HISCOX

CYBERCLEAR®

Hiscox Negocios

Hiscox CyberClear − Tecnología

Solicitud de Seguro

Debe cumplimentar todas las secciones y firmar la Declaración.

Hiscox CyberClear – Tecnología

Solicitud de Seguro

La intención de este cuestionario es conocer cómo su organización protege su información, sus sistemas, cómo detecta posibles incidentes, la respuesta que ofrece para la gestión de los mismos, incluyendo los servicios externalizados y en base a eso, presentar nuestra propuesta de seguro y servicios. En función del nivel de riesgo que hayamos detectado solicitaremos a una empresa especialista más información o solicitaremos realizar una valoración del riesgo más detallada.

Información general

Corredor de Seguros:

Nombre del tomador:

CIF:

Domicilio:

Años de actividad:

Filiales:

¿Requiere cobertura para sus filiales? Sí ☐ No ☐

Si ha respondido Sí, tenga en consideración que las siguientes preguntas de este cuestionario se refieren a todas las sociedades a asegurar bajo la póliza, incluyendo facturación y siniestralidad.

También deberá adjuntar un listado de todas las filiales.

Dirección web:

Estándares para la seguridad de la información:

¿Tiene usted alguna certificación de seguridad de la información (por ejemplo ISO/IEC 27002)? Sí ☐ No ☐

Si ha respondido Sí, proporcione detalles:

Facturación:

	Último año	Año en curso	Estimada para el próximo año
Facturación total			
Facturación en EEUU			
Facturación en Europa			
Facturación Online			

Número de empleados:

El número total de sus empleados, incluyendo filiales:

Actividades:

Por favor detalle las actividades de su negocio (incluya las actividades de sus filiales):

HISCOX
CYBERCLEAR®

Hiscox CyberClear – Tecnología
Solicitud de Seguro

Desglose de su facturación por los siguientes servicios:

Servicio	% de facturación aproximado
Desarrollo de software a medida	
Ciberseguridad	
Gestión de incidentes	
Cloud	
Venta de software de terceros	
Consultoría	
Servicios de Web (hosting, diseño, y registro de dominio)	
Plataforma de pagos	
Soluciones de Inteligencia Artificial	
Otros (especificar):	

Desglose de su facturación por los siguientes sectores:

Sector	% de facturación aproximado
Administración Pública	
Militar	
Financiero	
Producción industrial	
Ingeniería	
Construcción	
Minería	
Aeroespacial	
Salud/Medicina	
Comercio	
Industria farmacéutica	
Otros (especificar):	

Información de la gestión

1. **Gestión de la Seguridad de la Información (a nivel de la entidad)**

   a. ¿Existe un responsable de la seguridad de la información? Sí ☐ No ☐

   b. ¿Dispone de un equipo o persona encargada de poner en marcha las medidas definidas para protegerse? Sí ☐ No ☐

   c. ¿Dispone de un equipo o un tercero que verifique que las medidas para protegerse efectivamente se encuentran en marcha, distinto al departamento de Sistemas o IT? Sí ☐ No ☐

2. **Políticas de Gestión de la Seguridad de la Información**

   a. ¿En su organización está centralizada la aplicación de las medidas definidas para la protección de sus sistemas e información? Sí ☐ No ☐

   b. ¿Dispone de una política de protección de datos personales y de seguridad adaptada a la legislación, sector y jurisdicción donde opera la entidad? Sí ☐ No ☐

   c. ¿Dispone de un programa de concienciación en materia de seguridad de la información para sus empleados? Sí ☐ No ☐

d. ¿Dispone de alguno de los siguientes planes efectivamente implementados y testados en su organización en relación con la seguridad de la información o sistemas?

Contingencia o continuidad de negocio	Sí ☐ No ☐
Respuesta ante incidentes	Sí ☐ No ☐
Recuperación ante desastres	Sí ☐ No ☐

e. En caso de disponer de un plan de respuesta ante incidentes, ¿Contempla éste el registro, clasificación, escalamiento según criticidad/seriedad, tiempos de respuesta para cada instancia y control de cumplimiento de dicho proceso? Sí ☐ No ☐

3. **Sistema Informático**

a. ¿Cuántos usuarios tienen actualmente acceso a sus sistemas? ☐

b. ¿Realiza un inventario de sus activos/equipos informáticos? Sí ☐ No ☐

c. ¿Cuántos servidores dispone (tanto propios como de terceros)? ☐

d. Por favor indique, si lo conoce, el número de IP's públicas que tiene asignada su organización: ☐

e. Indique por favor los sistemas o áreas más críticas para su negocio. Si lo ha evaluado, indique el tiempo máximo que tardaría en volver a la normalidad tras sufrir un incidente (caída, bloqueo, etc.):

Sistema (o actividad)	Tiempo de recuperación

4. **Medidas de seguridad de su infraestructura tecnológica**

a. ¿Dispone de un antivirus actualizado en todos los equipos, los actualiza periódicamente, los administra y están centralizados? Sí ☐ No ☐

b. ¿Existe un proceso formal de implantación de parches? Sí ☐ No ☐

c. En caso de haber respondido de manera afirmativa a la pregunta anterio, ¿cuál es la frecuencia de implementación de parches? ☐

d. ¿Se exige un usuario y contraseña para acceder a todos sus sistemas? Sí ☐ No ☐

e. ¿Se utiliza el principio de privilegio mínimo para la configuración de los distintos perfiles de usuarios? Sí ☐ No ☐

f. ¿Existen usuarios fuera del departamento de Sistemas/IT o tercero autorizado con acceso a los sistemas con perfil de 'administrador' (acceso sin limitaciones al sistema)? Sí ☐ No ☐

g. ¿Se contempla una política de contraseñas compleja y un cambio periódico de las mismas? Sí ☐ No ☐

h. ¿Se contempla el control de acceso, bloqueo o medidas restrictivas ante sucesivos intentos erróneas de acceder a una cuenta? Sí ☐ No ☐

i. ¿Se contempla un segundo factor de autenticación para el acceso a los sistemas críticos? Sí ☐ No ☐

j. ¿Se realiza un proceso anual de verificación y corrección de las autorizaciones de acceso a su sistema? Sí ☐ No ☐

k. ¿Existe un procedimiento de baja de usuarios tras la finalización de un contrato laboral? Sí ☐ No ☐

l. ¿Existen medidas de seguridad mínimas definidas para los distintos equipos informáticos (incluyendo servidores, ordenadores y portátiles), y se controla periódicamente su correcta implantación? Sí ☐ No ☐

m. ¿El protocolo de actuación ante incidentes de pérdida de dispositivos físicos contempla la eliminación remota de la información? Sí ☐ No ☐

n. ¿Los procesos de recambio o reparación de hardware contemplan la eliminación previa de la información contenida? Sí ☐ No ☐

5. **Seguridad en la red**

a. ¿Se encuentran todos los puntos de acceso a Internet protegidos por Firewalls? Sí ☐ No ☐

b. ¿Existe una segmentación de la red entre recursos críticos y otros recursos? Sí ☐ No ☐

c. ¿Se configuran los sistemas críticos de acuerdo con una arquitectura Activa/Pasiva o Activa/Activa? Sí ☐ No ☐

d. ¿Se realiza un test de intrusión interno o externo al menos una vez al año, con un plan de acción tendiente a mitigar las vulnerabilidades identificadas? Sí ☐ No ☐

e. ¿Existe un proceso de recopilación, monitorización y análisis de logs (el histórico de los distintos eventos ocurridos en la red)? Sí ☐ No ☐

f. ¿El acceso de los usuarios internos a Internet se realiza a través de un proxy, con control antivirus y filtrado de contenido? Sí ☐ No ☐

g. Los accesos remotos se realizan mediante una red privada virtual (VPN) u otros mecanismos que garanticen el cifrado del canal de comunicaciones? Sí ☐ No ☐

h. ¿Existe un sistema de identificación y prevención de intrusos (IDS/IPS)? Sí ☐ No ☐

i. ¿Existe un proceso de monitorización del tráfico entrante y saliente? Sí ☐ No ☐

j. ¿Existe un proceso formal para aprobar y probar todos los cambios y las conexiones de red en la configuración de los firewalls y routers? Sí ☐ No ☐

6. **Gestión de datos personales e información confidencial de terceros**

a. ¿Existe un Delegado de Protección de Datos o persona que cumpla su función dentro de su organización? Sí ☐ No ☐

b. ¿Obliga a sus empleados a cumplir con la política (o equivalente) de protección de la información? Sí ☐ No ☐

c. ¿Realiza formaciones a sus empleados en el tratamiento y protección de la información? Sí ☐ No ☐

d. ¿Clasifica la información que gestiona (usted o un tercero en su nombre) en función de lo sensible o de lo crítico que sea para su negocio, de acuerdo a las normativas de protección de datos? Sí ☐ No ☐

e. ¿Con que frecuencia realiza copias de seguridad de sus sistemas o datos críticos? Sí ☐ No ☐

Al menos una vez al día	☐
Al menos cada 7 días	☐
Entre 8 y 14 días	☐
Entre 15 días y un mes	☐
Otra frecuencia (indíquela)	

f. ¿Confirma periodicamente que las copias de seguridad se han realizado correctamente? Sí ☐ No ☐

g. ¿Existe un procedimiento establecido para restaurar copias de seguridad? Sí ☐ No ☐

h. ¿Existen copias de seguridad adicionales en más de una ubicación física y/o servicio de nube? Sí ☐ No ☐

i. ¿Se permite la copia de información no cifrada en dispositivos de almacenamiento externos? Sí ☐ No ☐

j. ¿Se aplica cifrado a la información almacenada? Sí ☐ No ☐

k. ¿Se aplica cifrado a las copias de seguridad? Sí ☐ No ☐

l. Indique por favor el tipo de datos que recolecta, almacena o procesa (usted o algún tercero en su nombre), así como el volumen aproximado de los mismos:

Tipo de datos		Número de datos
Datos personales	Sí ☐ No ☐	
Tarjeta de pago (débito o crédito)	Sí ☐ No ☐	
Números de cuentas	Sí ☐ No ☐	
Datos médicos	Sí ☐ No ☐	
Propiedad Intelectual/ Secretos Comerciales	Sí ☐ No ☐	
Contratos/información confidencial de terceros	Sí ☐ No ☐	

m. Con respecto a los datos de tarjetas de pago, ¿cumple usted o el proveedor o con quien haya externalizado el procesamiento de pago, con la normativa del sector de tarjetas de pago en cuanto a la seguridad de los mismos (PCI-DSS)? Sí ☐ No ☐

n. En caso de respuesta afirmativa en la pregunta anterior, por favor indique el nivel asignado:

7. **Contenidos en medios digitales**

a. ¿Se incluyen en sus sitios webs y redes sociales contenido (como imágenes, videos, textos, por ejemplo) de terceros o facilitado por terceros? Sí ☐ No ☐

b. En caso de responder afirmativamente la pregunta anterior, ¿obtiene el consentimiento por escrito para poder hacer uso del contenido y su publicación? Sí ☐ No ☐

c. ¿Se revisa legalmente el contenido (propio y de terceros) en sus sitios webs y redes sociales antes de ser publicados? Sí ☐ No ☐

d. ¿Se han cambiado las contraseñas por defecto de administrador de gestión de su sitio web? Sí ☐ No ☐

8. **Medidas en la prestación de su servicio**

a. ¿Se han definido medidas de seguridad para garantizar el adecuado tratamiento de la información correspondiente a cada tipo de cliente, contemplando las medidas definidas en los contratos? Sí ☐ No ☐

b. ¿Existen medidas de seguridad que limitan el acceso a la información de un cliente popr parte de otros clientes? Sí ☐ No ☐

c. ¿La gestión de incidentes contempla la notificación en tiempo y forma a los clientes afectados? Sí ☐ No ☐

d. ¿Es necesaria la conexión al sistema informático de sus clientes para prestar sus servicios? Sí ☐ No ☐

9. **Medidas de seguridad física**

¿Se encuentran definidas las medidas mínimas de seguridad física para los Centros de Procesamiento de Datos (CPD), con un control periódico de cumplimiento? Sí ☐ No ☐

10. **Externalización de servicios**

a. ¿Cuáles de los siguientes servicios informáticos que se encuentran externalizados y quienes son los correspondientes proveedores?

Servicios externalizados		Nombre del proveedor
Seguridad de los sistemas	Sí ☐ No ☐	
Servicios de almacenamiento en lanube (Cloud) o servicios en la nube	Sí ☐ No ☐	
Plataforma de pagos con tarjetas	Sí ☐ No ☐	
Copias de seguridad	Sí ☐ No ☐	
Mantenimiento/Actualización de los sistemas	Sí ☐ No ☐	
Gestión de equipos informáticos	Sí ☐ No ☐	
Recolección o tratamiento de datos	Sí ☐ No ☐	

b. ¿Incluyen los contratos de servicios externalizados cláusulas de confidencialidad de la información y cumplimiento con la correspondiente normativa de protección de datos? Sí ☐ No ☐

c. ¿Incluyen los contratos de los servicios externalizados medidas o requerimientos mínimos de seguridad a cumplir y la posibilidad de ser auditados? Sí ☐ No ☐

d. ¿Se exige en los contratos de servicios externalizados la notificación de incidentes de seguridad que pudieran afectarle? Sí ☐ No ☐

e. ¿Se exige contractualmente a sus proveedores mantener un seguro de riesgo cibernético? Sí ☐ No ☐

HISCOX
CYBERCLEAR®

Hiscox CyberClear – Tecnología
Solicitud de Seguro

Reclamaciones, incidentes y pólizas de seguros

a. ¿Ha sufrido en los últimos 24 meses alguna: vulneración de datos; fallo de seguridad; extorsión cibernética; interrupción o caída de sus sistemas; destrucción de sus datos; acceso de personas no autorizadas a sus sistemas ,o cualquier otro incidente similar que haya dado lugar a una reclamación o inspección de datos? Sí ☐ No ☐

b. ¿Tiene conocimiento de algún hecho o circunstancia que pudieran dar lugar a una reclamación, inspección de datos o la activación de alguna de las coberturas de la póliza que le ofrecemos? Sí ☐ No ☐

c. ¿Dispone actualmente de cobertura de seguro de riesgos cibernéticos? Sí ☐ No ☐

En caso afirmativo por favor facilite una descripción del incidente, indicando sus consecuencias económicas y operativas, los archivos o componentes de su infraestructura tecnológica afectados, y las medidas correctoras aplicadas.

Declaración

Por favor, lea cuidadosamente esta declaración y firme al final.

Información material

Por favor, infórmenos de los detalles de cualquier información que pueda ser relevante para nuestra consideración de su propuesta de seguro. En caso de duda sobre la relevancia, infórmenos de dichos detalles.

Ley protección de datos

Los datos de carácter personal facilitados por Usted se incluirán en ficheros automatizados, del que es responsable Hiscox Insurance Company Limited, sucursal en España, de acuerdo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con el fin de que nosotros le informemos sobre nuestras actividades y productos, así como para la liquidación de siniestros y reclamaciones y la colaboración estadístico actuarial y de lucha contra el fraude.

Usted y la persona asegurada podrán dirigirse, para solicitar su consulta, actualización, rectificación o cancelación, si así lo desean, a Hiscox Insurance Limited Sucursal en España, Paseo de la Castellana 60, 28046 Madrid. Usted y la persona asegurada otorgan su consentimiento expreso para que dichos datos puedan ser cedidos a otras entidades aseguradoras u organismos públicos o privados relacionados con el sector asegurador con fines estadísticos y de lucha contra el fraude, así como por razones de coaseguro y reaseguro. Las sociedades del grupo Hiscox tendrán acceso a tales datos de carácter personal para los fines anteriormente mencionados.

Declaración

Declaro/Declaramos que (a) este solicitud de seguro ha sido completado después de una apropiada investigación; (b) sus contenidos son verdaderos y exactos y (c) todos los hechos y asuntos que puedan ser relevantes para la consideración de nuestra solicitud de seguro han sido comunicados.

Acuerdo/Acordamos que este formulario y toda información proporcionada será incorporada al contrato de seguro y formarán parte del mismo.

Firma, nombre y cargo

	/ /
En representación del Tomador	Fecha

Una copia de esta solicitud de seguro debería quedarse en su poder.

Hiscox
Paseo de la Castellana, 60 28046 Madrid

T +34 91 515 99 00
F +34 91 515 99 19
E riesgosprofesionales@hiscox.com
www.hiscox.es