Hace 15 años los riesgos más preocupantes para cualquier potencial asegurado eran los daños (incendio, inundaciones, catastróficos…) o las reclamaciones (Responsabilidad Civil, Profesional, Patronal, D&O…).

Hoy nos enfrentamos a una generación nueva de riesgos que pueden perfectamente llevar a la ruina a cualquier Pyme y profesional autónomo, derivados de la vulnerabilidad de los sistemas informáticos que contienen datos de los clientes o vitales para el devenir del negocio: sanciones, reclamaciones, gastos legales, notificaciones, extorsiones, pérdida de fondos, interrupción del negocio, reputación…

Un **buen seguro de riesgos cibernéticos** cubre una importante cantidad de los daños que se pueden sufrir en un ataque, fundamentalmente económicos, y proporcionan apoyo técnico y legal para minimizar el impacto y recuperar la actividad normal de la organización lo antes posible.

¿A qué riesgos nos enfrentamos?

- **9 de cada 10 empresas españolas** sufrieron al menos un ciberataque en el año 2021. **España** está **a la cabeza** en **ataques** de **escritorio remoto**

- Según el IBM Cyber Resilient Organization Study 2021, más del **51%** de los profesionales de seguridad IT han sufrido un ciberataque en los últimos 12 meses

- El **43%** de los ciberataques van contra pymes

- Los ataques en internet han **crecido un 140%** en los dos últimos años

- 6 de cada 10 pymes atacadas de forma grave **cerraron** seis meses después

- El **coste económico** medio de un ciberataque a una **pyme** es de 30.000€ a 50.000€, pero puede llegar a los 100, 200 o 300 mil €

- Además, el incremento del **teletrabajo** acentúa el riesgo de un ciberataque

¿Qué propicia los ciber ataques?

- **El gran número de víctimas potenciales**. Ninguna organización, grande o pequeña, está completamente a salvo de los ciberdelincuentes. El **43% de los ciberataques tienen a empresas europeas de menor tamaño** entre sus objetivos. Creer que estamos seguros nos convierte en potenciales víctimas del cibercrimen.

- **Desconocimiento de los usuarios**. Centrarse solamente en la seguridad tecnológica y obviar la formación para resistir los ataques de **ingeniería social** aumenta las posibilidades de ser atacados.

- **Dinamismo de la tecnología**. Las nuevas tecnologías nos han permitido mejorar la comunicación, la velocidad y la organización en nuestra manera de trabajar. Sin embargo, **cualquier nueva tecnología incorpora nuevos riesgos de Inseguridad** en los sistemas y aplicaciones.

¿Qué propicia los ciber ataques?

- **El desconocimiento sobre los estándares de seguridad**, la falta de capacidades en ciberseguridad y los recursos limitados, son barreras para la ciberseguridad de las pymes.

- Las **pymes,** que constituyen más del 99% del tejido empresarial europeo, presentan riesgos más que significativos en este ámbito y éstos constituyen una gran amenaza para su negocio.

Mapa de ciberataques en vivo

El mercado de seguro de ciber

DISTRIBUCIÓN DEL SEGURO CIBER EN EL MERCADO

POR COBERTURAS

El mercado de seguros de Ciber en España se subdivide fundamentalmente en función del tipo de producto que se ofrece:

a) De Daños a terceros o Responsabilidad Civil
b) De Daños a terceros y Daños propios
c) De Daños a Terceros, Daños propios y Fraude.

El seguro de Daños a Terceros cubre las reclamaciones como consecuencia de violaciones de la seguridad o la privacidad en los sistemas.

Daños a Terceros y Daños Propios cubre tanto las reclamaciones como los daños que el asegurado sufra como consecuencia de violaciones de la seguridad o de la privacidad en los sistemas.

El mercado de seguro de ciber

Daños a terceros, Daños Propios y Fraude. Es un producto que incluye lo anterior pero además el Fraude por suplantación de identidad. Esta última cobertura también se conoce en el mercado con el nombre de Crime, y de por sí constituye un seguro que se comercializa separadamente, para empresas ya de cierto tamaño.
Su inclusión en el seguro de Ciber establece la diferencia entre los productos más especializados y los más generalistas.

Cualquiera de los productos mencionados incluye servicios de respuesta de emergencia que vendría a ser como la "asistencia" del seguro de Ciber. En función de la complejidad del producto el servicio de respuesta de emergencia es más sofisticado.
Con carácter general los servicios de respuesta de emergencia hacen las veces de administradores de siniestros de las aseguradoras. Estos servicios incluyen un conjunto de expertos en reclamaciones, remediaciones, gestores de crisis, etc.

Finalmente tenemos los productos que incluyen todo lo anterior pero además ofrecen herramientas o servicios de prevención. Estos productos son los que se encuentran en el nivel óptimo en cuanto a calidad.

El mercado de seguro de ciber

POR FACTURACIÓN

El mercado de seguros de Ciber se subdivide también por la facturación de los asegurados.
Los tramos, en líneas generales, serían los siguientes:

a) Hasta 10 millones de euros de facturación. Este tramo es el que prácticamente la totalidad de las aseguradoras ofrecen.
b) De 10 a 25 millones. Este tramo lo ofrecen tan solo el 40% de las aseguradoras
c) De 25 a 50 millones. Tan solo el 10% de las aseguradoras.
d) Más de 50 a 500 millones. Se conoce como el Middle Market o Mercado Medio. Apenas unas pocas aseguradoras se atreven con este tramo y de forma muy restrictiva. Ha probado ser el tramo con mayores siniestros de todos los anteriores.

El mercado de seguro de ciber

Más de 500 millones. Es el tramo Grandes Empresas o Corporate y solo los grandes especialistas tienen capacidad. En este tramo hay más oferta que en el anterior ya que las empresas con estos niveles de facturación tienes unos niveles de seguridad en general muy superiores.

POR TIPOLOGÍA DE CLIENTES

En este caso tendríamos dos categorías:

a) Clientes particulares o familias
b) Profesionales y empresas