del riesgo cibernético significa que un evento cibernético puede provocar múltiples siniestros bajo diferentes pólizas (por ejemplo riesgo de reputación, daños materiales, indemnización profesional y administradores y directores). El mismo evento también podría provocar múltiples siniestros de múltiples clientes bajo diferentes pólizas en diferentes geografías. La interconectividad de los sistemas TI supone que los incidentes cibernéticos podrían activar varios productos de seguro y pólizas independientes en un mecanismo en cadena, similar a la cobertura de interrupción de negocios contingente (CBI, por sus siglas en inglés)[64].

... o de las exposiciones correlacionadas resultantes a diferentes eventos.

Además, el volumen de pérdidas global derivado del riesgo cibernético podría tener su origen en varios eventos de pérdidas no relacionados que afecten a numerosos asegurados durante un periodo de póliza determinado o a una combinación de escenarios[65]. También puede que los clientes de las aseguradoras tiendan a depender del mismo grupo de proveedores de servicios de TI (véase la Figura 10), lo que podría ocasionar concentración de pérdidas si se produce un corte o una violación en infraestructuras de red clave.

Figura 10:
Uso por parte de los asegurados de proveedores de servicio de Internet seleccionados en una cartera de seguros de muestra



Fuente: *Risk Degrees of Separation: The Impact of Fourth Party Networks on Organizations,* BitSight, 2016.

También puede ser difícil identificar la causa correlacionada de los siniestros, lo que dificulta su tramitación.

Además, en caso de ciberataque puede que no sea fácil identificar todos los siniestros que han sido causados por el mismo *malware,* o resultado del mismo método de ataque subyacente o delincuente. Puede tardarse en identificar la causa correlacionada, que quizás nunca llegue a entenderse por completo. En esas circunstancias, las aseguradoras pueden encontrar difícil diferenciar cuáles de los muchos siniestros a los que se enfrentan son atribuibles a la misma causa fundamental, o a otros incidentes secundarios o de fondo[66].

[64] *Cyber resilience: The cyber risk challenge and the role of insurance,* CRO Forum, diciembre de 2014.
[65] Cuestionario sobre seguro de riesgo cibernético para el sector privado, OCDE, 2016, http://www.gfiainsurance.org/en/upload/positionpapers/GFIA-16-11%20Response%20to%20OECD%20Cyber%20Insurance%20Questionaire.pdf
[66] *Managing Cyber Insurance Accumulation Risk,* Risk Management Solutions, Inc y Centre for Risk Studies, University of Cambridge, febrero de 2016.

El potencial de pérdidas acumuladas actúa como medida disuasoria clave para las re/aseguradoras que suscriben ciberprotección.

Hasta la fecha no ha habido un evento cibernético catastrófico verdaderamente sistémico que haya desencadenado un gran número de siniestros. Sin embargo, según una encuesta reciente, casi dos tercios de las aseguradoras encuestadas creen que las cuestiones de acumulación relacionadas con las exposiciones cibernéticas son significativas[67]. El potencial de pérdidas acumuladas sustanciales es una restricción clave en el deseo de las aseguradoras de asumir riesgos cibernéticos, y es una preocupación particular para reaseguradoras que están preparadas para absorber pérdidas extremas de múltiples cedentes. Sin controles efectivos de riesgo de acumulación, una re/aseguradora podría tener que cargar con pérdidas catastróficas que agotarían su capital, afectando a su capacidad para cumplir las promesas hechas a los tomadores[68].

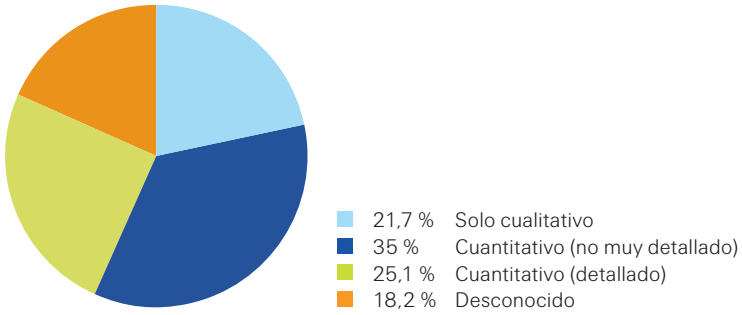
Análisis determinístico de escenarios

La mayoría de empresas no utiliza modelos de riesgo cibernético cuantitativos minuciosos.

Debido a las complejidades que entraña la cuantificación de toda la gama de riesgos cibernéticos, las empresas y aseguradoras han tendido a adoptar un enfoque relativamente rudimentario sobre la modelización. Una reciente encuesta realizada en Estados Unidos entre profesionales de seguridad indicó que solo una cuarta parte de las empresas emplean modelos de riesgo cibernético cuantitativos minuciosos, y la mayoría se basa en métricas simples o enfoques cualitativos (véase la Figura 11). Asimismo, sondeos recientes revelaron que solo alrededor de un tercio de las empresas británicas calcula el potencial impacto económico de ciberataques, y un 60 % de empresas en Europa continental nunca ha calculado el impacto económico de un escenario de pérdidas relacionadas con la cibernética[69].

Pregunta: ¿Desarrolla su empresa un modelo cuantitativo para evaluar y gestionar el riesgo cibernético?

Figura 11 :
Encuesta sobre enfoques de gestión del riesgo cibernético utilizados por empresas



Fuente: *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey,* SANS Institute, 2016.

[67] *Cyber Risk Survey Report,* Weightmans LLP & Insurance Day, noviembre de 2015.
[68] Para más información sobre el riesgo de acumulación cibernética, consulte *Casualty Accumulation Risk,* CRO Forum, octubre de 2015.
[69] *UK Cyber Risk Survey Report: 2016,* Marsh, septiembre de 2016 y *Continental European Cyber Risk Survey: 2016 Report,* Marsh, octubre de 2016.

En caso de que sea posible cuantificar el riesgo, se hace normalmente mediante análisis determinísticos de escenarios.

La mayoría de enfoques cuantitativos tiende actualmente a centrarse en la exposición potencial de las empresas en un número limitado de escenarios específicos, aunque hipotéticos. Los modelos adoptan normalmente una visión determinística para obtener estimaciones puntuales de la magnitud de posibles pérdidas si se diera el escenario. En otras palabras, buscan proporcionar estimaciones aproximadas del impacto del tipo «qué ocurriría si» en caso de que cristalizaran los riesgos adversos. Se puede crear un amplio panorama de la posición de riesgo de la empresa mediante la selección, construcción y análisis cuidadoso de diferentes escenarios[70].

Estos a menudo pretenden ofrecer estimaciones de las pérdidas máximas probables causadas por un incidente cibernético.

Un aspecto clave de este análisis de escenarios es incorporar el potencial de pérdidas acumuladas o individuales a gran escala. Varios corredores de seguros y proveedores de analítica de gestión de riesgos han desarrollado herramientas de escenario para ayudar a sus clientes y aseguradoras a evaluar y gestionar sus pérdidas máximas probables (PMP) causadas por peligros cibernéticos[71]. Por ejemplo, las empresas de modelización de riesgos AIR Worldwide y RMS han desarrollado bases de datos de exposición cibernética para una gran cantidad de empresas que pueden utilizarse para crear un panorama detallado de posibles pérdidas en varios escenarios determinísticos[72]. De modo similar, como parte de su marco ordinario de Escenario de Desastre Realista (RDS, por sus siglas en inglés), Lloyd's of London pidió en 2015 a sus sindicatos que diseñaran y pusieran a prueba sus exposiciones en tres escenarios extremos de ciberataque, y que calcularan su exposición agregada potencial en cada uno de ellos[73].

Un inconveniente de los enfoques determinísticos es calibrar la plausibilidad de los supuestos escenarios de pérdidas.

Sin embargo, un importante inconveniente de los análisis de escenarios determinísticos puros es la dificultad para establecer la plausibilidad de pérdidas en escenarios adversos. Siempre es posible diseñar un escenario que genere pérdidas catastróficas extremas, pero sin un mecanismo para calibrar la probabilidad de esos eventos, por no hablar de cómo se compara esto con la probabilidad de resultados alternativos, es difícil conocer cuánta importancia se debe dar a las pérdidas estimadas resultantes.

Hacia modelos probabilísticos de riesgo cibernético

Algunos investigadores están creando modelos probabilísticos para cuantificar los riesgos cibernéticos.

Como respuesta a esta debilidad, varios investigadores están desarrollando modelos probabilísticos para evaluar pérdidas cibernéticas potenciales, aunque su desarrollo se encuentra en una etapa incipiente. Comparados con herramientas deterministas, estos modelos pretenden cuantificar la distribución de probabilidad completa de pérdidas futuras en lugar de hacer una única mejor estimación. En este sentido están más cerca de los enfoques actuariales tradicionales sobre la modelización de riesgo. En ocasiones denominados valor en riesgo (VaR, por sus siglas en inglés) cibernético, los defensores sugieren que estos modelos constituyen una base para cuantificar riesgo e inculcar disciplina y rigor al proceso de evaluación de riesgos[74].

[70] T. Hull, «A Deterministic Scenario Approach to Risk Management», *2010 Enterprise Risk Management Symposium,* Society of Actuaries, 12-15 de abril de 2010.

[71] Por ejemplo, en mayo de 2016 Guy Carpenter anunció una alianza estratégica con Symantec Corporation para crear un modelo de agregación cibernética (véase http://www.gccapitalideas.com/2016/05/17/guy-carpenter-forms-strategic-alliance-to-develop-cyber-aggregation-model/). A principios de 2016, la empresa de modelización de catástrofes RMS lanzó Cyber Accumulation Management System, una herramienta para las aseguradoras para identificar sus acumulaciones y riesgo correlacionado, y poner a prueba sus carteras frente a una gama de pérdidas cibernéticas (véase http://www.rms.com/cyber). De modo similar, en abril de 2016, AIR Worldwide lanzó los primeros escenarios de riesgo cibernético determinísticos de fuente abierta del sector en una apuesta por comenzar a aumentar el conocimiento por parte de las aseguradoras de su riesgo agregado a partir de ciberataques a gran escala que podrían ocasionar pérdidas acumuladas catastróficas.

[72] S. Stransky, E. Ritt, *Cyber Scenario Modelling and Decision Making,* Air Worldwide, 2016.

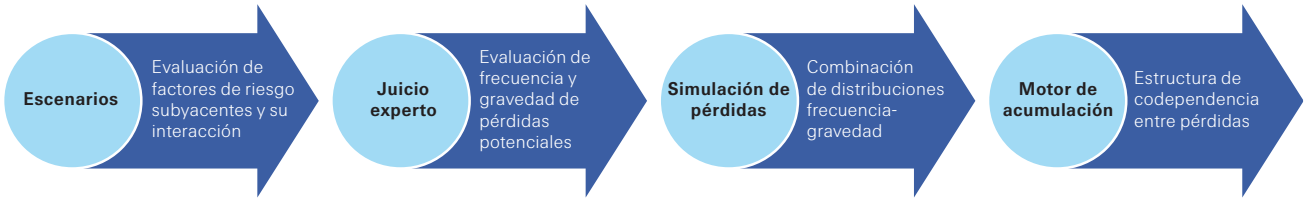
[73] «Cyber-attack: managing catastrophe-risk and exposures», *Lloyds.com,* 9 de noviembre de 2015, https://www.lloyds.com/~/media/files/the%20market/communications/market%20bulletins/2015/11/y4938.pdf

[74] Véase N. Sanna, «What is a Cyber Value-at-Risk Model?», *fairinstitute.org,* 28 de enero de 2016, http://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model

Estos generalmente combinan opiniones de expertos y suposiciones sobre la distribución frecuencia-gravedad de pérdidas futuras.

La poca frecuencia de pérdidas cibernéticas catastróficas extremas y la escasez de datos históricos de pérdidas incluso de algunos eventos relativamente menores, significa que los modelizadores tienen que basarse en información auxiliar para generar estimaciones de distribuciones de pérdidas agregadas. Un enfoque es combinar las opiniones de expertos sobre varias amenazas cibernéticas con hipótesis sobre las propiedades estadísticas subyacentes de la distribución frecuencia-gravedad de las pérdidas cibernéticas en diferentes escenarios. Estos últimos pueden seleccionarse para permitir explícitamente riesgos de pérdidas potencialmente graves consecuencia de un incidente cibernético[75].

Figura 12:
Representación esquemática de enfoques probabilísticos de modelización de riesgo cibernético



Fuente: Swiss Re Economic Research & Consulting basado en ideas de http://www.fairinstitute.org/

Combinados con métodos para contabilizar exposiciones correlacionadas, estos podrían finalmente utilizarse para cuantificar acumulaciones de pérdidas potenciales.

Junto con las hipótesis sobre la codependencia potencial de exposición de las empresas a las mismas amenazas, este enfoque puede utilizarse para obtener una perspectiva basada en riesgo sobre pérdidas acumuladas, lo que resulta fundamental para las aseguradoras que asumen riesgos de múltiples tomadores (véase la Figura 12)[76]. Sin embargo, independientemente de la estructura de dependencia que se adopte (ya sea, por ejemplo, basada en cópula, utilizando matrices de correlación o un enfoque de factor de riesgo común), debe ser capaz de ser puesto a prueba para reflejar la posibilidad de que el futuro sea más anómalo que el pasado[77].

Comparar las calibraciones de riesgo sin información de experiencia de pérdidas exhaustiva supone un desafío.

Estudios basados en información seleccionada sobre violaciones conocidas de privacidad y datos tienden a indicar que la distribución de costes es muy desigual. La mayoría de incidentes suele ocasionar pequeños daños, pero unos pocos pueden causar pérdidas a gran escala (véase la Tabla 2 en la página 3)[78]. No obstante, sin los detalles completos de toda la serie de eventos relacionados con la cibernética y las pérdidas asociadas (incluyendo daños materiales, daños a la reputación, interrupción del negocio y lesiones personales o muerte), es prácticamente imposible comparar/contrastar calibraciones de riesgo. En otras palabras, las distribuciones globales de pérdidas implicadas solo pueden ser ilustrativas, dado que están basadas en hipótesis simplificadas que no se fundamentan en experiencia de pérdidas real. Esta limitación es clara una vez se reconoce el potencial de eventos de pérdidas «desconocidas que desconocemos» o los factores de riesgo.

[75] Algunos investigadores abogan por utilizar análisis de escenarios para informar de estimaciones aproximadas expertas de los daños máximos y mínimos, así como de la cantidad más probable de daños que podrían derivarse de un incidente cibernético. Estas estadísticas después se utilizan junto con la simulación Monte Carlo y una hipotética distribución subyacente como beta-PERT para generar probabilidades frente a una gama de pérdidas cibernéticas.

[76] Para las re/aseguradoras, superar los desafíos en la modelización de la acumulación es posiblemente mucho más importante que intervenir sobre distribuciones de probabilidad de gravedad y frecuencia marginal.

[77] *A Clearer view of emerging risks,* Guy Carpenter, septiembre de 2015.

[78] Véase, por ejemplo, M. Kuypers, T. Maillart, E. Paté-Cornell, *An Empirical Analysis of Cyber Security Incidents at a Large Organization,* documento de trabajo, Freeman Spogli Institute for International Studies, Stanford University, 2016.

Como respuesta, algunos modelizadores subrayan la importancia de realizar evaluaciones probabilísticas minuciosas de todos los factores de riesgo y su interacción.

Para abordar parcialmente esta cuestión, algunos modelizadores sugieren un enfoque altamente granular en la elaboración de escenarios. Esto implica examinar el mismo escenario múltiples veces y desde diferentes ángulos para obtener una evaluación completa de los factores causales subyacentes y sus permutaciones que afectan a la frecuencia-gravedad de las pérdidas cibernéticas. Esta perspectiva probabilística se aplica a cada factor de riesgo que se analiza: los activos que podrían verse afectados, los actores que podrían suponer una amenaza, los tipos y magnitudes de la amenaza, las vulnerabilidades particulares y los mecanismos de mitigación implementados, etc[79].

Otros también abogan por el análisis de contraste para informar sobre posibles resultados extremos.

Algunos investigadores sugieren que el análisis de contraste puede ser útil como protección contra posibles sesgos cognitivos, por ejemplo, la tendencia a subestimar riesgos si todavía quedan por materializarse grandes pérdidas. Mediante el examen de eventos pasados y el análisis de lo que podría haber pasado para diferentes constelaciones de factores de riesgo, se puede crear un panorama completo de la gama de posibles pérdidas extremas que podrían haber surgido, las que todavía podrían surgir y las que deben mitigarse en el futuro. Podrían aumentar aún más los conjuntos de datos mediante escenarios inspirados y construidos a partir de modelización estocástica minuciosa de eventos históricos pasados. Estas evaluaciones probabilísticas retrospectivas pueden ofrecer una perspectiva útil sobre futuras catástrofes que no se han anticipado previamente y de ese modo también reducir las sorpresas por catástrofe[80].

Límites de los modelos

Los modelos son una ayuda para la comprensión, pero casi inevitablemente serán incorrectos.

Al final, todos los modelos son necesariamente una abstracción de la realidad. Son simplemente herramientas para ayudar a la comprensión. Incluso en la esfera de catástrofes naturales donde se han conseguido significativos avances de modelización, los últimos años han demostrado que el mundo real es a menudo muy diferente de la visión del modelo[81]. Además, las amenazas y vulnerabilidades pueden considerarse en muchas ocasiones como independientes entre sí en el mundo físico, pero en el riesgo cibernético hay un potencial de impactos no lineales mucho más correlacionados. El descubrimiento de una vulnerabilidad en un sistema TI suele provocar una avalancha de ataques destinados específica y exactamente a ese elemento[82].

La reciente crisis económica mostró la debilidad de modelos VaR al subestimar la probabilidad de eventos poco frecuentes.

La crisis económica de 2008–2009 reveló muy claramente la debilidad de modelos probabilísticos como VaR. En pos de la manejabilidad matemática se emplearon hipótesis de simplificación que subestimaban significativamente el potencial de grandes pérdidas sobre inversiones financieras (es decir, valores altos en los extremos de la distribución de pérdidas global). Pueden producirse eventos de pérdidas extremas más a menudo de lo que la gente cree. Además, los enfoques de medición de riesgo tradicionales como VaR suelen centrarse en la cuestión únicamente desde la perspectiva de la solvencia (tamaño de pérdidas en relación con los recursos de capital propios de una empresa), cuando otros factores como la posición de liquidez de una empresa (su capacidad para sufragar todas las obligaciones futuras) podrían ser igual de importantes a la hora de contener cualquier daño resultante.

[79] Por ejemplo, el enfoque Análisis de Factor de Riesgo de Información (Factor Analysis of Information Risk, FAIR) establece un marco para descomponer el conjunto de factores complejos que contribuyen al riesgo operativo y de información y cómo estos se afectan mutuamente. Al hacerlo pretende establecer una taxonomía y ontología estándares para el riesgo. Para más información, véase http://www.fairinstitute.org/

[80] G. Woo, *op. cit.*

[81] «The new approach to cat modelling» en *Specialty underwriters at a crossroads*, estudio de mercado de seguros, revista Reaction en asociación con Russell, otoño de 2013.

[82] I. Robertson y A. Warr, «Why we need a new approach to cyber-security and risk assessment», *www2.warwick.ac.uk*, 27 de abril de 2016, http://www2.warwick.ac.uk/research/priorities/cyber/blogs/?newsItem=094d4345545364160154580bc4622c40

Algunos críticos argumentan que los modelos de riesgo formales deben ser sustituidos por heurística que simplemente busque mejorar la resiliencia de las empresas.

Para algunos analistas, estas carencias suponen que el desarrollo de modelos para cuantificar lo que es en última instancia inmensurable podría ser inútil: intentar precisar números a partir de colas de distribuciones de pérdidas que son altamente inciertas y volátiles no sirve de nada y resulta potencialmente peligroso. Para ellos es mejor crear sistemas TI robustos que permitan a las empresas soportar eventos catastróficos difíciles de predecir. En lugar de basarse en modelos falsamente precisos, se trata más de definir, seguir y evaluar factores que afectan a la propensión a un evento cibernético catastrófico o que pudieran acarrear una agregación de pérdidas en serie. Las empresas también deben crear arquitecturas que sean «antifrágiles», en las que las perturbaciones e interrupciones hagan a las empresas más fuertes, más resistentes y más capaces de adaptarse a nuevas amenazas cibernéticas[83].

Aun así, la combinación de análisis estadístico formal y criterio experto...

Esta crítica a la modelización del riesgo formal es sin duda demasiado fatalista. Los modelos no pueden ni deben ser los árbitros finales o absolutos en las decisiones de gestión de riesgos de las empresas[84]. Las pérdidas cibernéticas también podrían verse abocadas a una incertidumbre irreducible que no puede ser remediada recopilando más datos, utilizando métodos estadísticos más sofisticados u ordenadores más potentes, o pensando con más intensidad o de forma más inteligente[85].

... ayudará a mejorar la evaluación del riesgo cibernético.

Sin embargo, empresas y aseguradoras pueden aumentar con el tiempo su comprensión del riesgo cibernético combinando conocimientos de modelización estadística y datos parciales con criterios basados en la experiencia. Este proceso probablemente se acelerará y mejorará si las lecciones extraídas del marco de fuente abierta Oasis para colaborar y compartir perspectivas sobre modelos de catástrofes naturales pueden aplicarse en el campo de la cibernética[86]. El trabajo realizado por el CRO Forum para desarrollar una categorización del riesgo cibernético común va en esta dirección[87]. Estas iniciativas, aliadas con plataformas de intercambio de información de pérdidas como ORX y ORIC International, deben posibilitar a empresas y aseguradoras la creación de un panorama más claro de la magnitud y el origen de los riesgos cibernéticos[88].

[83] Véase, por ejemplo, N. Taleb, *Anti-fragile: Things That Gain from Disorder,* Random House, noviembre de 2012.
[84] D. Rowe, *Value at Risk: A Valuable Tool That Was Greatly Oversold,* Notes from the Vault, Banco de la Reserva Federal de Atlanta, junio de 2013.
[85] Para más información sobre los límites de la modelización formal, véase A. Lo y M. Mueller, *WARNING: Physics Envy May Be Hazardous To Your Wealth!,* MIT, 12 de marzo de 2010, http://web.mit.edu/alo/www/Papers/physics8.pdf
[86] Oasis, una empresa sin ánimo de lucro, es propiedad de más de 40 de las principales aseguradoras, reaseguradoras y corredores de seguros y entidades mundiales, junto con una comunidad de miembros asociados de más de 100 empresas e instituciones académicas, una amplia comunidad de organizaciones dedicadas a mejorar la modelización de pérdidas por catástrofe.
[87] *Concept Proposal categorisation methodology for cyber risk,* CFO Forum, junio de 2016.
[88] ORX Association y ORIC International intercambian datos de riesgo operativo que ayudan a hacer avanzar la medición y la gestión de riesgo operativo a través del intercambio de información de riesgo operativo. Véase https://www.orx.org/Pages/HomePage.aspx y https://www.oricinternational.com/

Lecciones de otros peligros

La experiencia de modelización de catástrofes naturales alienta la esperanza de que finalmente se desarrollen mejores modelos cibernéticos.

La modelización de riesgos tiende a evolucionar a medida que aumenta la información y el conocimiento sobre los riesgos y peligros subyacentes. Este es ciertamente el caso con los modelos de riesgos de catástrofes naturales. Desde la introducción de los primeros modelos de catástrofes naturales comercialmente disponibles a finales de la década de 1980, se han producido actualizaciones regularmente y la convergencia entre modelos de diferentes proveedores indica que las incertidumbres se han reducido progresivamente[89]. Estas mejoras normalmente han reflejado avances en técnicas y capacidades de computación, mejorado la comprensión científica de los peligros naturales y su impacto, y ampliado la cobertura del fenómeno captado por los modelos[90]. Esto alienta la esperanza de que surjan modelos cibernéticos mejores a medida que aumente la comprensión de los factores de riesgo fundamentales y se disponga de más datos sobre procesos estocásticos subyacentes que generan pérdidas cibernéticas.

La modelización de riesgos cibernéticos de daños y responsabilidad civil puede requerir enfoques fundamentalmente diferentes.

Al mismo tiempo, es improbable que un enfoque universalista, donde se aplica la misma configuración genérica a diferentes riesgos, sea óptimo. Los riesgos cibernéticos de tipo daños y responsabilidad civil pueden requerir enfoques fundamentalmente diferentes, dependiendo de la magnitud del conocimiento, la experiencia siniestral y las fuentes de acumulación de pérdidas. En particular, el análisis de escenarios determinísticos para múltiples eventos fijos podría ser totalmente adecuado para conseguir una evaluación creíble y valiosa de escenarios de peores casos mientras que sigue siendo muy difícil definir las probabilidades de ocurrencia asociadas[91].

Se están estudiando varios enfoques de modelización que podrían ampliarse con el tiempo a la medición de riesgo cibernético.

En este sentido, algunas re/aseguradoras están desarrollando modelos de escenarios múltiples y altamente granulares para riesgos de responsabilidad con el objetivo de cuantificar el rango de pérdidas esperadas y su sensibilidad al cambio de las condiciones tecnológicas, económicas, legales y sociales[92]. Mientras tanto, otras consideran aplicar perspectivas de análisis de red o modelos de pandemias de enfermedades infecciosas para comprender la potencial acumulación de riesgo de accidente[93]. Con el tiempo, estos modelos pueden ampliarse para incluir riesgos cibernéticos, que cada vez más combinan características de exposiciones de riesgo de daños y responsabilidad civil, incluyendo interrupción del negocio (contingente). También están surgiendo modelos basados en agente que buscan incorporar las preferencias adaptativas y el comportamiento de atacantes y defensores a la hora de analizar ciberamenazas y vulnerabilidades, al igual que algunos modelos de riesgo de terrorismo.

89 *Managing Catastrophe Model Uncertainty: issues and challenges*, Guy Carpenter, diciembre de 2011.
90 *Ibíd.*
91 Para más información sobre las fortalezas relativas de modelos de escenarios determinísticos, véase K. Clark, «Measuring up the metrics», globalreinsurance.com, septiembre de 2010, http://www.karenclarkandco.com/news/pdf/20-21_GRSept10.pdf
92 *Bringing a forward-looking perspective into liability modelling: Liability Risk Drivers*, Swiss Re, abril de 2016.
93 Reactions en asociación con Russell, *op. cit.*

Iniciativas para promover la resiliencia cibernética

Autoprotección y prevención de riesgos

Los riesgos cibernéticos no pueden eliminarse por completo. Las empresas deben cumplir su parte para que la economía sea más resiliente.

Incluso con una mejor cuantificación será imposible eliminar totalmente los riesgos cibernéticos, especialmente dado que las amenazas continuarán evolucionando y las empresas y sociedades cada día dependerán más de las tecnologías digitales. Para que la economía sea más resiliente, la empresas deben mejorar su gestión de riesgos cibernéticos. Su primera línea de defensa contra amenazas cibernéticas es invertir más en tecnología de seguridad y aumentar la sensibilización de los empleados respecto a las últimas técnicas del *hacking* y otros riesgos cibernéticos. Muchas violaciones recientes de datos tienen su origen en fallos elementales del sistema como funciones de contraseñas con encriptaciones débiles o carencia de encriptado. Asimismo, los informes de investigaciones de violación de datos de Verizon revelan sistemáticamente que la mayoría de violaciones de datos se aprovechan de lagunas que se pueden evitar con higiene cibernética básica, entre las que se incluyen fallos de parche para defectos de *software* conocidos o la implementación de sistemas adecuados de autenticación de contraseña u otros sistemas de autenticación, susceptibilidad a ataques de suplantación de identidad e insuficiencia de sistemas de acceso reducido[94].

Las empresas están investigando exhaustivamente tanto en capacidades preventivas como de detección-respuesta.

Hay indicios de que las empresas están preparándose para abordar estas vulnerabilidades. El gasto global en productos y servicios de seguridad de la información ascendió, según se informa, a 81 600 millones de USD en 2016, un incremento del 7,9 % respecto a 2015, de acuerdo con estimaciones recientes[95]. Se espera que continúe esta tendencia al alza con una mayor inversión en estrategias de detección y respuesta mejoradas junto con seguridad preventiva más tradicional.

Pero la protección contra el riesgo cibernético no solo consiste en crear sólidos cortafuegos o contratar personal especialista en TI, sino que es una cuestión estratégica más amplia.

Sin embargo, no bastará con adoptar medidas de seguridad independientes y/o adicionales que se centren en un aspecto de las operaciones de las empresas, como cortafuegos informáticos o productos antivirus. Según un informe, en el 46 % de sistemas informáticos afectados en 2013 no había *malware*[96]. Del mismo modo, considerar simplemente las ciberamenazas a través del prisma del cumplimiento regulatorio no captará adecuadamente toda la gama de riesgos, aunque podría ayudar a catalizar la acción para reconocer y abordar debilidades obvias del sistema. En otras palabras, el riesgo cibernético no es solo una cuestión informática o regulatoria. Es un riesgo de negocio estratégico. Los *hackers* descubren continuamente nuevas formas de explotar vulnerabilidades y las empresas no pueden seguir asumiendo que sencillamente es suficiente con contratar profesionales informáticos competentes y tener implantados los últimos protocolos de seguridad[97]. La amenaza que pueden suponer empleados antiguos o actuales descontentos demuestra la importancia de la cultura de una organización a la hora de mitigar riesgos cibernéticos[98].

Se trata sobre todo de integrar resiliencia cibernética en los procedimientos globales de gestión de riesgo de las empresas.

La mitigación de riesgo es más eficaz cuando se integra dentro de una evaluación holística y rutinaria del cambiante panorama cibernético y los riesgos asociados. Las empresas deben aprovechar los conocimientos del departamento de TI interno para determinar sus vulnerabilidades e identificar los tipos de cibereventos que podrían causar daños importantes. Esto podría incluir ejercicios regulares de resistencia que tengan en cuenta la solidez de la empresa frente a varios eventos que podrían ser altamente perturbadores. Las nuevas tecnologías, aunque pueden añadir riesgos, también pueden ayudar a las empresas a identificar amenazas emergentes. Por

[94] Según una encuesta reciente, mientras el 55 % de encuestados indica que su organización ha cambiado o desarrollado procesos para gestionar cuentas privilegiadas, el 40 % todavía guarda contraseñas privilegiadas y de administrador en un documento Word o en una hoja de cálculo. Véase *Global Advanced Threat Landscape Survey 2016*, CyberArk, *2016*.

[95] *Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016*, Gartner, 9 de agosto de 2016, http://www.gartner.com/newsroom/id/3404817

[96] *M-Trends Report*, Mandiant, 2014.

[97] *How to make the case for buying cyber risk insurance to the board*, Aon 2014.

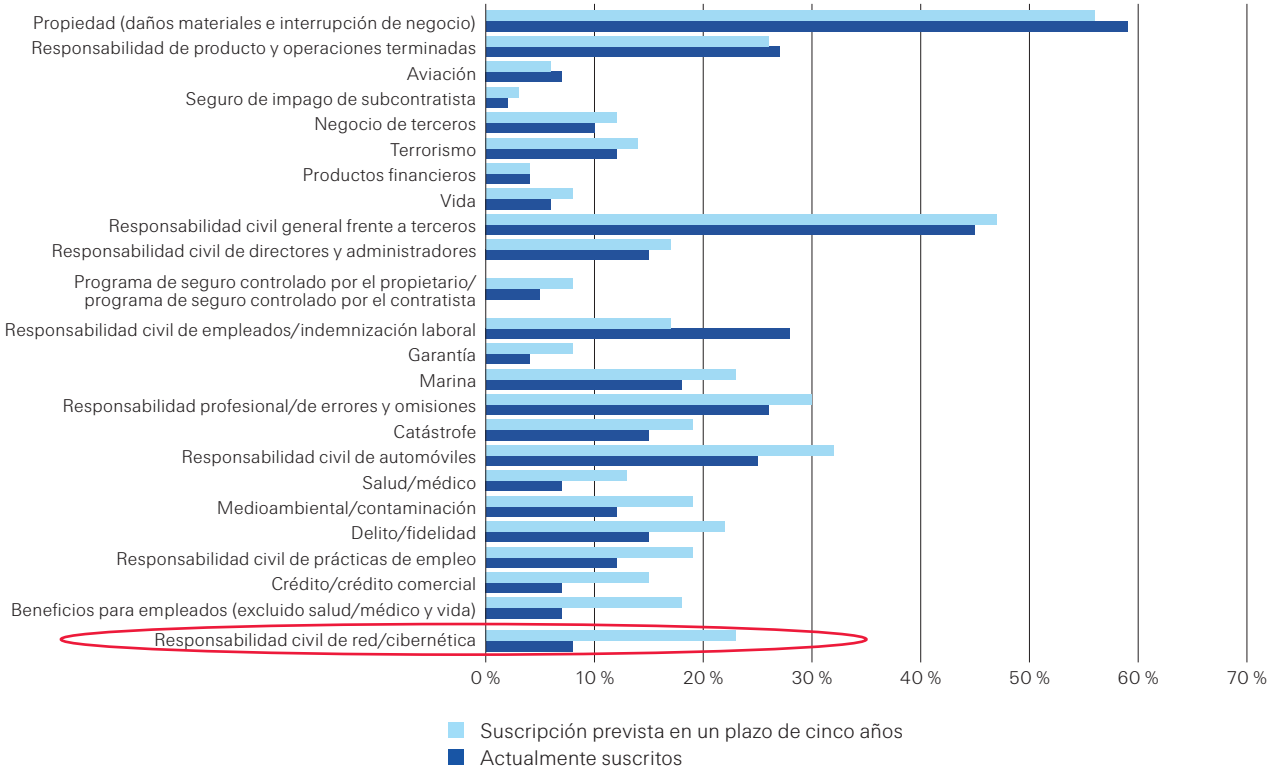
[98] Un reciente análisis global de encuestas a personal contratado indica que los empleados de organizaciones que experimentan violaciones de datos reciben menos formación favorable y remuneración relacionada con el rendimiento, al menos comparado con empleados de empresas líderes en sus sectores. Véase *The inside threat: Why employee behavior and opinions impact cyber risk*, Willis Towers Watson, mayo de 2016.

ejemplo, la computación cognitiva podría ayudar a anticipar riesgos cibernéticos cambiantes, reconocer desviaciones anómalas cuando un sistema está afectado y tomar medidas para contrarrestar nuevas amenazas conforme surjan[99].

Algunas empresas están estudiando el uso de cautivas para gestionar sus exposiciones a riesgos cibernéticos.

Como parte de las prácticas mejoradas de gestión de riesgo, algunas empresas están considerando el establecimiento de aseguradoras cautivas para organizar sus exposiciones a riesgos cibernéticos[100]. Tradicionalmente, las cautivas se han utilizado para suscribir daños materiales, indemnización a trabajadores, negligencia médica y riesgos de responsabilidad civil frente a terceros. Una encuesta de 2015 reveló que el 8 % de empresas suscribió riesgo cibernético a través de una cautiva, y que el 23 % tenía previsto hacerlo en un plazo de cinco años[101]. Esto representó el incremento más pronunciado del uso potencial de cautivas entre los diversos riesgos sobre los que se preguntó (véase la Figura 13).

Figura 13:
Riesgos suscritos por una cautiva, en la actualidad y en un plazo de cinco años



Fuente: Aon.

El uso de una cautiva puede favorecer una mejor apreciación de los riesgos cibernéticos a los que se enfrenta una empresa.

En la cautiva se acumulan fondos como medio para autoasegurarse contra riesgos. La consolidación de exposiciones dentro de una estructura corporativa independiente puede promover un mayor conocimiento, por ejemplo, de riesgos cibernéticos, incluyendo revisiones periódicas de las prácticas de protección de datos y de seguridad de red y recopilación de información crucial. Esto podría ser especialmente valioso para grandes empresas internacionales que dirigen negocios importantes y a veces diferentes en distintas ubicaciones. La información comercial

[99] E. Hunter, «Cognitive Computing Takes On Cyber-Security», *theinnovationenterprise.com*, 20 de enero de 2016, https://channels.theinnovationenterprise.com/articles/cognitive-computing-takes-on-cyber-security
[100] Una cautiva es un tipo especial de compañía de seguros creada por una empresa, asociación comercial o grupo de empresas para asegurar los riesgos de su propietario o propietarios.
[101] *Global Risk Management Survey*, Aon 2015.

extraída a través de una aseguradora cautiva también podría posibilitar que una empresa obtenga precios más favorables sobre el seguro y reaseguro cibernético.

Innovación en el seguro y reaseguro cibernético

Datos más completos sobre incidentes cibernéticos y su impacto respaldarán un mayor desarrollo del ciberseguro.

El ciberseguro también puede jugar un mayor papel en el fomento de la resiliencia. Un factor importante que influirá en el ritmo de desarrollo del mercado será la obtención y análisis de datos relevantes e información necesaria para suscribir riesgos cibernéticos con precisión. El conocimiento de la gama de riesgos cibernéticos, sus impactos y la fiabilidad de los datos es crucial para los esfuerzos actuariales a la hora de estimar actividades de riesgo y su impacto. Las compañías de seguros normalmente saben menos que sus asegurados sobre los riesgos, así como las medidas adoptadas para mitigar las pérdidas asociadas. Normalmente no tendrán noticias sobre los conatos de ataque, ni tienen señales de aviso temprano de un ataque. Incluso cuando la información es compartida por un tomador puede estar incompleta, ser ambigua o errónea. Esta asimetría de información tiene importantes implicaciones en las potenciales exposiciones de las aseguradoras y su disposición para ofrecer cobertura.

Muchas empresas parecen dispuestas a compartir información.

A primera vista, muchas empresas parecen dispuestas a compartir información de sus violaciones cibernéticas con terceros, entre los que se incluyen aseguradoras, si esto conduce a mejores soluciones de seguro. Esto es cierto globalmente y en la mayoría de sectores (véase la Figura 14). Puede haber algún resto de reticencia a la hora de revelar información forense sobre ciberataques, especialmente si se trata de cuestiones jurídicas y reglamentarias destacadas relacionadas con un evento, pero las empresas no tienen que adoptar un enfoque todo o nada. Pueden elegir cuántos datos relacionados con sus esfuerzos por combatir *malware* comparten y con qué frecuencia, aunque es importante reconocer la naturaleza parcial de la información compartida cuando se extraen conclusiones. Por ejemplo, algunas organizaciones pueden elegir distribuir datos a través de un proveedor de soluciones externo, que a su vez agrega los datos y los comparte sobre una base anónima[102].

Figura 14:
Encuesta sobre disposición de las empresas a compartir información

Sector	*Pregunta*: ¿cree usted que la aceptación en cuanto al compartir información en sentido general incrementará? (% sí)	*Pregunta:* ¿estaría usted preparado para aumentar su colaboración (ej., compartir información con la industria y con aseguradores)? (% sí)
Electrónica	57 %	51 %
Medios de comunicación	58 %	42 %
Atención sanitaria	64 %	42 %
Transporte	64 %	49 %
Banca	64 %	53 %
Infraestructura de telecom.	67 %	56 %
Farmacia y biotecnología	68 %	53 %
Productos químicos y petróleo	68 %	59 %
Todos los sectores	68 %	54 %
Producto consumo	68 %	60 %
Producto industrial	71 %	63 %
Fabric. automóviles	72 %	56 %
Servicios profesionales	73 %	53 %
Minorista	75 %	52 %
Servicios públicos	78 %	51 %
Hoteles	78 %	67 %

Fuente: *Cyber: in search of resilience in an interconnected world,* Swiss Re/IBM, 2016.

[102] *5 Key Ways To Detect Anomalous Behavior On Your network. Threat Intelligence for Your Data Security and Management Framework,* Information Security Media Group, 2016.

Se están desarrollando métodos para obtener datos estandarizados sobre exposición al riesgo cibernético.

Varios proveedores externos como AIR y RMS han creado programas de datos que proporcionan a las empresas un método estandarizado para identificar, cuantificar e informar sobre exposición cibernética a las aseguradoras[103]. De modo similar, el CRO Forum está promoviendo un lenguaje y marco común para captar información relevante sobre incidentes cibernéticos y vulnerabilidades[104]. Estas fuentes de información beneficiarán a las aseguradoras ofreciendo formas de controlar y evaluar el desarrollo de la exposición cibernética de sus clientes de una manera uniforme y sistemática y, por lo tanto, evaluar también su propio riesgo de acumulación.

Un mayor conocimiento de los riesgos cibernéticos posibilitará soluciones de seguro más flexibles y personalizadas.

Las aseguradoras, por su parte, tratan de desarrollar productos de seguro flexibles que sean menos complejos, satisfagan mejor las necesidades de las empresas y se adapten a la constante evolución de las ciberamenazas a las que se enfrentan. Esto incluye personalizar cobertura para pequeñas y medianas empresas que hasta ahora han estado desatendidas por el seguro y frecuentemente están peor situadas para hacer frente a riesgos cibernéticos que las empresas más grandes. El seguro también puede configurarse para un pago rápido, por ejemplo, a través de la liquidación por adelantado de siniestros de cobertura de interrupción de negocios. Esto puede ser particularmente importante dados los problemas de liquidez que podrían surgir después de un incidente cibernético. Los servicios complementarios proporcionados por las aseguradoras también pueden ayudar a la recuperación después del incidente.

La colaboración con expertos en ciberseguridad…

Algunas re/aseguradoras buscan colaborar con empresas de ciberseguridad y proveedores de analíticas de datos para llenar sus lagunas de conocimiento y ampliar/proporcionar servicios adicionales a sus clientes. Por ejemplo, en mayo de 2015, ACE Group anunció un acuerdo con FireEye para combinar la detección de ciberamenazas en tiempo real con servicios y asesoramiento en mitigación de pérdidas[105]. Asimismo, como complemento a sus productos de seguro y mitigación de riesgo cibernético, AIG adquirió una participación minoritaria en K2 Intelligence, una empresa de consultoría de investigación[106]. Por otro lado, Swiss Re ha añadido a su conjunto de herramientas de suscripción una plataforma de evaluación de riesgo cibernético proporcionada por Cyence, una empresa de analítica y modelización de riesgos cibernéticos. Estas empresas especializadas en evaluación de riesgos cibernéticos utilizan normalmente inteligencia sofisticada para obtener y analizar información presente en la parte pública y no pública de Internet.

[103] Véase, por ejemplo, RMS Launches New Data Standard for Managing Cyber Insurance, RMS, 19 de enero de 2016, https://www.rms.com/newsroom/press-releases/press-detail/2016-01-19/rms-launches-new-data-standard-for-managing-cyber-insurance y *Verisk Cyber Exposure Data Standard and Preparer's Guide,* air-worldwide.com, 2016, https://www.air-worldwide.com/Documentation/Cyber-Exposure-Data-Standard/air_cyber_exposure_data_schema_and_preparers__guide.htm

[104] CRO Forum, junio de 2016, *op. cit.*

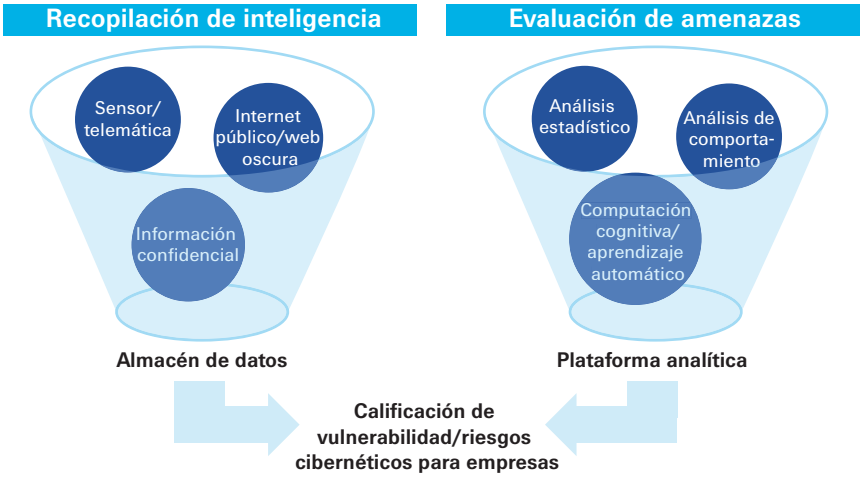
[105] *FireEye and ACE Group Announce Strategic Alliance to Mitigate Cyber Risk,* FireEye, 18 de mayo de 2015, http://investors.fireeye.com/releasedetail.cfm?ReleaseID=913633

[106] «AIG Invests in K2 Intelligence to Deepen Cyber, Other Risk Mitigation Capabilities», *businesswire.com,* 15 de abril de 2015, http://www.businesswire.com/news/home/20150415006706/en/AIG-Invests-K2-Intelligence-Deepen-Cyber-Risk

… y el impulso de analíticas inteligentes…

En líneas generales, el Big Data y la analítica inteligente podrían aumentar el análisis actuarial tradicional y permitir así a las re/aseguradoras crear un perfil de riesgo multidimensional de empresas y/o segmentos de la industria seleccionados y responder rápidamente a factores de riesgo subyacentes en rápida evolución. Por ejemplo, ¿los empleados de un asegurado acceden a Internet utilizando un navegador web obsoleto que es vulnerable a nuevos tipos de *spyware, malware* y virus? o ¿aparece propiedad intelectual de la empresa, información de seguridad o datos confidenciales, incluyendo contraseñas robadas, en foros web oscuros? La combinación de esta información con analíticas estadísticas y de comportamiento, en especial aquellas que no solo comprenden las conexiones de red, sino también la relevancia del negocio y el contexto de estas interacciones, podría ayudar a aislar estos movimientos y patrones que indican susceptibilidad a actividad maliciosa (véase la Figura 15)[107].

Figura 15:
Analítica inteligente como herramienta de suscripción complementaria



Fuente: Swiss Re Economic Research & Consulting.

… ayudará a las aseguradoras a evaluar riesgos cibernéticos.

Estos análisis no sustituirán la experiencia de suscripción y el criterio basado en riesgo[108]. Sin embargo, junto con información de análisis detallados de vulnerabilidad cibernética y pruebas de penetración, pueden formar una herramienta de evaluación de riesgos complementaria[109]. Con el tiempo, la innovación de procesos y productos puede ayudar a que el riesgo cibernético sea más asegurable. Esto, combinado con mayor certidumbre legal sobre la redacción de pólizas y los límites de responsabilidad, ayudará a rebajar las primas, ajustar límites (sumas aseguradas, retención, restablecimiento, etc.) para cubrir mejor las necesidades de los clientes y hará que la cobertura cibernética sea más asequible para un conjunto más amplio de asegurados. La mayor diferenciación en la evaluación de riesgos, si se refleja en las primas de seguro, también incentivará un buen comportamiento de gestión de riesgos.

[107] *Analytics steps up to meet evolving cybersecurity threats,* SAS, http://www.sas.com/en_us/insights/articles/risk-fraud/analytics-steps-up-to-meet-evolving-cybersecurity-threats.html

[108] Según una encuesta reciente entre corredores de seguros de EE. UU., la mayoría (60 %) de encuestados cree que las colaboraciones entre compañías de seguros y empresas de ciberseguridad serán más beneficiosas para consultoría y respuesta después del evento que para la cuantificación de riesgo antes del evento. Véase *Cyber Insurance Market Watch Survey,* The Council of Insurance Agents and Brokers (CIAB), octubre de 2016.

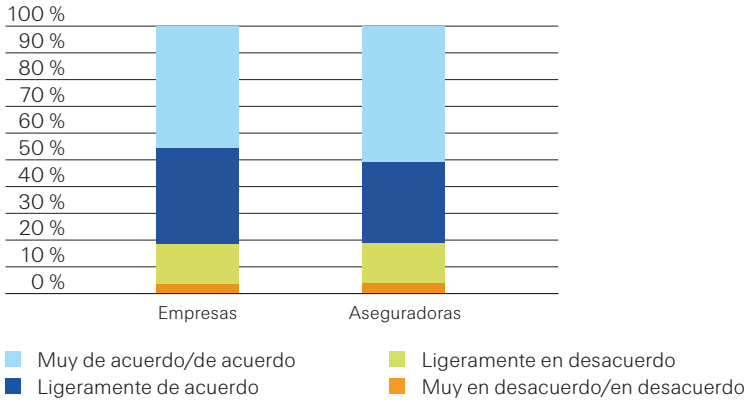
[109] Aunque a veces los términos se emplean de forma intercambiable, análisis de vulnerabilidad normalmente se refiere a identificar y medir vulnerabilidades de seguridad, mientras que prueba de penetración pretende replicar las acciones del intento de un *hacker* de violar protocolos de seguridad de información y/o interrumpir el funcionamiento normal de la organización.

Tanto empresas como aseguradoras prevén el potencial de la tecnología digital para facilitar soluciones de seguro flexibles.

Tanto aseguradoras como empresas parecen estar de acuerdo en el alcance de la nueva tecnología digital para promover soluciones de seguro flexibles. En una reciente encuesta de Swiss Re-IBM, cerca de la mitad de asegurados (51 %) y empresas (46 %) estaba abierta a la idea de que las tecnologías digitales facilitarán soluciones de seguro flexibles (véase la Figura 16). Estas podrían incluir productos de ciberseguro basados en uso donde, por ejemplo, los niveles de cobertura evolucionen al mismo tiempo que las tecnologías cambiantes, las nuevas formas de ciberataque y los nuevos enfoques de ciberdefensa. De una manera más especulativa, también podrían ser posibles soluciones paramétricas en las que el seguro esté vinculado a una evaluación cuantitativa obtenida de forma independiente del nivel de ciberamenaza presente si pueden desarrollarse índices de amenaza en la industria.

Figura 16:
Encuesta de opinión de las empresas/aseguradoras sobre el potencial de comprar/ofrecer soluciones de seguro tecnológicas flexibles

Pregunta: Si hay disponibles soluciones de seguro flexibles basadas en tecnología de interconexión digital es muy probable que mi empresa las compre/ofrezca.



Fuente: *Cyber: in search of resilience in an interconnected world,* Swiss Re/IBM, 2016.

Sin embargo, el potencial de grandes pérdidas individuales o acumuladas significa que hay límites a la cibercobertura que pueden ofrecer las re/aseguradoras.

Sin embargo, incluso con datos más completos, avances en cuantificación de riesgos y mayor colaboración con los tomadores, las aseguradoras de riesgos cibernéticos deben ser prudentes para no sobrepasar los límites de asegurabilidad. Las exposiciones cibernéticas presentan importantes riesgos de cola y agregación. Hasta ahora las pérdidas por potenciales eventos cibernéticos catastróficos han podido gestionarse. Por ejemplo, el ataque de Stuxnet a una planta nuclear iraní en 2012 y el ataque a una planta eléctrica ucraniana en 2015 ocasionaron daños físicos en la infraestructura aunque sin llegar a provocar una perturbación generalizada. Pero las aseguradoras deben estar alerta a las posibles grandes pérdidas imprevistas tanto a través de ciberpólizas especializadas como de cobertura silenciosa. Las propias empresas deberían también estar preocupadas por la agregación de riesgo dado que ataques individuales pueden acarrear pérdidas a un gran número de empresas, que pueden crear riesgo de contraparte (incluyendo en relación con sus aseguradoras).

Compartir riesgos entre aseguradoras dentro de un consorcio especializado en riesgos cibernéticos puede ser una forma de incrementar la capacidad de absorción de riesgo.

En una apuesta por aumentar la asegurabilidad de pérdidas cibernéticas catastróficas, algunos analistas han sugerido la creación de un mecanismo de consorcio especializado a través del cual las aseguradoras individuales puedan compartir riesgos[110]. Esto permitiría a las compañías de seguros más pequeñas que deseen expandir su negocio participar sin los costes iniciales habituales y limitar sus responsabilidades para que se ajusten a su propio apetito de riesgo. Además, para promover la estabilidad de capital en el mercado, un consorcio podría facilitar el intercambio rápido de información cuando se produjeran eventos cibernéticos, lo

[110] Véase, por ejemplo, T. Ryan y W Carbone, *Cyber liability insurance: As the market heats up, is it time to cool off in a pool?*, Milliman, 23 de mayo de 2016, http://us.milliman.com/insight/2016/Cyber-liability-insurance-As-the-market-heats-up--is-it-time-to-cool-off-in-a-pool/

que puede hacer que la respuesta y reacción sea más rápida y, con suerte, limitar la propagación de un problema.

Transferencia de riesgo a mercados de capitales

La transferencia de riesgos cibernéticos pico al mercado de capitales es otra.

Otra forma de incrementar la capacidad de absorción de pérdidas global para el riesgo cibernético es desarrollar vehículos de inversión que permitan a los inversores del mercado de capitales asumir algunas de las exposiciones. Los bonos de catástrofes naturales (cat bonds) se desarrollaron en la década de 1990 para cubrir riesgos pico de daños materiales, en parte como respuesta a las percepciones cada vez mayores de que las catástrofes podrían ocasionar daños de unas dimensiones que incluso las reaseguradoras no serían capaces de cubrir. Aunque los riesgos relacionados con daños materiales siguen dominando el bono de catástrofes y otros valores vinculados con el seguro (ILS, por sus siglas en inglés), se ha ampliado la transferencia de riesgos a mercados de capitales para incluir riesgos de vida, accidentes y salud, y *casualty*. También recientemente, el banco Credit Suisse titulizó parte de su exposición a riesgos operativos extremos, incluyendo pérdidas catastróficas relacionadas con la cibernética[111].

El mercado ILS de riesgos cibernéticos está todavía en sus inicios, pero probablemente se expandirá en el futuro.

Algunos analistas creen que a la larga otras innovaciones en ILS allanarán el camino para que se transfieran más riesgos cibernéticos a los mercados de capitales. Al igual que los bonos de catástrofes cibernéticas, aún podrían surgir estructuras adicionales que agrupen riesgos de empresas, vehículos de tipo cautivo financiados o alguna forma de instrumentos de capital contingente, facilitando a los mercados de capitales asumir exposiciones cibernéticas pico. El desarrollo de acuerdos proporcionales que permitan a los inversores compartir riesgos cibernéticos con suscriptores de seguro expertos (en lugar de estructuras más típicas de exceso de pérdidas) también podría estimular la expansión del mercado ILS[112].

Es posible que todavía sea necesario convencer a los inversores de los beneficios de la diversificación de carteras de riesgos cibernéticos.

Además de los desafíos de modelización de riesgo y datos, deben superarse otros obstáculos si van a desarrollarse mercados alternativos de transferencia de riesgos. En primer lugar, los inversores probablemente necesitarán más pruebas de que los rendimientos de los valores vinculados con riesgos cibernéticos están genuinamente desvinculados de otros tipos de activos. Uno de los atractivos de los bonos de catástrofes existentes es que los peligros subyacentes a los que están vinculados tienden a no ocurrir al mismo tiempo que otros eventos que afectan a los mercados de crédito y valores, ofreciendo a los inversores beneficios de diversificación. En contraste, los efectos de un ciberataque generalizado podrían, entre otros, afectar al valor de inversiones en los mercados de valores y de bonos.

La disposición para absorber riesgo de base también podría obstaculizar el desarrollo de valores ILS relacionados con la cibernética.

Un segundo factor que podría frenar los ILS para riesgos cibernéticos es el riesgo de base potencial: la diferencia entre las pérdidas reales del patrocinador y el pago de seguridad para un evento cubierto. Los patrocinadores de ILS normalmente quieren una cobertura lo más amplia posible de modo que puedan recuperar toda la gama de pérdidas en las que puedan incurrir. Sin embargo, los inversores a menudo quieren valores cuya liquidación sea desencadenada por métricas observables y bien definidas, porque esto reduce el potencial de selección adversa y riesgo moral (p. ej., menos motivación para limitar pérdidas) y además disminuye sus costes a la hora de evaluar suscripción y resultados económicos de una empresa. Estas

[111] En mayo de 2016, Credit Suisse emitió el primer ILS relacionado con riesgo operativo. De modo similar a un bono de catástrofe tradicional, la titulización permite al banco suizo transferir a inversores del mercado de capitales el riesgo de pérdidas extremas resultantes de procesos empresariales fallidos o inadecuados. Los valores proporcionan cobertura de amplio rango que incluye algunas exposiciones al riesgo cibernético, como un fallo del sistema TI que causa LC, así como fallos operativos más convencionales vinculados a, por ejemplo, actividad no autorizada, errores de contabilidad, errores de documentación y cumplimiento normativo. Véase «Credit Suisse Sells Operational Risk Bonds, Insuring Rogue Trading, Cyber Crime», *insurancejournal.com,* 27 de mayo de 2016, http://www.insurancejournal.com/news/international/2016/05/27/410088.htm

[112] R. Amaral, «Cyber Risks and ILS», *riskandinsurance.com,* 15 de octubre de 2016, http://www.riskandinsurance.com/cyber-risks-ils/

diferencias en las preferencias a menudo dificultan la formación de un mercado de transferencia de riesgos profundo y líquido, especialmente cuando la comprensión de los riesgos subyacentes sigue siendo incipiente.

Sin embargo, la experiencia de los bonos de catástrofes naturales sugiere que la innovación de producto puede alentar la transferencia de riesgos cibernéticos a mercados de capitales.

Sin embargo, la experiencia del mercado de bonos de catástrofes naturales sugiere que con el tiempo la innovación puede ayudar a alinear oferta y demanda de ciberprotección mediante vehículos del mercado de capitales. Ahora existe una gran variedad de bonos de catástrofe con desencadenantes basados en indemnizaciones donde los pagos están vinculados a las pérdidas reales incurridas. La mayor normalización de las ciberamenazas puede ayudar a definir riesgos impulsados por eventos con resultados binarios en un periodo de tiempo definido, y esto podría estimular el interés del inversor. Por ejemplo, algunos defensores de ILS sugieren un desencadenante basado en volumen de datos entrante, y el tiempo que dura una interrupción podría ser una manera sencilla de estimar el impacto de un ataque DDoS, aunque sería necesario asegurarse de que no pueda manipularse el mecanismo desencadenante[113]. También podrían reducirse las preocupaciones sobre riesgo de base si un mayor intercambio de información conduce a la correspondiente claridad en las condiciones, límites y exclusiones de la cobertura. Al mismo tiempo, los patrocinadores podrían sentirse más cómodos con indemnización de pérdidas no plena si eso da lugar a pagos más puntuales o les da mayor control sobre la divulgación de información relativa a sus vulnerabilidades cibernéticas.

Apoyo gubernamental

La intervención gubernamental puede fomentar una mejor resiliencia cibernética.

En la medida en que las empresas invierten colectivamente en ciberseguridad socialmente subóptima y/o hay fricciones inherentes que impiden el ciberseguro y otros mecanismos de transferencia de riesgos, los gobiernos tienen una función importante que desempeñar a la hora de promover resiliencia cibernética[114]. Al remodelar incentivos y aumentar la concienciación sobre las ciberamenazas, los gobiernos podrían conducir al sector privado hacia mejores soluciones impulsadas por el mercado. Destacan dos áreas en particular: obtención y divulgación de información sobre ciberamenazas y pérdidas y establecimiento del marco jurídico.

Coordinación y divulgación de información

Varios gobiernos han creado foros para intercambiar información sobre ciberamenazas en evolución y su impacto.

Varios gobiernos han puesto en marcha o están creando foros que facilitan a las empresas el intercambio de bases de datos, métodos, herramientas analíticas y modelos para promover buenas prácticas. Estos complementan iniciativas impulsadas por el sector privado para compartir información sobre amenazas emergentes (p. ej., a través del Financial Services Information Sharing and Analysis Center, un vehículo clave para que la industria financiera global comparta información de amenazas físicas y cibernéticas)[115]. Estas plataformas de intercambio de datos comunes en toda la industria ayudan a incrementar la preparación y conciencia del riesgo cibernético. También son un primer paso para mejorar la resiliencia cibernética (véase la Tabla 3). De forma anónima y sujeta al uso acordado, la información incrementará las posibilidades de modelización de riesgo y

[113] «Could the capital markets solve the $1B cyber insurance policy gap?», *artemis.bm,* 23 de marzo de 2015, http://www.artemis.bm/blog/2015/03/23/could-the-capital-markets-solve-the-1b-cyber-insurance-policy-gap/

[114] La interconexión de ciberespacio significa que si una empresa adopta medidas de ciberseguridad, la comunidad entera se beneficia, ya que se minimizan las infecciones que surgen de esta empresa. Igualmente, el no adoptar medidas de seguridad puede tener importantes efectos negativos sobre otros usuarios.

[115] Visite el sitio web del Financial Services Information Sharing and Analysis Center en https://www.fsisac.com/

ayudará a los suscriptores a comprender mejor la exposición individual y agregada, lo que conduce a un seguro más adecuado al riesgo (es decir, precios más baratos para las empresas más resilientes y aumento de la cantidad de capacidad de cobertura cibernética disponible)[116].

Tabla 3:
Programas de colaboración de información cibernética privados e impulsados por el gobierno

País	Iniciativa	Objetivo
Reino Unido	Cyber Security Information Sharing Partnership (CiSP)	Iniciativa colaborativa entre industria y gobierno para compartir información de amenazas cibernéticas y vulnerabilidad. El foro ha sido creado para captar amenazas cibernéticas emergentes y tendencias mientras se protege la confidencialidad de datos de la aseguradora individual y del asegurado.
Suiza	The Reporting and Analysis Centre for Information Assurance (MELANI)	Colaboración público-privada para recopilar y compartir información sobre amenazas de seguridad a sistemas informáticos, Internet e infraestructuras nacionales críticas. El sitio web de MELANI está abierto a usuarios privados de ordenadores domésticos e Internet, así como a pequeñas y medianas empresas (PYME) de Suiza.
EE. UU.	Ciberseguridad Information Sharing Act (CISA); Cyber Threat Intelligence Integration Center (CTIIC); Information Sharing and Analysis Centers (ISACs)	CISA proporciona incentivos, incluyendo protección de responsabilidad, a empresas para compartir información sobre violaciones de seguridad entre sí y con el gobierno. También posibilita que el gobierno federal comparta datos sin clasificar con otras agencias, negocios y el público. CTIIC coordina y analiza información relacionada con amenazas e incidentes cibernéticos. ISACs son entidades de confianza establecidas por propietarios y operadores de infraestructuras críticas para promover el intercambio de información y las buenas prácticas relativas a amenazas físicas y cibernéticas y a su mitigación.
Finlandia	Finnish communications regulatory activity authority (FICORA)	Una de las principales funciones de FICORA es divulgar información sobre ciberseguridad.
Países Bajos	Nationaal Cyber Security Centrum (NCSC)	NCSC es el facilitador de varios Information Sharing and Analysis Centres (ISAC), que están establecidos por sector (p. ej., agua, telecomunicaciones, nuclear, etc.). Cada ISAC está compuesto por miembros relacionados con el sector y tiene un presidente. NCSC fomenta encuentros entre los presidentes de diversos ISAC para el intercambio de información entre sectores.
Alemania	Kooperation zwischen Betreibern Kritischer Infrastrukturen (UP KRITIS)	Una iniciativa conjunta de la Oficina Federal de Protección Civil y Asistencia en Desastres (BBK) y la Oficina Federal de Seguridad de la Información (BSI). Su objetivo es facilitar la cooperación entre industrias para mantener el suministro de servicios de infraestructuras críticas en Alemania.
Bélgica	Cyber Threat Intelligence Research Project (CTISRP)	Lanzado por Deloitte Belgium en 2013 para empresas públicas y privadas de Europa para debatir el intercambio de información de ciberamenazas. Los miembros proceden de 13 sectores diferentes y se reúnen varias veces al año.

Fuente: Swiss Re Economic Research & Consulting, diversas fuentes públicas.

[116] Al desarrollar el producto de violación de privacidad para el mercado estadounidense, las aseguradoras se beneficiaron de la disponibilidad de una base de datos que compilaba todas las violaciones de datos conocidas gracias a la ley de este país de notificación casi universal y obligatoria de violaciones.

Los gobiernos están bien posicionados para coordinar la recopilación de información dado su acceso a información clasificada.

Los gobiernos se encuentran en una posición ideal para coordinar el intercambio de información, sobre todo porque tienen acceso a información clasificada, incluyendo información obtenida a través de redes y organismos supranacionales. Por ejemplo, el gobierno de Reino Unido ha puesto en marcha el Cyber Security Information Sharing Partnership (CiSP) y trata de colaborar con el sector privado para que este tipo de datos sea más accesible y útil para las aseguradoras. Sin embargo, algunas empresas se muestran inquietas por la coordinación de la información cibernética impulsada por el gobierno ya que podría crear vulnerabilidades de seguridad adicionales. Casi dos tercios de las empresas preguntadas en la encuesta realizada por Swiss Re-IBM indicaron que las acciones del gobierno pueden incrementar los riesgos cibernéticos, lo que podría reflejar la preocupación respecto a que la información pueda filtrarse o utilizarse incorrectamente.

También pueden respaldar el desarrollo de normas de ciberseguridad que faciliten la evaluación de riesgos.

Junto con el intercambio de información, los gobiernos pueden ser decisivos a la hora de desarrollar normas detalladas para promover sistemas TI altamente seguros. El cumplimiento de acuerdos de buenas prácticas puede a su vez ayudar a las aseguradoras a determinar la fortaleza de los controles internos de las empresas y evaluar mejor su resiliencia relativa contra riesgos cibernéticos. El marco del Instituto Nacional de Normas y Tecnología (NIST) en EE. UU. y la norma 27001 de la Organización Internacional de Normalización (ISO) facilitan a las empresas herramientas para evaluar e incrementar su propia ciberseguridad. Este enfoque basado en principios es probablemente más flexible que un régimen estricto basado en normas a la hora de adaptarse al panorama dinámico del riesgo cibernético. La obtención de certificación de seguridad, por ejemplo para ISO 27001, también puede incrementar los niveles de confort de las aseguradoras a la hora de ofrecer ciberseguro.

Marco legal

Algunos argumentan que el ciberseguro debería ser obligatorio.

Al elaborar leyes y reglamentos, los gobiernos tienen una influencia importante sobre cómo se utiliza y protege el ciberespacio. Algunos analistas van tan lejos como para sugerir que la compra de ciberseguro debería ser obligatoria, al menos para responsabilidad civil frente a terceros y algunas industrias clave con alto riesgo de ataques[117]. Este punto de vista se refleja en la evidencia de las encuestas, que revelan que más de tres cuartas partes de los encuestados, aseguradoras y no aseguradoras, sugieren que el ciberseguro debería ser obligatorio para algunos sectores, especialmente aerolíneas y servicios financieros[118].

Aunque a otros les preocupa que la cobertura obligatoria pueda ser administrativamente costosa y fomente el riesgo moral.

Los defensores de la cobertura obligatoria argumentan que alentaría a las empresas a invertir en ciberseguridad para ampliar el consorcio de seguros y reducir las primas asociadas. Al mismo tiempo, los detractores subrayan que aplicar este régimen, de no ser imposible, sería administrativamente complicado. Además, a algunos les preocupa que pueda crear riesgo moral, y que las empresas confíen en su seguro en lugar de invertir en mayor seguridad. Obligar a las aseguradoras a que compren ciberseguros de la competencia también podría plantear interrogantes sobre la eficacia y la integridad del mercado.

[117] Véase «Cyber-insurance: Is it necessary? Should be mandatory?», *techtalkgfi.com,* 4 de diciembre de 2014, http://www.gfi.com/blog/cyber-insurance-is-it-necessary-should-it-be-mandatory/

[118] Swiss Re/IBM, 2016, *op. cit.*

Otras iniciativas legales como límites reglamentarios de responsabilidad pueden estimular la penetración del ciberseguro.

Otras iniciativas políticas podrían ser de ayuda para aumentar la penetración del ciberseguro, como lo han sido en otros ramos. En particular, el hecho de proporcionar un medio para que las empresas pongan un límite a su responsabilidad jurídica si mantienen medidas de seguridad reforzadas podría alentar a las aseguradoras a ofrecer mejores términos y condiciones, haciendo más asequible el ciberseguro. Análogamente, en los EE. UU., según la SAFETY Act (Ley de seguridad) adoptada a raíz del ataque del 11 de septiembre, las empresas pueden limitar los daños legales resultantes de un fallo de una tecnología antiterrorismo particular si ha sido aprobada por el Departamento de Seguridad Nacional (DHS)[119]. Los corredores de seguros tienden a creer que medidas gubernamentales similares, incluyendo bonificaciones fiscales sobre primas, un depósito de datos de incidentes cibernéticos y directrices formales para salvaguardar información, podrían ayudar a respaldar la disponibilidad de sistemas de cobertura cibernética[120]. La legislación también puede ayudar a eliminar algunas de las incertidumbres legales sobre la responsabilidad potencial que podría resultar de compartir información de amenazas cibernéticas[121].

Los gobiernos también podrían facilitar el establecimiento de consorcios de seguros para cubrir riesgos cibernéticos.

Los gobiernos también pueden ser decisivos a la hora de establecer consorcios de seguros que permitan a las re/aseguradoras privadas compartir exposiciones a un peligro particular y suscribir riesgos entre sí. La asegurabilidad de algunos riesgos cibernéticos puede mejorarse si se agrupan los riesgos de los participantes del mercado, sobre todo debido a los beneficios de diversificación que podrían conseguirse[122]. La implicación del sector público puede facilitar la colaboración y el intercambio de información entre participantes del mercado y asumir potencialmente algunos de los costes de administración. Los consorcios de seguros patrocinados por el gobierno también pueden garantizar que ningún acuerdo de consorcio contravenga ninguna ley aplicable sobre competencia.

[119] La SAFETY Act exige que el DHS establezca el límite de responsabilidad para cada solicitante basándose en la cantidad de seguro disponible y la carga de comprar cobertura hasta ese límite.

[120] CIAB, *op. cit.*

[121] Esto es cierto, por ejemplo, con la ley estadounidense Cybersecurity Information Sharing Act CISA. Véase también A. Nolan, *Cyber Security and Information Sharing: Legal Challenges and Solutions,* Congressional Research Service, marzo de 2015.

[122] M. Eling y J. H. Wirfs, *Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class,* Institute of Insurance Economics, University of St. Gallen en colaboración con Swiss Re, marzo de 2016.

Conclusión

Está aumentando la concienciación sobre el riesgo cibernético aunque esta todavía tiene que traducirse en una gestión de riesgos institucionalizada.

El riesgo cibernético es una preocupación creciente para las empresas. Recientes ataques cibernéticos de gran repercusión han puesto de relieve las amenazas que plantean las violaciones de seguridad y lo mal preparadas que están algunas empresas para abordar este tipo de eventos. Además, los costes de una violación cibernética ya no se limitan a hacer frente a las consecuencias de la corrupción o pérdida de datos, sino que cada vez más incluyen daños potenciales a la reputación y los bienes físicos de una empresa, así como la perturbación de las operaciones empresariales habituales. Sin embargo, hasta el momento relativamente pocas empresas han implementado mejoras generalizadas en las prácticas generales de gestión de riesgos y ciberdefensa.

Las empresas necesitan aumentar la inversión en sus ciberdefensas, especialmente dado el mayor control normativo.

La regulación también podría ser un catalizador para el cambio. En muchas jurisdicciones se está desarrollando abundante legislación que obligará a las empresas a introducir mayores medidas de protección para la información privada de sus clientes o se enfrentarán a sanciones si no cumplen totalmente las normas exigidas. Pero las empresas no se pueden permitir esperar a que se produzcan cambios en las leyes: es necesaria ya una mayor inversión en arquitectura de ciberseguridad para desarrollar sólidas capacidades y procedimientos de gestión de riesgos antes y después de pérdidas. Esto se aplica tanto a grandes como a pequeñas empresas, siendo estas últimas objetivo cada vez mayor de los *hackers*.

Se está desarrollando seguro y mecanismos de transferencia de riesgos alternativos.

La transferencia de riesgos relacionados con la cibernética a aseguradoras e inversores del mercado de capitales se convertirá cada vez más en una solución viable, particularmente aquellos vinculados a fallos en higiene cibernética rutinaria como el mantenimiento de la integridad del cliente y la seguridad de red. Se está desarrollando ciberseguro especializado y muchas aseguradoras pretenden innovar y ampliar las pólizas cibernéticas para cubrir pérdidas más allá de las violaciones de privacidad de datos. Asimismo, están naciendo iniciativas para desarrollar valores vinculados al seguro que cubren riesgos de tipo operativo como el cibernético, aunque deben superarse importantes obstáculos para que se generalicen estos mecanismos de transferencia de riesgos alternativos.

Pero se necesita más innovación para controlar y cuantificar riesgos cibernéticos.

Resulta difícil comprender y cuantificar los riesgos cibernéticos, especialmente dado el potencial de pérdidas que se puede acumular. Son necesarias nuevas formas de pensar para calibrar los riesgos cibernéticos, determinar qué datos son más necesarios para la elaboración de los análisis actuariales y cómo pueden recopilarse estos datos y hacer que estén disponibles de modo que proporcionen suficiente confianza en su fiabilidad. Las aseguradoras están tratando de desarrollar marcos de medición y métricas que sean lo bastante flexibles como para tener en cuenta rápidos cambios en el entorno tecnológico y empresarial, aunque son necesarios mayores avances. Del mismo modo, las empresas están empezando a encontrarse más cómodas compartiendo información, lo que será crucial si las aseguradoras desean hacer un mejor trabajo evaluando y suscribiendo los riesgos.

Mediante la cooperación, aseguradoras y asegurados pueden ampliar la asegurabilidad, pero algunos riesgos cibernéticos no son asegurables y a la larga puede que se necesite un respaldo financiero del gobierno.

Para crear un mercado viable de ciberseguro privado, los asegurados y sus aseguradoras deberán cooperar para crear productos sostenibles. El gobierno también tiene una función importante que desempeñar a la hora de promover la obtención y difusión de información sobre ciberamenazas, y establecer el marco legal correspondiente. Sin embargo, puede que a la larga algunos riesgos cibernéticos, especialmente aquellos relacionados con eventos de pérdidas catastróficas extremas como una perturbación en redes o infraestructuras críticas, no sean asegurables. La ambigüedad respecto a la probabilidad de un evento de pérdidas y/o su magnitud junto con el potencial de pérdidas acumuladas significativas supone que existen límites naturales sobre la capacidad de absorción de riesgo de inversores y aseguradoras privadas.

Recientes publicaciones *sigma*

2017	N.º 1	Cibernética: cómo enfrentarse a un riesgo complejo
2016	N.º 1	Catástrofes naturales y siniestros antropógenos en 2015: Asia sufre cuantiosos daños
	N.º 2	Asegurando los mercados frontera
	N.º 3	El seguro mundial en 2015: crecimiento sostenido en un escenario de disparidades regionales
	N.º 4	El seguro mutuo en el siglo XXI: ¿regreso al futuro?
	N.º 5	Seguro y reaseguro estratégico: la tendencia creciente hacia soluciones personalizadas
2015	N.º 1	El seguro puede ayudar a mantener la salud en los mercados emergentes
	N.º 2	Catástrofes naturales y siniestros antropógenos en 2014: las tormentas invernales y las tormentas convectivas generan la mayoría de daños
	N.º 3	Fusiones y adquisiciones en el seguro: ¿comienza una nueva oleada?
	N.º 4	El seguro mundial en 2014: vuelta a la vida
	N.º 5	Infraseguros de riesgos de daños: cerrando la brecha
	N.º 6	El seguro de vida en la era digital: se avecina una transformación fundamental
2014	N.º 1	Catástrofes naturales y siniestros antropógenos en 2013: Grandes daños causados por inundaciones y granizo; el tifón Haiyan azota Filipinas
	N.º 2	Distribución digital en el seguro: una revolución silenciosa
	N.º 3	El seguro mundial en 2013: camino a la recuperación
	N.º 4	Tendencias de crecimiento de los siniestros de responsabilidad civil: riesgos emergentes y repunte de los factores económicos
	N.º 5	¿ Quién nos cuidará ? A la búsqueda de soluciones sostenibles de cuidados a largo plazo para un mundo que está envejeciendo
2013	N.º 1	Por un objetivo común: la seguridad alimentaria en los mercados emergentes
	N.º 2	Catástrofes de la naturaleza y grandes siniestros antropógenos en 2012: un año de fenómenos meteorológicos extremos en Estados Unidos
	N.º 3	El seguro mundial en 2012: Recorriendo el largo y difícil camino hacia la recuperación
	N.º 4	Navegando por los últimos avances en el seguro marítimo y aerocomercial
	N.º 5	Urbanización en los mercados emergentes: ventajas e inconvenientes para las aseguradoras
	N.º 6	Seguro de vida: enfoque hacia el consumidor
2012	N.º 1	La rentabilidad en el seguro de vida
	N.º 2	Catástrofes de la naturaleza y grandes siniestros antropógenos en 2011: pérdidas históricas a consecuencia de terremotos e inundaciones sin precedentes
	N.º 3	El seguro mundial en 2011: el ramo no-vida se prepara para el despegue
	N.º 4	Haciendo frente al desafío de los tipos de interés
	N.º 5	El seguro comercial: un mercado en constante evolución
	N.º 6	Reforma contable del sector asegurador: ¿ un vaso medio lleno o medio vacío ?
2011	N.º 1	Catástrofes de la naturaleza y grandes siniestros antropógenos en 2010: un año de eventos devastadores y costosos
	N.º 2	El seguro mundial en 2010: las primas vuelven a la senda del crecimiento – aumenta la base de capital
	N.º 3	La participación del Estado en los mercados aseguradores
	N.º 4	Innovación de productos en los mercados aseguradores no-vida: innovaciones a pequeña y gran escala
	N.º 5	El seguro en los mercados emergentes: motores del crecimiento y la rentabilidad
2010	N.º 1	Catástrofes de la naturaleza y grandes siniestros antropógenos en 2009: menos víctimas y reducción de los daños asegurados
	N.º 2	El seguro mundial en 2009: las primas descendieron ligeramente pero mejoró la base de capital del sector
	N.º 3	Desafíos regulatorios en materia de seguros
	N.º 4	El impacto de la inflación en las aseguradoras

Editado por:
Swiss Re Ltd
Economic Research & Consulting
Apartado postal
8022 Zúrich
Suiza

Teléfono +41 43 285 2551
Fax +41 43 282 0075
Correo electrónico: sigma@swissre.com

Oficina Armonk:
175 King Street
Armonk, NY 10504

Teléfono +1 914 828 8000

Oficina Hong Kong:
18 Harbour Road, Wanchai
Central Plaza, 61st Floor
Hong Kong, SAR

Teléfono + 852 25 82 5644

Autores:
Darren Pain
Teléfono +41 43 285 2504

Jonathan Anchen
Teléfono +1 91 80 4900 2650

Redactor de *sigma*:
Paul Ronke
Teléfono +41 43 285 2660

Redactor jefe:
Kurt Karl, Director de Economic Research & Consulting, responsable de la publicación *sigma*.

Explore y visualice los datos de *sigma* sobre catástrofes naturales y los mercados mundiales del seguro en www.sigma-explorer.com.

El número se cerró el 24 de enero de 2017.

sigma se publica en inglés (idioma original), alemán, francés, español, chino y japonés.

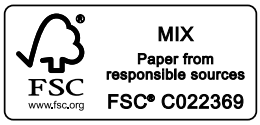
sigma se encuentra disponible en el servidor de Swiss Re:
www.swissre.com/sigma

La versión publicada en Internet puede contener información ligeramente más actual.

Traducciones:
Alemán: Diction AG
Francés: ithaxa communication SARL
Español: Traductores Asociados Valencia S.L.

Diseño gráfico y producción:
Corporate Real Estate & Services / Media Production, Swiss Re, Zúrich

Impresión: Multicolor Print AG, Baar



Pedido n.º: 270_0117_es

Swiss Re Ltd
Economic Research & Consulting
Apartado de correos
8022 Zúrich
Suiza

Teléfono +41 43 285 2551
Fax +41 43 282 0075
sigma@swissre.com
www.swissre.com