

# **Cyber, un riesgo difícil de precisar**



**Luis Alonso Serrano**  
Suscriptor Ciber Riesgos  
Cyber Underwriter



Los factores tecnológicos y regulatorios, que cambian a gran velocidad, hacen que los ciberriesgos sean impredecibles, pero con mayor experiencia y mejores herramientas, la amenaza puede hacerse más manejable.

## Resumen

Los ciberriesgos son una de las mayores amenazas que conforma el panorama del riesgo a día de hoy. Las encuestas <sup>(1)</sup> de los ejecutivos globales han situado los riesgos cibernéticos en una posición elevada, junto con la volatilidad geopolítica y el cambio climático, mientras que una encuesta a los gerentes de riesgos europeos citó los ciberriesgos como el riesgo de principal preocupación.

La tecnología es un impulsor importante del cambio político y económico, las dos causas principales de la creciente imprevisibilidad para las empresas, según revela el Índice de Imprevisibilidad de QBE. Las redes sociales están cambiando el debate político, mientras que se espera que las nuevas tecnologías, como por ejemplo los coches sin conductor, la robótica y la inteligencia artificial, tengan un gran impacto en la vida de las personas. Según McKinsey,

alrededor del 60% de las profesiones se verán afectadas de alguna manera por la automatización, mientras que podrían eliminarse hasta 800 millones de empleos actuales de aquí al 2030.

Actualmente la tecnología es un aspecto fundamental en la mayoría de las organizaciones, ya que da impulso a sus operaciones, cadenas de suministro y distribución. Sin embargo, el ritmo de adopción de la tecnología parece estar superando

# 800 millones

**de puestos de trabajo actuales podrían ser eliminados por la automatización antes del 2030**

las capacidades técnicas y de seguridad cibernética de la mayoría de los usuarios y empresas. Muchos no entienden completamente lo que significa el ciberriesgo para ellos, ni anticipan el impacto que puede causar en su negocio cuando algo falla.

En retrospectiva, muchos incidentes cibernéticos parecen predecibles, incluso prevenibles. Sin embargo, en comparación con riesgos como las catástrofes naturales o los

incendios, que se entienden bien y se pueden modelizar utilizando datos históricos de pérdidas, el riesgo cibernético es particularmente difícil de detectar. Cuándo, dónde y cómo se desarrollará un evento cibernético es muy difícil de predecir. Incluso cuando se pueden identificar escenarios probables, el impacto probable y la posible pérdida financiera pueden ser difíciles de anticipar y calcular.

(1) World Economic Forum Global Risks, 2019 PwC survey, <https://www.ferma.eu/2018-european-risk-manager-report>

## Incógnitas innumerables

La tecnología y los eventos cibernéticos implican lidiar con muchas incógnitas. Los incidentes cibernéticos provienen de una amplia gama de fuentes y desencadenantes, como por ejemplo ciberataques maliciosos, fallos técnicos, a través de la cadena de suministro o por un empleado deshonesto.

Las organizaciones no sabrán en qué parte del espectro recibirán el impacto o el grado del mismo. Además, como cada empresa tiene su propia configuración de TI, es difícil aprender de la experiencia de otras empresas.

Mantenerse al tanto del riesgo cibernético es también un desafío. Es una carrera interminable donde los hackers están siempre un paso por delante y las nuevas vulnerabilidades pueden surgir de situaciones inesperadas. Las amenazas emergentes incluyen la explotación

Mantenerse al tanto del riesgo cibernético es también un desafío. Es una carrera interminable donde los hackers están siempre un paso por delante y las nuevas vulnerabilidades pueden surgir de situaciones inesperadas.

de dispositivos IoT y las vulnerabilidades de hardware (tales como las amenazas Meltdown y Specter de 2018), mientras que la atención se

está centrando ahora en los ciberataques impulsados por la inteligencia artificial. Por muy robustas que sean las defensas de seguridad cibernética de una organización, ésta nunca será inmune.

Predecir el impacto de un incidente cibernético es particularmente difícil y varía ampliamente según la compañía, incluso para el mismo incidente. Por ejemplo, el ataque de malware NotPetya de 2017 causó una interrupción masiva en varias compañías, mientras que otras en el mismo sector resultaron ilesas.

La escala y la interconectividad impulsan los factores impredecibles: la violación de los datos del hotel Marriott del año pasado afectó a 500 millones de personas, mientras que el brote de ransomware de

WannaCry en 2017 afectó a unos 300.000 ordenadores en 150 países. Según una investigación reciente de Lloyd's de Londres, un gran ataque de malware contagioso a nivel mundial podría afectar a más de 600.000 empresas en todo el mundo y costaría unos 193 mil millones de dólares, tanto como lo que cuesta una catástrofe natural de gran envergadura.

### QBE Cyber

Nuestra póliza Cyber Response otorga protección frente a los distintos riesgos asociados a la tecnología digital.

[qbeespana.com/productos](https://qbeespana.com/productos)



Cyber es un área emergente de responsabilidad, donde vemos un alto grado de incertidumbre. El RGPD, por ejemplo, aún está en ciernes, pero la forma en que los reguladores obliguen a cumplir las nuevas leyes de protección de datos y privacidad será fundamental para las empresas tanto dentro como fuera de la Unión Europea.



## Interrupción de negocio

Eventos tales como WannaCry y NotPetya destacan el potencial de interrupción de negocio y pérdidas contingentes de interrupción de negocio relacionadas con incidentes de Cyber, que son particularmente difíciles de predecir y cuantificar dada la complejidad y las concentraciones de riesgo dentro de las cadenas de suministro físico y digital.



Por ejemplo, un fabricante que sufre una interrupción de los sistemas de TI podría compensar la pérdida de producción, pero se enfrentaría al coste adicional de encontrar soluciones y la posible pérdida de negocio. El año pasado, el fabricante de semiconductores TSMC se vio afectado por malware, lo que resultó en una pérdida de ingresos y costes adicionales del 3%. Las pérdidas por interrupción de negocio y gastos adicionales derivados del ataque NotPetya costaron 300 millones de dólares tanto al grupo de transporte Maersk como a la empresa de logística FedEx, mientras que como resultado de este ataque, el fabricante de alimentos Mondelez informó de pérdidas que superaron los 100 millones de dólares .

Como aseguradores de riesgos cibernéticos, vemos muchos incidentes en los que las empresas no han entendido completamente las repercusiones de un incidente cibernético. Incluso cuando una empresa se prepara para posibles escenarios cibernéticos, el desempeño de los planes de continuidad de negocio en la práctica es difícil de predecir. Reiniciar los sistemas en un entorno controlado, por ejemplo, es muy diferente a la realidad de reiniciar después de una interrupción o un ataque de ransomware.

## Incertidumbre regulatoria

El ritmo acelerado del cambio tecnológico es tal que los marcos regulatorios y legales están en continua evolución. Esto es especialmente cierto de cara a las leyes de privacidad y protección de datos, pero también en relación a los requisitos de seguridad cibernética y los regímenes de responsabilidad, por ejemplo, la introducción de automóviles autónomos, el IoT y la inteligencia artificial plantean cuestiones legales y reglamentarias.


Las nuevas regulaciones y las leyes no probadas crean incertidumbre para las empresas, desde el importe de las multas hasta la compensación que buscan los individuos afectados. Esto ya se puede ver en el Reglamento General de Protección de Datos (RGPD) de la UE, que introdujo estrictas normas de protección de datos y privacidad en mayo de 2018. El RGPD otorga mayores poderes a los reguladores y mejores

derechos a los consumidores, pero pasarán varios años antes de que las implicaciones del RGPD se entiendan completamente.

Cyber es un área emergente de responsabilidad, donde vemos un alto grado de incertidumbre. El RGPD, por ejemplo, aún está en ciernes, pero la forma en que los reguladores obliguen a cumplir las nuevas leyes de protección de datos y privacidad será fundamental para

las empresas tanto dentro como fuera de la Unión Europea. El RGPD se aplica a las empresas que tratan datos de la UE en cualquier parte del mundo, mientras que un número creciente de países están buscando ahora introducir requisitos similares.

El litigio también es un área emergente para Cyber. Hasta ahora, no hemos visto un volumen elevado de litigios, pero es evidente que existe un potencial de responsabilidad de terceros mucho mayor en el futuro. Las leyes como el RGPD facilitan que los individuos reclamen una indemnización después de un incidente cibernético, incluso por daños no financieros, como el daño moral. Las actitudes hacia la privacidad y la interrupción de servicio están cambiando, y un número creciente de incidentes



**Disponible próximamente**

Sea de los primeros en recibir una copia del Índice de Imprevisibilidad de QBE cuando sea publicado.

[qbeespana.com](http://qbeespana.com)

cibernéticos está llevando a acciones colectivas a medida que los inversores y los consumidores buscan una compensación por los daños sufridos.

## Prevención

Está claro que el riesgo cibernético no va a desaparecer. Sin embargo, una gestión sólida de los riesgos y una cobertura completa de seguros pueden cambiar las probabilidades y pueden ayudar a las organizaciones a lidiar mejor con los efectos.

La experiencia ha demostrado que una buena preparación puede reducir significativamente el impacto de una violación de datos, y al desarrollar una capacidad de recuperación general, una organización debería poder responder a cualquier evento cibernético, por inesperado que sea.

# 93%

**de los gerentes de riesgos están trabajando en estrecha colaboración con sus compañeros de TI**

# 37%

**ya identifica y evalúa los riesgos antes de que la empresa adopte nuevas tecnologías**

Las técnicas de gerencia de riesgos bien establecidas, por ejemplo, pueden ayudar a las empresas y a sus juntas directivas a medida que adopten la tecnología y acojan la digitalización. Una encuesta de gerentes de riesgos realizada por la Federación de Asociaciones de Gestión de Riesgos (FERMA) encontró que el 93% de los gerentes de riesgos están trabajando en estrecha colaboración con sus compañeros de TI y de seguridad cibernética, mientras que el 37% ya

identifica y evalúa los riesgos antes de que la empresa adopte nuevas tecnologías.

La digitalización está aún en una etapa incipiente. Pero a través de la experiencia, las empresas podrán llegar a comprender mejor el riesgo cibernético y la prevención. Mientras tanto, hay pasos que las empresas pueden tomar a día de hoy para reducir el riesgo. Por ejemplo, además de mantener una seguridad cibernética básica - como

tests de penetración, parches y formación, la planificación de un evento cibernético, como por ejemplo una interrupción o una violación de datos, puede reducir significativamente el impacto.

En un nivel alto, las empresas deberían planear detenidamente los casos hipotéticos de una interrupción o violación de datos, identificando los datos, servicios y terceros que son críticos para su negocio. Vale la pena dedicar



tiempo a analizar los escenarios con anticipación, preparando respuestas a las crisis y los planes de continuidad de negocio. La experiencia ha demostrado que una buena preparación puede reducir significativamente el impacto de una violación de datos, y al desarrollar una capacidad de recuperación general, una organización debería poder responder a cualquier evento cibernético, por inesperado que sea.

La tecnología también podría asistir a las empresas, proporcionando herramientas para ayudar a evaluar y cuantificar el riesgo cibernético. Las plataformas de evaluación de riesgo cibernético ya pueden evaluar y comparar el

riesgo cibernético y la seguridad cibernética de una organización, así como ayudar a cuantificar las pérdidas o mapear las cadenas de suministro. Estas herramientas se encuentran en sus primeras etapas de desarrollo, pero es probable que se vuelvan indispensables en los próximos años.

Las empresas también pueden transferir riesgos a las compañías de seguros, así como acceder a sus servicios y experiencia. Los productos de seguros cibernéticos están mejorando de manera constante y pueden aportar mayor comodidad a medida que las organizaciones invierten en nuevas tecnologías y modelos de negocios digitales.

## Pasos que puede aplicar para reducir el ciberriesgo:

### Buenas practicas de ciber seguridad:

✓ test de penetración

✓ parcheado

✓ formación

### Planificación en caso de un evento cibernético:

✓ corte

✓ violación de datos

## Sigamos en contacto

Si no se ha inscrito ya para recibir el  
Unpredictability Series, puede hacerlo en

**[qbeespana.com](http://qbeespana.com)**

abril 2019

QBE Europe SA/NV  
Sucursal en España  
Paseo de la Castellana, 31 – 5ª Planta  
28046 Madrid  
España

T: +34 91 789 39 50 | [qbe@es.qbe.com](mailto:qbe@es.qbe.com)

QBE European Operations es un nombre comercial de QBE UK Limited, QBE Underwriting Limited y QBE Europe SA/NV. QBE UK Limited está autorizada por el organismo Prudential Regulation Authority y regulada por los organismos Financial Conduct Authority y Prudential Regulation Authority. QBE Europe SA/NV. CIF: BE 0690 537 456. RPM/RPR Brussels, IBAN No. BE53949007944353 y SWIFT/BIC N° HSBCBEBB, autorizada por el Banco Nacional de Bélgica con número de licencia 3093.