La póliza de ciber protección es un seguro diseñado para ayudar a una empresa cuando sufre un incidente de ciberseguridad, como un secuestro de datos, un robo de datos, un acceso indebido a sus sistemas o un fallo que expone información sensible.

Piensa en ella como un equipo de emergencia + un seguro financiero: primero actúan para ayudarte a solucionar el problema, y después cubren los costes derivados.

1. Ayuda inmediata cuando ocurre un incidente

En cuanto la empresa detecta un problema, puede llamar al equipo de respuesta de la aseguradora. Este equipo trabaja 24/7 y coordina todo lo que hay que hacer.

- ✓ Forenses informáticos: especialistas que investigan qué ha pasado, qué sistemas han sido afectados, si siguen en riesgo y cómo frenar el ataque.
- ✓ Gestión de crisis: expertos que ayudan a la empresa a organizarse en momentos de caos, priorizar decisiones y mantener la calma.
- ✓ Coordinación con proveedores expertos: la aseguradora tiene acuerdos con empresas líderes en ciberseguridad, legales y de comunicación, y los activa de inmediato.

En lugar de buscar proveedores en mitad de la crisis, ya los tienes disponibles automáticamente.

Y se presta sin aplicación de franquicia alguna

2. Cumplir las leyes y obligaciones en caso de fuga de datos

Si la empresa pierde datos personales (clientes, empleados, usuarios…), hay normas que obligan a:

- informar a las autoridades (como la AEPD) comunicar a los afectados
- documentar qué ocurrió demostrar que se ha actuado correctamente

La póliza ofrece:

- ✓ Asesoramiento legal especializado
- ✓ Abogados expertos en privacidad te explican qué leyes aplican y qué pasos debes dar.
- ✓ Preparación y envío de notificaciones oficiales Ellos redactan, revisan y gestionan todo el proceso.
- ✓ Respuesta legal ante requerimientos de autoridades, Por ejemplo, si la AEPD pide explicaciones.

3. Comunicación a los afectados

Si los datos de clientes o empleados quedan expuestos, la póliza cubre:

- ✓ El coste de enviarles comunicaciones formales: Emails, cartas, llamadas… todo lo necesario.
- ✓ Call center o líneas de atención para atender preguntas de las personas afectadas.
- ✓ Servicios de protección de identidad (en países donde aplique), como

monitorización de crédito.

Objetivo: que la empresa gestione la situación con transparencia y profesionalidad.

4. Gastos propios para recuperar sistemas y operaciones

Tras un ataque, es habitual que los sistemas estén caídos, corruptos o dañados. La póliza de ciber protección cubre:

- ✓ Restauración de datos: recuperar bases de datos, aplicaciones y configuraciones.
- ✓ Restauración de sistemas: volver a poner en funcionamiento servidores, equipos, redes…
- ✓ Servicios técnicos externos: cuando se necesita personal especializado para restablecer la actividad.

5. Extorsión cibernética / ransomware

Si los atacantes exigen un rescate para devolver datos o desbloquear sistemas, la póliza incluye:

- ✓ Expertos en negociación: gente con experiencia que trata directamente con los delincuentes.
- ✓ Análisis de legalidad: determinar si es legal o no pagar un rescate en ese caso.
- ✓ Gastos derivados de la extorsión: incluido el rescate y los costes técnicos asociados al incidente.

6. Pérdida de ingresos y gastos adicionales (interrupción del negocio)

Si la empresa se paraliza por un ataque, puede perder ventas y tener gastos extra para seguir operando.

La póliza cubre:

- ✓ Los ingresos perdidos durante el tiempo que el negocio no puede funcionar.
- ✓ Los gastos adicionales para continuar la actividad (por ejemplo, alquilar equipos temporales).

7. Responsabilidad frente a terceros

Si un cliente, proveedor u otra persona te reclama porque sus datos fueron comprometidos, la póliza cubre:

- ✓ Defensa legal: Abogados, costes de juicio…
- ✓ Indemnizaciones: Las cantidades que la empresa deba pagar a los afectados.
- ✓ Acuerdos extrajudiciales: soluciones negociadas antes del juicio.

8. Daño reputacional y comunicación

En casos graves, puede haber impacto mediático.

La póliza cubre:

- ✓ Consultores de comunicación Gestión de reputación
- ✓ Mensajes clave para medios y clientes

Lo que ayuda a que la empresa mantenga la confianza de sus clientes durante la crisis.

¿Qué cubren los servicios?

La póliza de ciber protección cubre los servicios de emergencia para contener y gestionar un ataque + los costes para recuperar la actividad + la responsabilidad legal frente a terceros.

Es un producto muy orientado a gestión de incidentes y no solo a "pagar indemnizaciones".

Los servicios de la póliza de ciber protección, ¿aplican a cualquier incidente cubierto?

Sí, los servicios de respuesta se activan para la mayoría de los incidentes cubiertos por la póliza, especialmente cuando hay:

- ✓ acceso indebido a sistemas fuga o,
- ✓ posible fuga de datos ransomware
- ✓ ataque de malware
- ✓ compromiso de cuentas (phishing, BEC, etc.)
- ✓ interrupción del sistema causada por un ataque extorsión cibernética

En todos estos casos, el panel de respuesta de la aseguradora (forenses, abogados, comunicación, etc.) se pone en marcha desde el minuto cero, que es lo que constituye el valor diferencial de estas pólizas.

Resumen rápido:

¿Qué tipo de incidente?	¿Se activan los servicios BBR?	Comentario
Ransomware	Sí	Uno de los casos más típicos
Fuga o posible fuga de datos	Sí	Se activa legal + forense + comunicación
Malware en sistemas críticos	Sí	Si afecta a operaciones o datos
Compromiso de correo (BEC)	Sí	Muy habitual
Fallo interno sin ataque	No	No es incidente cibernético cubierto
Extorsión sin evidencia	Depende	Se analiza caso a caso
Problemas operativos no ciber	No	No aplica el panel

Cobertura del Proveedor Externo

La cobertura de la póliza entra en funcionamiento, aunque el incidente se origine en un proveedor externo, pero no cubre al proveedor como asegurado, sino las consecuencias que su fallo cause en tu empresa.

Ejemplos:

- ✓ Un proveedor de IT sufre un ataque y contagia tus sistemas.
- ✓ Un servicio cloud sufre una brecha y exponen datos de tu empresa.
- ✓ Un outsourcer borra datos accidentalmente o por error.
- ✓ Una consultora deja un puerto abierto y facilita un ataque.
- ✓ Si el proveedor es un "encargado del tratamiento" (RGPD): los incidentes en un encargado del tratamiento se consideran incidentes de tu propia empresa a nivel normativo.

Aunque técnicamente el proveedor sea quien falla, legalmente la responsabilidad primaria es tuya y los daños los sufres tú, así que la póliza te protege. Todos los servicios de la póliza se activan de la misma manera.

Lo que NO incluye esta cobertura:
Casos en los que:

- ✓ El proveedor no tenga relación con datos o sistemas críticos de tu empresa
- ✓ No haya impacto en tu empresa.
- ✓ El incidente ocurra solo dentro del entorno del proveedor, sin afectarte.
- ✓ La relación contractual no está clara o no involucra datos/sistemas de tu empresa.

El proveedor no está cubierto por tu póliza.
No cubre gastos propios del proveedor
No cubre sanciones al proveedor
No cubre interrupción de negocio del proveedor
No cubre servicios para el proveedor directamente

Tú estás cubierto. El proveedor no.