Ciberriesgos: un acercamiento desde la perspectiva del gestor de riesgos

José Manuel García // Actuario CERA
Sonia Latorre // Actuaria CERA

Seguramente todos estamos más o menos familiarizados con el término "phishing" o "spyware" dentro de la categoría de delitos digitales (malware), y en alguna ocasión habremos oído hablar de los "troyanos" o los "gusanos", lo cual nos da la falsa sensación de que tenemos cierto conocimiento sobre la materia, pero no hay nada como intentar profundizar un poco para ser consciente de tus limitaciones. No es sólo el descubrimiento del elenco de términos que puede haber detrás de un ciberataque, sino de los matices que los diferencian y que en definitiva determinan a qué tipo de riesgo nos estamos enfrentando y cómo gestionarlo.

A lo largo de los últimos años hemos sido testigos de algunos ciberataques a nivel global que ponen de manifiesto el alcance e impacto potencial que pueden tener ya no sólo a nivel de empresa, como es el caso del ramsomware[1] *WannaCry*, que afectó a unos 200.000 sistemas informáticos de 150 países, sino a nivel estatal, como fue el caso del ataque *Sunburst* que afectó a los sistemas de las principales agencias gubernamentales estadounidenses. No menos impactantes son los medios utilizados en los ciberataques: desde el uso de Inteligencia Artificial para simular la voz del CEO de la empresa y ordenar una transferencia millonaria, hasta acceder a la base de datos de casino por medio del termómetro de su acuario conectado a internet

Los recientes ataques en el sector asegurador que han dejado en jaque dos de las principales aseguradoras españolas nos han mostrado una realidad a la que no podemos darle la espalda. En Segurcaixa, un ciberataque detectado el pasado 9 de septiembre apagó digitalmente por completo a la compañía, dejando de funcionar de un día para otro los sistemas informáticos, como los que gestionan las autorizaciones de pruebas médicas y las pólizas de los usuarios. Inmediatamente se activó el plan de contingencia y se trabajó para solucionar los efectos. El ciberataque provocó seis semanas de intentos de recuperación del apagón digital provocando una situación muy delicada durante ese mes y medio.

Segurcaixa no fue el único en sufrir un ataque el verano pasado, Mapfre España también fue víctima de un ataque informático similar que ralentizó la capacidad de los equipos y afectó a sus dispositivos. La misma compañía comunicó el ciberataque sufrido a través de sus redes sociales haciendo gala de un ejercicio de transparencia muy bien recibido por todos los grupos de interés y que aumentó la comprensión de todos ellos respecto a la crisis que estaba afrontando la compañía. El 90% de los dispositivos de la empresa no pudieron trabajar con normalidad durante dos semanas. La buena ejecución del Plan de continuidad de negocio de la compañía se vuelve esencial para acortar los tiempos de espera en la recuperación tras un ataque de estas características y el gestor de riesgos en una persona clave en la gestión de la emergencia.

Las autoridades europeas no han sido ajenas a esta realidad y han querido alinearse con la evolución tecnológica de las empresas y de sus riesgos, desarrollando una serie de normativa que, si bien se solapa en algunos aspectos, tiene la vocación de ser exhaustiva y no dejarse a nadie fuera. Hablamos del borrador del *Reglamento de resiliencia digital operativa* (**DORA** por sus siglas en inglés: Digital Operational Resilience Act) que afecta al sector financiero, pero también de la propuesta de *Directiva sobre resiliencia de las infraestructuras críticas* (**CIR:** Critical Insurance Resilience) y de la actualización de la Directiva para salvaguardar la seguridad de la información (Network and Information Security –NIS[2] en sus siglas en inglés– y su modificación conocida como **NIS2**[3]) cuyos borradores fueron ambos emitidos en diciembre del año pasado. No podemos olvidar los dos grupos de Directrices recientemente publicadas desde EIOPA dentro del ámbito del sector seguros (las *Directrices sobre la externalización a*

1 Código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario no pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga.

2 DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

3 DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148.

proveedores de servicios en la nube, aplicable desde el 01/01/2021 y las *Directrices sobre gobernanza y seguridad de la tecnología de la información y las comunicaciones*, de aplicación a partir del 01/07/2021); en definitiva un completo marco regulatorio que incluye, entre otros aspectos, las pautas de gestión y control de los que aquí denominamos ciberriesgos.

La Dirección General de Seguros y Fondos de Pensiones (DGSFP), conocedora de esta realidad, incluye entre sus prioridades de supervisión en materia de riesgos para los ejercicios 2020-2022 el control del riesgo cibernético o ciberriesgos en las entidades y espera su inclusión dentro del riesgo operacional de las entidades, así como formando parte de sus escenarios ORSA.

En este contexto normativo, el gestor de riesgos ha de ser proactivo, tanto por la rápida evolución en la complejidad y alcance de esta tipología de riesgos, como por la normativa que lo acompaña, en caso contrario corre el riesgo de verse sobrepasado y quedar obsoleto. El área de Riesgos no puede, por tanto, permitirse el lujo de adoptar una postura reactiva ante los ciberriesgos ya que podría ser ya demasiado tarde para la empresa, ha de formarse e informarse para la adecuada toma de decisiones empresariales relativas a cualquier tipología de riesgos combinando la ciencia actuarial con los principios teóricos, prácticos y profesionales de ERM.

No existe un método infalible y único para evitar un ciberataque, sino una serie de herramientas y acciones complementarias que la empresa ha de integrar en su operativa diaria para mitigar su frecuencia y/o su impacto. Hablamos principalmente de medidas de seguridad tecnológica (antivirus, contraseñas seguras, copias de seguridad, cifrado de información, etc.), pero también de acciones de comunicación, concienciación y formación a los empleados para que interioricen la magnitud y complejidad del riesgo cibernético, y por supuesto de un sistema de gobierno que garantice la idoneidad, coherencia y coordinación de todas las estrategias de seguridad llevadas a cabo.

La complejidad a la hora de cuantificar en este tipo de riesgos operacionales y de definir un apetito de riesgo asociado es una complicación adicional en su proceso de valoración. La monitorización de toda la información de los dispositivos y sistemas de la empresa con el fin de detectar errores, vulnerabilidades o ataques es el punto de partida para una adecuada valoración. El objetivo de los procesos de monitorización de datos no es únicamente extraerlos, sino ser capaz de procesarlos e interpretarlos, así como definir un mitigante adecuado para reducir su potencial impacto, como, por ejemplo, una póliza de seguro adecuada.

El gestor de riesgos tiene el papel de liderar un proceso que cubre desde la propia identificación del riesgo, pasando por su incorporación y clasificación dentro del mapa de riesgos de la compañía, la medición de su frecuencia e impacto, establecimiento de posibles controles y planes de acción, e integración de su gestión dentro del sistema de gobierno de la entidad a través de su normativa interna (políticas, manuales, procedimientos, etc.).

La actual gestión de riesgos ha de clasificar y valorar riesgos que rara vez se encuadran en una sola categoría (financieros, técnicos o legales), sino que los impactos en muchos casos son transversales y difíciles de cuantificar porque apenas se cuenta con experiencia previa. Sin ir más lejos, los riesgos operacionales (clasificación en la que tendrían cabida los ciberriesgos), tienen hoy en día implicaciones de muy diversos tipos y con un componente reputacional cada vez más relevante e incierto.

No es un caso aislado, la evolución de los riesgos de ciberseguridad es asimilable a la de los riesgos ESG[4] y a los escenarios de pandemia, los cuales años atrás los identificábamos como riesgos "emergentes" pero que ahora forman parte tanto de nuestra realidad actual como de la emergente, dada su rápida evolución o mutación. En un escenario como el actual, donde las empresas han tenido que adaptarse a una situación creciente de teletrabajo, los ciberriesgos han tenido, si cabe, una mayor trascendencia, ya que los sistemas se han visto más expuestos a ciertas vulnerabilidades (asociadas fundamentalmente a la seguridad de la información) que antes de la pandemia eran limitadas en volumen y por tanto más sencillas de gestionar.

Para ello se ha de contar, por tanto, con la complicidad de toda la organización, desde el Consejo de Administración –responsable último de las políticas y del sistema de gobierno– hasta las áreas de negocio que tienen un conocimiento más preciso del riesgo y de su eventual impacto en la empresa.

Los ciberriesgos son sólo un ejemplo más de la importancia de la gestión de riesgos como motor y catalizador de las respuestas de la empresa ante este mapa de riesgos cambiante y complejo. Su adaptabilidad en este escenario va a ser capital y el gestor de riesgos ocupará un rol fundamental: su capacidad, experiencia, su visión global y sobre todo su actitud y anticipación ante los nuevos riesgos permitirá a la empresa estar mejor preparada frente a los próximos retos y eventos futuros. ●

4 Environmental, Social and Governance.