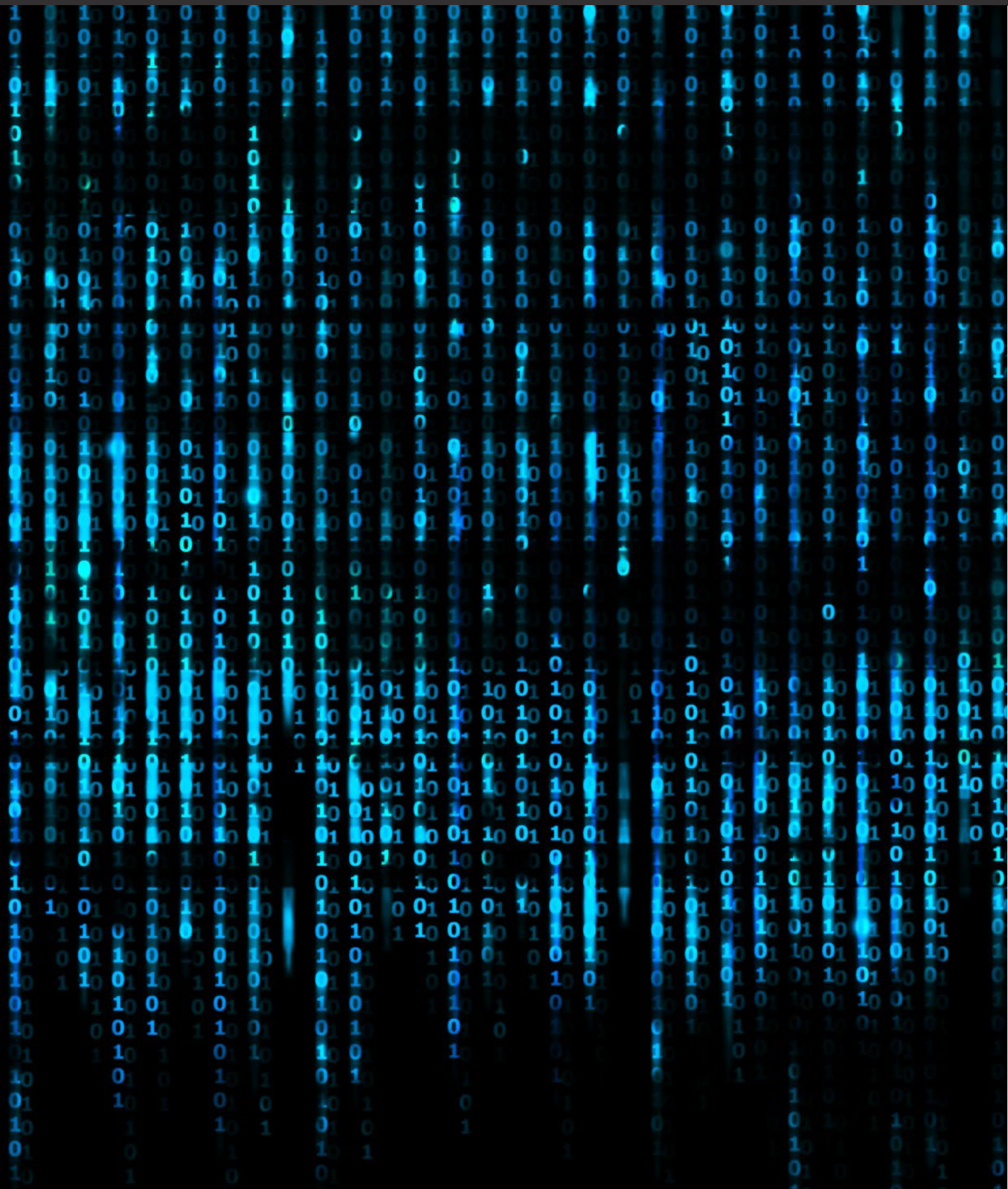
HISCOX

# HISCOX CYBERCLEAR 360º

## CONDICIONES ESPECIALES



# Índice de contenidos

# Resumen de coberturas*

| | | |
|---|---|---|
| **Servicio de respuesta a incidentes** | | 100% del límite |
| a. | Servicio de contención tecnológica | ✓ |
| b. | Servicio de asesoramiento jurídico y de comunicación y relaciones públicas | ✓ |
| c. | Gastos de notificación y monitorización | ✓ |
| **Pérdidas del asegurado** | | |
| a. | Gastos de recuperación de datos y sistemas | 100% del límite |
| b. | Extorsión cibernética | mínimo 50% del limite |
| c. | Protección de equipos (sustitución o reparación de equipos) | mínimo 20.000€ por incidente y periodo de seguro |
| d. | Pérdida de beneficios (opcional) | Consulte las condiciones particulares |
| e. | Proveedor externo tecnológico (opcional) | Consulte las condiciones particulares |
| **Fraude tecnológico** | | |
| a. | Uso fraudulento de su identidad electrónica | mínimo 25.000€ |
| b. | Robo electrónico de fondos | mínimo 25.000€ |
| c. | Modificación de precios online | mínimo 25.000€ |
| d. | Fraude en servicios contratados | mínimo 25.000€ |
| e. | Suplantación de identidad (opcional) | Según sublímite seleccionado |
| **Responsabilidad tecnológica** | | 100% del límite |
| a. | Indemnizaciones por responsabilidad ante terceros | ✓ |
| b. | Gastos de defensa | ✓ |
| c. | Gastos forenses privacidad | ✓ |
| d. | Gastos de inspección privacidad | ✓ |
| e. | Gastos de asistencia a juicio | Socio, administrador o directivos hasta 500€ al día; o cualquier empleado hasta 250€ al día |
| f. | Sanciones del regulador en protección de datos | 100% |
| g. | Sanciones PCI (normativa tarjetas de pago) | mínimo 50.000€ por sanción y periodo de seguro |
| **Gastos de mitigación** | | mínimo 30.000€ por incidente y periodo de seguro |

*Coberturas y límites de indemnización indicativos sujetos a las condiciones particulares

# Introducción

Muchas gracias por elegir a Hiscox para proteger a su empresa. El seguro Hiscox CyberClear 360° ha sido diseñado específicamente para dar soporte y proteger ante los riesgos cibernéticos de empresas de todo tipo de tamaño.

Durante todo el contrato hemos empleado un estilo y un lenguaje claro para que pueda entender el alcance de la cobertura proporcionada por su póliza 'Hiscox CyberClear 360°' así como las obligaciones que le incumben.

Esperamos que no tenga necesidad de hacer uso de las coberturas otorgadas en esta póliza, pero si así fuera, pondremos todo nuestro empeño en minimizar el impacto sobre su negocio con un servicio de respuesta ante incidentes proporcionado por empresas líderes en su campo y resarcirle del perjuicio que haya sufrido. Si en alguna ocasión considera que nuestro servicio está por debajo de sus expectativas, no dude en ponerse en contacto con nosotros.

Su tranquilidad y negocio son clave para nosotros. En Hiscox llevamos más de un siglo dedicados al seguro y más de 15 años asegurando riesgos ciber. Hoy día protegemos a más de un millón de empresas en todo el mundo. Nuestra experiencia compartida en EEUU, Reino Unido y Europa nos enriquece en el conocimiento de riesgos cada vez más globales.

Hoy, un ataque puede afectar a miles de equipos por todo el mundo, independientemente del tamaño. Pymes y gran empresa pueden ver su negocio bloqueado por la imposibilidad de acceder a sus equipos informáticos o perder datos de gran valor. Sin contar, además, que las normas de protección de datos son cada vez más estrictas y las sanciones más severas, lo que pone en peligro la viabilidad de muchos negocios.

El riesgo ciber debe ser una preocupación. Ha dado un paso importante eligiendo esta póliza. Desde ahora una buena política de prevención junto con este seguro le dará mayor tranquilidad sabiendo que si sucede lo peor, está en buenas manos.

Si desea conocer más información sobre nosotros, por favor visite www.hiscox.es.

**David Heras**Director General Hiscox Iberia

# Servicios preventivos Hiscox CyberClear 360º

La póliza de Hiscox CyberClear 360º es mucho más que un seguro. Es el seguro ciber de nueva generación. Le da acceso a una serie de **servicios y herramientas sin coste adicional** para ayudarle a gestionar mejor su riesgo además de ofrecerle una plataforma para **formar a sus empleados y proteger su negocio, lo cual constituye una pieza clave para la protección de su negocio.** Puede consultar en la siguiente página web todos los servicios en detalle, y cómo darse de alta en cada uno de ellos. www.hiscox.es/hiscox-cyberclear-servicios.

**RECUERDE REVISAR CON SU MEDIADOR DE SEGUROS LAS CONDICIONES PARA ACCEDER A ESTOS SERVICIOS.**

**Noticias y alertas en materia de ciberseguridad**

La información y prevención es parte de una efectiva estrategia de ciberseguridad. Mantenerse informado con artículos, guías e informes sobre ciberseguridad, las tendencias y novedades le puede facilitar esta tarea. También podrá darse de alta en nuestro servicio de Alertas por email ofrecidas por el Instituto Nacional de Ciberseguridad (INCIBE). Este le informará sobre las últimas vulnerabilidades y ataques ciber para poder tomar las medidas necesarias y proteger tu negocio.

Acceda aquí: www.hiscox.es/hiscox-cyberclear-servicios.

**Hiscox CyberClear Academy**

Módulos de formación online e interactivos diseñados para reducir el riesgo de que su empresa caiga víctima de un incidente online. Los contenidos se adaptan a la experiencia y función de cada empleado formándole sobre las actuales amenazas y tendencias. Este programa de formación exclusivo de Hiscox le ayudará a usted y a sus empleados a cumplir con los requisitos de los reguladores y para prepararles a comprender las amenazas ciber.

Más información: www.hiscox.es/hiscox-cyberclear-academy.

Para acceder a Hiscox CyberClear Academy asigne a un administrador de la cuenta en su organización. Éste deberá de dar de alta su empresa con el número de póliza de Hiscox en www.hiscoxcyberclearacademy.com. Para dar de alta a más diez empleados, envíenos un correo a info_spain@hiscox.com.

Alta aquí con su número de póliza: www.hiscoxcyberclearacademy.com.

**Calificación y gestión de su ciberseguridad**

Mida su nivel de ciberseguridad: damos acceso a nuestros clientes a condiciones ventajosas para obtener una calificación de su ciberseguridad con Leet Security, primera empresa europea de calificación del nivel de seguridad. Además, aquellas empresas que soliciten esta calificación disfrutarán de condiciones especiales al renovar o contratar su póliza.

Acceder al servicio: www.hiscox.es/leet-security.

**Informe sobre ciberseguridad más técnico**

Para empresas con equipos de ciberseguridad en plantilla podemos ofrecer acceso, con condiciones especiales, a un informe sobre su ciberexposición elaborado por BitSight. Dicha calificación técnica le mostrará los peligros a los que se enfrenta y que complementa la visión aportada por la calificación. BitSight es una referencia en seguridad global que ayuda a las compañías a identificar y gestionar su seguridad.

Envíenos un correo electrónico a para acceder a este servicio: riesgosprofesionales@hiscox.com.

# Servicios de ciberseguridad Hiscox


**Asistencia con expertos 27/7 online y presencial:**

Resolvemos y ayudamos en cualquier incidencia técnica en tus dispositivos. Si no se pueden solucionar de forma remota, mandaremos un técnico a dónde te encuentres.

**Avisos de ciberseguridad**:

Servicio de alertas por email ofrecidas por el Instituto Nacional de Ciberseguridad (INCIBE), informándote sobre las últimas vulnerabilidades y ataques cibernéticos para poder tomar las medidas necesarias y proteger tu negocio.

**Análisis de vulnerabilidades de tu red interna y de internet:**

Chequeamos tu red interna para descubrir y solucionar sus vulnerabilidades. Además de revisar las conexiones wifi para mejorar su velocidad de conexión y seguridad.

**Sistema autenticación de doble factor:**

Te ayudamos a configurar esta capa adicional de seguridad para que tus cuentas estén aún más protegidas.

**Informe presencia internet:**

Realizamos un análisis de la presencia del usuario en internet y damos soluciones si detectamos algún tipo de conflicto.

**Copia de seguridad:**

Sistema de almacenamiento de 20GB encriptado con ayuda y soporte en la gestión.

**Revisión y puesta a punto:**

Revisamos y configuramos cualquier dispositivo para sacarle el máximo partido.

**Borrado digital:**

Eliminamos de internet cualquier información falsa o injuriosa hacia el usuario.

**Localizador de dispositivos:**

Ayudamos a localizar cualquier dispositivo robado o perdido.

**Antivirus: Bitdefender total Security:**

Instalamos en cualquier tipo de dispositivo uno de los antivirus más avanzados del mercado.

**Soporte Office 365:**

Resolvemos dudas acerca de estos servicios de Microsoft.

# Condiciones especiales

Por favor, lea con detenimiento estas condiciones especiales, así como las condiciones particulares y generales y los posibles suplementos a las mismas, estos documentos conforman su **p**óliza de seguro. Si hubiera algún error en ellos, por favor contacte con su mediador de seguros tan pronto como sea posible.

La **aseguradora** se compromete a dar cobertura a lo recogido en esta **p**óliza a cambio del pago de la prima acordada.

# 1. Definiciones

Las palabras en negrita o cursiva recogidas a continuación tienen un significado concreto en el contexto de esta **p**óliza.

**Afectados**

Cualquier persona física titular de los **datos personales**.

**Amenaza de extorsión**

Cualquier amenaza directa a la **entidad** por parte de un tercero, si la misma no paga el rescate exigido, de:

1. cometer un ataque deliberado contra el **sistema informático,** o los datos en el **sistema informático**, incluyendo el ataque a través de la introducción de un **virus**; o
2. cometer un ataque deliberado al **sistema informático** de un tercero con el uso del **sistema informático**, incluyendo con carácter enunciativo pero no limitativo el ataque a través de la transmisión de un **virus**; o
3. divulgar públicamente **información corporativa, información confidencial** o **datos personales** de los cuales se ha apropiado indebidamente del **sistema informático**.

**Asegurado/usted**

1. El Tomador, sus **filiales**, las **nuevas entidades**, así como cualquier fundación donde el tomador o una **filial** ostente la mayoría de los derechos de voto del órgano de gobierno (en su conjunto, la '**entidad**').
2. La **persona asegurada**.

**Ataque de ingeniería social**

El engaño de un tercero dirigido a una **persona asegurada,** mediante la suplantación de i) otra **persona asegurada**, o ii) un proveedor, cliente o prestador de servicio de la **entidad**, a través de correo electrónico (phishing), mensajes de texto (smishing), voz sobre IP (vishing) o estafas similares con el fin de obtener **datos personales, información confidencial o información corporativa**.

**Ciberataque**

Cualquier fallo en garantizar la seguridad del **sistema informático**, y que resulte en:

1. un acceso o uso no autorizado al **sistema informático**; o
2. una alteración, corrupción, destrucción, o pérdida de **datos personales**, **información corporativa o información confidencial**; **o**
3. la introducción o recepción de un **virus**, independientemente de su forma de transmisión; o
4. un **ataque de denegación de servicio** al **sistema informático** entendiéndose como tal, una privación maliciosa temporal, total o parcial, del acceso o uso del **sistema informático**., incluido pero no limitado a un ataque de denegación de servicio distribuido.

   Entendemos por ataque de denegación de servicio distribuido, aquel que se produce por un ataque desde múltiples ordenadores (o vectores) en lugar de uno solo.

**Contaminantes**

Se entiende como cualquier irritante o contaminante sólido, líquido, gaseoso, biológico, radiológico o térmico, incluyendo pero sin limitarse a, humo, vapor, asbesto/amianto, sílice, polvo, nano partículas, fibras, hollín, gases, ácidos, álcalis, productos químicos, materiales nucleares, gérmenes y residuos. Los residuos incluyen, pero no se limitan a, materiales para reciclar, reacondicionar o recuperar.

**Cuenta bancaria**

Cualquier cuenta de la que la **entidad** sea titular en una entidad financiera, a través de la cual una **persona asegurada** puede enviar órdenes de transferencia de fondos:

i. a través de una orden electrónica o telefónica; o

ii. a través de instrucciones escritas que establezcan las condiciones bajo las cuales las transferencias deberán ser procesadas por un sistema electrónico de transferencia de fondos.

**Datos personales**

Cualquier información personal de la cual la **entidad** sea responsable, independientemente del formato en que se encuentre, que permita identificar al **afectado** y que no sea del dominio público, según se defina en la normativa que resulte aplicable relativa al cuidado, la custodia, el control y el uso de información personal, incluyendo pero no limitándose a la información protegida por el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de Abril de 2016, o cualquier otra normativa que la sustituya.

**Descubierto**

Se entenderá como la primera vez en la que la **entidad**, tenga conocimiento de un hecho o sospecha, que pueda activar la presente póliza, incluso aunque en ese momento se desconozcan los detalles y el posible impacto del mismo.

**Empleado**

Cualquier persona física que mantiene un contrato laboral con la **entidad**, y que realiza labores para ella.

**Error humano**

Una interrupción no intencionada y no programada, parcial o total del **sistema informático**, o la falta de disponibilidad de los datos de la **entidad** en el **sistema informático**, que no se derive de una **vulneración de datos** o **ciberataque**, y que sea causada por:

1. un error humano por parte de una **persona asegurada**, incluyendo un error en la programación, parametrización, actualización o selección de un **programa**, siempre y cuando dicho **programa** no esté en fase de pruebas y haya sido testado con éxito durante un periodo mínimo de 30 días, o la alteración, corrupción, destrucción, o pérdida de **información corporativa** o **información confidencial**; o
2. un fallo eléctrico, incluyendo sobretensión o caída de tensión del sistema eléctrico o el acto de desconectar el **sistema informático** de la corriente eléctrica, causado accidentalmente y exclusivamente por una **persona asegurada**, siempre y cuando no se derive de un **daño material**.

**Fianzas**

La constitución de fianzas civiles que puedan ser exigidas a una **persona asegurada** por su eventual responsabilidad civil, así como los gastos que una **persona asegurada** incurra para la constitución y mantenimiento de un fianza penal para garantizar su libertad provisional, como consecuencia de una **reclamación**.

**Filial**

Cualquier persona jurídica en la que el tomador:

1. ostente más de un 50% de las acciones o participaciones, o más de un 50% de los derechos de voto a la fecha de efecto de la **póliza** o con anterioridad a la misma, ya sea directa o indirectamente; o
2. que no cumpliendo con el punto 1 anterior, ostenta el derecho legal de elegir a la mayoría de su consejo de administración o similar órgano de gobierno;
3. y en cualquiera de los dos casos anteriores, se encuentra domiciliada en el Espacio Económico Europeo (EEE) o en Reino Unido, o fuera de dichos territorios siempre y cuando hayan sido notificadas y aceptadas por **nosotros** mediante suplemento o por escrito.

**Franquicia**

Las cantidades y/o periodo de tiempo expresamente pactadas en la condiciones particulares que se deducirán del importe a abonar por la **aseguradora** por cualquier concepto cubierto por la **póliza**, en cada **incidente** o **reclamación**.

**Gastos de defensa**

Los gastos incurridos con el consentimiento previo por escrito de la **aseguradora** para investigar, liquidar o defender una **reclamación** contra el **asegurado**.

**Gastos de mitigación**

Se entienden como los gastos incurridos por la **entidad** y distintos a los ofrecidos en el resto de coberturas y servicios de esta **póliza**, con nuestro previo consentimiento por escrito, con el propósito de minimizar potenciales pérdidas derivadas de un **incidente** cubiertas en la presente **póliza** hasta el sublímite indicado en las condiciones particulares. Los **gastos de mitigación** incluyen sin ánimo limitativo:

a. el alquiler de equipos informáticos de terceros;

b. los honorarios de un proveedor externo, especialmente contratado con el fin de coordinar la aplicación de un plan de continuidad de negocio de la **entidad**;

c. gastos necesarios y razonables para restaurar el ranking otorgado por el motor de búsqueda a la **entidad** en la posición anterior al **incidente**;

d. el incremento de costes de la mano de obra de la entidad, que incluye sin ánimo limitativo la contratación de trabajadores temporales, o el pago de horas extraordinarias a los empleados;

e. la actualización o sustitución de hardware o software ya existente que forme parte del sistema informático;

f. pago de recompensas a informantes. Entendido como el reembolso al asegurado del importe previamente abonado por éste al Informante a cambio de información que ayude al arresto y condena de cualquier persona o personas que cometan o intenten cometer cualquier ciberataque o amenaza de extorsión;

informante: se entiende como un tercero que no mantenga vínculos ya sea de forma directa o indirecta con el asegurado, que proporcione información que no pueda ser obtenida de otra forma, a cambio de una recompensa ofrecida por el asegurado. Entre otros, se excluyen empleados, directivos y cualquier otros relacionado con las empresas contratadas por el asegurado para investigar cualquier acto ilegal o para realizar labores de auditoría.

Los **gastos de mitigación** no podrán exceder en ningún caso la cantidad económica que nosotros hubiésemos pagado por el **incidente** si la **entidad** no hubiera incurrido en dichos gastos.

**Incidente**

Una **vulneración de datos**, **ciberataque**, **error humano**, **amenaza de extorsión** o **ataque de ingeniería social**.

**Información confidencial**

La información comercial confidencial de terceros, calificada como tal bajo contrato, de la cual la **entidad** sea responsable, independientemente del formato en que se encuentre.

**Información corporativa**

La información propia de la **entidad** que no sea de dominio público, distinta de la información de **datos personales,** independientemente del formato en que se encuentre.

**Nuevas entidades**

1. Cualquier entidad que el tomador adquiera (entendido como tomar posesión de más del 50% de las acciones en circulación, participaciones, o activos de cualquier entidad) durante el **periodo de seguro**, pero exclusivamente en la medida en que realice la misma actividad que el **tomador**, tenga las mismas medidas de seguridad informática que el tomador o sus **filiales**, esté domiciliada en el Espacio Económico Europeo o Reino Unido, y los ingresos brutos anuales de dicha entidad sean inferiores al 20% de los ingresos brutos anuales del tomador y sus **filiales**; o

2. Cualquier entidad que el tomador adquiera, (entendido como tomar posesión de más del 50% de las acciones en circulación, participaciones, o activos de cualquier entidad), durante el **periodo de seguro** y que no realice necesariamente la misma actividad que el Tomador, o cuyos ingresos brutos anuales superan el 20% de los ingresos brutos anuales del tomador y sus filiales, o cuyas medidas de seguridad informáticas sean distintas a las del tomador y sus **filiales** pero exclusivamente si:

   a. el tomador ha proporcionado a la **aseguradora** una notificación por escrito de la adquisición en los 30 días siguientes a la adquisición, y la **aseguradora** ha dado su consentimiento por escrito aceptando otorgar cobertura a dicha entidad; y

   b. el tomador ha pagado la prima adicional y aceptado cualesquiera de los términos especiales, condiciones adicionales o exclusiones adicionales propuestas por la **aseguradora**; y

   c. dicha entidad está domiciliada en el Espacio Económico Europeo o en el Reino Unido.

Las mismas reglas aplicarán a las entidades constituidas directa o indirectamente (que sean constituidas por una **filial**) por el tomador durante el **periodo de seguro**.

La cobertura solo resultará aplicable a **reclamaciones** presentadas, o **incidentes** descubiertos por primera vez durante el **periodo de seguro** cuando las causas de las mismas/os se hayan generado durante el **periodo de seguro** tras la adquisición o constitución de la nueva entidad.

**Periodo de seguro**

El periodo de tiempo, indicado en las condiciones particulares, durante el cual el presente contrato está en vigor, por el que el tomador habrá pagado, y la **aseguradora** habrá aceptado una prima. Esto no incluye cualquier periodo adicional de notificación.

**Persona asegurada**

Se entenderá como:

1. cualquier persona física que sea, haya sido o durante el **periodo de seguro** llegue a ser socio, administrador, directivo, miembros del consejo de administración, delegado de protección de datos, personal en prácticas, o **empleado** de la **entidad**, pero únicamente en el desempeño de sus funciones para la **entidad**;

2. cualquier trabajador temporal, contratista o subcontratista independiente, que sea persona física, incluidos autónomos, o cualquier trabajador con contrato laboral de un contratista o subcontratista, pero únicamente en el desempeño de sus funciones para la **entidad,** y cuando utilicen el **sistema informático** de la **entidad** con un usuario propio facilitado por la **entidad**;

**No se considera como *persona asegurada* a ningún auditor, síndico, liquidador, o administrador concursal.**

**Programa**

Una secuencia de instrucciones escritas que interactúan con un equipo informático o de telecomunicaciones para la ejecución de una tarea de procesamiento de datos o de interacción con otros equipos.

**Proveedor externo tecnológico**

Sin perjuicio de la exclusión 1 (Infraestructura) de la sección 'Lo que no está cubierto', se entiende como una persona jurídica o una persona física (autónomo) a quién la **entidad** contrata servicios para su propio uso a través de un contrato escrito, a cambio del pago de honorarios a un tercero y relacionados con: 1) la instalación, administración o seguridad de equipos de tecnología de la información; 2) operación, supervisión o mantenimiento de la infraestructura tecnológica; 3) asistencia técnica a los usuarios; y/o 4) servicios de computación en la nube (en inglés, 'cloud computing') y servicios de hosting.

**Reclamación**

Cualquier requerimiento escrito, demanda escrita o procedimiento civil, penal, administrativo, o arbitral presentado contra cualquier **asegurado** con el objetivo de obtener una indemnización económica a causa de un **incidente**. También se entenderá por reclamación: un procedimiento administrativo de protección de datos iniciado contra cualquier **asegurado** por un organismo regulador en materia de protección de datos.

**Sistema informático**

Todos los ordenadores electrónicos interconectados o inalámbricos y sus componentes, incluyendo pero sin limitarse a:

— sistemas operativos, hardware o software;

— dispositivos asociados de entrada y salida, dispositivos de almacenamiento de datos y servicios, dispositivos o herramientas de copia de seguridad;

— dispositivos móviles usados por la **persona asegurada** y autorizados por la **entidad** para acceder a sus sistemas;

— componentes periféricos relacionados, como dispositivos del Internet de las cosas (en inglés, Internet of Things);

— sitio web (incluyendo extranet e intranet) y cuentas de redes sociales; y

— sistemas en la nube;

siempre que sea propiedad de la **entidad,** esté directamente bajo el control y administración de la **entidad**, y usado por la **entidad** y para su propio beneficio, por lo que no se incluye los facilitados por **un proveedor externo tecnológico**.

**Virus**

Programas maliciosos introducidos en el sistema informático, sin el permiso o conocimiento de la entidad incluyendo, a título enunciativo pero no limitativo, gusanos, troyanos, 'malware', o 'spyware'.

**Vulneración de datos**

La apropiación o robo, copia, difusión, acceso, uso, divulgación, no autorizados, de:

a. **datos personales**; y/o

b. **información corporativa**; y/o

c. **información confidencial**.

# 2. Lo que está cubierto

En contraprestación por el pago de la prima, de conformidad con el cuestionario de suscripción y sujeto a la contratación efectiva de las coberturas indicadas a continuación, la **aseguradora** y el **asegurado** acuerdan lo siguiente:

## 2.1. Servicio de respuesta a incidentes

**Activación del servicio**

Si, durante el **periodo de seguro**, el **asegurado** descubre un **incidente**, real o presunto, la **aseguradora**:

a. abonará el coste de los Servicios de Respuesta a Incidentes indicados en este apartado prestados por los especialistas previstos en el Anexo **Panel de Expertos**.

Podrá acceder llamando al número de teléfono indicado en el mencionado Anexo.

En el caso de que alguno de dichos especialistas no pueda prestar el servicio requerido, la **aseguradora** reembolsará los gastos en los que pueda incurrir el **asegurado**, previa verificación y aprobación escrita de los mismos, para contratar otro especialista fuera del ***panel de expertos***; o

b. le reembolsará los gastos en los que pueda incurrir el **asegurado**, previa verificación y aprobación escrita de los mismos, y descontada la franquicia indicada en las Condiciones Particulares, para contratar otro especialista fuera de nuestro ***panel de expertos*** para prestarle los Servicios de Respuesta a Incidentes indicados en este apartado.

En cualquier caso no pagaremos gastos de corrección o mejora, ni gastos superiores a los que hubiésemos tenido con el uso de nuestro **panel de expertos**.

**Franquicia y uso de proveedores del panel de expertos**

Siempre y cuando el **asegurado** haga uso del Servicio de Respuesta a Incidentes, mediante los especialistas indicados en **Anexo panel de expertos,** no se aplicará **franquicia** alguna a los siguientes servicios:

a. servicios de contención tecnológica;

b. servicio de asesoramiento jurídico y de comunicación y relaciones públicas;

c. a los gastos de notificación y monitorización previstos en el punto i. c. del apartado Alcance de los Servicios de Respuesta a Incidentes;

d. al pago de horas extras de **personas aseguradas** dedicadas a los servicios antes mencionados.

**Exoneración de responsabilidad**

La **aseguradora** no será responsable, ni formará parte de ningún servicio que pueda acordarse con cualquiera de las empresas especialistas que forman parte del Servicio de Respuesta a Incidentes y el **asegurado**, distintos a los gastos de respuesta de **incidentes** que se incurran al activar dicho servicio.

La aseguradora no garantiza la capacidad ni el servicio de los expertos previstos en el panel del Servicio de Respuesta a incidentes.

**La responsabilidad máxima que asumirá el proveedor respecto de los tomadores/asegurados de la *póliza* será equivalente al valor del servicio de respuesta a incidentes que se hubiera prestado.**

**Alcance de los Servicios de Respuesta a Incidentes**:

a. **Servicios de contención tecnológica**

El servicio de especialistas en ciberseguridad para:

i. darle asesoramiento sobre como detener o contener un **incidente**;

ii. establecer, en la medida de lo posible, la causa y el alcance de un **incidente**;

iii. confirmar la ocurrencia de una **vulneración de datos**, e identificar, en la medida de lo posible, a los **afectados**;

iv. emitir las recomendaciones oportunas para evitar la repetición del **incidente**, siempre y cuando la causa haya podido ser detectada.

b. **Servicio de asesoramiento jurídico, de comunicación y relaciones públicas**.

i. El servicio de asesoramiento jurídico externo para asesorar sobre las actuaciones que deben ser tomadas para gestionar la respuesta al **incidente**, cuando sea necesario.

ii. **Gastos de relaciones públicas**, entendidos como los servicios:

a. de un consultor especializado en ayudar al **asegurado** a reestablecer su reputación y gestionar su comunicación externa derivado de un **incidente,** incluyendo el desarrollo y comunicación de una estrategia para dicho fin, cuando sea necesario;

b. para emitir comunicados vía correo electrónico o en su sitio web y redes sociales; y

c. cualquier otra medida razonable y proporcionada para reestablecer su reputación, con nuestro consentimiento previo por escrito.

c. **Gastos de notificación y monitorización**

i. gastos para notificar a cualquier entidad reguladora, u otras autoridades competentes la **vulneración de datos**, siempre que el **asegurado** esté legalmente obligado a hacerlo, con nuestro previo consentimiento;

ii. gastos de uso de un centro de atención telefónica externo para responder a consultas de los **afectados**, previamente notificados, a consecuencia de una **vulneración de datos**, con nuestro previo consentimiento;

iii. **gastos de monitorización de la identidad:** la contratación de un servicio de monitorización de la información comprometida de los **afectados**, en sitios públicos de Internet, con el fin de evitar un uso inadecuado, durante un periodo máximo de un año desde la fecha de activación. El servicio deberá activarse únicamente tras la notificación, previo acuerdo con la **aseguradora**, a los **afectados** a consecuencia de una **vulneración de datos**;

iv. gastos para notificar a los **afectados** la **vulneración de datos**, con nuestro previo consentimiento;

v. **gastos por monitorización de crédito**: reembolso de los gastos razonables y necesarios incurridos por la **entidad,** con nuestro previo consentimiento, para la contratación de un servicio de monitorización de crédito o similar para los **afectados**, previamente notificados, a consecuencia de una **vulneración de datos**.

Extensión de cobertura para sistemas alojados en la nube de un **proveedor externo tecnológico**

Se hace constar que quedan cubiertos en los mismos términos, el servicio de respuesta a incidentes en caso de un **incidente** que afecte a un sistema:

a. usado por la **entidad** para el desarrollo de su actividad y para su propio beneficio;

b. que sea facilitado por un **proveedor externo tecnológico**; y

c. que esté alojado en la nube de un **proveedor externo tecnológico**;

siempre y cuando, el **incidente** sea descubierto durante el **periodo de seguro** y tenga su origen en el s**istema informático** de la **entidad o** se haya producido a través del **sistema informático** de la **entidad**.

## 2.2. Pérdidas del asegurado

Si durante el **periodo de seguro** el **asegurado** descubre un **incidente,** real o presunto, la **aseguradora abonará**:

**a. Gastos de recuperación de datos o sistemas**

Los gastos incurridos, con el consentimiento previo por escrito de la **aseguradora** para:

i. recuperar el acceso a los **programas, sistema informático**, o datos electrónicos de la **entidad**;

ii. reconfigurar, instalar a partir de copias de seguridad, copias originales u otras fuentes o, en caso de ser necesario, sustituir un **programa** de terceros (legalmente adquirido) en el **sistema informático**;

iii. recrear los datos electrónicos de la **entidad**;

iv. **gastos de mitigación**.

Si no se puede acceder, recuperar, sustituir, reparar o recrear los **programas** o datos electrónicos, los gastos que la **aseguradora** abonará no excederán los gastos incurridos para llegar a esa conclusión.

**En cualquier caso no pagaremos por gastos de recuperación de datos derivados del robo de un hardware que forme parte del sistema informático.**

Extensión de cobertura para sistemas alojados en la nube de un **proveedor externo tecnológico**

Se hace constar que quedan cubiertos en los mismos términos, los gastos de recuperación de datos o sistemas en caso de un **incident**e que afecte a un sistema:

a. usado por la **entidad** para el desarrollo de su actividad y para su propio beneficio;

b. que sea facilitado por un **proveedor externo tecnológico**; y

c. que esté alojado en la nube de un **proveedor externo tecnológico**;

siempre y cuando, el **incidente** sea descubierto durante el **periodo de seguro** y tenga su origen en el s**istema informático** de la **entidad o** se haya producido a través del **sistema informático** de la **entidad**.

**b. Extorsión cibernética**

La aseguradora reembolsará:

i. el importe económico del rescate pagado por el **asegurado** o, si el tercero ha exigido el pago del rescate en la forma de bienes o servicios, el valor de mercado de dichos bienes o servicios en el momento de la entrega del rescate;

ii. los honorarios y otros gastos incurridos por un consultor especializado para ayudar al **asegurado** en la gestión y negociación del rescate;

iii. el importe de un rescate robado por un tercero, siempre que dicho robo ocurra en el lugar acordado para el pago del rescate, o de camino al mismo;

iv. **gastos de mitigación**.

La **aseguradora** sólo reembolsará los gastos que hubiere realizado la **entidad** por la **amenaza de extorsión** cuando se produzcan las siguientes circunstancias:

i. el **asegurado** informe inmediatamente a la **aseguradora**, y la mantenga informada de la **amenaza de extorsión** en todo momento, y obtenga el consentimiento por escrito de la **aseguradora** previo pago del rescate;

ii. el **asegurado** notifique la **amenaza de extorsión** a la policía u a otra autoridad competente;

iii. un especialista informático autorizado por la **aseguradora** determine que no existe posibilidad técnica de restaurar los datos;

iv. el **asegurado** demuestre a la **aseguradora** que el rescate ha sido abonado, o los bienes o servicios han sido entregados, bajo coacción o amenaza, y que ha hecho todos los esfuerzos para determinar que la amenaza era real y no ficticia, y que ha realizado todas las acciones necesarias para evitar la **amenaza de extorsión**; y

v. un administrador, directivo (o cargo equivalente) de la **entidad** haya dado su consentimiento al pago del rescate o a la entrega de los bienes o servicios.

vi. el importe del rescate exigido es proporcional a las pérdidas que la **entidad** pudiera sufrir en el caso de no aceptar el pago del rescate.

Extensión de cobertura para sistemas alojados en la nube de un **proveedor externo tecnológico**

Se hace constar que quedan cubiertos en los mismos términos, una amenaza de extorsión a la **entidad** sobre un sistema:

a. usado por la **entidad** para el desarrollo de su actividad y para su propio beneficio;

b. que sea facilitado por un **proveedor externo tecnológico**; y

c. que esté alojado en la nube de un **proveedor externo tecnológico**.

siempre y cuando, la **amenaza de extorsión** sea descubierta durante el **periodo de seguro** y sea consecuencia de un acceso no autorizado al s**istema informático** de la **entidad**.

**c. Protección de equipos**

Hasta el sublímite indicado en las condiciones particulares, reembolsaremos a la **entidad**, el coste de reparación o sustitución de un equipo informático (hardware o móvil) que forme parte del **sistema informático** y sea de su propiedad, usado para el desarrollo de su negocio, incluyendo pero sin limitarse a ordenadores, servidores, teléfonos, smartphones, tablets, televisores, impresoras, escáneres, cámaras, sensores, altavoces inteligentes y otros dispositivos conectados a Internet, siempre y cuando:

— los equipos informáticos contengan **datos personales**, **información confidencial** o **información corporativa** de la **entidad**; y

— los equipos informáticos hayan sido afectados por un **incidente** y ya no puedan ser usados para las funciones para las cuales se destinaban; y

— no se active la cobertura de **gastos de mitigación**.

La **aseguradora** sólo asumirá el coste de sustitución de un equipo informático en el caso de que:

— el equipo no pueda ser reparado; o que

— el coste de reparación supera el coste de sustitución.

**Garantías adicionales – verifique las condiciones particulares para comprobar si lo tiene contratado**

**d. Pérdida de beneficios**

La **aseguradora** abonará la pérdida de beneficios hasta el límite establecido en las condiciones particulares, resultante de una interrupción parcial o total del **sistema informático** siempre y cuando i) ocurra durante el **periodo de seguro**, ii) el **periodo de indemnización** supere la **franquicia temporal**, y iii) la interrupción sea consecuencia directa y exclusiva de un **incidente** en el **sistema informático de la entidad**.

Dicha pérdida de beneficios se calculará conforme a uno de los dos siguientes supuestos:

1. En el caso de que en las Condiciones Particulares se establezca un límite por día para la cobertura de Pérdida de Beneficios, la aseguradora pagará, durante la interrupción del **sistema informático** y conforme al **periodo de indemnización**, el límite de indemnización por día fijado en las Condiciones Particulares.

   El importe a abonar en concepto de indemnización por pérdida de beneficios no podrá ser en ningún caso superior a la pérdida real sufrida.

   La aseguradora se reserva el derecho de verificar la pérdida sufrida por la **entidad** y a solicitar la documentación necesaria para su cálculo conforme se indica abajo, pudiendo abonar un importe inferior al indicado en las condiciones particulares si la pérdida real es inferior al límite de indemnización diario fijado en las mismas.

   **Cálculo de la reducción del resultado de explotación**

   El cálculo de la pérdida de beneficios se realizará comparando el resultado de explotación (beneficio o pérdida) real obtenido durante la paralización del **sistema informático**, con el resultado de explotación (beneficio o pérdida) que la **entidad** haya obtenido en el mismo periodo del año anterior. Si este fuera su primer año de actividad, el cálculo del resultado de explotación se hará comparando el periodo de interrupción del **sistema informático** y el periodo inmediatamente anterior a la interrupción.

2. En el caso que en las Condiciones Particulares se establezca un límite de indemnización por **periodo de seguro** para la cobertura de Pérdida de Beneficios, la **aseguradora** pagará, tanto durante la interrupción del **sistema informático** como tras la finalización de dicha interrupción, y durante el **periodo de indemnización**:

   i. la reducción del resultado de explotación (beneficio o pérdida) incluidos los costes operacionales fijos incurridos por la **entidad** afectada; y

   ii. los **gastos de mitigación**.

   Cálculo de la reducción del resultado de explotación

   La **aseguradora** pagará la diferencia entre el resultado de explotación (beneficio o pérdida) real obtenido durante el **periodo de indemnización**, comparado con el resultado de explotación (beneficio o pérdida) que la **entidad** haya obtenido en el mismo periodo del año anterior. Si este fuera su primer año de actividad, el cálculo del resultado de explotación se haría comparando el **periodo de indemnización** y el periodo inmediatamente anterior a la interrupción.

En el caso de que sea previsible que la **entidad** pueda recuperar parcial o totalmente las pérdidas sufridas durante la interrupción de su **sistema informático**, la **aseguradora** se reserva el derecho de esperar hasta el final del **periodo de indemnización** para calcular la indemnización a que tiene derecho la **entidad**, en concepto de Pérdida de Beneficios.

Extensión de cobertura para sistemas alojados en la nube de un **proveedor externo tecnológico**

Se hace constar que queda cubierta en los mismos términos, la pérdida de beneficios de la **entidad** a consecuencia de una interrupción parcial o total de un sistema:

a. usado por la **entidad** para el desarrollo de su actividad y para su propio beneficio;

b. que sea facilitado por un **proveedor externo tecnológico**; y

c. que esté alojado en la nube de un **proveedor externo tecnológico**.

siempre y cuando, el **incidente** sea descubierto durante el **periodo de seguro** y tenga su origen en el s**istema informático** de la **entidad o** se haya producido a través del **sistema informático** de la **entidad**.

**Definiciones aplicables a esta cobertura**

A los efectos de esta cobertura serán de aplicación las siguientes definiciones:

**Franquicia temporal:** el periodo de tiempo, indicado en las condiciones particulares, durante el cual la cobertura de **pérdida de** b**eneficios** no toma efecto.

**Periodo de indemnización**: el periodo de tiempo máximo en días naturales, indicado en las condiciones particulares, una vez transcurrida la **franquicia temporal**, durante el cual la **aseguradora** asumirá la pérdida de beneficios conforme se dispone en la cobertura. El **periodo de indemnización** no se verá interrumpido si ocurre una nueva interrupción del **sistema informático** por la misma causa en el plazo máximo de una hora desde la resolución de la primera interrupción.

El **asegurado** deberá facilitar toda la información que le solicite la **aseguradora** con el objeto de poder verificar la reducción del resultado de explotación real que se haya podido producir. Para más detalles por favor consulte el apartado 1.2 del anexo '**Proceso de notificación de incidentes y reclamaciones**' de la presente **póliza**.

**e. Proveedor externo tecnológico**

A consecuencia de un **ciberataque** a su **proveedor externo tecnológico,** y hasta el sublímite y **periodo de indemnización**, y descontando las franquicias correspondientes indicadas en las condiciones particulares, la **aseguradora** abonará a la **entidad** las siguientes coberturas:

i. gastos incurridos, con el consentimiento previo por escrito de la **aseguradora**, para restaurar los **programas** o datos electrónicos de la **entidad** alojados en la nube de un **proveedor externo tecnológico** a partir de copias de seguridad, siempre y cuando la copia de seguridad esté disponible; o gastos, incurridos con nuestro consentimiento previo por escrito para recrear los datos electrónicos de la **entidad** alojados por un **proveedor externo tecnológico**;

   Si no se puede, recuperar, o recrear los **programas** o datos electrónicos, los gastos que la **aseguradora** abonará no excederán los gastos incurridos para llegar a esa conclusión.

ii. Pérdida de beneficios de la **entidad** resultante de una interrupción parcial o total del **sistema informático de un proveedor externo tecnológico** siempre y cuando i) ocurra durante el **periodo de seguro**, ii) el **periodo de indemnización** supere la **franquicia temporal**, y iii) la interrupción sea consecuencia directa y exclusiva de un **ciberataque** al **sistema informático de un proveedor externo tecnológico**.

   El cálculo de la pérdida de beneficios se establece conforme a lo indicado en el apartado 2.2. d. Pérdida de Beneficios.

iii. **gastos de mitigación**, para restablecer el servicio a la **entidad** prestado por el **proveedor externo tecnológico**.

El límite máximo a pagar en la presente cobertura, con independencia del número de **ciberataques** o **incidentes** cubiertos en la presente **póliza**, no superará el sublímite indicado en las condiciones particulares para la cobertura de Proveedor Externo Tecnológico.

Consulte la documentación que se solicitará para la tramitación de la solicitud de abono de este apartado en el Anexo **proceso de notificación de incidentes y reclamaciones**.

**Definiciones aplicables a esta cobertura**

A efectos de la activación de la presente cobertura se hace constar que se aplican las definiciones de **periodo de indemnización** y **franquicia temporal** que constan en el apartado de **Pérdida de Beneficios**.

A efectos de la activación de la presente cobertura la definición de '**sistema informático**' se sustituye por '**sistema informático de un proveedor externo tecnológico**', indicada a continuación.

**Sistema informático de un proveedor externo tecnológico**

Todos los ordenadores electrónicos interconectados o inalámbricos y sus componentes, incluyendo pero sin limitarse a:

— sistemas operativos, hardware o software;

— dispositivos asociados de entrada y salida, dispositivos de almacenamiento de datosy servicios, dispositivos o herramientas de copia de seguridad;

— componentes periféricos relacionados, como dispositivos del Internet de las cosas (en inglés, Internet of Things);

— sitio web (incluyendo extranet e intranet) y cuentas de redes sociales; y

— sistemas en la nube, incluyendo pero no limitado a la infraestructura subyacente (hardware).

siempre que estén directamente bajo el control y administración del **proveedor externo tecnológico**, y usado por el **proveedor externo tecnológico** para la prestación de sus servicios a la **entidad**.

Se hace constar que la presente cobertura no se activa en el caso de que no se pueda acreditar la ocurrencia de un **ciberataque** al **Sistema informático de su proveedor externo tecnológico**. Corresponde al Asegurado acreditar que dicho ciberataque se ha producido y que ha supuesto una paralización total o parcial del **sistema informático** de la **entidad**.

## 2.3 Responsabilidad tecnológica

Si, durante el **periodo de seguro** el **asegurado** a consecuencia de un **incidente**:

1. Protección de la información y privacidad

Recibe una **reclamación** alegando:

a. incumplimiento, violación o infracción involuntaria de cualquier normativa de protección de **datos personales** o derecho a la privacidad, siempre y cuando, la reclamación no esté basada directa o indirectamente en la recogida y/o el tratamiento de **datos personales** por la **entidad**, o por cualquiera que actúe en su nombre, sin haber obtenido previamente el consentimiento suficiente con respecto al marco legal o regulatorio Se hace constar que se da cobertura bajo esta sección a las **reclamaciones** presentadas por los **empleados**, en el caso de que sus **datos personale**s se hayan visto vulnerados. No se cubren reclamaciones presentadas por cualquier socio, administrador o directivo.

b. incumplimiento de cualquier deber de confidencialidad de datos personales o información confidencial; o

c. incumplimiento de cualquier deber contractual para mantener la seguridad o confidencialidad de datos personales, información confidencial o información corporativa, incluyendo un incumplimiento de la política de privacidad de la **entidad**.

2. Inspección de protección de datos

Es objeto de una **inspección de datos** o de cualquier otro procedimiento normativo en materia de protección de datos.

3. Incumplimiento de la normativa PCI DSS

Es objeto de un procedimiento por incumplir con el estándar de seguridad de los datos de la Industria de las tarjetas de pago (en inglés: **payment card industry data security standard)**.

4. Responsabilidad por contenido digital

Recibe una ***reclamación*** derivada directamente de la modificación por parte de un tercero o de un ***empleado*** (excluyendo socios, administradores o directivos) y como consecuencia de un ***ciberataque*** del contenido del correo electrónico, redes sociales, intranet, extranet o sitio web de la **entidad** y en la que se alegue:

a. un incumplimiento de cualquier derecho de propiedad intelectual; o

b. difamación, incluyendo injuria, calumnia o menosprecio hacia un producto o servicio; o

c. incumplimiento de cualquier licencia.

5. Por fallo de ciberseguridad

Recibe una **reclamación** basada en la transmisión de un virus, en un acceso o uso no autorizado del **Sistema informático de un tercero** o en un **ataque de denegación de servicio** a un tercero, realizado a través o utilizando el **sistema informático** de la **entidad**.

A efectos de esta cobertura se entiende por:

**Sistema informático de un tercero**

Todos los ordenadores electrónicos interconectados o inalámbricos y sus componentes que sean propiedad de un tercero y estén bajo su control y administración y usados por el tercero para su propio beneficio.

**Ataque de denegación de servicio a un tercero**

Privación maliciosa temporal, total o parcial, del acceso o uso del **sistema informático de un tercero** a consecuencia de un ataque desde un ordenador. Se incluye también bajo esta definición un ataque de denegación de servicio distribuido, que se produce por un ataque desde múltiples ordenadores (o vectores) en lugar de uno solo.

La **aseguradora**, según cada caso (puntos 1 a 5 arriba indicados), pagará:

a. el importe económico acordado entre el **asegurado** y la **aseguradora** tras una negociación de buena fe, mediación o cualquier otra forma alternativa de resolución de disputas, para resolver la **reclamación**, o la cantidad económica a la que resulte condenado el **asegurado** para dar cumplimiento a una sentencia o resolución arbitral contra el **asegurado**.

A los efectos de esta cobertura se considera también como **reclamación**, aquellas en las que se solicite una indemnización económica por angustia mental o emocional derivada de un **incidente**;

b. **la sanción administrativa** que se imponga a la **entidad**;

c. **los gastos y sanciones PCI** que se impongan a la **entidad**;

d. **los gastos forenses de protección de datos**;

e. **los gastos de inspección de protección de datos** en los que incurra **la entidad**;

f. **los gastos de defensa** del **asegurado y fianzas** impuestas a una **persona asegurada**;

g. **los gastos de mitigación**; **y/o**

h. **los gastos de asistencia a juicio**.

A los efectos de esta cobertura y al objeto de determinar lo que la **aseguradora** abonará, se deberá estar a las definiciones contenidas en la sección 'definiciones' de las presentes condiciones especiales.

Así mismo, si durante la defensa de una **reclamación,** la **persona asegurada** debe asistir a efectos de prueba ante el juzgado, el **asegurador** le pagará los gastos justificados por cada día, o parte de cada día, que la **persona asegurada** o alguno de sus **empleados** deba dedicar a dicha asistencia bajo requerimiento de su abogado o experto del **asegurador** de acuerdo con las siguientes tasas:

a. cualquier socio, administrador o miembro del consejo de administración de la **entidad**, hasta 500 € al día;

b. cualquier **empleado** hasta 250 € al día.

No será aplicable ninguna **franquicia** a dichos gastos.

**Definiciones aplicables a esta cobertura**

**Gastos forenses de protección de datos:** entendidos como los gastos incurridos por el **asegurado**, previo consentimiento por escrito de la **aseguradora**, para utilizar servicios de especialistas forenses externos a fin de preparar la defensa contra una **reclamación**.

**Gastos de inspección de protección de datos: entendidos como los honorarios de abogados y peritos, incurridos por el asegurado, previo consentimiento por escrito de la aseguradora, para la investigación, defensa, apelación o avenimiento a consecuencia de una inspección de datos.**

**Inspección de datos: cualquier investigación, consulta o examen oficial no rutinaria derivado de una vulneración de datos de un regulador, organismo gubernamental o cualquier otra autoridad de control que vele por el cumplimiento de la legislación sobre protección de datos personales.**

**Gastos y sanciones PCI: entendidas como multas, sanciones y reembolsos de gastos (incluyendo pero no limitándose a gastos operacionales, gastos de nueva emisión de tarjetas de pago y recuperaciones de fraudes) que la entidad esté legalmente obligado a pagar como resultado de su fallo en cumplir con el estándar de seguridad de los datos de la industria de las tarjetas de pago (en inglés: payment card industry data security standard).**

**Sanción administrativa: entendidas como las multas o sanciones por vulneración involuntaria de la normativa de protección de datos, impuestas a la entidad por cualquier entidad gubernamental o cualquier organismo supervisor, siempre que sean asegurables por Ley en la jurisdicción en la cual se impone la sanción por primera vez, sin incluir las sanciones PCI.**

## 2.4 Fraude tecnológico

La **aseguradora** reembolsará a la **entidad**, conforme se indica en este apartado, hasta el sublímite indicado en las condiciones particulares, **y hasta un máximo de 60 días naturales por periodo de seguro**, por las pérdidas financieras directas de la **entidad descubiertas** por primera vez durante el **periodo de seguro,** a consecuencia de un **ciberataque** de un tercero, exclusivamente por los supuestos indicados a continuación.

a. Uso fraudulento de su identidad electrónica

Por el uso fraudulento o deshonesto de la identidad electrónica de su negocio, incluyendo pero sin limitarse a:

i. la obtención de un crédito a su nombre;

ii. la firma electrónica de cualquier contrato;

iii. la creación o uso de un sitio web diseñado para copiar o imitar el de su negocio; o

b. Robo electrónico de fondos

Por el robo electrónico de dinero o valores de la **entidad**, siempre y cuando, dicha pérdida resulte en instrucciones fraudulentas por medios electrónicos por la que dicho tercero sin autorización, ordene un movimiento financiero para adeudar fondos en una **cuenta bancaria**.

c. Modificación de precios online

Por la diferencia entre los precios oficiales autorizados por la **entidad** publicados en sus sitios web y los precios modificados, a la baja, intencionalmente por un tercero no autorizado.

d. Fraude en servicios contratados

Por el uso fraudulento del **sistema informático**, que derive en el incremento en los gastos incurridos por la **entidad** en:

i. el servicio de suministro eléctrico;

ii. servicio telefónico (sean a través de teléfonos móviles o fijos, o a través de Internet);

iii. servicio de Internet, incluidos los datos móviles;

iv. el coste de cualquier pago por clic malicioso;

v. para minar criptomonedas (cryptojacking).

En cualquier caso, no cubriremos cualquier incremento en los gastos incurridos por la **entidad** relacionados con el uso fraudulento de sistemas en la nube.

La **aseguradora** reembolsará en el caso de que se produzca alguno de los supuestos indicados:

i. el valor o cantidad de cualquier dinero, título o propiedad, tomado o sustraído y/o,

ii. los gastos necesarios y razonables incurridos con nuestro previo consentimiento por escrito para desvincular su negocio de cualquier contrato o acuerdo contraído mediante el uso fraudulento o deshonesto de la identidad electrónica de su negocio.

A efectos del punto d., pagaremos siempre que tales gastos sean cargados a **usted** en una factura periódica por el proveedor de tal servicio conforme a un contrato o acuerdo por escrito entre **usted** y el proveedor que fuera ejecutado antes de que se descubriera el fraude del servicio, y que no sean cargados a una tarifa plana.

Consulte la documentación que se solicitará para la tramitación de la solicitud de reembolso de este apartado en el Anexo **proceso de notificación de incidentes y reclamaciones**.

# Lo que no está cubierto

**La aseguradora no hará ningún pago que se base en, se derive de, o sea atribuible directa o indirectamente a:**

**1. Infraestructura**

**Cualquier fallo o interrupción de un servicio prestado por un proveedor de servicios de Internet, sistema de nombres de dominio (o DNS por sus siglas en ingles), autoridades de certificación (o CA por sus siglas en inglés), red de distribución de contenido (o CDN por sus siglas en inglés), telecomunicaciones, satélites, de suministro eléctrico o cualquier otro proveedor de un servicio público (entre otros y sin limitarse a, agua, gas, hidrógeno); no obstante esta exclusión no aplicará a una *vulneración de datos*, cuando los datos estén almacenados en la nube, servidores remotos o almacenados en un centro de procesamiento de datos externo y el fallo o interrupción se derive de dichos servicios.**

**2. Propiedad intelectual**

**Cualquier infracción, uso, apropiación indebida, o transmisión de cualquier propiedad intelectual, incluyendo pero no limitándose a patentes, secretos comerciales, o marca registrada; no obstante, esta exclusión no aplicará a:**

**a. una *vulneración de datos***

**b. un *ciberataque*; o**

**c. una *reclamación* por responsabilidad por contenido digital.**

**3. Daños materiales**

**La pérdida, daño, desgaste ordinario, deterioro gradual o destrucción de cualquier bien tangible. Sin embargo, esta exclusión no aplicará a:**

**a. la pérdida, daño o destrucción de datos electrónicos;**

**b. una vulneración de datos, o un ciberataque, resultante de daños a, o destrucción de, cualquier bien tangible**

**c. lo recogido en la cobertura 2.2. c. Protección de equipos.**

**4. Daños personales**

**La muerte, enfermedad o daño físico sufridos por cualquier persona. Sin embargo, esta exclusión no aplicará a cualquier parte de una *reclamación* por angustia mental o emocional derivada de un incidente.**

**5. Conflictos violentos y Guerra**

**La aseguradora no hará ningún pago que se base en, se derive de, o sea atribuible directa o indirectamente a:**

**a. *Invasión, huelga, motín, revuelta, toma de poder por la fuerza (militar o no)***

**b. *guerra*; o**

**c. una *operación cibernética* que es atribuible a un estado y:**

**i. se lleva a cabo en el curso de la *guerra*; y/o**

**ii. debido a su efecto directo o indirecto cause un *impacto* en el funcionamiento de un *estado,* en la disponibilidad, integridad o prestación de un *servicio esencial* en ese *estado*; y / o**

**iii. causa un *impacto* en la seguridad o defensa de ese *estado*.**

**Una operación cibernética puede ser atribuible a un estado si el gobierno o una agencia de seguridad (incluyendo agencias de inteligencia) de un estado relevante lo comunica públicamente.**

**En el caso de que exista un conflicto de atribución de una operación cibernética dentro de un estado relevante, la atribución hecha por el gobierno del estado relevante en comunicaciones oficiales debe prevalecer.**

**En el caso de que exista un conflicto de atribución de una operación cibernética entre diferentes estados relevantes, la atribución hecha por el estado afectado debe prevalecer.**

**Si el estado afectado no ha hecho una atribución de la operación cibernética, la atribución hecha por un estado relevante debe ser suficiente, aunque otros estados relevantes estén en desacuerdo o lo contradigan.**

**En el caso de inexistencia de una atribución de una operación cibernética por un estado relevante, una operación cibernética también puede ser atribuible a un estado si la aseguradora lo prueba con evidencias apropiadas.**

**Serán de aplicación las siguientes definiciones a la presente exclusión:**

**Operación cibernética:** se entiende como un acceso o uso no autorizado a un ordenador o red o sistema en el territorio de un **estado** por parte de otro **estado** o en su nombre, así como el uso de un ordenador o red o sistema por un **estado** o en su nombre, para afectar negativamente un ordenador o red o sistema de otro **estado,** incluyendo sin limitarse a la introducción de un **virus** o un ataque de denegación de servicio contra un ordenador o red o sistema en el territorio de un **estado**.

**Servicio esencial:** se entiende como el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos o el eficaz funcionamiento de las instituciones de un **estado** y las administraciones públicas, que dependa para su provisión de redes y sistemas de información, según lo establecido por el Real Decreto- Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información o en cualquier otra normativa que lo sustituya.

**Estado:** se entiende como país soberano, reconocido como tal en el orden internacional, asentado en un territorio determinado y dotado de órganos de gobiernos propios.

**Estado afectado** significa cualquier **estado** que sufre un impacto perjudicial en su funcionamiento debido al efecto directo o indirecto de una **operación cibernética** sobrela disponibilidad, integridad o prestación de un **servicio esencial** o de su seguridad o defensa.

**Guerra:** se entiende como el uso de la fuerza física por un **estado** contra otro **estado**, ya sea declarado o no, así como una guerra civil.

**Estado relevante:** un estado afectado, un **estado** miembro de la Unión Europea o un **estado** miembro de la OTAN.

**6. Incautación, confiscación y/o prohibición de acceso**

**a. Cualquier acción de un gobierno o autoridad pública de incautación, expropiación, confiscación, apropiación o destrucción de bienes, o cualquier orden de dicho gobierno o autoridad pública para desactivar, bloquear o no permitir el acceso o el uso de todo o parte del *sistema informático* de la entidad o del *sistema informático de un proveedor externo tecnológico.***

**b. Cualquier acción del gobierno o autoridad pública por la que directa o indirectamente se regule, limite o prohíba el uso de energía por parte de la *entidad* o del *proveedor externo tecnológico*.**

**c. Cualquier orden del gobierno o autoridad pública que impida o restrinja el acceso a cualquier espacio físico o local de trabajo de la entidad o de un *proveedor externo tecnológico*, incluyendo pero no limitado el acceso a data centers.**

**7. Problemas preexistentes**

**Cualquier hecho, circunstancia o *incidente* de la que tuviera conocimiento el *asegurado* con anterioridad al inicio del primer *periodo de seguro.* Cualquier procedimiento civil, mercantil, penal, laboral, administrativo, regulatorio o de arbitraje, o cualquier procedimiento alternativo de resolución de conflictos iniciado con anterioridad a la primera fecha de efecto de la presente póliza, o basado en los mismos o esencialmente los mismos hechos alegados en dicho procedimiento anterior.**

**8. Actos intencionados o deshonestos**

**a. Cualquier acto u omisión fraudulento, doloso, deshonesto, ilegal o malicioso cometido por el *asegurado*, así como el de cualquier otra persona que el a*segurado* haya consentido o tolerado, incluyendo el uso u obtención no autorizada de datos de forma intencional o en violación de la Ley**

**b. Cualquier acto u omisión cuya intención sea obtener un beneficio indebido o una ventaja a la cual el *asegurado* no tuviera legalmente derecho.**

**Esta exclusión tiene las siguientes salvedades:**

**a. Aplicará únicamente si dicho acto u omisión se establece por medio de sentencia u otra resolución firme, o si el *asegurado* así lo reconoce;**

**b. Las actuaciones de un *empleado* no serán imputados a la *entidad*, salvo que dichas actuaciones hayan sido cometidas o hayan sido del conocimiento de algún antiguo o presente socio, administrador o directivo.**

**La *entidad* reembolsará a la *aseguradora* cualquier pago efectuado por la *aseguradora* en relación con dicho acto u omisión.**

**9. Cobertura Internacional**

**Cualquier *reclamación* o cualquier i*ncidente* fuera de la jurisdicción aplicable, entendiéndose como tal los procedimientos en tribunales, o basadas en la jurisdicción de dicho país o territorio y/o fuera de los territorios definidos (ámbito territorial) en las condiciones particulares, sin perjuicio de cualquier limitación legal adicional que pudiera existir en cualquier territorio o jurisdicción.**

| | |
|---|---|
| **10. Responsabilidad contractual** | **Cualquier garantía, promesa u obligación asumida bajo contrato por el *asegurado*. No obstante, esta exclusión no aplicará:**<br>**a. a la responsabilidad que el *asegurado* hubiera asumido en ausencia de dicho contrato;**<br>**b. cuando descubra una *vulneración de datos; o***<br>**c. cuando ocurra un incumplimiento del estándar de seguridad de los datos de la Industria de las tarjetas de pago (en inglés: payment card industry data security standard).** |
| **11. Asegurado contra asegurado** | **Cualquier *reclamación* interpuesta por:**<br>**a. el propio *asegurado;* o**<br>**b. por cualquier persona física o jurídica que detenga directa o indirectamente más de un 15% de las participaciones o acciones emitidas de la *entidad*, o que directa o indirectamente la gestione, controle o dirija parcial o totalmente; o**<br>**c. por cualquier persona jurídica en la que la *entidad* ostenta, directa o indirectamente, más de un 15% de las participaciones o acciones emitidas, o que la *entidad* gestiona, controla o dirija parcial o totalmente.**<br>**Esta exclusión no aplicará a una *reclamación* presentada por un *empleado* a consecuencia de una *vulneración de datos*.** |
| **12. Multas, penalizaciones y sanciones** | **Multas o sanciones, penalizaciones contractuales, daños punitivos o ejemplarizantes, no restitutorios o no indemnizatorios.**<br>**Esta exclusión no aplicará:**<br>**a. a las sanciones derivadas del *incumplimiento de la normativa PCI DSS;* o**<br>**b. cualquier *sanción administrativa*.** |
| **13. Fondos y valores** | **El robo, pérdida o transferencia de dinero, fondos, valores o bienes materiales, salvo lo recogido en la sección Fraude Tecnológico.** |
| **14. Mejora** | **Cualquier gasto de reparación, mejora, corrección, retirada, sustitución, eliminación**<br>**No obstante, esta exclusión no aplicará a:**<br>**a. *gastos de mitigación*;**<br>**b. los gastos de recuperación de datos y sistemas que se indican como cubiertos en la sección 2.2.a Gastos de recuperación de datos o sistemas; o**<br>**c. a la cobertura 2.2.c Protección de equipos.** |
| **15. Exclusiones aplicables a responsabilidad tecnológica (contenido digital)** | Únicamente respecto a la cober**tura 2.3.4. Responsabilidad por contenido digital.**<br>**a. cualquier infracción, uso, apropiación indebida, o transmisión de cualquier patente o secreto comercial; o**<br>**b. una obligación de pagar honorarios de licencias o royalties; o/y**<br>**c. cualquier *incidente* cometido por una *persona asegurada distinta de un empleado*.** |
| **16. Exclusiones aplicables a 2.2.a. Gastos de recuperación de datos o sistemas** | Únicamente respecto a las coberturas 2.2.a. Gastos de recuperación de datos o sistemas:<br>**a. los gastos para identificar o remediar las vulnerabilidades del *sistema informático*, del *sistema informático de un proveedor externo tecnológico* o programas;**<br>**b. sin perjuicio del punto a. ii. de la cobertura 2.2.a. Gastos de Recuperación de Datos o Sistemas, el valor económico de los programas, *datos personales*, datos electrónicos, *información corporativa* o *información confidencial*, incluyendo secretos comerciales;**<br>**c. los gastos para sustituir, restaurar o actualizar programas o datos electrónicos a un nivel superior al que existía antes de la ocurrencia del *incidente*.**<br>**d. los gastos incurridos en el desarrollo de nuevos programas o datos electrónicos.** |

| | |
|---|---|
| **17. Contaminación y radiación nuclear** | **Cualquier descarga, dispersión o escape (real, presunto o amenaza) de *contaminantes*, incluida cualquier instrucción o solicitud para realizar pruebas, monitorizar, limpiar, eliminar, contener, tratar, desintoxicar o neutralizar *contaminantes,* así comocualquier pérdida derivada de un accidente nuclear que cause entre otros un pulso electromagnético (o EMP por sus siglas en inglés).** |
| **18. RC profesional y productos** | **Cualquier *reclamación* contra el *asegurado* resultante de su prestación de servicios profesionales o productos suministrados o producidos por la *entidad (incluyendo pero no limitado a retirada o sustitución de productos)*. No obstante, esta exclusión no aplicará a una *reclamación* contra *usted*, alegando 1) la transmisión de un *virus* desde el *sistema informático,* 2) *un ataque de denegación de servicio* a un tercero con el uso del *sistema informático* de la *entidad* o con el uso del *sistema informático de un proveedor externo tecnológico, 3 una vulneración de datos*** |
| **19. Riesgos de la naturaleza** | **Los daños derivados de un riesgo natural, incluyendo pero no limitándose a terremoto, incendio, viento, inundación, volcanes, super volcanes, inversión de los polos magnéticos de la Tierra, tormenta solar o llamarada solar.**<br><br>**Asimismo se excluyen los daños causados por el clima espacial entendiendo como tal las condiciones del sol y del viento solar, magnetosfera, ionosfera y termosfera que pueden afectar al rendimiento y la fiabilidad de los sistemas tecnológicos espaciales y terrestres y que de alguna manera afectan a la infraestructura, tecnología, salud y la vida humana . De manera enunciativa pero no limitativa quedaría excluidos los daños producidos por asteroides, fulguraciones, llamaradas solares, erupciones solares o Eyecciones de Masa Coronal que pueden producir, entre otras cosas, apagones de radio o tormentas de radiación solar.** |
| **20. Exclusión Recogida y tratamiento ilegal de datos personales** | **Los incidentes/reclamaciones derivadas del incumplimiento negligente o no de las disposiciones legales o reglamentarias en materia de protección de datos, en el marco de la recogida y/o el tratamiento de datos personales por la entidad, o por cualquiera que actúe en su nombre, sin haber obtenido previamente el consentimiento suficiente con respecto al marco legal o regulatorio.** |
| **21. Transacciones financieras** | **Cualquier reclamación o pérdida que se base en, se derive de, o sea atribuible directa o indirectamente a la compra o venta de cualquier fondo o valor, acciones, derivados u otros activos financieros.**<br><br>**Asimismo, queda excluido cualquier daño derivado de la pérdida de oportunidad de efectuar una transacción financiera.** |
| **22. Sanciones internacionales** | **La aseguradora no estará obligada a proporcionar cobertura ni será responsable de pagar ninguna reclamación o pérdida o proporcionar ningún beneficio bajo la presente póliza, en la medida en que el proporcionar dicha cobertura, el pago de dicha reclamación o el proporcionar tales beneficios expusiera a la aseguradora o a cualquier miembro del Grupo al que pertenece la aseguradora a cualquier sanción, prohibición o restricción en virtud de las resoluciones de la Organización de Naciones Unidas o regulaciones, leyes, sanciones económicas o de comercio impuestas por la Unión Europea, el Reino Unido o los Estados Unidos de América.** |

# 3. Disposiciones generales

**3.1. Cuánto abonaremos**

a. El límite máximo total agregado de indemnización que la **aseguradora** pagará por el conjunto de todas las coberturas previstas en el presente módulo o póliza, es el límite de indemnización indicado en las condiciones particulares.

b. El **asegurado** deberá abonar la **franquicia** correspondiente indicada en las condiciones particulares.

c. Cualquier sublímite de indemnización que pudiera establecerse formará parte integrante del límite de indemnización indicado en las condiciones particulares para el presente módulo de cobertura o póliza, y no será en ningún caso en adición al mismo, y además será la cantidad máxima a pagar por **incidente** y **periodo de seguro** para la correspondiente cobertura.

d. En caso de que dos o más coberturas sean activadas por una misma causa o hecho generador, el **asegurado** abonará una única **franquicia**. La **franquicia** que aplicará en este caso será la más alta de las que se indican en las condiciones particulares. Este criterio no será de aplicación para la '**franquicia temporal**', la cual se aplicará de forma independiente.

e. Dos o más **incidentes/reclamaciones** atribuibles a una misma causa o hecho generador tendrán la consideración de un solo y mismo **incidente/reclamación**, con independencia del número de reclamantes o asegurados involucrados y aunque se formulen en tiempos y lugares distintos. Se imputarán dichos **incidentes/reclamaciones** al **periodo de seguro** en el cual se ha producida la primera comunicación de dichos **incidentes/reclamaciones**.

f. En el caso de que existan dos o más **pólizas** de seguro emitidas por **nosotros** o por cualquier otra sociedad que pertenezca al Grupo Hiscox y otorguen cobertura por una misma **reclamación** o **incidente**, el importe total a pagar para el conjunto de todas estas **pólizas** no excederá el mayor límite o sublímite de indemnización de todas estas **pólizas**.

**3.2. Ámbito temporal**

En relación con las coberturas de la presente póliza, se otorga cobertura únicamente a los **incidentes descubiertos** y notificados a la **aseguradora** durante el **periodo de seguro**.

Adicionalmente, en relación con las coberturas de la sección 2.3 Responsabilidad Tecnológica, y siempre que las misma figure en las condiciones particulares, se otorga cobertura a las **reclamaciones** presentadas contra el **asegurado** durante el **periodo de seguro o periodo adicional de notificación**, independientemente de la fecha de ocurrencia del **incidente**, pero siempre y cuando el **incidente** haya sido **descubierto** y notificados durante el **periodo de seguro.**

**3.3. Ámbito territorial**

Las garantías de este módulo de cobertura se extienden y se limitan a **incidentes** ocurridos o **reclamaciones** presentadas en los territorios definidos en las condiciones particulares.

**3.4. Control de la defensa**

La aseguradora tendrá el derecho, pero no la obligación, de tomar el control y dirigir en nombre del asegurado la investigación, liquidación o defensa de cualquier reclamación o inspección de datos. Si la aseguradora lo considera necesario, designará un perito, tasador, abogado o cualquier otra persona apropiada para tratar o gestionar la reclamación o inspección de datos.

La aseguradora no hará ningún pago por cualquier parte de cualquier reclamación o inspección de datos no cubierta por este módulo.

**3.5. Confidencialidad**

El asegurado deberá tomar todas las medidas necesarias en todo momento para que, en la medida de lo posible, ningún tercero conozca la existencia de la presente póliza, salvo consentimiento previo por escrito de la aseguradora. Dicha cláusula no será de aplicación a las aseguradoras de exceso cuando el presente contrato actúe como póliza primaria.

**3.6. Obligaciones del asegurado**

a. El asegurado deberá notificar a la aseguradora cualquier incidente o reclamación conforme al proceso de notificación anexo a la presente póliza tan pronto cuanto posible, pero siempre dentro del periodo de seguro.

b. El asegurado podrá notificar a la aseguradora cualquier incidente o circunstancia que pueda derivar en una reclamación, gasto o servicio cubiertos bajo este módulo de cobertura, lo antes posible y durante el periodo de seguro, salvo impedimento legal.

Si la aseguradora acepta la notificación del asegurado, cualquier reclamación, gasto o servicio cubiertos derivados de los mismos hechos se entenderá presentada, a efectos de este módulo de cobertura, en el momento en que dichos hechos fueran comunicados por primera vez, siempre que, al notificar los hechos, se hubiera facilitado información detallada sobre los mismos, las fechas y los posibles perjudicados.

c. La entidad se compromete a facilitar toda la asistencia que la aseguradora pudiera requerir para el recobro ante un tercero de la cantidad económica que le reembolsemos.

### 3.7. Periodo adicional de notificación

**Gratuito:**

Si este módulo de cobertura se cancela o no se renueva, la **entidad** tendrá derecho a un periodo adicional de notificación de:

a. 30 días naturales sin abonar prima adicional, o

b. 12 meses por una prima adicional del 75% de la última prima anual,

desde la fecha de vencimiento del **periodo de seguro**, durante el cual podrá notificar por primera vez a la **aseguradora** una **reclamación** presentada frente al **asegurado durante el periodo adicional de notificación**, cuya causa sea un **incidente descubierto** durante el **periodo de seguro**.

Por periodo adicional de notificación se entenderá un periodo de tiempo a partir de la fecha de vencimiento del **periodo de seguro**, durante el cual el **asegurado** podrá notificar a la **aseguradora** cualquier **reclamación** cubierta bajo este módulo de cobertura por hechos ocurridos conforme al ámbito temporal de la **póliza**, pero antes de la fecha de vencimiento del **periodo de seguro**.

Este periodo adicional de notificación no será de aplicación si:

a. la póliza ha sido cancelada por impago de la prima o de cualquiera de sus fracciones;

b. este módulo de cobertura ha sido reemplazado por otra póliza que otorgue, en todo o en parte, las mismas coberturas.

La totalidad de la prima correspondiente al periodo adicional de notificación deberá ser abonada íntegramente al inicio de dicho periodo.

El límite de indemnización aplicable durante el periodo adicional de notificación será el límite de indemnización remanente de la póliza cancelada o no renovada. En ningún caso se otorgará un límite separado o adicional para este periodo.

### 3.8. Condiciones generales aplicables

Se modifican las siguientes cláusulas de las condiciones generales:

Se sustituye la cláusula 'Para comunicar reclamaciones' de las condiciones generales por la cláusula '3.6. Obligaciones del asegurado' de las presentes condiciones especiales.

Se sustituye la cláusula 'varios asegurados' de las condiciones generales por la cláusula '3.1. Cuanto abonaremos' de las presentes condiciones especiales.

### 3.9 Declaración sobre el riesgo

La **aseguradora** ha suscrito el contrato considerando el estado de los riesgos y en base a la información comunicada por el tomador y/o **asegurado** con carácter previo a la contratación de acuerdo con el Cuestionario de seguro que le ha sometido la **aseguradora**. Todas estas informaciones han sido valoradas como elementos esenciales para aceptar la cobertura, estimar la prima y fijar las obligaciones entre las partes. Si estas informaciones no fueran correctas, completas o exactas, el contrato no se hubiera suscrito o se hubiera aceptado en otras condiciones más gravosas.

El Cuestionario de seguro proporcionado por el tomador y/o **asegurado**, así como la proposición de la **aseguradora** en su caso, en unión de esta póliza y sus eventuales suplementos (de haberlos), constituyen un todo unitario, fundamento del seguro, que sólo alcanza, los riesgos en la misma especificados en los límites acordados.

Si el tomador y/o **asegurado,** al formular las declaraciones del cuestionario, incurriera en reserva o inexactitud sobre las circunstancias por él conocidas que puedan influir en la valoración del riesgo, se aplicará lo siguiente:

a. La **aseguradora** podrá rescindir el contrato, mediante declaración dirigida al tomador en el plazo de un mes, a contar desde el conocimiento de la reserva o inexactitud. Corresponderán a la **aseguradora**, salvo que concurra dolo o culpa grave por su parte, las primas relativas al **período de seguro** en curso en el momento en que se haga la declaración.

b. Si la reclamación o incidente sobreviene antes de que la **aseguradora** efectúe dicha declaración, la indemnización se reducirá proporcionalmente a la diferencia entre la prima convenida y la que se hubiese aplicado de haberse conocido la verdadera entidad del riesgo. Si medió dolo o culpa grave del tomador/asegurado, la **aseguradora** quedará liberada del pago de la indemnización.

Si el contenido de la póliza difiere de la proposición de seguro o de las cláusulas acordadas, el tomador podrá reclamar a la **aseguradora** en el plazo de un mes a contar desde la entrega de la póliza para que subsane la divergencia existente. Transcurrido dicho plazo sin efectuar **reclamación**, se estará a lo dispuesto en la póliza.

### 3.10. Agravación de riesgo

El tomador del seguro o el ***asegurado*** deberán durante la vigencia del contrato comunicar a la aseguradora, tan pronto como les sea posible, la alteración de los factores y las circunstancias declaradas y/o que agraven el riesgo.

Entre otros que pudieran ser constitutivos de un aumento del riesgo, se considerarán en todo caso factores o circunstancias que agravan el riesgo y que, por tanto, el tomador y/o ***asegurado*** debe comunicar a la aseguradora, en función del cuestionario de riesgo que hubiere cumplimentado, los siguientes, cuando la entidad:

a. Hubiere incrementado en más de un 20% sus ingresos brutos anuales consolidados o en su defecto de todos los asegurados, con respecto a los declarados ante la **aseguradora** en el último año.

b. Realizase una actividad distinta, o prestase a terceros un nuevo servicio en remoto o desde la nube.

c. Hiciese uso de sistemas informáticos sin soporte del fabricante.

d. Aplicara los parches (o actualizaciones) del fabricante a los sistemas en una frecuencia superior a 30 días, o superior a 15 días en caso de parches criticas (CVSS 8.0 o superior)

e. Haya dejado de usar doble factor de autenticación para el acceso remoto a cualquier sistema incluyendo pero no limitado al correo electrónico web.

f. Haya dejado de dar acceso a sus empleados únicamente a la información y sistemas que requieren para desarrollar sus funciones, y haya dejado de eliminar el acceso a sus sistemas e información a sus empleados, cuando dejan de serlo.

g. No disponga de copias de seguridad completas al menos cada 7 días de todos sus datos y sistemas almacenadas:

   i. en un soporte físico desconectado de sus sistemas tanto durante el ejercicio de su actividad como durante la realización de la copia y dichas copias de seguridad se realicen cada vez en soportes externos distintos (una sola escritura) o

   ii. en un proveedor de nube, en el que NO se requiera el doble factor de autenticación para acceder a la consola de copias de seguridad.

h. respecto a todas las copias de seguridad NO retenga al menos copias semanales de los últimos 30 días.

i. Utilice **proveedores externos tecnológicos** de servicios en la nube que no están certificados con la ISO 27001 o que no tengan un TIER inferior al 3 (solo aplicable si la entidad ha contratado la cobertura 2.2 e. Proveedor Externo Tecnológico y salvo que la entidad haya comunicado en el momento de la emisión de la póliza o sucesivas renovaciones que utiliza un proveedor que no cumple con estas características, y eso haya sido aceptado expresamente por la **aseguradora***)*.

La **aseguradora** puede, en un plazo de dos meses a contar del día en que la agravación le ha sido declarada, proponer una modificación del contrato incluyendo cualquiera de las condiciones, limites garantías o coberturas contratadas, la prima o cualquier otro termino acordado.

En tal caso, el tomador dispone de quince días a contar desde la recepción de esta proposición para aceptarla o rechazarla.

En caso de rechazo, o de silencio por parte del tomador, la **Aseguradora** puede, transcurrido dicho plazo, rescindir el contrato previa advertencia al tomador, dándole para que conteste un nuevo plazo de quince días, transcurridos los cuales y dentro de los ocho siguientes comunicará al tomador la rescisión definitiva.

La **aseguradora** también podrá optar por rescindir el contrato comunicándolo por escrito al **asegurado** dentro de un mes, a partir del día en que tuvo conocimiento de la agravación del riesgo.

En el caso de que el tomador del seguro o el **asegurado** no haya efectuado su declaración y sobreviniere un incidente, la ***aseguradora*** queda liberada de su prestación si el tomador o el **asegurado** ha actuado con mala fe. En otro caso, incluyendo en aquellos casos en que no hubiera transcurrido el plazo de dos meses indicado en el párrafo (3) o si el tomador o **asegurado** no hubieran aceptado y cumplido las obligaciones de pago u otras exigidas por la **aseguradora**, la prestación de la **aseguradora** se reducirá proporcionalmente a la diferencia entre la prima convenida y la que se hubiera aplicado de haberse conocido la verdadera entidad del riesgo.

### 3.11. Aceptación expresa y constancia de recibo de información

El tomador reconoce expresamente que ha recibido las condiciones generales, especiales y particulares que integran esta póliza manifestando su conocimiento y conformidad con las mismas.

Igualmente, de acuerdo con lo previsto en el artículo 3 de la ley 50/80 de 8 de Octubre, del contrato de seguro, el tomador manifiesta que ha leído, examinado y entendido el contenido y alcance de todas las cláusulas del presente contrato y, especialmente, aquellas que, debidamente resaltadas en letra negrita, pudieran ser limitativas de derechos. Por último, el tomador reconoce expresamente haber recibido antes de la celebración del contrato la oportuna información relativa al seguro, a la legislación aplicable al contrato de seguro, las diferentes instancias de reclamación, el estado miembro del domicilio de la **aseguradora** y su autoridad de control, la denominación social, dirección y forma jurídica de la **aseguradora**.

### Firmas

(Indicar nombre y cargo)

En nombre y representación del Tomador Fecha

# Anexo

## Servicio de respuesta a incidentes (cobertura 2.1)

Servicio de contención tecnológica

**En caso de sufrir un incidente, comuníquelo a través de la página web www.hiscox.es/notificarsiniestro o siniestros@hiscox.com**

**En caso de un incidente en el que necesite asistencia inmediata para contener el mismo, contacte con el Servicio de Respuesta a Incidentes disponible 24x7x365 al teléfono**

**+34 910 386 819**

**¿Qué información debe facilitar?**

1. Nombre del asegurado (persona jurídica) y número de póliza
2. Datos de contacto del asegurado (persona física) para futuras comunicaciones
3. Breve descripción del **incidente**

**¿Cómo se apertura el expediente?** El proveedor del Servicio de Respuesta a Incidentes* procederá , una vez realizada las verificaciones previas necesarias, y siempre que se trate de un **incidente** real y no un falso positivo, a la apertura de un ticket en el sistema interno de ticketing y a comunicar el **incidente** a la propia **aseguradora** quien informará a su mediador de seguros.

* En el caso de Conflictos de Intereses, se procederá a nombrar al Back up previsto en el panel de expertos de Hiscox quien prestará el servicio en las mismas condiciones.

**¿Cuándo se inicia la gestión del incidente?** Confirmada la recepción del **incidente** mediante la apertura del ticket, comienza el proceso de dar soporte al mismo por parte de los equipos y técnicos especializados, conforme se dispone en la póliza. Un técnico especializado estará en contacto, en todo momento, con el **asegurado**.

**¿Qué información se solicitará para la gestión del incidente?** Se solicitará al **asegurado** toda la información necesaria para poder gestionar el **incidente** como por ejemplo diagramas de red, máquinas afectadas, logs (de correo electrónico, de navegación), volcados de memoria, discos duros, muestras de malware, emails originales, etc. En caso de que el cliente no tenga la capacidad técnica para facilitar tal información, el Proveedor facilitará las instrucciones necesarias para la obtención de la misma. Es responsabilidad del **asegurado** facilitar la información solicitada en tiempo y forma.

**¿Dónde se prestará la gestión del incidente?** El servicio se ejecutará en remoto. En caso de que el **asegurado** requiera la presencia on-site de técnicos especializados en las instalaciones del afectado por el siniestro, procederá a dar respuesta tras aprobación previa de Hiscox.

**¿Qué actuaciones realizará el servicio de gestión de incidentes?** El Proveedor del Servicio de Respuesta a Incidentes, siempre dentro de la capacidad disponible, realizará las actuaciones necesarias para prestar los servicios cubiertos en la póliza.

**¿Qué información obtendrá tras el servicio?** Tras la finalización del proceso de gestión del **incidente**, se procederá a la elaboración, emisión y distribución del correspondiente informe que facilitará tanto al **asegurado** como a Hiscox.

**Servicio de asesoramiento jurídico y de comunicación y relaciones públicas**

Cuando se produzca la apertura del **incidente**, Hiscox designará cuando sea necesario, e experto legal y/o de comunicación y relaciones públicas del **panel de expertos de Hiscox**, al objeto de puedan asesorarle sobre las medidas a tomar para gestionar la respuesta del **incidente**.

**Gastos de notificación y monitorización**

El **asegurado** podrá requerir a Hiscox la prestación de los servicios adicionales incluidos en la cobertura 2.1. **Servicio de respuesta a incidentes**, en el caso de que requiera que sean prestados a través del **panel de expertos de Hiscox**. Hiscox deberá dar su consentimiento por escrito.

## Proceso de notificación de incidentes y reclamaciones

1.1. Servicio de respuesta a incidentes

En caso de que se produzca un **incidente**, y **usted** decida acudir a otro especialista distinto del servicio de contención tecnológica de Hiscox, deberá informar a la **aseguradora** del **incidente** en el plazo máximo de siete días desde su ocurrencia a través de su mediador de seguros, con la descripción del **incidente**, indicando fecha, tipo y alcance del **incidente**, así como el informe del especialista que ha o se encuentra gestionado el **incidente**.

1.2. Perdidas del asegurado

Para la activación de estas coberturas, en el caso de que no haya hecho uso del **servicio de contención tecnológica**, **usted** deberá ponerse en contacto con su mediador de seguros para comunicar el **incidente**.

La **aseguradora** le solicitará según cada caso, la documentación que considere necesaria al objeto del análisis de la cobertura en la póliza. Entre otros, acreditación de la ocurrencia del **incidente**, justificación de los gastos a incurrir (presupuestos, actividades a realizar, etc.), documentos contables para la cobertura de pérdida de beneficios, etc.

Por favor, verifique en la póliza los procesos a seguir para cada cobertura y los consentimientos a solicitar a Hiscox.

a. En relación con la sección 2.2, apartado **a. Gastos de recuperación de datos o sistemas y e. Proveedor externo tecnológico**.

   En el caso de una pérdida cubierta por esta garantía, asumiremos, en las condiciones previstas por la **póliza** y dentro del límite indicado en las condiciones particulares, el pago de las facturas de recuperación de datos o sistemas de la **entidad.**

   La **aseguradora** asumirá el reembolso de la cantidad, excluyendo cualquier impuesto aplicable, de las facturas pagadas por **usted**, y previa presentación de documentación acreditativa, incluyendo pero sin limitarse a:

   — informe sobre el alcance de la pérdida de datos o sistemas;

   — presupuesto de intervención del proveedor designado por el **asegurado**, desglosado por acciones a realizar y/o horas a invertir por los técnicos.

   — facturas por la intervención del proveedor designado por el **asegurado**.

b. En relación con la sección 2.2, apartado **d. Pérdida de beneficios y e. proveedor externo tecnológico,** y únicamente si la entidad tiene contratado un límite de indemnización:

   **usted** debe acreditar por escrito dentro de un plazo máximo de 120 días tras descubrir la existencia de una pérdida de beneficios (a menos que hayamos aceptado ampliar dicho periodo) la pérdida sufrida aportando la siguiente información:

— una descripción completa de las circunstancias relacionadas con la pérdida de beneficios, incluyendo, sin restricciones, el momento, el lugar y la causa de la pérdida;

— un cálculo detallado de cualquier pérdida de beneficios, o en caso de que desee que realicemos el cálculo de dicha perdida rogamos nos facilite impuesto de sociedades, cuenta de resultados y balance de situación de los últimos tres ejercicios de las empresas afectadas; y

— toda la documentación y el material justificativo que razonablemente forme parte de o guarde relación con el fundamento de la prueba de tal pérdida de beneficios, al menos la información solicitada en los puntos a y b.

Los costes y gastos incurridos por **usted** para probar o justificar la pérdida de beneficios sufrida correrán por su cuenta y no están cubiertos por la presente póliza.

La reducción del resultado de explotación se calculará diariamente.

c. En relación con la sección 2.2, apartado b. **Extorsión cibernética.**

En el caso de una pérdida que pueda estar cubierta por esta garantía, la **aseguradora** le solicitará la documentación que considere oportuna, entre otras:

— la documentación recogida en el apartado 1.1 Servicio de respuesta a Incidentes del presente anexo;

— la descripción del **incidente**, indicando entre otras cosas fecha, tipo e impacto conocido;

— La notificación por parte de la **entidad** de la **amenaza de extorsión** a la policía u otra autoridad responsable de hacer cumplir la ley;

— la autorización del pago del rescate por parte de un administrador, directivo (o cargo equivalente) de la **entidad**;

— factura acreditativa del pago del rescate.

d. En relación con la sección 2.2, apartado c. Protección de equipos.

La **aseguradora** le solicitará facturas de reparación o sustitución de equipos informáticos afectados por un **incidente**.

La **aseguradora** asumirá el reembolso de la cantidad, excluyendo cualquier impuesto aplicable, de las facturas pagadas por **usted**, y previa presentación de documentos justificativos indicados en la garantía.

1.3. Responsabilidad tecnológica

En el caso de que reciba una **reclamación** o sea objeto de una inspección de datos, por favor, póngase en contacto con su mediador de seguros.

Al objeto de poder tramitar el expediente correctamente, Hiscox le solicitará a través de su mediador, la documentación necesaria para el análisis de la cobertura de la póliza. Entre otras, **reclamación** formal escrita del perjudicado, documentación judicial o procedimiento administrativo, versión detallada de los hechos por parte del **asegurado**, información sobre el error supuestamente cometido, etc.

En el caso de que el **asegurado** desee nombrar un abogado, perito o experto forense para que le asistan en su defensa, deberá solicitar la previa autorización por escrito de Hiscox, y facilitarle el presupuesto de honorarios para su aprobación. El **asegurado** podrá designar si lo desea, previa solicitud a Hiscox, alguno de los profesionales previstos en el **panel de expertos de Hiscox**.

Por favor, verifique en la póliza los procesos a seguir para cada cobertura y los consentimientos a solicitar a Hiscox.

1.4. Fraude tecnológico

La **aseguradora** podrá solicitar la documentación acreditativa de las pérdidas del **asegurado**, que puede incluir pero sin limitarse a:

— informe sobre el alcance de las pérdidas y/o gastos sufridos;

— justificantes de las pérdidas correspondiente a las diferencias entre los precios oficiales y los precios modificados a causa de un **ciberataque**;

— facturas emitidas por su operador de telecomunicaciones.

Cualquier gasto en los que **usted** incurra en relación con la acreditación de las pérdidas cubiertas por la sección **fraude tecnológico**, correrán por cuenta de la **entidad** y no están cubiertas por la presente **póliza**.

**Panel de expertos de Hiscox**

| | |
|---|---|
| Servicio de Respuesta a Incidentes | Puede contactar a nuestro proveedor en el siguiente teléfono:<br>+34 910 386 819 |