Revista de Pensamiento Estratégico y Seguridad CISDE

CISDE Journal, 3(1), 2018

Recibido: 12-03-2018 / Revisado: 01-05-2018
Aceptado: 01-05-2018 / Publicado: 30-05-2018

La transferencia de los riesgos cibernéticos en empresas internacionales con alto nivel de capitalización bursátil

The transfer of cyber risks in international companies with a high level of market capitalization

Félix Jiménez Naharro[1], Carmen Sánchez Montañés[2], Mariano Sánchez Barrios[1]

[1] Universidad de Sevilla, España.
[2] UNED, España.

fjimenez@us.es , menchu0001@hotmail.com , msanchez@us.es

RESUMEN. *"La ciberseguridad se ha instalado en nuestras vidas y está aquí para quedarse", "Como Estado estamos obligados a disponer de un sistema de ciberseguridad que gestione con eficacia los riesgos y sólo es posible con la colaboración del sector privado, de todos los ciudadanos y de organismos internacionales".* Así se expresaba la embajadora en misión especial para la Ciberseguridad del Ministerio de Asuntos Exteriores y Cooperación durante la inauguración de la Jornada Empresarial Ciberseguridad: Las empresas frente al incremento de ciberataques. España no es ajena a estas circunstancias y registró en el año 2017 el mayor número de ciberataques de su historia. Por otro lado, la ciberseguridad es un tema incluido en la Estrategia de Seguridad Nacional, aprobado por el Gobierno el día 1 de diciembre de 2017. El Consejo de Seguridad ha sido el órgano responsable de su elaboración.
El Instituto Nacional de Ciberseguridad gestionará 135.000 ciberataques. Además, en base a los datos de la citada Institución, el cibercrimen *"es un negocio muy lucrativo"* que podría mover entre el 0,1 por ciento del PIB y un billón de euros. En el ámbito empresarial, Telefónica es la empresa en el Ibex-35 más implicada en la ciberseguridad, como se puede observar en los últimos informes anuales. El objetivo del artículo es la valoración de los intangibles para la ciberseguridad en la nueva economía con especial énfasis el ciberseguro.

ABSTRACT. "Cybersecurity has been installed in our lives and is here to stay", "As a State we are obliged to have a cybersecurity system that effectively manages the risks and is only possible with the collaboration of the private sector, of all citizens and of international organizations ". This is how the ambassador expressed her special mission for the Cybersecurity of the Ministry of Foreign Affairs and Cooperation during the inauguration of the Cybersecurity Business Conference: Companies facing the increase in cyberattacks. Spain is not immune to these circumstances and will register in 2017 the largest number of cyberattacks in its history. On the other hand, cybersecurity is a subject included in the National Security Strategy, approved by the Government on December 1, 2017. The Security Council has been the body responsible for its preparation.
The National Cybersecurity Institute will manage 135,000 cyberattacks. In addition, based on the data of the aforementioned Institution, cybercrime "is a very lucrative business" that could move between 0.1 percent of GDP and one billion euros. In the business field, Telefónica is the company in the Ibex-35 most involved in cybersecurity, as can be seen in the latest annual reports. The objective of the article is the valuation of intangibles for cybersecurity in the new economy, we want to pay special attention aboutcybersecurity.

PALABRAS CLAVE: Ciberseguros, Ciberseguridad, Criptografía, Criptología, Criptomonedas, Intangibles, Criptoactivos.

KEYWORDS: Cibersecurity, Cryptography, Criptology, Cryptocurrencies, Intangible, Criptoactive.

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

1. Introducción

El cifrado de mensajes se lleva practicando desde hace muchos años y el origen de este término es del griego clásico que significa "escritura oculta". Una comunicación está cifrada cuando emisor y receptor son capaces de extraer la información del mensaje; por tanto, para cualquier persona fuera de este circuito la información le quedará totalmente oculta. El único objetivo de la criptografía es conseguir la confidencialidad de los mensajes para lo cual se diseñan sistemas de cifrados y códigos. La aparición de la informática y el uso masivo de las comunicaciones digitales, han producido un número creciente de problemas de seguridad. Los grandes avances que se han producido en el mundo de la criptografía, han sido posible gracias a los grandes avances que se han producido en el campo de las matemáticas e informática.

La criptografía se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican (diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de seguridad a los agentes autorizados del circuito emisor-receptor). Entre sus propiedades: confidencialidad, integridad, vinculación, autenticación.

Se están logrando avances en este tema en el Consejo Superior de Investigaciones Científicas en el área de la criptografía cuántica. La Distribución Cuántica de Clave, en inglés Quantum Key Distribution (QKD) es el único método de transmisión de claves criptográficas de forma incondicionalmente segura, al estar garantizadas por leyes físicas.

No existe una escala para medir el impacto de los ataques cibernéticos. Sin embargo, WannaCry[1] (2018) impactó sobre el ciberespacio a nivel mundial de tal manera que consiguió extender el miedo entre todas las empresas, este hecho provocó un incremento de la demanda de pólizas de seguros por parte de las empresas. Los delitos que emergen de los usuarios de las nuevas tecnologías afectan a empresas y particulares. Esta problemática es latente, como señala la memoria de 2016 de la Unidad de Criminalidad Informática de la Fiscalía General del Estado. En España se incoaron 18.344 procedimientos por estafas a través de la Red, 272 procedimientos por descubrimiento de secretos empresariales, 295 por daños informáticos, 68 por delitos contra la propiedad industrial y 144 por falsificación a través de las TIC. Este tipo de delitos genera un gasto a las pymes entre 20.000 y 50.000 euros.

La aplicación del Reglamento General de Protección de Datos[2] que comenzará a aplicarse el 25 de mayo de 2018 puede conlleva rmultas de hasta 20 millones de euros o el 4% de la facturación de una compañía que incumpla la normativa.

Siguiendo a Ferré, X.[3], socio responsable de ciberseguridad de EY en Barcelona, en Estados Unidos la cobertura de este tipo de siniestros está mucho más avanzada porque las compañías "tienen históricos de datos para confeccionar las pólizas". Estas cubren una amplísima gama de riesgos que se pueden englobar en dos grandes grupos: daños propios y daños a terceros, sin olvidar los daños que pueda sufrir la propiedad industrial o las violaciones de secretos comerciales (onemagazine.es, 2018). Un documento interno de Zurich, prevé que para 2020 el mundo pasará a tener 50 millones de aparatos conectados, lo que multiplicará las amenazas.

Un gran problema de las empresas hoy es la seguridad de la información y más concretamente la ciberseguridad.

Desde finales de los 90 hasta la actualidad el mundo empresarial y los mercados financieros han sufrido una serie de cambios y transformaciones que han hecho que aparezcan nuevos riesgos y, a su vez, muchas oportunidades. Así la empresa se ha convertido en más dinámica y flexible buscando una adaptación al nuevo entorno que aún hoy se está construyendo.

[1] Ataque informático que usa el criptogusano wannacry dirigido al sistema operativo.

[2] El nuevo Reglamento de Protección de Datos entró en vigor en mayo de 2016 y será aplicable en mayo de 2018.

[3] Ferre Cabre, X.,Partner en Ernst & Young.

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

Entre los cambios más significativos podemos destacar:

- Hemos pasado de un modelo de negocio tradicional a un modelo de negocio innovador, donde la tecnología ha creado muchas oportunidades. Entre las tecnologías más disruptivas podemos destacar: Inteligencia Artificial, Internet de las Cosas, Fabricación Digital, Robótica, Blockchain, Vehículos aéreos no tripulados y Realidad Virtual y aumentada, entre otras. Las tecnologías apuntadas han dado paso a nuevos modelos de negocio que están cambiando la economía, nuestras expectativas y nuestro comportamiento. Este proceso responde a una dinámica clara, a una estructura que se ha dado a lo largo de todas las olas tecnológicas y que sigue un proceso que empieza con: (1) un avance científico, (2) que se materializa en una nueva tecnología, (3) que llega al mundo de los negocios, (4) y cambia la organización económica y/o social.

Hay una gran variedad de modelos de negocio disruptivos que están surgiendo, pero por su relevancia e impacto, vamos a resumirlos en cuatro bloques: los derivados de la transformación digital de las empresas, la economía de plataformas, el modelo descentralizado y la economía pop-up y de mercados superfluidos.

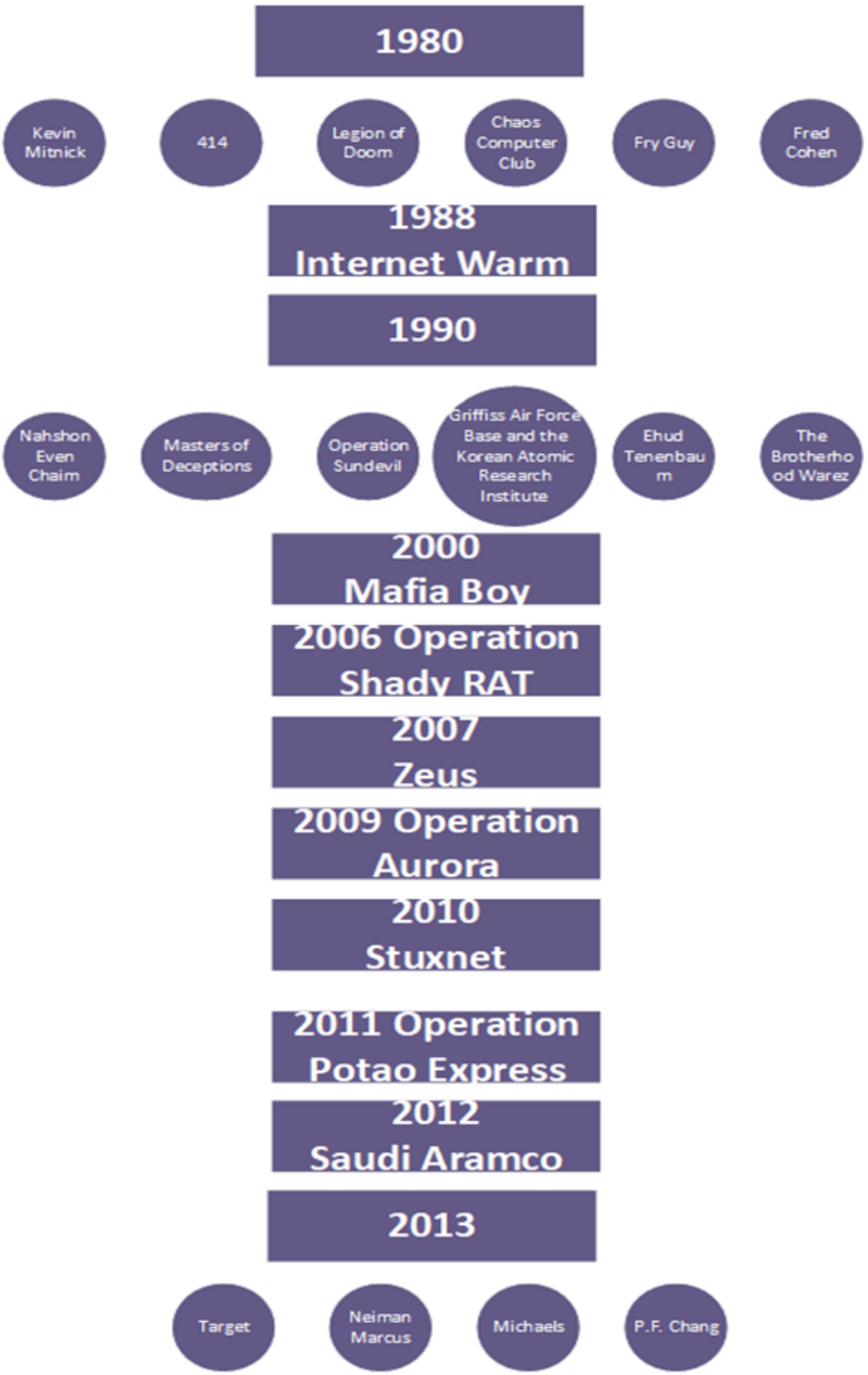
- Hemos pasado de depender de un mercado nacional a un mercado internacional.
- Hemos pasado de una empresa donde la fuente de valor estaba en los activos tangibles a una empresa donde los activos intangibles han tomado una gran importancia.

Es por ello que activos como patentes, licencias, marcas, base de datos, aplicaciones y cualquier otro know-how se convierta en la principal fuente de valor de cualquier empresa. Este conocimiento o activo intangible es el que abre un abanico de oportunidades y recursos que le permite a la empresa acceder tanto al mercado actual como otros que se abren continuamente.

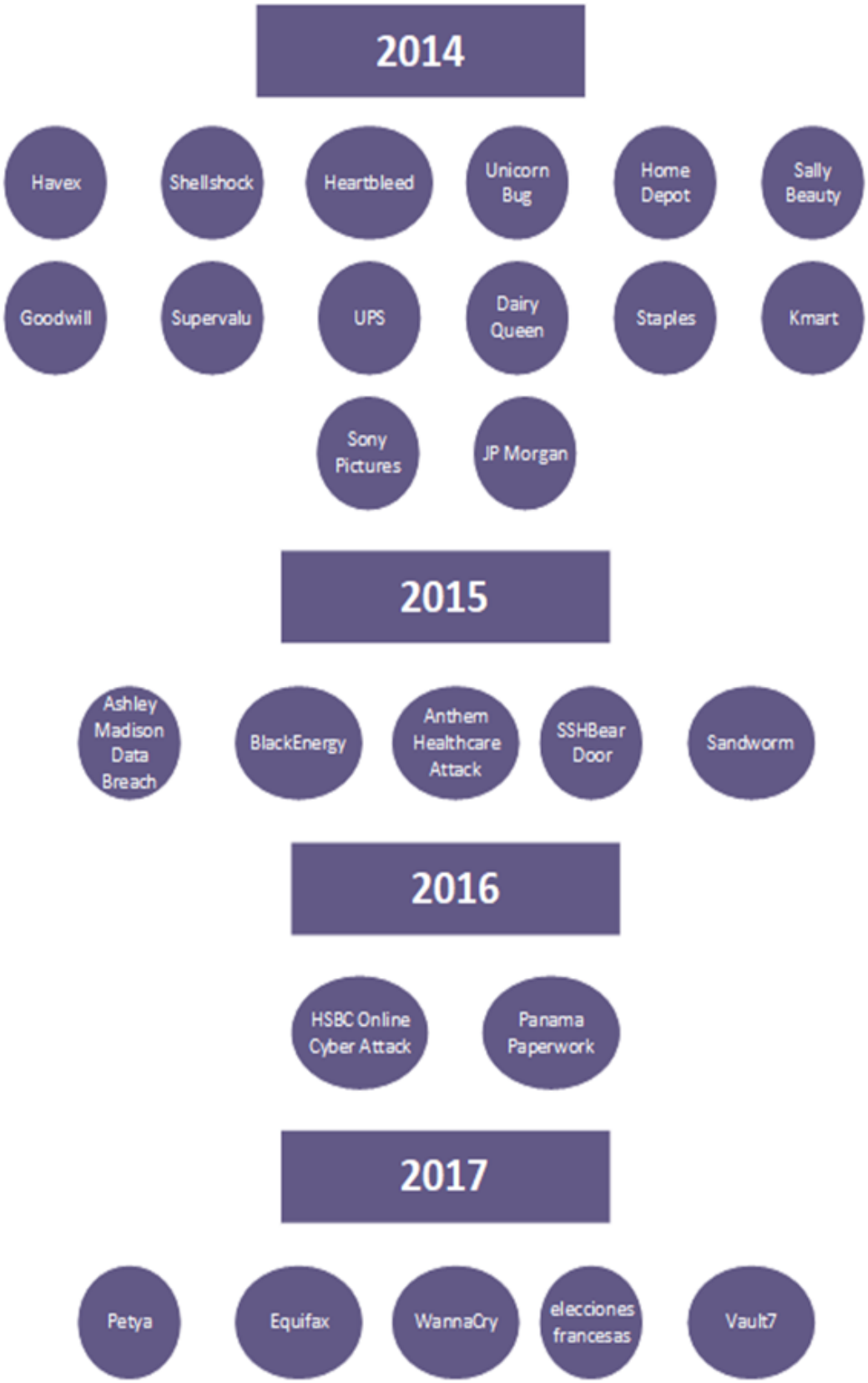
No obstante, este mundo de oportunidades no está exento de riesgos , muchos de ellos derivados del desarrollo tecnológico que propicia la capacidad a algunos de adueñarse de lo ajeno o, simplemente, hacer daño mediante la proliferación de virus informáticos en la red. Esto hace que sea muy importante desarrollar actividades relacionadas con la ciberseguridad y desarrollar métodos que nos permitan valorar ese conocimiento con el propósito de cuantificar las riquezas que pueden generar esas nuevas oportunidades y/o valorar lo que una empresa puede perder cuando ha sido víctima de un ciberataque (robo de una patente, de base de datos, destrucción de información, etc.).

En este contexto tecnológico, todos los activos relacionados con la información, almacenamiento de la misma y con los aspectos intangibles de la empresa y mercados tienen cada vez mayor valor, además, debido a la facilidad de movimiento, estos activos pueden dar la vuelta al mundo en un segundo a través de la red y ser almacenados en cualquier punto de la red. Esta facilidad de intercambio, almacenamiento y también de ocultación de los mismos (en una gran parte de las ocasiones son activos estratégicos para la empresa y debido a su alto nivel de confidencialidad son conocidos por pocos responsables de la empresa) hace que su atractivo para ser atacados, robados, etc. sea cada vez mucho mayor y la recompensa que se pueda obtener por conseguirlo sea muy suculenta. Es por este y otros motivos por el que en el 2016 las profesiones relacionadas con la ciberseguridad en la empresa se han convertido en una de las más demandadas y con mayor nivel de crecimiento (Acquisdata. Industry Snashoot (2017): United States Software and Information Technology. Australia).

Los principales ciberataques desde los 80 podemos verlo en la siguiente figura.



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



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

En este artículo vamos a recoger la importancia que tienen los ciberseguros en esta nueva economía ante este nuevo mapa de riesgos. Una de las dificultades que tienen los ciberseguros es la valoración de los intangibles o activos subyacentes que tienen que ser asegurados para repercutirle una prima razonable.

2. El ciberseguro. Un poco de historia

"Cuando los ciudadanos observan que las grandes corporaciones son atacadas, es difícil convencerlos de que ellos están a salvos. Las crisis de confianza son el germen de grandes crisis económicas". Evitar ataques es imposible, pero minimizar su poder destructivo no[5]. Los ciberseguros añaden confianza a las instituciones por los daños propios, ante terceros y sus empleados.

Los ciberseguros son un tipo de seguros que sirve para cubrir los daños que pueda causar un delito informático (robo de datos de clientes, proveedores, empleados, accionistas, etc.). En el caso de que una empresa sea víctima de robo de datos de terceros, o pierda datos de clientes debido a un error informático o humano se puede enfrentar a sanciones importantes estipuladas en el nuevo Reglamento Europeo de Protección de Datos Personales.

Los ciberseguros protagonizarán el gran negocio del sector asegurador en la próxima década (El Economista, 2018), en el año 2020 se calcula que las empresas gastarán unos 7.000 millones de euros.[6]

El instituto Nacional de Ciberseguridad señala que hay cuatro maneras de tratar los ciberriesgos: evitarlos, mitigarlos, aceptarlos o transferirlos. Los ciberseguros se enmarcan en el último apartado (transferirlos). Básicamente, los ciberseguros ofrecen protección frente a reclamaciones de terceros y de empleados, y ante las posibles investigaciones de la Agencia Española de Protección de Datos por incumplimiento de la legislación en esta materia.[7]

Los daños que cubren son de daños propios y daños a terceros. En el primer caso, son los derivados de la pérdida de ingresos como resultado de una vulneración de seguridad o de un ataque de denegación de servicios (ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, provocando la pérdida de conectividad con la red que causa que un servicio o un recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo de ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado. Ataques entre empresas, una de ella inunda a la otra de correos basura, provocando una ralentización general de internet. También a través de saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio. Una ampliación de este tipo de ataque es el llamado ataque de denegación de servicio distribuido, el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino. La forma más común de realizar un ataque de denegación de servicio distribuido es a través de debots[8], siendo esta técnica el ciberataque más eficaz por su sencillez tecnológica.

Los ciberriesgos que se cubren en los daños propios: la cobertura para los datos alojados en la nube; gastos de gestión y comunicación de la crisis a través de consultoras tecnológicas; asistencia técnica y gastos de investigación del siniestro, informes forenses; gastos de reparación y restauración de los datos borrados y de los equipos dañados; pagos de rescates; defensa jurídica y protección contra multa o sanciones de organismos reguladores.

[5] Santiago Carbó Valverde, 15 de mayo de 2017. El País, Opinión "Ciberataques y nueva economía": la economía colaborativa el riesgo de la candidez y la vulnerabilidad de los usuarios y el anonimato de los terroristas. Lo que ocurre con los ciberataques es que afectan a cualquier ámbito de nuestra vida.

[6] Insurance 2020 and beyond: Reaping the dividends of cyber resilience. PWC.

[7] Blog.signaturit.com "ciberseguros ante las exigencias del Reglamento General de Protección de Datos".

[8] Un bot es un programa informático que efectúa automáticamente tareas repetitivas a través de internet (rastreadores web de los motores de búsquedas de internet.

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

Los ciberriesgos que se cubren en relación conlos daños a terceros: cobertura de responsabilidad civil por pérdidas de datos de carácter personal; gastos de notificación de vulneraciones, privacidad a los dueños de los registros o a terceros que estén interesados; protección frente a reclamaciones de terceros por incumplimiento en casos de custodia de datos; difamación en medios corporativos o infección por malware; cobertura de delitos cibernéticos (estafas de phishing, suplantación de identidad, hacking telefónico, fraude electrónico y extorsión cibernética).

Además, algunas compañías aseguradoras ofrecen coberturas adicionales en sus ciberseguros para la prevención, como auditorías de seguridad, analizando el estado de protección de los sistemas e implementación de herramientas para la adecuada adaptación al Nuevo Reglamento Europeo de Protección de Datos (2018).

La base teórica de este artículo está en consonancia con el publicado por "Thiber: The cyber security Think Tank" (www.thiber.com) (Ciberseguros-Thiber, 2018). "La transferencia del ciberriesgo en España" (IEAF, 2018), patrocinado por AIG, K2Intelligence, Marsh, Minsaltby Indra, Telefónica, Partner Académico: IE Business School.

Las primeras estrategias contemporáneas de transferencia de riesgos tecnológicos vieron la luz en Estados Unidos a mediados de los noventa. Sin embargo, no fue hasta finales de la década cuando estos seguros comenzaron a comercializarse de una manera más regular al albor de los siguientes acontecimientos:

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

2.- El nacimiento de las empresas puntocom que aprovechando la financiación de los fondos de capital riesgo y una corriente especulativa favorable, explotaron nuevas formas de negocios digitales. Empresas como Amazon, Yahoo, Ebay, Altavista y Google, se convirtieron en clientes potenciales de estos productos de seguro que pretendían cubrir su negocio ante un panorama de amenazas digitales creciente.

3.- La profesionalización del cibercrimen, pasando de una práctica desarrollada por aficionados. En pocos años se produjo un importante proceso de profesionalización: actualmente los cibercriminales actúan perfectamente coordinados mediante estructuras jerarquizadas y ejecutando campañas de forma descentralizada en distintos países de forma simultánea.

4.- La promulgación en California el día uno de julio de 2003 de la SB1386 la primera ley a nivel mundial que obligaba a que cualquier agencia estatal, persona o empresa que lleve a efecto negocios en el Estado de California y queopere con datos informatizados con información de carácter personal, deberá comunicar cualquier brecha de seguridad que implique una fuga de datos, esta norma sentaba las bases del denominado Data Breach Notification, es decir, la obligatoriedad de notificar al regulador ciertos incidentes de ciberseguridad asociadas a una fuga de datos digitales.

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

Esos primeros productos de transferencia del riesgo tecnológico eran concebidos como productos financieros centrados en cubrir las pérdidas económicas asociadas a un incidente de seguridad. No obstante, dado que estos productos tenían un origen estrechamente vinculado con la normativa relativa a la notificación de fugas de información, sus coberturas eran limitadas y focalizadas en la responsabilidad civil asociada a los gastos de reclamación y responsabilidad ante terceros derivada de un fallo de seguridad de los sistemas informáticos del asegurado (Hernández & Fojón, 2016).

La falta de datos históricos de ciberincidencias, su impacto, provocado por el oscurantismo reinante y la reticencia en el sector empresarial a notificar y compartir datos sobre incidentes y amenazas, redundó en la imposibilidad de los departamentos actuariales de las aseguradoras de disponer de datos fiables para elaborar los modelos estadísticos y matemáticos necesarios para la evaluación de los ciberriesgos (fireeye.com, 2018).

Las empresas e instituciones interesadas en contratar estas pólizas de seguro deben someterse a un conjunto de procedimientos de evaluación de su madurez en seguridad de la información y seguridad informática. Ello implica revelar el estado de sus infraestructuras tecnológicas y sus políticas o procedimientos de gestión de las tecnologías de la información. Al mismo tiempo al complementar los formularios de contratación aportados por las aseguradoras, se suele subestimar el riesgo por parte del asegurado siendo además respondidos por el área de Tecnologías de la Información y no intervienen las áreas de la empresa que son sensibles a la información como activo, como las comisiones de auditoría interna y externa que forman parte del control de los consejos de administración.

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

3. El ciberseguro en la actualidad

El mercado de los ciberseguros es un mercado cada vez más establecido, con un número creciente de proveedores y una cadena de valor cada vez más madura, formado por aseguradoras, reaseguradoras, brokers y empresas de servicios. El aumento de oferta y de la competencia en el sector está, a su vez, reduciendo los precios de las pólizas. Además, existe un buen número de mercados primarios disponibles para colocar los grandes riesgos, y empresas de todos los tamaños están contratando cada vez más este tipo de productos como una compra obligatoria.

Según datos de Marsh and McLennan y Chertoff Group (2014), el mercado de los ciberseguros generó en Estados Unidos 1.000 millones de dólares en 2013, cantidad que se duplicó en 2014. El mercado europeo de ciberseguros es aún pequeño comparado con Estados Unidos, pero crece también a buen ritmo. En cualquier caso, es indiscutible que los ciberseguros son uno de los productos de más rápido crecimiento en el mercado asegurador. A medio plazo, éste alcanzará los 7.500 millones en ventas anuales en 2020.

En el caso español, este tipo de productos han sido trasladados desde los mercados norteamericano y británico principalmente. En España, los productos presentaban coberturas y estructuración similar a sus homólogos extranjeros para, paulatinamente, ir adaptándose a la realidad de las empresas españolas. Las compañías internacionales de seguros, así como los grandes brokers, debido al profundo conocimiento de estos productos, están liderando esta adaptación a las necesidades nacionales. Adicionalmente, la crisis económica en España, ha obligado a muchas empresas a internacionalizarse y a operar en otros mercados para sobrevivir, enfrentándose muchas con la necesidad de adquirir este tipo de seguros a consecuencia de cumplir con las normativas de seguridad exigidas en los mismos.

3.1. El Ciberseguro: contexto en el mercado de la seguridad y en la gestión de ciberriesgos

En el mercado privado de la ciberseguridad nacional es posible hallar la siguiente cadena de valor: Fabricantes de software y hardware, mayoristas y distribuidores actuando como canal de los fabricantes, proveedores locales de servicios especializados, consultoras, integradores de tecnologías de seguridad, proveedores de servicios de seguridad gestionada.

Dichos proveedores han establecido una carta de servicios y de productos que generalmente se suelen clasificar en soluciones o servicios de tipo de detección, prevención y reacción. Así pues, los ciberseguros

quedarían incluidos entre los servicios reactivos, orientados a la gestión directa de incidentes de ciberseguridad, cuyo objetivo es mitigar el impacto.

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

De forma general, los ciberseguros o pólizas de ciberriesgos son productos aseguradores cuyo objetivo es proveer protección ante una amplia gama de incidentes derivados de los riesgos en el ciberespacio, el uso de infraestructuras tecnológicas y las actividades desarrolladas en este entorno (Bandyopadhyay, 2012).

Un contrato de seguro ante ciberriesgos vincula y obliga legalmente a una compañía aseguradora ante la ocurrencia de determinados eventos ciber definidos contractualmente que conlleven pérdidas, pagando una cantidad especificada (reclamación/siniestro) al asegurado. En contraprestación, el tomador del seguro paga una suma fija (prima) a la compañía aseguradora.

El contrato es firmado por la compañía y el asegurado e incluye aspectos como los tipos de coberturas, límites y sublímites, exclusiones, definiciones y, en algunos casos, cómo se va a proceder a evaluar el nivel de seguridad del asegurado. Los apartados a tener en cuenta serían: indentificación del asegurador y asegurado; fecha de emisión de la póliza y período de vigencia; descripción del seguro, los riesgos cubiertos y las sumas aseguradas, la designación y el estado de los bienes que son asegurados, la especificación de la prima, forma y el lugar de pago; las causas de la resolución del contrato; el procedimiento para reclamar la indemnización en caso de siniestro; definiciones, exclusiones y desencadenantes, condiciones generales, particulares y especiales.

Sobre la base de los puntos anteriores se fijará el valor neto de la prima a pagar, su valor es altamente dependiente fundamentalmente del valor de los activos bajo amenaza del tipo de negocio, tamaño de la compañía, nivel de exposición digital, volumen de datos digitales a salvaguardar y nivel de seguridad de la organización. La falta de consenso en la definición del producto se pone de manifiesto en la heterogeneidad de denominaciones que adquieren estos productos entre la propia industria aseguradora.

Así aparecen referencias en lengua inglesa a Cyberrisk, Network Risk, Privacy Protection, Network Liability, Security & Privacy Liability, Professional Liability Privacy, Media Liability, Technology & Privacy Professional Liability o Data Privacy & Network Security con sus respectivas traducciones a nuestro idioma.

Se pone de manifiesto la gran diversidad de la oferta, ya que cada asegurador ha desarrollado el producto de seguro bajo la premisa de su comprensión de qué es lo que necesitan las empresas para mitigar los ciberriesgos, lo que implica también muy diversa terminología en cuanto a las garantías y al alcance de los riesgos cubiertos.

En consecuencia, se pueden hallar seguros enfocados a responsabilidad frente a terceros por vulneración de datos personales o violaciones de seguridad, riesgos regulatorios y gastos diversos, y otros que incorporan coberturas de daños propios y que, por lo tanto, dan cobertura a pérdida de beneficios o lucro cesante, robo y otros gastos y pérdidas relacionadas.

Se debe señalar que el fallo de seguridad no es la única causa de riesgo. Existen otros factores, como puede ser el riesgo de errores humanos, fallos técnicos o de programación, riesgos de difamación o usurpación negligente de propiedad intelectual de terceros o fallo en la cadena de suministro, que pueden ocasionar un

perjuicio financiero, interrupción del negocio o un daño de reputación.

Estas coberturas no suelen ser ofrecidas de forma estándar y hay que negociar normalmente de forma expresa su inclusión en el cuadro del seguro. Se han excluido otras causas de riesgo como pueden ser los riesgos naturales o el riesgo de incendio y explosión, que también dan lugar a los mismos perjuicios financieros, de interrupción o de daño reputacional. Este conjunto de riesgos suele estar contemplado en seguros tradicionales, pero el enfoque frente al riesgo de cada organización es muy distinto y no siempre está asegurado. Son muy distintas las necesidades de cobertura de las organizaciones.

Entre las coberturas básicas tenemos las responsabilidades frente a terceros por privacidad de datos y seguridad de redes: se da cobertura frente a reclamaciones de terceros (indemnización y gastos de defensa) por perjuicios causados a dichos terceros como consecuencia de un fallo en la privacidad de datos de carácter personal o información corporativa de terceros, o por un fallo en la seguridad (como por ejemplo, transmisión de códigos maliciosos, participación en ataques de denegación de servicios o por un impedimento de acceso a datos y sistemas como consecuencia de un virus o intrusión, entre otros).

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

Gastos de gestión de incidentes: siempre que se incurra en estos gastos mediante contratación de servicios externos:

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

Entre las garantías opcionales o complementarias, deben estar expresamente indicadas como cubiertas en las condiciones particulares del contrato e implican una prima mayor.

Entre las pérdidas pecuniarias propias:

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

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

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

Coberturas de un producto típico de ciberriesgos.[9] A modo de ejemplo podemos citar también la información en el Confidencial (2016) "CaixaBank se blinda con American International Group (AIG), la mejor aseguradora de ciberriesgo con quince años de experiencia, de los hackers con una póliza ciberriesgo ante los ataques masivos. Con tres grandes preocupaciones en la banca: los bajos tipos de interés que erosionan su negocio día a día; la presión de los supervisores para aumentar sus colchones de capital para evitar otra crisis sistémica; ataques cada vez constantes de los hackers a sus servidores, donde guardan los datos de sus millones de clientes. Otro Banco español en manos de AIG es BBVA, Banco de Santander con Zurich Insurance. Para el mismo periódico en noviembre de 2016, el Banco de Santander sufrió un ataque a sus servidores de su filial de tasación inmobiliaria, donde se guardan las bases de datos con la información hipotecaria de sus clientes. Una documentación vital para la entidad que ahora está en mano de unos hackers.

Responsabilidades y procedimientos regulatorios. Defensa, Perjuicios, Multas regulatorias: Fallo seguridad redes; protección indebida de la información/Revelado no autorizado de información confidencial (datos personales e información corporativa); investigaciones autoridades regulatorias (privacidad/seguridad); cometidos por un proveedor de datos/IT; infracción en contenido multimedia (propiedad intelectual)/contenido difamatorio.

Pérdida económica del asegurado. Pérdida de beneficios derivada de la interrupción en redes por fallo de seguridad; pérdidas de beneficios derivadas de fallos de sistemas en función del asegurador/negociación; pérdidas de beneficios contingente; daños a activos intangibles; amenazas a sistemas y datos (extorsión).

Servicios de crisis, gastos pagados a expertos. Gastos de gestión de crisis/publicidad; gastos de asesoramiento legal; gastos de investigación forense; gasto de notificación a afectados; gastos de respuesta a afectados (líneas calientes, monitorización de crédito, control de identidad; seguros de robo de identidad); paneles de servicios pre-acordados gestión de siniestros (consultores de IT, asesores legales; asesores de comunicación, consultores de crisis).

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

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

Por otra parte, en relación a la pérdida de beneficios existe la problemática asociada a las dos

[9] Fuente AON (http://www.thiber.org>ciberseguros).

aproximaciones predominantes: el enfoque americano (calcular la pérdida de beneficios hasta que se reinician las operaciones) y el enfoque de pólizas de londinenses o europeo (hasta el restablecimiento de la producción al nivel normal), así como las dificultades que normalmente encuentran las empresas para separar y cuantificar los factores que inciden en una reducción o aumento de los beneficios esperados que están directamente relacionados con el siniestro.

Pero también hay otras distinciones que son relevantes a la hora de seleccionar un producto frente a otro, como pueden ser la prestación de servicios de consultoría pre-siniestro o los servicios vinculados con la gestión de siniestros. Los servicios pre-siniestro están muy poco extendidos en España. Ello obedece a varios factores, entre los que se hallan la escasa percepción del valor que pueden aportar estos servicios a las empresas de tamaño medio o grande y, quizá también en vista del escaso interés que suscitan estos servicios, la oferta se limita de forma general a unas horas gratuitas de expertos en materia de seguridad tecnológica y algún dispositivo que combina herramientas de información de amenazas con herramientas de información.

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

Los servicios de gestión de siniestros son más habituales. Los aseguradores que prestan estos servicios ya han negociado con expertos forenses, legales y de comunicación y crisis (pudiéndose extender al establecimiento de servicios adicionales de respuesta a afectados) con proveedores de prestigio y experiencia tarifas exclusivas y los ofrecen como "paneles" dentro de las pólizas.

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

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

Exclusiones. Se pueden citar actos deshonestos y fraudulentos y deliberados del asegurado: hay que delimitar claramente cómo afecta esta exclusión a actos de empleados, cuando éstos son asegurados bajo la póliza.

Daños personales y materiales. Responsabilidades asumidas por contrato o acuerdo: las pólizas de responsabilidad civil asumen principalmente responsabilidad extracontractual y sólo responden si existiera responsabilidad en ausencia de dicho contrato o acuerdo.

Reclamaciones previas y litigios previos e incidentes que hubieran ocurrido y fueran conocidos con anterioridad a la fecha de efecto del contrato.

Infracción de secretos comerciales y patentes.

Guerra y terrorismo, a pesar de que a día de hoy existen coberturas afirmativas o expresas relacionadas con ataques ciberterroristas.

Existe otra exclusión que es la relativa a datos no declarados o mantenimiento de datos y seguridad por

debajo de lo declarado al asegurador durante el proceso de suscripción. Esta exclusión o condición causa mucha controversia, los asegurados deben tener en cuenta que la información y cuestionarios de riesgo se consideran parte inseparable del contrato, y existen pólizas en las que pueden incluso invalidar la cobertura. En consecuencia, es necesario analizar esta cláusula, proponer medidas que suavicen dicha exclusión otorgando cobertura, pero, sobre todo, ser conscientes que cualquier cambio en el riesgo debe ser declarado, ya que el asegurador también tiene derechos contractuales de analizar el riesgo durante el ciclo de vida completo de la póliza, proponiendo cambios que se ajusten al estado de riesgo en cada momento.

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

Estos sistemas tienen que interactuar con nuevas soluciones tecnológicas y aplicaciones interconectadas y, en algunos casos, con acceso a Internet. Una incidencia en uno de esos sistemas podría conllevar daños físicos, materiales, adicionalmente a los meramente financieros.

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

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

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

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

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

Sin embargo, las pequeñas y medianas empresas son ahora los objetivos comunes de los ciberdelincuentes, no porque sean lucrativas de forma individual, sino porque la automatización hace que sea fácil de atacar en masa siendo víctimas fáciles. Así pues, se puede afirmar que:

Las pequeñas y medianas empresas se enfrentan a las mismas ciberamenazas que las grandes empresas, pero con una fracción del presupuesto para hacerlas frente.

La inversión en seguridad es impulsada por la necesidad de cumplir con el marco regulatorio, como Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS), Ley Orgánica de Protección de Datos (LOPD), etc.

Las organizaciones más pequeñas carecen de la experiencia interna para gestionar sus ciberriesgos.

Aunque cada sector empresarial posee sus propios componentes, riesgos y exposición, existen sectores más sensibles que representan un mayor riesgo desde el punto de vista del análisis asegurador (gestion.pe, 2018), a saber: Instituciones financieras (incluyendo las aseguradoras), sector sanitario, tanto por el tipo de datos que manejan, así como el volumen de los mismos. No obstante, el sector financiero suele presentar un nivel de madurez de seguridad mayor; Telecomunicaciones y proveedores de servicios tecnológicos, tanto por la información gestionada, así como por los datos de terceros procesados; Sector energético y utilities en general, por el impacto de una potencial pérdida y quizá los que están en clara desventaja desde el punto de vista de medidas de seguridad preventivas en los sistemas industriales.

Las necesidades del asegurado en el ámbito de la ciberseguridad no vienen solo motivadas por el mayor uso de las tecnologías y una mayor conectividad, sino también por las obligaciones legales impuestas por los órganos regulatorios. Es el caso de las obligaciones impuestas a todos aquellos proveedores de servicios de telecomunicaciones o redes electrónicas. Desde la Directiva Marco 2002/21/CE, relativa a un marco regulador común de las redes y de los servicios de comunicaciones electrónicas, en España se traspuso a través de la ley 9/2014, ley general de Telecomunicaciones.

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

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

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

Adicionalmente, el procesamiento, almacenamiento o transmisión de datos de tarjeta de crédito por parte de las organizaciones obliga al cumplimiento del estándar de seguridad de los datos de tarjeta, PCI-DSS[10] versión 3, entre cuyos requisitos se encuentra la notificación a los titulares de tarjeta en caso de fuga de datos relativos a los mismos.

Ante la necesidad de reducir el impacto de los ciberseguros, los riesgos cibernéticos que pueden cernirse sobre las empresas pueden ser:

De carácter directo, destacando el robo de datos personales, de contraseñas o de know-how; la utilización

[10] El Estándar de Seguridad de Datos para la industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) fue desarrollado por un comité conformado por las compañías de tarjetas. Los 12 requisitos son un conjunto de controles de seguridad que las empresas están obligadas a implementar.

indebida de información privilegiada, el sabotaje a sistemas o programas informáticos de la compañía; abusos en el acceso a correos e internet; accesos no autorizados; redes de equipos infectados remotamente; daños físicos de los equipos; captura de contraseñas; extorsiones; explotación de servidores y navegadores; hurtos y robos de ordenadores o dispositivos móviles entre otros.

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

Un único incidente de ciberseguridad puede provocar varios tipos de responsabilidad de forma que algunas de sus consecuencias queden cubiertas en las pólizas: responsabilidad civil frente a terceros, clientes y/o usuarios; responsabilidad laboral frente a los trabajadores de la compañía que se han visto afectados por el ciberincidente; responsabilidad penal de la compañía y/o sus administradores o directivos surgida, como consecuencia de la actuación en el ciberespacio de un tercero (ajeno a la compañía o no), o de la propia compañía por actuaciones poco diligente; responsabilidad administrativa que pudiera derivarse frente a organismos regulatorios por el incumplimiento de obligaciones legales tendentes a garantizar un determinado nivel de seguridad; responsabilidad contractual en caso de que se produzca la paralización de la actividad y la imposibilidad de prestar servicio a los clientes y usuarios; responsabilidad extracontractual en caso de que haya terceros, ajenos a la prestación del servicio, afectados por el ciberincidente.

Finalmente, en relación a las medidas a adoptar por los potenciales asegurados, es preciso comentar que, con objeto de que los proveedores de ciberseguros acepten dar cobertura a las compañías en el ámbito de la ciberseguridad, es imprescindible que los interesados acrediten primero que ejercen un determinado nivel de monitorización, control y supervisión de las herramientas utilizadas para el desarrollo de su actividad (software y hardware) y que implementan y actualizan los procedimientos de control y fomentan una mayor concienciación de los trabajadores de la compañía en el ámbito de la ciberseguridad, así como demostrar un nivel de cumplimiento determinado ante el marco regulatorio y normativo de aplicación en cada caso (LOPD, PCI-DSS, etc.).

Por otro lado, y respecto a la obligación de informar a las autoridades de cualquier vulneración de seguridad sufrida, se consolida la tendencia dirigida a que las autoridades incentiven a las compañías eventualmente afectadas, de manera que éstas no teman represalias o la imposición de sanciones elevadas por haber sufrido una vulneración de sus sistemas de seguridad.

Es importante que estén decididas a informar (e informen) a las autoridades sobre cualquier violación de seguridad que sufran. Es conveniente que la colaboración entre el sector privado y público sea continua y transparente, de forma que las compañías favorezcan el intercambio de información sobre incidentes que afronten.

Es conveniente que el asegurado adopte con carácter preventivo y proactivo en el diseño, adopción e implementación de todas esas medidas, antes de suscribir un ciberseguro (El País, 2018). De lo contrario, puede encontrarse con que el asegurador o bien no acepte inicialmente suscribirle un seguro específico o bien, una vez suscrito, no otorgue cobertura al incidente en concreto por falta de cumplimentación de lo antes mencionado. El resultado, en cualquiera de los casos, es que el interesado no habrá transferido los ciberriesgos de manera eficiente, y no verá cubiertas sus necesidades en el ámbito de la ciberseguridad en caso de sufrir un ciberincidente. "El hecho de que se adquiera un seguro, no significa que se pueda ignorar la seguridad tecnológica. Los aspectos tecnológicos, operacionales y del seguro van de la mano".

Las recomendaciones para realizar la contratación consisten en identificar correctamente el alcance

necesario de la cobertura a contratar:

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

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

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

c) Ámbito territorial: en el contexto empresarial es habitual la existencia de servicios TIC[11] en la nube u otros servicios externalizados ubicados en otros territorios; por lo que es importante acotar el ámbito geográfico de aplicación de la póliza a contratar.

Conocer el negocio, los procesos y sus riesgos. Aunque no es necesario disponer de conocimientos avanzados en la gestión de riesgos de ciberseguridad, es importante entender e identificar el tipo de ciberamenazas asociadas al sector de actividad y a la exposición al mundo digital. Los brokers, las aseguradoras y determinadas empresas de ciberseguridad son actores habilitados para asesorar en la priorización y cuantificación de dichos riesgos.

La selección de los límites de indemnización, franquicias y coberturas más adecuadas debería estar basada en el análisis de posibles escenarios derivados de la identificación de estas amenazas y sus riesgos. Es importante comprender qué tipo de coberturas deben contratarse en función del análisis de riesgo comentado en el punto anterior. Del mismo modo, es recomendable efectuar una auditoría del programa de seguros de la empresa, ya que algunas coberturas ciber podrían estar aseguradas bajo otras pólizas de seguros corporativas contratadas.

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

Definir de forma adecuada límites y sublímites. Este punto es, con toda probabilidad, uno de los aspectos más delicados e importantes al contratar la póliza. Incluso ahora, los ejercicios prospectivos para tratar de determinar el impacto económico directo e indirecto de un ciberincidente es un ejercicio arduo y complicado. Ello, unido a la falta de datos históricos detallados, hace especialmente relevante la selección de límites, para no caer en un error de percepción versus realidad. Ante estas circunstancias, es aconsejable efectuar un

[11] El término Tecnología de Información tiene dos acepciones. Por un lado, a menudo, se usa el término "tecnología de la información" para referirse a cualquier forma de hacer cómputo; por otro, como las ciencias de la computación.

análisis de posibles escenarios derivados de la identificación de las amenazas y los riesgos cibernéticos que permitirá plantear varios escenarios de pérdidas económicas ayudando a elegir el límite de indemnización y franquicia a asumir por el asegurado más adecuado o conveniente.

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

Existen pólizas que sólo se activan ante una brecha de seguridad en los sistemas informáticos, y otras más amplias, admiten también causas de índole técnica como la sobrecarga de la tensión eléctrica, daños al sistema derivados de Incendio o Inundación afectando a los ficheros electrónicos, o eventos como el robo o pérdida de un dispositivo móvil cuando éstos contienen datos de carácter personal.

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

3.2. Ciberseguros como elemento de mejora de la seguridad

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

En consecuencia, las aseguradoras juegan un papel clave para mejorar la madurez de ciberseguridad del mercado, ya que pueden requerir a sus clientes el cumplimiento de unas cautelas mínimas de ciberseguridad como condición, sine qua non, para la contratación de las pólizas incluyendo, entre éstas, la adopción demostrada (auditada) de un marco de buenas prácticas de seguridad, ya sea a través de modelos de gestión internacionales como la ISO 27001 o bien mediante el desarrollo de un modelo de gobierno de seguridad específico desarrollado, por ejemplo, para la industria española.

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

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

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

derivados de los mismos.

Las propias aseguradoras desplegarán mecanismos de monitorización del estado de ciberriesgo de los mercados de sus clientes, jugando un papel importante en alerta temprana ante incidentes. Es factible imaginarse, como ya sucede en otras ramas de seguro, como por ejemplo el seguro de automóvil que presenta un coste reducido para aquellos conductores que autoricen la instalación de un GPS[12] en su vehículo, una aproximación en la cual el asegurado autorice la instalación de sondas en sus sistemas informáticos de forma que tanto la aseguradora, como el propio asegurado, disponga de una visión del riesgo informático en tiempo real, combinado con estrategias de monitorización de internet y fuentes abiertas para detectar amenazas externas. De este modo, los precios de las pólizas podrán ser totalmente ajustados a lo largo del ciclo de vida del producto al nivel de riesgo del asegurado.

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

A corto plazo para los sujetos asegurados, ya que permite una gestión más efectiva de forma directa (transferencia de riesgo) e indirecta (mejora de los controles preventivos) de los impactos asociados a un ciberincidente (Eleven Paths Blog, 2018).

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

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

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

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

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

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

[12] Global Positioning System, sistema de posicionamiento global, se trata de un sistema que permite determinar en toda la Tierra la posición de un objeto.

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

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

En esta línea, el mercado del ciberseguro en España debe dar el siguiente paso en su evolución hacia la madurez (El Diario, 2018), mediante la implementación de cinco elementos básicos: la concienciación del cliente respecto del alcance de su propia exposición a los ciberriesgos; la gestión integral de todas las fases y sujetos relacionados con este tipo de riesgos y su aseguramiento; la colaboración entre agentes la Administración Pública y organismos oficiales, empresas del sector asegurador (asociaciones, aseguradoras, brokers, proveedores de servicios) y los asegurados; la retroalimentación; el aprendizaje continuo.

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

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

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

Una mayor fluidez y transparencia en este tipo de comunicación ayudaría a los ya citados actuarios a realizar mejor su trabajo, contribuyendo con ello a la obtención de un mayor experto en materia de ciberseguros y, a la postre, a la maduración del sector. De la mano de lo anterior va la conveniencia y/o necesidad de que exista una retroalimentación entre aseguradoras, asegurados, Administración, instituciones o gobiernos.

En este sentido, los condicionados que comienzan a manejarse en las ciberpólizas de las mayores aseguradoras proveedoras de estos productos prevén específicamente coberturas consistentes en servicios especializados de análisis continuo de la situación real del asegurado, de constatación o auditoría casi continua del nivel de actualización de los sistemas del asegurado, de compartición de know-how específico de las aseguradoras con los clientes y de un apoyo y asistencia casi en tiempo real tan pronto se detecta una posible incidencia cibernética.

No es exagerado identificar una tendencia a que los centros de gestión de incidentes o crisis de las

aseguradoras actúen casi como una extensión de los departamentos de tecnología de la información de los asegurados, en los supuestos de compañías de cierto tamaño.

Según el Instituto Nacional de la Ciberseguridad (INCIBE, 2018), el mercado del ciberseguro en España mueve unos 500 millones de euros anuales, con ritmo de crecimiento anual estimado entorno al 12%. Este crecimiento va parejo al de la frecuencia e impacto de los ciberincidentes. El Instituto de Comercio Exterior (ICEX) apunta que las compañías españolas pueden estar perdiendo más de 13.000 millones de euros anuales como consecuencia de ciberincidentes.

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

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

El Estado puede favorecer el establecimiento de unos criterios comunes de seguridad a través de un marco de controles de seguridad de referencia cuya observancia y cumplimiento por parte de las empresas facilitase al sector asegurador la suscripción de seguros de ciberriesgos. Las Administraciones Públicas tienen una doble función, como proveedores de servicios críticos a la sociedad y como reguladores del mercado y de la economía. Esta doble responsabilidad les ofrece también la capacidad de fijar los requisitos mínimos que deben cumplir no sólo sus servicios y proveedores TIC; sino también aquellos considerados críticos para la sociedad siguiendo el ejemplo de la Directiva Europea de Servicios de Confianza.

Esta regulación tiene una doble función: definir los límites por encima de los cuales deben situarse los planes de seguridad de las empresas; ayudar a los responsables de seguridad a conseguir los recursos necesarios para implantar los mecanismos mínimos de seguridad requeridos en la regulación; la acreditación de capacidades de las empresas que optan a ofrecer servicios a la Administración Pública ha sido siempre objeto de polémica, ya que no siempre son uniformes o están armonizados con los de otras administraciones europeas.

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

La Administración Española podría mantener un listado de compañías que demostrasen su alineamiento con este marco de control. Mediante la constitución de una lista pública de empresas certificadas, países como el Reino Unido o Australia han dado respuesta a la necesidad de regular un mercado creciente con unas garantías de profesionalidad y calidad.

Estas listas centralizadas actuarían como punto de referencia público en el mercado aportando: un impacto positivo comercial y reputación entre las empresas; un nivel demostrable de seguridad de los procesos y procedimientos y validación de competencias técnicas de las organizaciones miembros; orientación, normas y

oportunidades para compartir y mejorar los conocimientos; medio ágil de inserción en el mercado de competencias, servicios y tecnologías de ciberseguridad.

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

4. Trabajo empírico

El objetivo de este trabajo empírico es analizar la composición de la información financiera relacionada con el riesgo cibernético y la posterior transferencia del riesgo a través del ciberseguro en las cuatro empresas españolas de mayor capitalización bursátil en millones de euros en el ránking global a 31 de diciembre de 2017: Inditex en el puesto 78 con una capitalización de 90.523; Banco de Santander en el puesto 81 con una capitalización de 88.410; BBVA en el puesto 208 con una capitalización de 47.422; Telefónica en el puesto 252 con una capitalización de 42.186.

En relación con la metodología vamos a observar los siguientes documentos: La carta del presidente, las cuentas anuales (la importancia de los intangibles), el informe de gestión, el informe de auditoría, el informe de buen gobierno. Los daños propios que se cubren y lo riesgos a terceros que se cubran, el importe de la prima anual, la actitud proactiva de la compañía, las auditorías de seguridad de la información, información histórica de amenazas y vulnerabilidades, relaciones institucionales en materia de ciberseguridad.

HOJA DE TRABAJO SOBRE LA INFORMACIÓN RELACIONADA CON LOS RIESGOS CIBERNÉTICOS
Y POSTERIOR TRANSFERENCIA DEL RIESGO A TRAVÉS DE LOS CIBERSEGUROS

CONCEPTOS RELACIONADOS	INDITEX	BANCO SANTANDER	BBVA	TELEFONICA
Carta del presidente	no existe	no existe	no existe	no existe
Porcentaje del Inmovilizado intangible respecto al total activo en materia de ciberseguridad	no existe	no existe	no existe	no existe
Información sobre sistemas de gestión propios relacionados con seguridad de la información y el control del mismo por parte de las empresas aseguradoras	no existe	no existe	no existe	no existe
Informe de Buen gobierno de la empresa respecto a la seguridad de la información	no existe	existe información sobre relaciones institucionales a este respecto	existe una comisiónn de ciberseguridad relacionada con la comisión de auditoría	se percibe una actitud proactiva en relación con los riesgos cibernéticos y la problemática de los ciberseguros
Visión holística sobre los distintos sistemas de gestión integrados, siendo uno de ellos la contabilidad como sistema de información integrada	no existe	no existe	no existe	no existe
Objetivos de la Comisión de auditoría interna en su reglamento, respecto al sistema de gestión de la seguridad de la información	no existe	no existe	existe una comisión de ciberseguridad relacionada con la comisión de auditoría interna	existe una comisión relacionada con los riesgos cibernéticos

Objetivos de la Comisión de la Seguridad de la Información en su reglamento	no existe	no existe	existe un reglamento	existe un reglamento
Relación documentada entre la Comisión de Auditoría, la Comisión de Comunicación, la Comisión de Seguridad de la Información	no existe	no existe	no existe	no existe
Informe de auditoría	no existe	no existe	no existe	no existe
La información en los estados contables, normalizados, memoria, informe de gestión, informe de buen gobierno, responsabilidad social corporativa, informe sobre reputación, sobre las consecuencias de los riesgos cibernéticos y seguridad de la información.	no existe	no existe	existe información en el informe de gestión	existe información en el informe de gestión
Alusión a los presupuestos en materia de ciberseguridad y seguridad de la información.	no existe	no existe	no existe	no existe

Actitud proactiva en relación con la ciberseguridad y seguridad de la información. Relación con consultores externos e instituciones nacionales e internacionales.	no existe	información de la relación con consultores	Informaciónsobre la relación con consultores	tiene una filial: Eleven Path
Primas de seguros por coberturas de riesgos cibernéticos y seguridad de la información. Sus distintas coberturas	no existe	no existe	no existe	no existe
Relación detallada de todos los activos de información y sus propietarios.	no existe	no existe	no existe	no existe
Aparecen detallados los activos de información dentro de las distintas masas patrimoniales en el balance y en otros estados	no existe	no existe	no existe	no existe
Información sobre el capital humano que implique mayor legitimidad y ventaja competitiva.	no existe	no existe	no existe	no existe
Cambio organizacional ante el nuevo paradigma digital (cambio tecnológico, información y cambio organizacional).	no existe	no existe	comisiones de seguridad de la información	comisiones y filiales encaradas de esta responsabilidad

5. Conclusiones

1.- No aparece información sobre las transferencias de riesgos cibernéticos a través de los ciberseguros en la carta del presidente de las entidades estudiadas. Tampoco una información explícita sobre seguridad de la información.

2.- Las empresas son reacias en general de dar información sobre los riesgos cibernéticos tampoco sobre la historia de los ciberataques y sus causas. Igualmente, hemos podido observar en las empresas estudiadas que no aparece información sobre los ciberseguros, tampoco sobre el importe de la prima, riesgos cubiertos y exclusiones. Tampoco existe información entre el importe de la prima y la actitud proactiva ante riesgos cibernéticos.

3.- No se da información en las empresas estudiadas sobre el sistema de gestión de la seguridad de la información y su visión holística en relación con otros sistemas de gestión, así como la falta de información

sobre los informes de auditoría del sistema de gestión.

4.- No existe información en los informes de gestión sobre los riesgos de ciberseguridad en los grupos de empresas estudiados, tampoco existe información sobre los tipos de coberturas, sobre las relaciones institucionales, con otras empresas y con empresas consultoras en materia de ciberseguridad y ciberseguros.

5.- Si existe información en el informe del buen gobierno de alguna empresa sobre la existencia de comisiones de ciberseguridad, comisiones de auditoría interna y la relación entre ambos. En los informes de auditoría no aparecen salvedades relacionadas con la ciberseguridad ni sobre el impacto reputacional. Falta información presupuestaria, así como las hipótesis donde se basan sus estimaciones en relación con los riesgos.

Cómo citar este artículo / How to cite this paper

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

Referencias

Bandyopadhyay, T. (2012). Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management – A Modelling Approach. In Proceedings of the Southern Association for Information Systems Conference (pp. 23-29).

Ciberseguros-Thiber (2018). La transferencia del ciberriesgo en España. Patrocinado por AIG, AON EmpowerResults, K2Intelligence (Investigations. Compliance. CyberDefense), Marsh, Minsaltby Indra, Telefónica. Partner académico: IE Business School. (www.thiber.org)

El Diario (2018). El auge de los ciberseguros llega a España (detrás del miedo a los ataques). m.eldiario.es

El Economista (2018). Ciberseguros, el negocio de la próxima década. (www.eleconomista.es)

El País (2018). Ciberseguros a la medida del ataque. (https://elpais.com)

Eleven Paths Blog (2018). Nuevo Informe. Ciberseguros: la transferencia del ciberriesgo. Blog.elevenpaths.com

fireeye.com (2018). Evaluación de riesgos para ciberseguros. https://www.fireeye.com

Gestion.pe (2018). Ciberseguros: Estos son los sectores más expuestos a un ataque de hackers. (https://gestion.pe)

INCIBE (2018). Pólizas de ciberseguros: ¿cuál me conviene? INCIBE. https://incibe.es

Nuevo Reglamento General de Protección de Datos (2018). Ciberseguros ante las exigencias del Nuevo Reglamento General de Protección de Datos. (https://blog.signaturit.com)

IEAF-Instituto de Analistas Financieros (2018). Ciberseguros: la transferencia del ciberriesgo en España. (www.ieaf.es)

onemagazine.es (2018). Ciberseguros: Qué te cubren y qué no…y qué saber para elegir mejor. (https://www.onemagazine.es)

WannaCry (2018). WannaCry, el detonador de un negocio casi en pañales: los ciberseguros. (https://m.elblogsalmon.com)