



**Súmate y aprovecha nuestra experiencia**  
**Protección ante las consecuencias de los ciber riesgos**

A close-up photograph of a person's hands typing on a laptop keyboard. The person is wearing a green long-sleeved shirt. The background is blurred, showing a white surface and a blue light source. The text '¿En qué consiste el ciber riesgo?' is overlaid on the image, framed by four white corner brackets.

¿En qué consiste  
el ciber riesgo?

**CyberEdge® es una solución aseguradora completa de gestión de riesgos ofrecida por AIG. La mejor forma de protegerse ante ciber ataques es la prevención aunque en ocasiones ello no resulta suficiente para sufrir una fuga de datos. En el caso de que se vea comprometida su primera línea de defensa, CyberEdge responde en la gestión y control del impacto que ello supone para así desarrollar normalmente la actividad empresarial.**

CyberEdge combina protección aseguradora y herramientas de gestión de riesgo con acceso a expertos independientes. Ayudamos a las entidades a proteger su patrimonio ante posibles fugas de seguridad, ataques hacker, virus informáticos, empleados deshonestos o negligentes, fuga de información y robo de identidad entre otros.



Cyberedge proporciona cobertura ante las evidentes, y no tan evidentes, consecuencias de los ciber riesgos. Contamos con un equipo de suscriptores y tramitadores de siniestros con amplia experiencia en este campo, así como un panel de expertos independientes que ayudan a afrontar la estrategia de gestión de este tipo de riesgo.



CyberEdge está diseñado para responder ante las diferentes modalidades de los ciber riesgos no cubiertos por los seguros tradicionales de responsabilidad civil y daños propios



CyberEdge proporciona acceso a recursos de terceros con experiencia en la gestión de riesgo de fugas de seguridad, incluyendo servicios de informática forense, asesoramiento legal y restitución de imagen.



## ¿Qué ofrece CyberEdge?

CyberEdge ayuda a gestionar un incidente de forma ágil y eficaz.

Porque no todo riesgo es igual, ofrecemos diferentes módulos de cobertura adaptadas a las necesidades de cada empresa.

### **Gestión de incidentes**

Contamos con un centro de atención telefónico 24horas/7 días a la semana para reportar fallos de seguridad o sistemas y fugas de datos. CyberEdge cubre los gastos de asesores legales, informáticos forense y consultores de imagen para gestionar y mitigar cualquier incidente cibernético. Si el incidente convierte datos o software en ilegibles, CyberEdge cubre los gastos de su reconstrucción. La notificación y el control de identidad también quedan cubiertos.

### **Seguridad y responsabilidad**

Se proporciona cobertura ante reclamaciones de terceros derivadas de un fallo de seguridad, error de mantenimiento de sistemas e incidente de protección de datos. También responde ante inspecciones regulatorias derivadas de un uso indebido, control o proceso de datos personales.

### **Interrupción en las redes**

Mediante esta cobertura se responde a una interrupción material del negocio derivada de un fallo del sistema de seguridad, reembolsando los gastos incurridos para paliar la interrupción, el incremento de gastos operacionales y el cálculo de la pérdida de beneficio.

## Una solución completa

Una respuesta adecuada incluiría:

- Acceso a consultores globales 24h/7 días semana
- Un asesor de respuesta con experiencia en este complejo ámbito regulatorio
- Asesoría a la hora de notificar a los afectados
- Informáticos forense para investigar, contener, resolver y remediar el incidente para así continuar desarrollando la actividad empresarial
- Gestión del riesgo para mitigar el daño reputacional
- Control de identidad de crédito a los sujetos afectados
- Expertos para ayudar a calcular la pérdida de beneficio derivada de una interrupción en la red

### Cobertura proveedor externo de servicios

Se proporciona cobertura a los fallos de seguridad padecidos por el proveedor externo de servicios que conlleven la pérdida de datos protegidos o que impidan acceder a los datos o servicios que presta. Cyberedge cubre los costes de asesoramiento para gestionar y mitigar el incidente así como los gastos de reconstrucción de los datos, software y pérdida de beneficios.

### Incidente de datos electrónicos

Las pólizas de daños tradicionales proporcionan cobertura a los daños tangibles que padecen los bienes asegurados mientras que esta extensión cubre los gastos de reconstrucción y recreación de datos afectados como consecuencia, entre otros, de un incendio, tormenta e inundación. Se proporciona cobertura a la reconstrucción de datos y software así como a la interrupción de redes en el caso que se activen los supuestos de cobertura y no se pueda acceder o usar los datos.

### Ciber extorsión.

Se da cobertura a la amenaza de ataques de seguridad intencionados por parte de un tercero con el propósito de recibir una recompensa económica o cualquier otro tipo de valor mobiliario. Se incluyen también los gastos de investigación y el dinero del rescate para poner fin a la amenaza.

Cobertura aseguradora completa y acceso a expertos que proporcionan consejo y actúan en nombre de la compañía ante un incidente

### Cronología de una fuga de seguridad y respuesta proporcionada por CyberEdge

Riesgos a considerar

Respuesta CyberEdge



# Aplicaciones CyberEdge

## CyberEdge App

Nuestra app muestra las últimas noticias relacionadas con el ciber riesgo, información en tiempo real de fugas de seguridad por países de ocurrencia, una herramienta para calcular el impacto económico de una fuga, calendario de eventos y un glosario de ciber términos. Se incluyen más de 20 casos de siniestros con una descripción de cómo han gestionado otras empresas las fugas que han padecido.



## CyberEdge RiskTool

Un sitio web que simplifica el proceso de gestión de riesgo en función del tamaño o complejidad de cada entidad. CyberEdge RiskTool ofrece consejo sobre cómo gestionar los diferentes riesgos regulatorios y normativos vinculados a las fugas de datos así como información diversa relativa a los ciber riesgos. Puede también ser utilizado por nuestros clientes como herramienta de formación de gestión de riesgo y procesos normativos.

## AutoShun®

AutoShun es un aparato de hardware proporcionado por un tercero que se sitúa entre el firewall de nuestros clientes y el internet externo. Ayuda a parar ciber ataques en tiempo real bloqueando comunicación interna y externa provenientes de direcciones IP no identificadas.

