Póliza de Riesgos Cibernéticos

Berkley Cyber Risk Protect - ESP

Para empresas con facturación anual consolidada inferior a 500 millones de euros

Preliminar

Por favor lea la siguiente información antes de rellenar el cuestionario:

1. El solicitante del seguro debe facilitar toda la información solicitada en el cuestionario. El cuestionario ha de ser rellenado, firmado y fechado por la persona legalmente capacitada para suscribir la solicitud de seguro.
2. El solicitante del seguro debe facilitar toda la información solicitada en el cuestionario, así como poner en conocimiento del asegurador cualquier hecho relevante que razonablemente pueda dar lugar a una reclamación.
3. Este cuestionario no obliga a la formalización del contrato de seguro pero formará parte del mismo en caso de emitirse.

Tomador del seguro

Nombre de empresa _____

Dirección _____

Ciudad _____ C.P. _____

Nº de empleados _____ ¿Cuántos empleados de informática tiene la empresa? _____

Fecha de constitución _____ ¿Cotiza en bolsa? ☐ Sí ☐ No

Sitio web _____

Descripción de la actividad _____

Situación financiera

Por favor, especifique los siguientes datos financieros (consolidados):

	Último ejercicio 20__	Año anterior 20__
Ventas totales:		
– en España		
– en Europa		
– en Estados Unidos/Canadá		
– en el resto del mundo		
– Online		
Activos totales		
Presupuesto en informática		

Filiales y Participadas

Por favor, enumere todas las filiales, sucursales o participadas fuera de la UE / EEE.

Nombre de la compañía	País	Actividad (en caso de que sea distinta a la del tomador):

Registro de datos personales en la empresa

La empresa dispone del siguiente número de registros de datos personales:

- ☐ 1 – 20.000 registros
- ☐ 20.001 – 100.000 registros
- ☐ 100.001 – 500.000 registros
- ☐ 500.001 – 1.000.000 registros
- ☐ más de 1.000.000 registros

Distribución de registro de datos por zona:

España: _____
Europa: _____
Estados Unidos/Canadá: _____
Resto del mundo: _____

Política de privacidad

¿Dispone de política de privacidad por escrito?	☐ SÍ	☐ NO
¿La política de privacidad ha sido auditada por un abogado externo?	☐ SÍ	☐ NO
¿Tiene un Responsable de seguridad, un Responsable de protección de los datos, un asesor legal interno o cualquier otra persona formalmente responsable de la protección y seguridad de los datos (interno o externo)?	☐ SÍ	☐ NO
Los empleados que manejan datos personales, ¿han firmado una declaración o documento de confidencialidad?	☐ SÍ	☐ NO
¿Existen autorizaciones de acceso para los usuarios que manejen o traten datos personales, y estos son regularmente comprobados?	☐ SÍ	☐ NO
¿Los datos personales se almacenan de manera encriptada?	☐ SÍ	☐ NO
¿Cumple con la normativa aplicable en materia de protección de datos? En especial, el Reglamento General de Protección de Datos, y la LOPD 2018.	☐ SÍ	☐ NO

Seguridad física: sala de ordenadores/central de datos

¿Existen medidas adecuadas de protección, tales como protección contra intrusos, permisos de acceso, suministro energía ininterrumpida, etc.?	☐ SÍ ☐ NO

Gestión de riesgos

¿Están capacitados los empleados para el manejo de información personal / información confidencial, y hay instrucciones para el almacenamiento y/o eliminación de documentos?	☐ SÍ ☐ NO
La entidad solicitante, ¿forma regularmente a sus empleados en materia de seguridad de la información o riesgos cibernéticos? (por ejemplo, información sobre correos electrónicos sospechosos o tipos de ataque)	☐ SÍ ☐ NO
¿Dispone la entidad solicitante de una política de seguridad para el uso de los sistemas de información y la misma se comunica a todos los empleados?	☐ SÍ ☐ NO
¿Se han identificado sistemas/medios de información vulnerables para las empresas y se están utilizando instrumentos de control adecuados?	☐ SÍ ☐ NO
¿Se ha formalizado un procedimiento de clasificación de la información según su nivel de seguridad (confidencialidad, disponibilidad, integridad)?	☐ SÍ ☐ NO
¿Existe un principio obligatorio de "doble firma" para transferencias, pagos, retiradas de fondos de cuyos valores sean superiores a 25.000 euros?	☐ SÍ ☐ NO
¿Se toman medidas adecuadas para evitar entregas no autorizadas de mercancías?	☐ SÍ ☐ NO
¿Se han modificado las contraseñas y pins que venían por defecto en los dispositivos o sistemas de telecomunicaciones?	☐ SÍ ☐ NO

Medidas de Protección

¿Todos los equipos informáticos tienen instalado un antivirus actualizado y cuya actualización se supervisa centralmente y regularmente?	☐ SÍ ☐ NO
¿Existe un proceso controlado o automático para instalar parches de seguridad, actualizaciones de *firmware* y paquetes de servicio?	☐ SÍ ☐ NO
Si es así, ¿se hacen pruebas en entornos de prueba antes de importarlos al entorno real?	☐ SÍ ☐ NO
¿Se realizan copias de seguridad diarias, y se inspeccionan y almacenan en otro lugar?	☐ SÍ ☐ NO
¿Es necesario que los usuarios modifiquen sus contraseñas con regularidad y existen normas sobre la complejidad y la validez temporal?	☐ SÍ ☐ NO

¿El acceso a la información o datos que tiene la sociedad se autoriza en función del rol que desempeñe el usuario/empleado dentro de la organización y se basa en el principio del menor privilegio (se otorgan únicamente permisos de acceso a la información cuando sea necesario para el desempeño de la actividad)?	☐ SÍ	☐ NO
¿Existe un proceso para borrar, bloquear o ajustar los permisos y la recuperación de la información incluida en el inventario en el caso de cese de un empleado o recolocación del mismo en otro puesto dentro de la organización, así como para terceros externos que tuvieran permisos de acceso?	☐ SÍ	☐ NO
¿Son seguras las configuraciones de referencia utilizadas en ordenadores portátiles, servidores y dispositivos móviles?	☐ SÍ	☐ NO
¿Procede un endurecimiento de los sistemas informáticos vía la eliminación y/o desactivación de partes o funciones de software en el sistema que no se necesiten?	☐ SÍ	☐ NO
Los empleados no pueden instalar su propio software por su cuenta y sin la supervisión del equipo informático.	☐ SÍ	☐ NO
Se han tomado las medidas adecuadas en relación con el uso de puertos USB (encriptación automática, escáner vírico, prohibición de equipos externos, etc.)	☐ SÍ	☐ NO
¿Existe alguna directriz de seguridad sobre el uso de dispositivos móviles privados dentro de la red de la empresa y sobre el uso de redes de wifi públicas?	☐ SÍ	☐ NO

Seguridad en la red

¿Dispone de un *firewall* entre la red interna e Internet? El mismo se actualiza periódicamente y el tráfico de datos se filtra y se controla.	☐ SÍ	☐ NO
¿Se implementan sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusiones (IPS)? ¿Los mismos se actualizan y monitorizan regularmente?	☐ SÍ	☐ NO
¿La red está segmentada de forma que las áreas críticas se separan del resto?	☐ SÍ	☐ NO
¿Los accesos remotos de red utilizan doble autentificación ?	☐ SÍ	☐ NO
¿Se llevan a cabo evaluaciones de las vulnerabilidades de forma regular, y su caso, se toman las medidas oportunas?	☐ SÍ	☐ NO
¿Existe un equipo de gestión de incidencias y un equipo de gestión de cambio?	☐ SÍ	☐ NO
¿Se registran y supervisan los incidentes de seguridad, tales como malware o intentos de acceso no autorizado?	☐ SÍ	☐ NO

Certificaciones

¿Dispone su empresa de certificación? En caso afirmativo, ¿cuáles?

Externalización: el uso de los proveedores de informática externos y de servicios en la nube

La entidad delega (total o parcialmente) actividades, procesos, servicios y actividades empresariales relacionadas con la tecnología de la información o el procesamiento de datos en terceros. ¿Usa los servicios de la nube? (Si la respuesta es NO pase directamente a la sección Gestión de crisis cibernética)	☐ SÍ ☐ NO
¿Existe un acuerdo escrito de externalización que incluya los requisitos de seguridad que debe cumplir este proveedor de servicios?	☐ SÍ ☐ NO
¿Se han suscrito Acuerdos de Nivel de Servicio (SLAs) con el subcontratista?	☐ SÍ ☐ NO
¿Existen acuerdos de exención de responsabilidad con el servicio externo?	☐ SÍ ☐ NO
¿Qué áreas se han externalizado a proveedores externos de informática y/o a proveedores en la nube y son críticos con la empresa? Por favor, indique detalle a continuación del área, proveedor y funciones: _____ _____ _____	

Gestión de crisis cibernética

¿Dispone de un plan de emergencia en respuesta/ actuación ante una crisis cibernética?	☐ SÍ ☐ NO
¿Incluye el plan, al menos, los siguientes elementos?:	
• En caso de avería, ¿se prevé el mantenimiento de los sistemas operativos necesarios?	☐ SÍ ☐ NO
• Plan de comunicación/notificación para los afectados	☐ SÍ ☐ NO
• Distribución de tareas fijadas para la gestión del incidente	☐ SÍ ☐ NO
• Capacidad de externalización alternativa en el caso de un fallo de un Proveedor de servicios en áreas críticas del negocio.	☐ SÍ ☐ NO
¿Tiene un Plan de Continuidad de Negocio (BCP) o un Plan de Recuperación de Emergencias?	☐ SÍ ☐ NO
¿Se ha probado el plan de respuesta rápida, el plan de continuidad del negocio (BCP) y/o el plan de recuperación de emergencia / desastre (DR)?¿Se actualiza regularmente?	☐ SÍ ☐ NO

Tecnología

Indique el tiempo estimado en que una caída de los sistemas/equipos tendría un impacto significativo en su negocio: ☐ Inmediatamente ☐ tras 6h ☐ tras 12h ☐ tras 24h ☐ tras 48h

¿Están separadas IT (tecnologías de la información) y OT (tecnologías de las operaciones) por redes y las transacciones se encuentran aseguradas por un cortafuego *firewall*?	☐ SÍ ☐ NO
¿En caso de fallo de los sistemas informáticos, es posible que la producción continúe manualmente?	☐ SÍ ☐ NO

En caso afirmativo: ¿Durante cuánto tiempo puede operar? _____

¿Cómo continuarían la producción y los procedimientos de logística en este caso? _____

_____

¿Se ha probado este escenario de emergencia?	☐ SÍ ☐ NO
En caso de fallo informático en la producción, ¿puede recurrirse a un almacén de productos acabados?	☐ SÍ ☐ NO

En caso afirmativo, ¿durante cuánto tiempo es posible que esto ocurra antes de que se produzca una escasez de suministro y se produzca una completa paralización de la entrega? _____

_____

¿Existen accesos de mantenimiento remoto en su producción?	☐ SÍ ☐ NO

En caso afirmativo, explique cómo se asegura y supervisa este acceso _____

_____

Pagos electrónicos (Industrias de Tarjetas de Pago)

¿Almacena, procesa o transmite el Tomador o su proveedor externo de servicios información de tarjetas de crédito? (Si la respuesta es No, continúe con el cuestionario)	☐ SÍ ☐ NO
¿Cumple con los Estándar de Seguridad de la Industria de tarjetas de pago (PCI DSS)?	☐ SÍ ☐ NO

¿Cuál es el volumen promedio de transacciones y pagos pendientes al año? _____

¿El almacenamiento, procesamiento o transmisión de información de tarjetas de crédito ha sido subcontratado a un proveedor de servicios de certificación? Nombre del servicio externo: _____	☐ SÍ ☐ NO

PCI Nivel: ☐ Nivel 1 ☐ Nivel 2 ☐ Nivel 3 ☐ Nivel 4

Reclamaciones y circunstancias

¿Tiene la sociedad o sus filiales conocimiento de alguna circunstancia, hecho o incidente, que pudiera resultar en una reclamación derivada de una intrusión en la red, fallo de los sistemas informáticos, corrupción en la red o los datos, incumplimiento de los derechos de propiedad intelectual de terceras partes, protección de datos, imposición de multa, investigación de la Agencia de Protección de datos o cualquier otra autoridad local similar o alguna instancia de negligencia profesional?

☐ Sí
☐ No

Esto incluye también, ataques cibernéticos, investigaciones internas, ciberextorsión, pérdidas de datos, incidentes de programas maliciosos.

Por favor, facilite más información sobre las circunstancias, daños reales o potenciales. (Medidas adoptadas, coste/daño, fecha, descripción del hecho...)

Declaración

El solicitante declara que lo detallado en la presente solicitud es verdadero y que no se han declarado falsamente hechos materiales, tergiversado o suprimido después de conocerlos. El solicitante está de acuerdo en que esta solicitud, junto con otra información adjunta, forman las bases de un contrato de seguro efectuado entre W.R. Berkley y el solicitante.
El Tomador o el Asegurado se compromete a informar a W.R. Berkley de cualquier modificación de aquellos hechos ocurridos antes de formalizar el contrato de seguro o durante la vigencia de la póliza.

Nombre y cargo del Representante de la Sociedad	
Firma	Fecha

5. Orden de domiciliación de adeudo directo SEPA

A CUMPLIMENTAR POR EL ACREEDOR

Referencia de la orden de domiciliación (*):	
Identificador del acreedor:	ES46633W0371455G
Nombre del acreedor:	W.R. BERKLEY EUROPE AG, Sucursal en España
Dirección del acreedor:	PASEO DE LA CASTELLANA, 141. 18º PLANTA
Código postal/Población/Provincia:	28046 MADRID
País de residencia del acreedor:	ESPAÑA

* constará de su CIF/NIF y su nº de cuenta

Mediante la firma de esta orden de domiciliación, el deudor autoriza a (A) WR W.R. BERKLEY EUROPE AG, Sucursal en España a enviar instrucciones a la entidad del deudor para adeudar su cuenta y (B) a la entidad para efectuar los adeudos en su cuenta siguiendo las instrucciones de W.R. BERKLEY EUROPE AG, Sucursal en España.

Como parte de sus derechos, el deudor está legitimado al reembolso por su entidad en los términos y condiciones del contrato suscrito con la misma. La solicitud de reembolso deberá efectuarse dentro de las ocho semanas que siguen a la fecha de adeudo en cuenta.

A CUMPLIMENTAR POR EL DEUDOR

Su nombre: _____

Su dirección: _____

Código postal/Población/Provincia: _____

País de residencia: _____

Número de cuenta ☐☐☐☐ (IBAN) ☐☐☐☐ (entidad) ☐☐☐☐ (oficina) ☐☐ (DC) ☐☐☐☐☐☐☐☐☐☐ (10 dígitos nº cuenta)

Swift - BIC: ☐☐☐☐☐☐☐☐☐☐☐

(puede contener de 8 a 11 posiciones)

Tipo de pago: Pago recurrente ☒ o Pago único ☐
(renovación/fraccionamiento/ajustes)

Lugar y fecha de la firma _____

Firma del deudor: (Por favor firme aquí)

Nota: Puede obtener información adicional sobre sus derechos en su entidad financiera.

TODOS LOS CAMPOS HAN DE SER CUMPLIMENTADOS OBLIGATORIAMENTE.

UNA VEZ FIRMADA ESTA ORDEN DE DOMICILIACIÓN DEBE SER ENVIADA AL ACREEDOR PARA SU CUSTODIA.

LA ENTIDAD DEL DEUDOR REQUIERE AUTORIZACIÓN DE ÉSTE PREVIA AL CARGO EN CUENTA DE LOS ADEUDOS DIRECTOS SEPA.

EL DEUDOR PODRÁ GESTIONAR DICHA AUTORIZACIÓN CON LOS MEDIOS QUE SU ENTIDAD PONGA A SU DISPOSICIÓN.

Política de privacidad de Berkley España

ÚLTIMA ACTUALIZACIÓN: 26 de julio de 2018

Ponemos a su disposición nuestra Política de Privacidad para proporcionarle toda la información relativa a los datos personales que podemos recoger y el uso que daremos a dicha información y para garantizar el puntual cumplimiento de la legislación en materia de protección de datos personales.

Es importante que lea esta Política de Privacidad atentamente. Por favor, en caso de duda contacte con nosotros mediante correo postal o electrónico en las direcciones que figuran más abajo.

¿Quién trata sus datos?

El Responsable del tratamiento de sus datos es W.R. BERKLEY EUROPE AG, SUCURSAL EN ESPAÑA (en adelante BERKLEY).

Hemos nombrado a una persona encargada de salvaguardar su privacidad en nuestra entidad (el Delegado de Protección de Datos o "DPD"), ante quien podrá ejercer sus derechos, presentar cualquier reclamación o solicitar la aclaración de cualquier duda, mediante correo postal dirigido a la dirección Paseo de la Castellana 141, 28046, Madrid o en el correo electrónico GDPRinfo@wrberkley.com

¿Para qué finalidades se tratan sus datos?

Los datos personales que recogemos dependerán de su relación con nosotros. Recogeremos distintas categorías de datos personales dependiendo de si Usted es un tomador, asegurado o potencial asegurado, un beneficiario de una póliza de seguro de BERKLEY, un perjudicado o reclamante, un testigo, un corredor, otro tipo de mediador de seguros y/o reaseguros, representantes designados u otro tercero –socio comercial, prestador de servicios en relación con un contrato de seguro, etc.

Así, podremos utilizar sus datos personales para:

- Valorar una solicitud de seguro, analizar y evaluar el riesgo y, de conformidad con las condiciones aplicables, poder ofrecerle un seguro. Dentro del proceso de suscripción puede existir la elaboración de perfiles, donde se recurre a procesos automatizados. Una vez que le hayamos proporcionado su póliza, utilizaremos sus datos personales para administrar su póliza, tratar sus consultas y gestionar el proceso de renovación.
- Prestar servicios relacionados con el seguro, las reclamaciones y la asistencia, así como otros productos y servicios que nosotros facilitemos, incluyendo la evaluación, administración y resolución de siniestros y reclamaciones, así como la solución de conflictos relacionados con estos.
- Prevenir, detectar e investigar delitos, incluyendo el fraude y el blanqueo de capitales, así como para analizar y gestionar otros riesgos comerciales.
- Ofrecer información de marketing, de conformidad con las preferencias que usted nos haya comunicado (la información de marketing puede ser acerca de productos y servicios que terceros en tanto socios nuestros le ofrezcan, en virtud de las preferencias que usted haya mencionado). Es posible que llevemos a cabo actividades de marketing por medio del correo electrónico, SMS y demás servicios de mensaje de texto, correo postal y teléfono.
- Cumplir con la legislación aplicable y con las obligaciones de las autoridades reguladoras (incluyendo aquellas leyes y regulaciones de fuera del país donde resida); por ejemplo, aquellas leyes y regulaciones relacionadas con las medidas frente al blanqueo de capitales, las sanciones y el antiterrorismo; para cumplir con procedimientos judiciales y resoluciones judiciales; y para responder a solicitudes de autoridades públicas y gubernamentales (incluyendo aquellas de fuera de su país de residencia).

Antes de recoger y/o tratar datos personales sensibles, nos aseguraremos de contar con una de las siguientes bases de legitimación:

- Usted haya prestado su consentimiento explícito;
- Necesitemos usar dichos datos personales para formular, ejercitar o defender reclamaciones; o
- Necesitemos usar sus datos personales por razón de un interés público esencial, como podría ser el tratamiento de sus datos personales sensibles para el pleno desenvolvimiento del contrato de seguro cuando las leyes nacionales o la normativa europea directamente aplicable contemplasen específicamente esta posibilidad.

No obstante lo anterior, en ciertas circunstancias, necesitaremos su consentimiento explícito para tratar datos personales sensibles (por ejemplo, si no existiese una base de legitimación más adecuada, podríamos necesitar recabar su consentimiento explícito para tratar datos personales sobre salud). En los casos en los que no exista una base de legitimación más adecuada y tengamos que recabar su consentimiento explícito, es posible que, sin este consentimiento, no podamos proporcionarle una póliza o tramitar sus reclamaciones. En todo caso, siempre le explicaremos por qué el consentimiento es necesario y cuáles son las consecuencias de no prestarlo o de retirarlo –pues tendrá derecho a ello en todo momento.

¿Por qué se tratan sus datos?

Los tratamientos necesarios lo son para cumplir el ordenamiento jurídico y sus contratos, o solicitudes. Los adicionales, si es Usted cliente o acepta nuestra política de protección de datos, están basados en su consentimiento, que siempre puede revocar sin detrimento alguno, o en el interés legítimo, ponderado con el derecho a su privacidad. Esta ponderación se ha realizado de acuerdo con la normativa y los criterios comunicados por las autoridades en materia de protección de datos, siempre pensando que con ello podemos mejorar la calidad de nuestros productos y servicios para atenderte de manera más personalizada y comunicarte nuestras ofertas.

¿Quiénes podrán ver sus datos?

Trabajamos con un gran número de terceros para ayudar a gestionar nuestro negocio y prestar servicios. Estos terceros pueden ocasionalmente tener acceso a sus datos personales. Entre estos terceros podrán figurar:

- Mediadores, otros aseguradores / reaseguradores y TPAs que trabajen con nosotros para ayudar a gestionar el proceso de suscripción, administrar nuestras pólizas, prestar asistencia o gestionar siniestros.
- Proveedores de servicios, que ayudan a gestionar nuestros sistemas de Márketing, TI y back office.
- Otras compañías pertenecientes a W.R. Berkley Corporation.
- Organismos oficiales.

Podemos estar obligados legalmente a comunicar sus datos personales a tribunales, reguladores, autoridades policiales o, en determinados casos, a otras aseguradoras o reaseguradoras. En el caso de operaciones societarias, podríamos transferir sus datos personales a las diferentes partes involucradas.

¿Por cuánto tiempo conservaremos sus datos?

El período de tiempo exacto durante el cual conservemos sus datos personales, dependerá de su relación con nosotros y del tipo de datos personales que poseamos. En este sentido, conservaremos sus datos personales durante el tiempo que sea razonablemente necesario para los fines enumerados en el apartado segundo.

Debe tener en cuenta que, entre las finalidades establecidas para el tratamiento de sus datos personales, se encuentra el cumplimiento de nuestras obligaciones legales y regulatorias. Por tanto, en circunstancias específicas, también podremos conservar sus datos personales durante períodos de tiempo más prolongados para tener un registro preciso de las gestiones que ha realizado con nosotros en caso de reclamaciones o impugnaciones, o si consideramos razonablemente que existe la posibilidad de un litigio en relación con sus datos personales o gestiones.

¿Cuáles son sus derechos?

Podrá acceder, rectificar, suprimir sus datos, oponerse al uso de los mismos, revocar sus consentimientos, así como otros derechos reconocidos por la normativa como el derecho de portabilidad, limitación del tratamiento, o presentar reclamación ante la Agencia de Protección de Datos, o a nuestro Delegado de Protección de Datos.

Además, si se tomaran decisiones automatizadas que le afecten, siempre puede solicitar intervención humana para revisarlas, y siempre puede oponerse a cualquier tratamiento, o revocar el consentimiento sin ningún perjuicio para Usted.
Puede ejercitar sus derechos remitiéndonos una carta adjuntando copia de su DNI, o documento oficial equivalente, con el asunto "PROTECCIÓN DE DATOS" en la siguiente dirección: Paseo de la Castellana 141, 28046 Madrid, o a través del correo electrónico GDPRinfo@wrberkley.com.