INNOVACIÓN | 20.05.2022

# Ciberriesgos, el gran desafío de las pymes

Redacción MAPFRE

@mapfre

## En 2022 los ciberdelitos volverán a registrar cifras récord y serán las pequeñas y medianas empresas las más vulnerables. Medir y tarifar los riesgos cibernéticos no es sencillo. Las aseguradoras empiezan a posicionarse y la IA se postula como imprescindible.

El año pasado, un 53 % de pymes sufrió algún tipo de ciberataque y responsables de ciberseguridad y altos directivos de 66 países han concluido que los ataques cibernéticos volverán a registrar cifras récord en 2022. Ante este escenario, el papel de los (re) aseguradores y las tecnologías que trabajan para estimar el impacto de los ciberriesgos es clave.

Una pandemia y un confinamiento global, la expansión del teletrabajo y la consolidación del comercio digital, el uso intensivo de las pantallas y los dispositivos electrónicos... En marzo de 2020 **comenzó la tormenta perfecta** para la ciberdelincuencia. Los ciberataques se han sucedido, la mayoría sufridos en silencio y otros convertidos en noticia mundial como el reciente contra el Comité Internacional de la Cruz Roja, cuyas bases de datos pirateadas contenían información sobre más de medio millón de personas vulnerables debido a conflictos armados, migración y desastres naturales.

Tal y como refleja el estudio *Digital Trust Survey 2022*, realizado por la consultora PwC con más de 3.600 entrevistas a responsables de ciberseguridad y altos directivos de 66 países, **los ciberataques volverán a registrar cifras récord** este año. Los ataques *online* que más crecerán tendrán como objetivos los servicios de almacenamiento de datos en la nube, el secuestro de datos (*ransomware*), la infección de equipos informáticos a través de las

actualizaciones de *software* (*malware*) y los asaltos al *software* de las cadenas de suministros y correos electrónicos corporativos.

El negocio que genera este fraude cibernético no es una broma. Que se lo digan la FinCEN (Financial Crimes Enforcement Network), oficina del Tesoro de EE. UU. que recopila y analiza las transacciones de dinero para combatir el lavado de capitales, la financiación del terrorismo y los delitos financieros. En su última investigación denuncia que entre enero y junio de 2021 **identificó más de 5,2 billones de dólares** (4.500 millones de euros) en transacciones con *bitcoins* "potencialmente vinculadas a pagos por *ransonware*". O lo que es lo mismo, por pagos del rescate solicitado tras sufrir el secuestro de datos.

## Más de la mitad de las pymes sufrió ciberataques

La ciberseguridad es una premisa para la supervivencia de cualquier empresa. Es cierto que las grandes compañías están más y mejor preparadas para soportar este tipo de incidencias. Por poner un ejemplo, en agosto de 2020 –pocos meses después de declararse la pandemia del coronavirus– MAPFRE sufrió un ciberataque y la propia Agencia Española de Protección de Datos (AEPD) resaltó que "los intentos de exfiltración (extracción de datos) fueron detectados y evitados, lo que unido a la rapidez para hacer público el cibertaque permitió la eficaz actuación de clientes, trabajadores, colaboradores y proveedores, minimizando los efectos".

Las pymes, con menos presupuesto y hasta ahora menos concienciadas, se han convertido en la principal diana del cibercrimen. Su principal reto para 2022 son estar preparadas para cualquier ciberriesgo porque con la llegada de la COVID-19 se han visto obligadas a replantear sus modos de trabajo, incorporando el teletrabajo y la digitalización a marchas forzadas. El año pasado las pymes fueron las principales damnificadas, **un 53 % de ellas sufrió algún tipo de ciberataque** y más de un 40 % fueron víctimas de más de tres ciberdelitos, según el último informe de Hiscox. De

media, cada ciberataque le costó a una empresa pequeña 75.000 euros, como reconocen desde SSH Team Consulting.

"Las pymes todavía están poco preparadas en tecnologías y prevención frente a los ciberriesgos. **Las de menos de 10 trabajadores** tienen la sensación de que no pueden ser objetivos de ciberataques, pero deben preguntarse qué porcentaje dentro de sus procesos productivos dependen de los datos y la tecnología. Seguramente casi todos. Si sufren una paralización de su actividad debido a un ciberataque y no están debidamente preparadas, las consecuencias pueden llegar a suponer en el peor de los casos hasta el cierre de sus negocios", explica Óscar Taboada, responsable de negocio Cyber de MAPFRE RE.

"Cuando se habla de ciberseguridad nos referimos al **grado de madurez de la pyme** para afrontar este problema, de cuánto ha estado preocupada la empresa desde su fundación para formar en ciberseguridad a sus informáticos, para implementar programas de concienciación. Es importante también disponer de un director de seguridad de la información –CISO (*Chief Information Security Officer*), en sus siglas en inglés–, el responsable de garantizar la protección y buena gobernanza de los datos. Depende mucho del sector empresarial, aquellas que utilizan la tecnología como parte operativa seguro que han tenido en cuenta la ciberseguridad", explica en declaraciones a MAPFRE Marc Rivero, investigador *senior* del Equipo Global de Control de Amenazas de Kaspersky, multinacional de seguridad informática que trabaja en más de 195 países.

Es un hecho que la pandemia ha acelerado el proceso de transformación digital de las pequeñas y medianas empresas. En España las pymes suponen más del 99 % del tejido empresarial, **representan el 62 % del PIB nacional y crean más del 60 % del empleo empresarial total.** Y en el mundo dan trabajo a más de 2.000 millones de personas.

Los últimos datos sobre digitalización de las pymes facilitados por el Observatorio Nacional de Tecnología y Sociedad (ONTSI), dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, muestran una puesta al día digital de muchas

de las empresas medianas y pequeñas. La penetración de Internet alcanza prácticamente a la totalidad de las pymes (98 %). Por ejemplo, el 77,3 % de la pymes y grandes compañías y el 55,1 % de las microempresas han facilitado a sus empleados dispositivos móviles con acceso a internet para uso empresarial. El 63 % de las primeras y el 35 % de las más pequeñas utilizan las redes sociales y casi una de cada tres empresas tienen contratados servicios de *cloud computing* (almacenamiento en nube). En cuanto a las compras mediante comercio electrónico, un 35 %.

"**Los delincuentes están adaptándose a la digitalización muy rápidamente** y aprovechándose de ella. Por tanto, para hacerles frente se requiere un entendimiento más amplio de la ciberseguridad, así como una preparación previa para evitar riesgos de ataques, algo que no siempre está al alcance de pymes y autónomos", afirma Jorge Sicilia, director de desarrollo de negocio de Empresas de MAPFRE España.

## ¿Como podemos cuantificar, medir y tarificar los ciberriesgos?

Una vez reconocida esta realidad, las (re) aseguradoras necesitan cuantificar y medir este riesgo para posteriormente poder dar un precio adaptado a la exposición que asumirán.

Según los datos de ObservaCiber, espacio creado recientemente por el Instituto Nacional de Ciberseguridad y el ONTSI, en España el 18 % de las empresas disponen de un seguro para hacer frente a las posibles incidencias de seguridad cibernética, cifra por debajo de la media europea, que se situó en el 24 %.

"Tenemos que distinguir entre ciberseguridad, es decir, las medidas de protección y prevención que una empresa puede implementar en sus protocolos informáticos para evitar lo máximo posible la entrada de un ciberataque que conlleve robo de datos, paralización de actividad, etc.;  y por otro lado el seguro de ciberriesgos que serían las coberturas en base a unos límites que una compañía (re) aseguradora estaría dispuesta a suscribir y, por tanto, asumir",

explica Oscar Taboada, responsable de negocio Cyber de MAPFRE RE.

“La naturaleza de este tipo de riesgos y su complejidad dentro de un entorno dinámico, global y cambiante hacen que sea fundamental su correcto entendimiento, análisis, control y medición”, asegura Óscar Taboada.

## El papel del reaseguro frente al ciberriesgo

El reaseguro en el ámbito del ciberriesgo, al igual que en otras líneas de negocio, juega un papel fundamental facilitando la transferencia de riesgo por parte de las aseguradoras, gestionando el control de la potencial acumulación catastrófica y contribuyendo al desarrollo de productos con aporte de soluciones y asesoramiento para la mitigación y prevención de dichos riesgos.

“En el caso de MAPFRE RE, por ejemplo, estamos trabajando activamente en el aprendizaje y análisis de distintos modelos y escenarios de acumulación catastrófica frente a eventos de gran magnitud aplicando IA (inteligencia artificial), lo que nos permiten llegar a modelos estadísticos predictivos con los que estimar las posibles pérdidas potenciales”, comenta el responsable de negocio Cyber de MAPFRE RE. (Ver despiece).

Entre los meses de enero y julio de 2021, MAPFRE realizó una innovadora investigación, basada en la escucha de la conversación en torno a la ciberseguridad en redes sociales y foros. La principal conclusión es que los usuarios, cada vez más acostumbrados a realizar gestiones digitales, se muestran preocupados por la seguridad digital de las empresas en las que consumen productos y servicios y a las que facilitan sus datos personales.

Por ello, y ante la vulnerabilidad a ataques informáticos de las pymes, MAPFRE ha desarrollado el seguro CIBER On para autónomos y pequeñas y medianas empresas que facturen hasta 10 millones de euros. Con este ciberseguro, el cliente tiene a su disposición equipos especializados para que tenga la mejor cobertura frente a cualquier

ciberataque y sus consecuencias. De esta forma, las pymes podrán protegerse de daños a los sistemas informáticos, interrupción del negocio, amenaza de ciberextorsión, responsabilidad civil y cobertura de soporte tecnológico para recuperar la normalidad en la actividad.

## KOVRR, soluciones para cuantificar financieramente el riesgo ciber

La tecnología, los algoritmos y la inteligencia artificial (IA) se han convertido en **herramientas esenciales para crear modelos predictivos** que ayuden a las compañías (re) aseguradoras a estimar el potencial impacto de un evento cibernético.

A principios de 2021, MAPFRE RE firmó un acuerdo con KOVRR, empresa líder en modelización y cuantificación de riesgos ciber, con sede en Tel Aviv (Israel), para poder profundizar en el conocimiento, análisis y valoración de esta tipología de riesgos. Mediante un sofisticado análisis de evaluación de los sistemas tecnológicos de cada riesgo /empresa, KOVRR es capaz de estimar en base a modelos predictivos la potencial pérdida máxima esperada en base a una serie de eventos cibernéticos.

“Esto permite determinar las exposiciones a las que se enfrenta una compañía en base a una cartera en un momento determinado pudiendo cuantificar, medir y tarificar el riesgo en base a las coberturas ofrecidas”, comenta Oscar Taboada responsable de negocio Cyber de MAPFRE RE.

Joan Cuscó, director global de transformación de MAPFRE Open Innovation (MOi) ha asegurado que “KOVRR es **un gran caso de éxito** de nuestro programa de compromiso con las *startups*. Nuestra misión es adoptar soluciones disruptivas para el sector de los seguros, y la colaboración con MAPFRE RE es un ejemplo de lo que pueden conseguir las (re)aseguradoras y las startups tecnológicas cuando combinan sus conocimientos”.