Aon publica el II Estudio sobre **la ciberseguridad y la gestión del riesgo Ciber.**

Carmen Segovia Blázquez
Directora de Líneas Financieras y Ciber riesgos de AON para Cataluña y Baleares

En nuestra primera publicación del **año pasado cerrábamos la edición con un capítulo especial sobre el impacto que la pandemia covid-19** estaba teniendo con respecto al riesgo cibernético.

Era un capítulo en el que, aunque muy a corto plazo, empezábamos a vislumbrar una serie de factores que iban a ser determinantes en un cambio de tendencia que afectaría tanto a la sensibilidad de las organizaciones en relación con la ciberseguridad como al mercado asegurador en cuanto al análisis del riesgo y a la suscripción de este.

Durante aquellos meses de 2020, y como consecuencia de la **implementación rápida e improvisada del teletrabajo por parte de la mayoría de las empresas españolas, identificamos en nuestros análisis de riesgos, la adopción de estructuras de ciberseguridad menos robustas,** como las conexiones de los dispositivos a los servicios centrales no cifradas; el uso de dispositivos no corporativos, o la ausencia del doble factor de autenticación. Sin embargo, también identificábamos, **como consecuencia de esto y el aumento de los incidentes ciber, una mayor concienciación de las organizaciones frente al riesgo.**

ENDURECIMIENTO DEL MERCADO. ¿QUÉ LE PREOCUPA A LOS ASEGURADORES?

Pues bien, en **nuestro informe de 2021 podemos afirmar el cumplimiento de las tendencias que identificábamos el año anterior,** vinculadas a la situación desencadenada por la pandemia y las nuevas formas de trabajo telemático, dando lugar al inicio de una **etapa de mercado duro que viene marcado por las siguientes consideraciones principales** del mercado asegurador **que centra el foco de sus análisis de riesgo en estos principales aspectos:**

1. Ciber extorsión: El robo y el uso indebido de información personal identificable ya no es el objetivo principal de los cibercriminales. Los ataques de ransomware han evolucionado para incluir no sólo el cifrado de datos sensibles (incluida la IPP y la información corporativa confidencial) sino también la amenaza de exposición de dichos datos en Internet. Este tipo de ataques puede dar lugar a tiempos de inactividad de la empresa debido a las redes cifradas, así como a posibles consecuencias de responsabilidad en términos de sanciones administrativas o demandas de terceros.

2. El riesgo del proveedor: A medida que las organizaciones continúan adaptándose al entorno empresarial actual y a las necesidades del mercado asociadas, la dependencia de la tecnología de terceros y de las aplicaciones de back-end son mayores que nunca. Las normas de ciberseguridad de los proveedores son una parte fundamental de esta ecuación, exigiendo a las empresas mayor diligencia en la contratación de los servicios electrónicos.

3. Trabajo en remoto: El teletrabajo ha contribuido a aumentar las vulnerabilidades potenciales como el software del Remote Desktop Protocol (RDP), la seguridad del acceso remoto, la dependencia de terceros proveedores de servicios de IT y la comunicación digital como el principal medio para compartir información.

4. Tecnología no cubierta: La coyuntura que se deriva de la pandemia COVID-19 ha acelerado las iniciativas de transformación digital de muchas organizaciones. La aparición de servicios y productos tecnológicos en sectores más tradicionales representa una exposición de IP potencialmente "descubierta" que puede no estar contemplada desde el punto de vista de la responsabilidad y las pérdidas financieras.

5. Incumplimiento de la normativa: El entorno normativo sigue creciendo en complejidad. Las recientes multas impuestas en virtud del Reglamento General de Protección de Datos (RGPD) de la Unión Europea demuestran que las organizaciones deben ser conscientes del impacto de una violación de datos. Más de 160.000 violaciones de datos se han notificado desde que el GDPR entró en vigor el 25 de mayo de 2018. **Las sanciones aumentaron casi un 40% en 2020,** alcanzando la cifra de 158,5 millones de euros, **siendo la mayor sanción de 35 millones de euros emitida por el regulador alemán.** La evolución en este ámbito podría traer consigo mayores problemas financieros desde el punto de vista de las multas y sanciones.

¿QUÉ RESTRICCIONES SE ESTÁN APLICANDO A LAS COBERTURAS?

Como consecuencia de estos nuevos focos de atención, los aseguradores están ajustando su suscripción, revisando los términos y condiciones de la cobertura y reevaluando el despliegue de la capacidad. Los siguientes son ejemplos específicos de consideraciones de cobertura que los asegurados están teniendo en consideración en 2021:

1. Cobertura de ransomware: las pérdidas asociadas son citados por muchas aseguradoras como un factor importante que impacta en sus ratios de siniestralidad. Si no se proporciona la información de suscripción adecuada, o si la información proporcionada se considera desfavorable, las aseguradoras pueden tratar de limitar su cobertura para las pérdidas por eventos de ransomware de la siguiente manera:

- Limitar el agregado que ofrecen a algún factor del límite total de la póliza.
- Se está proponiendo el co-aseguro (con el asegurado), en algunos casos, junto con un sub-límite.
- Se están revisando los periodos de espera para los acuerdos de seguro de interrupción de la actividad empresarial relacionados con eventos de ransomware, que en algunos casos pueden llegar a ser de 24 horas.
- En los casos más extremos, cuando faltan controles críticos, las aseguradoras pueden tratar de incluir exclusiones de "eventos de ransomware" en las pólizas.

Es fundamental tener en cuenta que, aunque las aseguradoras están utilizando estos enfoques para limitar su exposición, estas restricciones de cobertura no están diseñadas para aplicarse únicamente a un acuerdo de seguro de ransomware o ciberextorsión. Más bien, la restricción está redactada de tal manera que se aplica al ransomware como vector de ataque, y por lo tanto puede aplicar la limitación a cualquier pérdida que se derive de tal ataque.

2. Interrupción del negocio: las aseguradoras revisan su exposición global a los riesgos sistémicos, agregados y correlacionados, relacionados con la cadena de suministro de software, por lo que varias aseguradoras están revisando y ajustando la amplitud de la cobertura ofrecida para las pérdidas por interrupción de la actividad, con la intención de limitar la exposición financiera a un evento sistémico de las siguientes maneras:

> "Identificamos una mayor concienciación de las organizaciones frente al riesgo...

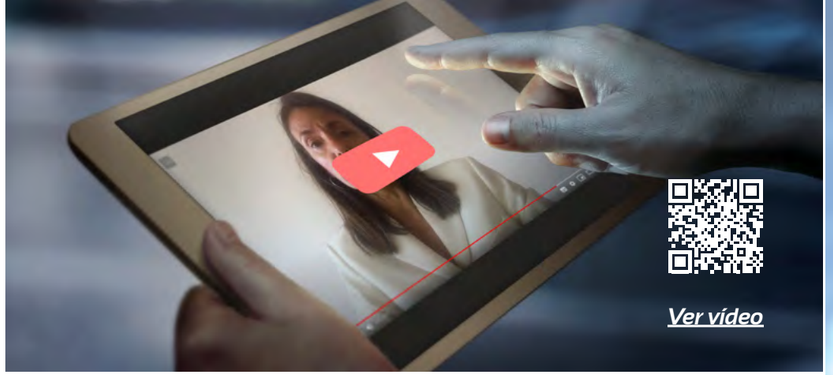
- El mercado está empezando a presionar para que los periodos de espera se acerquen a las 24 horas.

- Limitación de la exposición al límite agregado. Esto se está consiguiendo mediante la reintroducción de sublímites o la exigencia de coaseguro.

- Incorporación de exclusiones específicas para SolarWinds, así como para el uso de sistemas obsoletos.

3. Proveedores de Primera Respuesta: A medida que los índices de siniestralidad se deterioran, las aseguradoras están revisando de cerca los costes de los proveedores de terceros en los que se incurre para investigar y responder a los incidentes cibernéticos.

Para reducir (o al menos combatir el aumento de) estos costes, **las**



Ver vídeo

aseguradoras están demostrando menos flexibilidad en el uso de proveedores no pertenecientes al panel o preacordados. Cada vez es más frecuente que las aseguradoras sólo reembolsen una cantidad igual a la que habrían pagado a un proveedor de panel teniendo que asumir el asegurado el resto de la factura de honorarios. Así mismo, **algunos aseguradores han empezado a aplicar franquicia** en la cobertura de Primera Respuesta.

TENDENCIAS PARA LOS PRÓXIMOS MESES.

Por último, no podemos cerrar nuestro II Estudio sin una previsión de las Tendencias que van a dominar los próximos meses, así que **viviendo ya los últimos coletazos del Covid-19 y resituándonos en el nuevo contexto social, económico y político es momento para reflexionar y evaluar la situación dando lugar a una predicción de las principales tendencias** que se están produciendo este año con respecto a la gestión y transferencia del riesgo cibernético:

1. Ha aumentado la **frecuencia y la virulencia de los siniestros Ciber,** de manera que ya estamos viendo cómo fallos de seguridad (sobre todo centrados en ataques ransomware) dan lugar a unas **pérdidas que consumen la totalidad del límite de la póliza e incluso, los asegurados deben asumir pérdidas por encima del límite contratado.** Esto pone de manifiesto también que las capacidades que se compran bajo los contratos de seguro son pequeñas e insuficientes para asumir las pérdidas generadas tras un incidente Ciber.

2. En cuanto al **ámbito legislativo,** destacamos la actividad por parte de los reguladores europeos en la aplicación del RGPD, dado que la otra cobertura más afectada en póliza y, que contribuye de manera significativa al consumo de la totalidad del límite de las pólizas, está siendo las **sanciones administrativas en materia de protección de datos.** Hasta hace poco, este tipo de pérdidas era residual en el ramo. Así mismo prevemos que **podría haber cambios en el marco legal vinculados al pago de rescates por ransomware** e incluso cambios en la propia cobertura introducidos a iniciativa de los propios aseguradores.

3. Una de las primeras consecuencias que se derivan de los puntos anteriores es que **se mantiene e incrementa la tendencia alcista de primas,** identificando un **incremento medio en 2021 del 60%** de las primas de renovación. De momento no prevemos una estabilización de los precios dado que el objetivo principal del mercado es corregir y rentabilizar el ramo para poder mantener una suscripción óptima.

4. El aumento significativo de la siniestralidad en tan poco tiempo ha dado lugar a una **reducción de capacidad aseguradora** (en 2019 identificábamos una capacidad general de 250 Millones y ahora apenas llegamos a los 100 Millones en el mercado español). Dado que continua **el incremento sostenido de pérdidas, así como la incerteza ligada a posibles cúmulos de riesgo y otros factores, inciden en que durante los próximos meses no se prevea la entrada de nuevo capital** en el ramo que contribuya a armonizar los precios de la capacidad.

5. Los ramos de Daños materiales y Responsabilidad Civil General están incluyendo de manera generalizada exclusiones para evitar posibles vacíos de cobertura con respecto a lo que se ha dado en llamar ***Ciber silenciosa.*** Este es un trabajo pendiente de resolver por parte del mercado asegurador que debe dar solución a esas posibles coberturas pasivas, que pueden incluir o no excluir expresamente los riesgos Ciber bajo pólizas tradicionales. De momento **identificamos algunas soluciones, pero muy incipientes, y que se encuentran con el problema principal de que no hay capacidad suficiente para asumir los daños materiales y corporales** que se deriven de un incidente Ciber.

El mercado asegurador no identifica ningún parámetro que permita prever una reducción de la siniestralidad en el corto plazo por lo que **recomendamos a las empresas ser muy proactivas en la gestión del riesgo cibernético y, en la medida de lo posible, cuenten también con un programa de seguros que les permita garantizar la continuidad de su negocio a pesar de las pérdidas** que pudieran derivarse de un evento Ciber. ■

Para descargarte la nota de prensa, visita: ***https://agers.es/wp-content/uploads/2021/06/np_estudio_ciber_riesgos_Espana-AON.pdf***