Markel Cyber

Asegura tu tranquilidad

MARKEL

Markel Cyber

La transformación digital ha cambiado de forma irreversible la manera en que operan los negocios. La tecnología ya no es un recurso auxiliar, sino el núcleo de la actividad empresarial: optimiza procesos, mejora la experiencia del cliente y abre nuevos mercados. Sin embargo, esta dependencia creciente también amplía la superficie de exposición al riesgo. Los ciberincidentes, ya sea por la sofisticación de los ataques o por la sensibilidad de los datos gestionados, pueden comprometer la continuidad del negocio con consecuencias financieras y reputacionales severas.

Gestionar este riesgo de forma adecuada es hoy una necesidad estratégica. El seguro Markel Cyber está diseñado precisamente para ello: ofrece cobertura frente a las responsabilidades y pérdidas derivadas de incidentes cibernéticos que puedan producirse en el desarrollo de la actividad empresarial, brindando una respuesta integral cuando más se necesita.

¿Qué pérdidas puedo tener?

- Gastos de defensa
- Daños
- Costes de notificación y mitigación de violación de la privacidad
- Costes de restablecimiento de sistemas y datos
- Pérdida de beneficio
- Daño reputacional
- Costes de extorsión

¿A qué reclamaciones puede enfrentarse?

- Demanda de indemnización, daños y perjuicios o reparación interpuesta por un tercero, incluyendo medidas cautelares o la afirmación de responsabilidad.
- Procedimiento civil que solicite daños, reparación no monetaria o medidas cautelares, iniciado mediante demanda o escrito equivalente.
- Arbitraje, mediación u otro mecanismo alternativo de resolución de conflictos que solicite daños o reparación.
- Solicitud escrita para suspender o renunciar a un plazo de prescripción aplicable a cualquiera de las reclamaciones anteriores.
- Requerimiento de información o procedimiento iniciado por una autoridad gubernamental o reguladora, ya sea a nivel nacional o extranjero.

Más allá de los ataques externos, las empresas también se exponen a sanciones derivadas del incumplimiento de normativas como PCI DSS y el Reglamento General de Protección de Datos, cuya aplicación en España corresponde a la AEPD. El incumplimiento de PCI DSS puede acarrear multas significativas y la pérdida de la capacidad para procesar pagos con tarjeta, con el consiguiente daño operativo y reputacional. Las infracciones en materia de protección de datos, por su parte, pueden derivar en sanciones de gran cuantía, especialmente cuando se acredita que la empresa no adoptó medidas razonables para proteger la información personal de sus clientes.

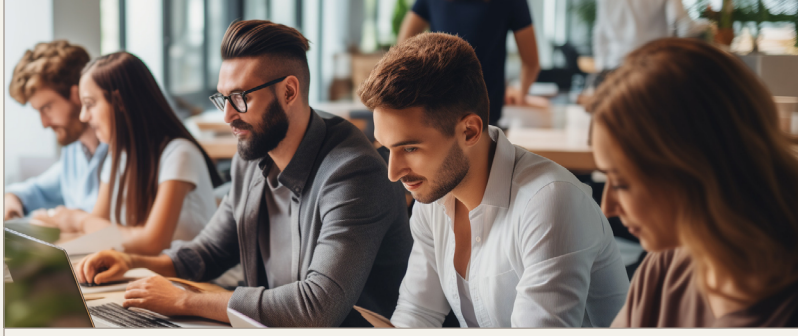
El cumplimiento normativo, en definitiva, no es solo una obligación legal: es un factor determinante para la estabilidad financiera y la confianza del cliente.

¿Cómo pueden protegerse las PYMEs?

La ciberseguridad no es exclusiva de las grandes corporaciones. Con recursos limitados pero bien dirigidos, una PYME puede reducir significativamente su exposición al riesgo. Estas son las medidas fundamentales:

- **Formación del personal:** el error humano sigue siendo la principal puerta de entrada de los ciberataques. Formar a los empleados en buenas prácticas, mantener contraseñas robustas y realizar simulaciones de phishing periódicas son acciones de alto impacto y bajo coste.
- **Protección del entorno tecnológico:** contar con software antivirus actualizado y aplicar los parches de seguridad de sistemas y aplicaciones de forma sistemática elimina gran parte de las vulnerabilidades conocidas.
- **Copias de seguridad:** realizar copias regulares de los datos críticos y almacenarlas en ubicaciones seguras, ya sea en la nube o en dispositivos externos, es la primera línea de defensa frente a un ataque de ransomware.
- **Control de accesos:** limitar el acceso a la información sensible exclusivamente al personal autorizado reduce el riesgo de brechas internas y minimiza el daño en caso de que una cuenta se vea comprometida.
- **Transferencia del riesgo residual:** ninguna medida preventiva elimina el riesgo por completo. Contar con un ciberseguro permite afrontar las consecuencias financieras y operativas de un incidente cuando las barreras técnicas no son suficientes. Además, pone a disposición de la empresa un gestor de incidentes especializado desde el primer momento, eliminando la improvisación en situaciones de alta presión.

Implementar estas medidas no solo protege a la empresa frente a posibles ataques, sino que refuerza la confianza de clientes y socios en su capacidad para gestionar la información con responsabilidad.



Ejemplos de incidentes:

- **Ransomware:** un ataque cifra los sistemas y exige un rescate para restablecer el acceso, paralizando la operativa.
- **Brecha de datos:** un acceso no autorizado expone información de clientes, con el consiguiente riesgo regulatorio y reputacional.
- **Ataque a proveedor tecnológico:** una brecha en un tercero con acceso a los sistemas provoca una interrupción del negocio sin que la empresa sea el objetivo directo.
- **Ataque de Denegación de Servicio (DoS):** una avalancha de tráfico malicioso inutiliza la plataforma digital, generando pérdida de ingresos y daño reputacional.
- **Transferencia fraudulenta de fondos:** un empleado es manipulado para ejecutar un pago a una cuenta fraudulenta suplantando a un proveedor o directivo.

Coberturas disponibles para hacer frente a los incidentes:

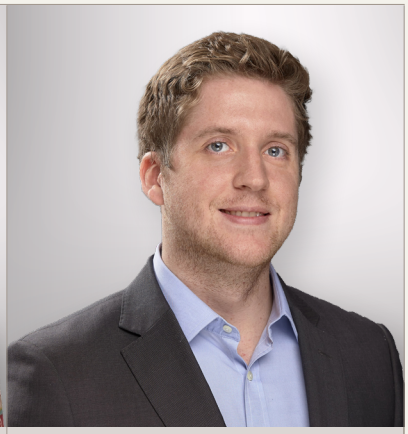
- Respuesta a Incidentes
- Responsabilidad Cibernética y de Privacidad
- Investigaciones Regulatorias y Multas
- Responsabilidad por Contenidos Digitales
- Investigaciones y Multas PCI DSS
- Costes de Notificación y Mitigación por Brecha de Privacidad
- Costes de Restablecimiento de Sistemas y Datos
- Interrupción del Negocio
- Costes de Extorsión
- Robo Cibernético
- Robo por Ingeniería Social
- Daño al Hardware (Bricking)
- Fraude en Telecomunicaciones
- Crypto-Jacking

Nuestro equipo

Nuestro equipo de Riesgo Cibernético está formado por especialistas con amplia experiencia en la evaluación y transferencia del riesgo digital. Con un conocimiento profundo del panorama de amenazas, asesoramos a nuestros clientes en la estructuración de coberturas adaptadas a su perfil de exposición y les acompañamos en cada etapa, desde el análisis previo hasta la gestión del siniestro. Nuestro enfoque combina rigor técnico y visión aseguradora para convertir la incertidumbre cibernética en un riesgo gestionado.

Lola Cabello

Head of Corporate Financial Lines



Benjamín Pellegrini

Senior Underwriter Cyber

MARKEL

Madrid
Torre de Cristal, Paseo de la Castellana 259C, Planta 34,
28046 Madrid
Tel: +34 917 88 61 50

Barcelona
Avenida Diagonal, 613. Plta. 4-A, 08028 Barcelona
Tel: +34 93 445 3430

markel.com.es