Markel Cyber

Asegura tu tranquilidad

MARKEL

Markel Cyber

El auge de las tecnologías y la mayor dependencia en los negocios de los sistemas informáticos ha supuesto una revolución de la que somos partícipes día a día y que está en continua evolución. La inversión en nuevas tecnologías se convierte en clave para optimizar los negocios y mejorar los servicios a los clientes independientemente de la rama de negocio. Sin embargo, la otra cara de la moneda es que éstas tecnologías suponen una nueva vulnerabilidad para los negocios, tanto si es por la alta sofisticación de las tecnologías utilizadas, como por la sensibilidad de los datos gestionados por la empresa. Por tanto, es fundamental tomar las medidas pertinentes para gestionar este creciente riesgo.

Una solución dentro de la gestión de los riesgos cibernéticos es el seguro Markel Cyber que está diseñado para protegerle frente a responsabilidades y pérdidas específicas a las que pueda verse expuesto como resultado de incidentes cibernéticos concretos que se produzcan en el transcurso de sus actividades empresariales.

¿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
- Pérdida de beneficio por fallo del sistema
- Costes de extorsión

¿A qué reclamaciones puede enfrentarse?

- Demanda por parte de un tercero de indemnización o daños y perjuicios o de reparación no monetaria o cautelar o la afirmación de responsabilidad
- Procedimiento civil que solicite daños y perjuicios o reparación no monetaria o cautelar, iniciado mediante la notificación de una demanda o escrito similar
- Arbitraje, mediación u otro procedimiento alternativo de resolución de conflictos que solicite daños y perjuicios o reparación no monetaria o cautelar
- Solicitud por escrito para que se suspenda o se renuncie a un plazo de prescripción aplicable a una Reclamación de las mencionadas en los apartados (a) a (c) anteriores;
- Solicitud o requerimiento de información o demanda civil, procedimiento incoado por o en nombre de cualquier entidad gubernamental federal, estatal, local o extranjera con capacidad reguladora u oficial.

Además de los desafíos de seguridad cibernética, las PYMEs deben tener en cuenta las repercusiones financieras derivadas del incumplimiento de regulaciones como PCI DSS y la AEPD. El no cumplir con PCI DSS puede acarrear multas cuantiosas y la revocación de la capacidad para procesar pagos con tarjeta, lo que podría afectar negativamente a la reputación y la estabilidad financiera de la empresa.

Por otro lado, las multas impuestas por la AEPD por infringir la privacidad de los datos pueden ser considerablemente elevadas. Especialmente si se demuestra que la empresa no ha implementado medidas suficientes para proteger la información personal de sus clientes, estas multas podrían tener un impacto devastador en las finanzas y la reputación de la empresa.

En resumen, el cumplimiento de estas regulaciones va más allá de una cuestión de seguridad, ya que también es vital desde una perspectiva financiera para evitar sanciones económicas y salvaguardar la confianza del cliente.

¿Cómo pueden protegerse las PYMEs?

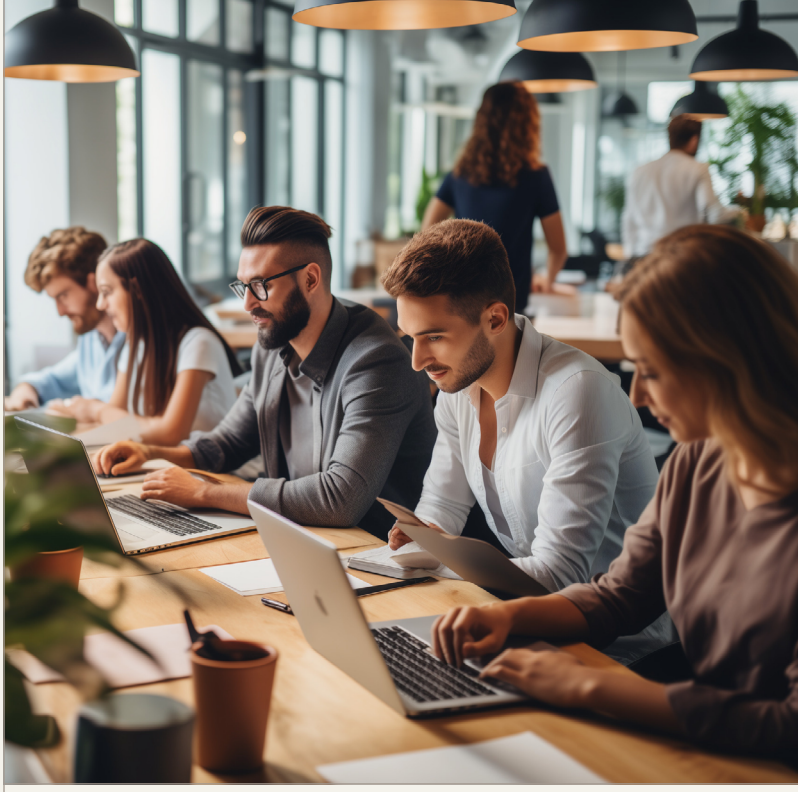
En la era digital actual, la ciberseguridad es fundamental para proteger los datos sensibles y la continuidad del negocio en las PYMEs. Aunque pueden carecer de los recursos de grandes corporaciones, existen medidas clave que pueden implementar para mejorar su ciberseguridad.

Primero, es crucial educar a los empleados sobre prácticas seguras y la importancia de mantener contraseñas robustas y actualizadas. Realizar formaciones periódicas y simular ataques de phishing puede ayudar a sensibilizar al personal.

Además, implementar un software antivirus y mantenerlo actualizado es esencial para detectar y eliminar amenazas. Asimismo, es importante realizar copias de seguridad regulares de los datos críticos y almacenarlas en ubicaciones seguras, ya sea en la nube o en dispositivos externos. Otro paso importante es mantener actualizados todos los sistemas y aplicaciones, ya que los parches de seguridad suelen corregir vulnerabilidades conocidas.

Limitar el acceso a los datos sensibles solo a empleados autorizados mediante controles de acceso también puede reducir el riesgo de brechas de seguridad.

Implementar estas medidas no solo protegerá a la PYME de posibles ataques cibernéticos, sino que también fortalecerá la confianza de los clientes y socios comerciales en su capacidad para proteger sus datos.



Ejemplos de incidentes:

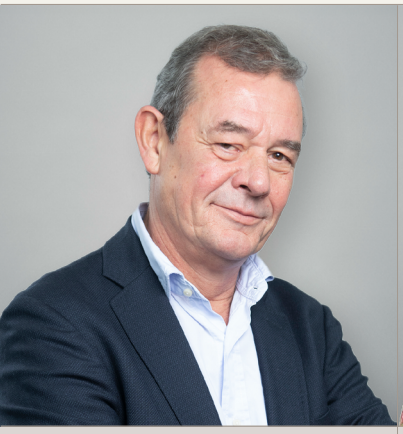
- Incidentes de seguridad en la red como Virus Informático, Incidente de Hacking, Ataque de Denegación de Servicio
- Incidente de violación de datos físicos
- Incidente de violación de datos electrónicos

Coberturas disponibles para hacer frente a los incidentes:

- Respuesta a incidentes
- Responsabilidad cibernética y de privacidad
- Procedimientos legales y multas reglamentarias
- Costes de Notificación y Mitigación de Violación de la Privacidad
- Costes de restablecimiento de sistemas y datos
- Pérdida de beneficio
- Costes de extorsión

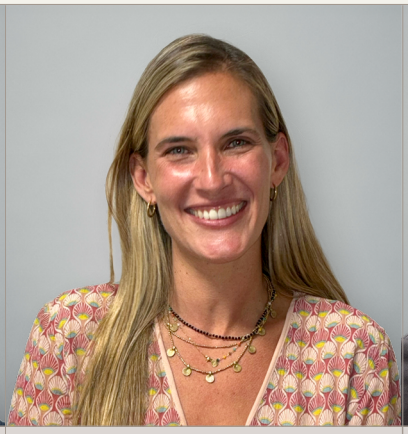
Nuestro equipo

Nuestro equipo de ciberseguridad está compuesto por un grupo de expertos altamente capacitados y dedicados a proteger su información más valiosa. Con años de experiencia en el campo y un profundo conocimiento de las amenazas actuales, nuestro equipo trabaja incansablemente para garantizar la seguridad y la integridad de sus datos. Con soluciones innovadoras y un enfoque proactivo, estamos aquí para brindarle la tranquilidad que necesita en un mundo digital en constante evolución.



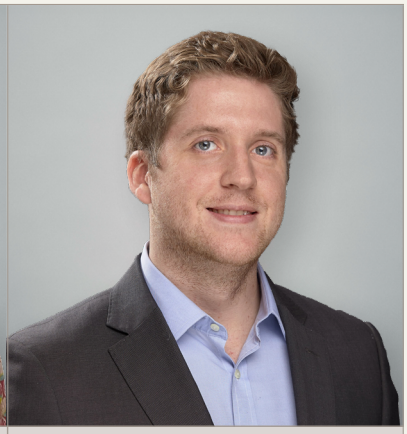
Carlos Peña

Director de Líneas Financieras



Lola Cabello

Head of Corporate Financial Lines



Benjamín Pellegrini

Senior Underwriter Cyber

MARKEL

Markel

Madrid
Plaza Pablo Ruiz Picasso, 1. Planta 35.
Edificio Torre Picasso. 28020 Madrid
Tel: +34 91 788 6150

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

markel.com.es