Beazley Logo

Artículo

Ciberseguridad, inteligencia artificial y responsabilidad de los directivos: un nuevo frente de riesgo

Alberto Trojsi, Estefania Taboada • septiembre 23, 2026

La creciente digitalización de las empresas y la acelerada adopción de tecnologías como la inteligencia artificial han redefinido el mapa de riesgos corporativos en la actualidad. En España, donde el tejido empresarial combina grandes corporaciones con pymes altamente dependientes de terceros tecnológicamente, esta evolución traslada la exposición desde el ámbito operativo al de la alta dirección.

Cada vez con más frecuencia, incidentes tecnológicos (ya sean ataques deliberados o fallos internos) **derivan en pérdidas económicas relevantes, interrupciones de negocio y**, en última instancia, **en cuestionamientos sobre la actuación de los órganos de gobierno.**

Del ciberataque al error sistémico

Tradicionalmente, el foco de la ciberseguridad se centraba en prevenir ataques externos, como el ransomware o el robo de datos. Sin embargo, recientes incidentes han demostrado que **los eventos no maliciosos también pueden generar un impacto significativo**. Casos como interrupciones en servicios digitales, fallos en proveedores tecnológicos o errores en actualizaciones de software han puesto de manifiesto la fragilidad de los ecosistemas digitales. Estos eventos, aunque no respondan a una intención maliciosa, pueden provocar paradas operativas, pérdida de ingresos y daños reputacionales.

A este cambio de paradigma se suma además una evidencia creciente sobre el impacto real de los incidentes cibernéticos en el negocio. Un análisis reciente publicado por el *Harvard Law School Forum on Corporate Governance*[1] muestra que las empresas afectadas por

ciberincidentes de relevancia no solo sufren una caída inmediata en el valor de sus acciones, sino que este impacto es sostenido en el tiempo y puede prolongarse más allá de un año desde el incidente. La investigación apunta a que estos eventos generan una infravaloración progresiva frente al mercado, con efectos acumulativos que reflejan no solo el daño inicial, sino también la pérdida de confianza, la disrupción operativa y las debilidades estructurales que el incidente pone al descubierto.

“Las empresas deben asumir que el riesgo ya no proviene únicamente de ataques externos, sino también de la complejidad de sus propias infraestructuras digitales a escala global” señala **Alberto Trojsi, Cyber Regional Manager para el sur de Europa.**

El riesgo escala al consejo

Cuando un incidente afecta significativamente al negocio , ya sea desde un punto de vista financiero, operativo o reputacional, **la atención se desplaza rápidamente hacia el consejo de administración y el equipo directivo**. Los accionistas, inversores y otras partes interesadas analizan entonces si los responsables de la empresa han cumplido con su deber y se investiga si han evaluado adecuadamente los riesgos, si han implementado medidas de protección suficientes y si han reaccionado de forma adecuada ante el incidente. Como explica **Estefanía Taboada, Underwriting Manager Financial Lines**: “Cualquier evento que impacte en el rendimiento de la compañía puede derivar en una reclamación contra directivos si existe la percepción de que no se ha actuado con la diligencia debida”.

Este tipo de reclamaciones, además, no se resuelven de forma inmediata. Pueden prolongarse durante años, obligando a los directivos a justificar decisiones tomadas antes, durante y después del incidente.

La inteligencia artificial añade presión

A este escenario se suma la irrupción de la inteligencia artificial, que introduce nuevas variables de riesgo. **La IA está abriendo nuevas áreas de análisis para los aseguradores, especialmente en lo que respecta a la toma de decisiones estratégicas por parte de los equipos directivos.**

Esto es debido a que, mientras las empresas están invirtiendo en estas tecnologías con expectativas de eficiencia y crecimiento, también existe un alto grado de incertidumbre en torno a ellas y a su implementación. **Los mercados y los inversores comienzan a exigir transparencia sobre el uso de la IA, su impacto en el negocio y el retorno esperado de estas inversiones.** Una gestión inadecuada o una comunicación poco clara pueden generar dudas y, en consecuencia, conflictos legales.

Gobernanza y resiliencia: claves para mitigar el riesgo

Ante este entorno, la gestión del riesgo ciber y tecnológico se ha convertido en una cuestión de gobierno corporativo. Ya no se trata únicamente de una responsabilidad del departamento de IT, sino de un tema estratégico que debe abordarse desde el consejo. Por esta razón,

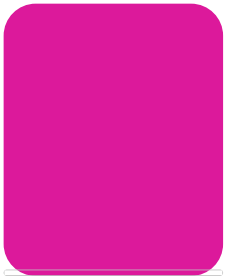
entre otros aspectos, en la actualidad se analizan la existencia de planes de continuidad de negocio, la realización de simulaciones de incidentes, la gestión de proveedores tecnológicos, la inversión en ciberseguridad y la contratación de coberturas adecuadas.

En este contexto, soluciones como el seguro de responsabilidad de administradores y directivos (D&O), combinado con soluciones como Full Spectrum Cyber, permiten a las empresas transferir parte del riesgo y acceder a servicios de prevención y respuesta.

Más allá de la protección

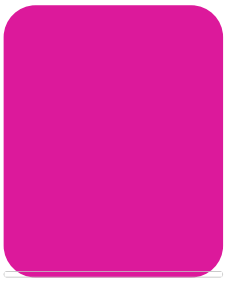
El papel del seguro está evolucionando desde una función reactiva hacia una herramienta estratégica. No solo cubre las pérdidas económicas, sino que también proporciona acceso a expertos, apoyo en la gestión de crisis y acompañamiento en la toma de decisiones. En un entorno donde los riesgos son cada vez más complejos y están interconectados, la combinación de prevención, gobernanza y transferencia del riesgo es fundamental para proteger tanto a las empresas como a sus equipos directivos.

En definitiva, la convergencia entre ciberseguridad, inteligencia artificial y responsabilidad de los directivos está configurando un nuevo escenario en el que la anticipación y la resiliencia marcan la diferencia.



Alberto Trojsi

Cyber Regional Manager para el sur de Europa



Estefania Taboada

Underwriting Manager - Financial Lines

1. The Sustained Negative Impacts of Cyber Incidents on 1. Shareholder Value

Home