Cuestionario de Riesgos Cibernéticos

Markel Cyber

Solicitud De Seguro

MARKEL

Cuestionario de Riesgos Cibernéticos

Solicitud De Seguro

Se ruega leer estas notas orientadoras antes de rellenar el Cuestionario

El Cuestionario deberá ser cumplimentado, firmado y fechado por una persona que esté legalmente capacitada y autorizada para suscribir la solicitud de seguro de Riesgos Cibernéticos en representación de la empresa que actúa como solicitante. Tal y como se indica en el Art. 10 de la Ley 50/80 de Contrato de Seguro, es deber del solicitante aportar toda la información que en el cuestionario se indica así como dar a conocer cualquier hecho relevante.

Este Cuestionario no obliga a la formalización del seguro pero formará parte de cualquier Contrato de Seguro que pueda emitirse con posterioridad. Es imprescindible contestar a todas las preguntas contenidas en este Cuestionario.

A: Datos Generales De La Empresa

Tomador del Seguro: C.I.F:

Dirección: Código Postal:

Localidad: Provincia:

Descripción de la actividad de la Entidad Tomadora del Seguro y de sus Entidades Filiales:

Facturación total de la **Solicitante** y sus filiales en el último año:

Porcentaje de facturación online

Si realiza atividades de distinta naturaleza, indicar % de facturación que representa cada actividad.

B: Actividad

1. ¿Tiene la **Solicitante** sucursales o filiales en el extranjero? Sí ☐ No ☐
2. ¿Se encuentran los **Sistemas** informáticos de la **Solicitante** ubicados en España? Sí ☐ No ☐

   En caso afirmativo detallar localización y % de facturación.

MARKEL

3. Página web principal

4. ¿Qué aplica a la infraestructura de red del **Solicitante**?

- ☐ servidores propios operados por usted
- ☐ servidores propios operados por terceros
- ☐ cloud
- ☐ otro:
- ☐ N° de servidores (si aplica):

5. ¿Qué aplica a su política de seguridad informática en caso de que tenga filiales?

☐ a. centralizada ☐ b. descentralizada ☐ c. combinación de a y b

Aportar más información en caso de b o c:

El término **"Sistemas"** se refiere a cualquier sistema, dispositivo o equipo de tecnología de la información y/o comunicación, incluido cualquier hardware, software o firmware y los datos almacenados en ellos, pero no incluye los sistemas telefónicos (ya sean digitales, analógicos, habilitados para IP (protocolo de Internet) o cualquier otro tipo de sistema telefónico), independientemente de dónde estén alojados, ya sea propiedad del Asegurado o arrendado a éste.

El término **"Solicitante"** hace referencia al futuro Asegurado y a las filiales cubiertas por la póliza.

C: Tratamiento de Datos

6. Número de registros:

- ☐ PII
- ☐ PHI
- ☐ PCI

7. ¿Cómo está gestionada en su organización la responsabilidad de la seguridad de los datos?

- ☐ CIO/CISO
- ☐ DPO interno ☐ DPO externo
- ☐ Departamento IT ☐ Legal & Compliance ☐ IT con Legal & Compliance
- ☐ Un miembro del consejo es explícitamente responsable
- ☐ Otro

8. Confirme que cumple con toda la regulación aplicable relativa a Protección de Datos Sí ☐ No ☐

9. ¿Están cifrados sus "datos en tránsito"?

- ☐ sí ☐ sí, pero sólo si los datos están marcados como confidenciales ☐ no / no se
- ☐ Otro

MARKEL

10. ¿Están cifrados sus "datos en reposo" (incluidas las copias de seguridad)?

☐ si ☐ si, pero sólo si los datos están marcados como confidenciales ☐ no / no se

☐ Otro

11. ¿Qué software utiliza para bloquear el correo electrónico (posiblemente) malicioso?

☐ Spamfilter ☐ DMARC ☐ Otro

12. ¿Organiza formaciones entre sus empleados con el fin de aumentar su concienciación sobre los ciberriesgos incluido el phishing? Sí ☐ No ☐

En caso afirmativo, determinar:

☐ online-training ☐ phishing test ☐ otro:

☐ continuo ☐ anual ☐ otro:

☐ obligatorio para todos los empleados ☐ obligatorio para parte de los empleados

D: Seguridad de la red

13. ¿Su infraestructura informática (incluido el entorno de copia de seguridad) está protegida por un software antimalware que se actualiza automática e inmediatamente después de la disponibilidad de una nueva actualización? Sí ☐ No ☐

14. ¿Están protegidas por cortafuegos todas las conexiones entre su infraestructura informática e Internet? Sí ☐ No ☐

15. ¿El acceso remoto a su infraestructura de IT y a su entorno de copia de seguridad requiere autenticación multifactor y una conexión segura? Sí ☐ No ☐

16. El acceso a la infraestructura informática de la **Solicitante** está protegido con contraseñas seguras de al menos 8 caracteres y que son modificadas periódicamente; Sí ☐ No ☐

17. ¿Dispone de una política documentada de gestión de parches? Sí ☐ No ☐

18. Tiempo máximo en el que se despliegan los parches críticos para los sistemas críticos de la empresa.

19. ¿Utiliza un producto de protección de terminales (EPP) en su infraestructura de IT? Sí ☐ No ☐

☐ Software:

20. ¿Utiliza Endpoint Detection & Response (EDR) en su infraestructura de IT? Sí ☐ No ☐

☐ Software:

En caso afirmativo, ¿incluye todos terminales y servidores?

Sí ☐ No ☐ % terminales

Sí ☐ No ☐ % servidores

21. Seleccione qué soluciones de protección de red están implementadas en su infraestructura de IT

☐ SIEM ☐ SOC interno ☐ SOC externo ☐ Intrusion Detection System (IDS)

☐ Otro

22. ¿Disponen sus administradores de cuentas separadas para las actividades administrativas? Sí ☐ No ☐

23. ¿Utiliza una solución PAM (Privileged Access Management)? Sí ☐ No ☐

24. ¿Permite su organización que empleados no administradores tengan derechos de administrador? Sí ☐ No ☐

En caso afirmativo, explique:

25. ¿Se encuentra su red debidamente segmentada? Sí ☐ No ☐

En caso afirmativo, explique: (geográficamente/unidad de negocio, etc.)

26. Si alguna OT es vital para las operaciones de su empresa, ¿ha segmentado la red OT de la red IT y controlado el tráfico con cortafuegos? Sí ☐ No ☐

E: Recuperación y Respuesta ante incidentes

27. ¿Guarda sus copias de seguridad separadas físicamente de la red de su empresa? Sí ☐ No ☐

en la nube ☐ off line ☐

28. ¿Con qué frecuencia realiza copias de seguridad de los datos críticos de su empresa?

Copia de seguridad incremental:

Copia de seguridad completa:

29. ¿Se comprueba si las copias de seguridad son correctas y están libres de malware? Sí ☐ No ☐

En caso afirmativo, ¿con qué frecuencia? Frecuencia:

¿Se comprueban los procedimientos de copia de seguridad Sí ☐ No ☐

30. ¿Ha determinado un objetivo de tiempo de recuperación (RTO) para sus aplicaciones más críticas? Sí ☐ No ☐

RTO:

31. Planes de gestión de crisis implementados:
☐ DRP ☐ BCP ☐ IRP

¿Se abordan específicamente los incidente de ciberseguridad? Sí ☐ No ☐

F: Proveedores externos

28. ¿Con qué frecuencia realiza copias de seguridad de los datos críticos de su empresa?

G: Información Sobre Siniestralidad

1. Determinar si la entidad Solicitante ha experimentado en alguna ocasión algún incidente o se ha visto afectada por alguna investigación por parte de cualquier autoridad competente en materia de ciberseguridad o relacionado con las coberturas de la presente Póliza, o si existe algún hecho o circunstancia que razonablemente pueda dar lugar a una Reclamación contra la Solicitante: Sí ☐ No ☐

MARKEL

En caso afirmativo amplíen la información:

Información Precontractual

De acuerdo con lo dispuesto en la Ley 20/2015, de 14 de julio, de Ordenación y Supervisión y Solvencia de las Entidades Aseguradoras y Reaseguradoras, el Asegurador a quien se ha solicitado cobertura declara:

1. Que el presente contrato de seguro se celebra en régimen de Derecho de Establecimiento con MARKEL INSURANCE SE, Sucursal en España, con domicilio en Torre de Cristal, Paseo de la Castellana 259C, Planta 34, 28046 Madrid (España), que consta inscrita en el Registro de Entidades Aseguradoras de la Dirección General de Seguros bajo la clave de autorización Nº E 0235.
2. El Estado Miembro a cargo de la supervisión de las actividades del Asegurador es Alemania, la Autoridad de Control es BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), con domicilio en Graurheindorfer Str. 108l, 53117 Bonn, Alemania.
3. Que la legislación aplicable al presente contrato será la Ley 50/1980 de 8 de octubre, del Contrato de Seguro, y la Ley 20/2015, de 14 de julio, de Ordenación y Supervisión de los Seguros Privados Supervisión y Solvencia de las Entidades Aseguradoras y Reaseguradoras y demás normativa española de desarrollo.
4. Que las disposiciones relativas a las reclamaciones serán las siguientes:

   a. Instancias internas de reclamación:

   En el supuesto de que tenga alguna queja o reclamación, podrá Ud. dirigirse por escrito, al corredor que intermedió la póliza, en su caso, o al departamento o área implicada de Markel Insurance SE, Sucursal en España.

   En caso de no quedar satisfecho, si Ud. quisiera presentar una queja o reclamación relacionada con sus intereses y derechos legalmente reconocidos, podrá dirigirla por escrito a nuestro Servicio de Atención al Cliente:

   Titular del Servicio: Dª Sandra Santos Matarranz
   C/ Serrano 76, 6 Derecha
   28006 – Madrid
   Teléfono: 91 556 19 78
   E-mail: atencioncliente@markel.com

   b. Instancias externas de reclamación:

   En caso de que su reclamación o queja no haya sido admitida, o se haya desestimado total o parcialmente su petición, o haya transcurrido el plazo de dos meses desde la fecha de su presentación ante el Servicio de Atención al Cliente sin que haya sido resuelta, Ud. podrá acudir al Servicio de Reclamaciones de la Dirección General de Seguros y Fondos de Pensiones.

   En caso de disputa, usted podrá reclamar, en virtud del Artículo 24 de la Ley de Contrato de Seguro, ante el Juzgado de Primera Instancia correspondiente a su domicilio.

   Así mismo, podrá usted someter voluntariamente sus divergencias a decisión arbitral en los términos previstos en el Artículo 31 de la Ley General para la Defensa de los Consumidores y Usuarios y sus normas de desarrollo, sin perjuicio de lo establecido en la Ley de Arbitraje, para el caso de que las partes sometan sus diferencias a decisión de uno o varios árbitros.

Se ruega leer estas notas orientadoras antes de rellenar el Cuestionario

RESPONSABLE: MARKEL INSURANCE SE SUCURSAL EN ESPAÑA, Paseo de la Castellana, 259C, Planta 34 (Torre de Cristal), 28046 de Madrid, markel@delegado-datos.com, W2764898I. **FINALIDADES:** Tramitación del siniestro involucrado, cuantificación de la indemnización que le pudiera corresponder y pago de la misma. **LEGITIMACIÓN:** Ejecución del contrato de seguro del tomador. **CESIONES:** En los casos legalmente establecidos, al tomador de la póliza contratada, durante la tramitación de los siniestros, a corredores y agentes de seguros, compañías aseguradoras y todas las entidades, organismos o personas legitimadas y necesarias para la resolución y tramitación de siniestros. **CONSERVACIÓN:** Durante la vigencia del siniestro y, finalizada éste, durante los plazos exigidos legalmente para atender responsabilidades. **DERECHOS:** Tiene derecho a solicitar el acceso, rectificación, supresión, oposición, limitación y portabilidad de sus datos dirigiéndose a los datos de contacto del responsable. En caso de divergencias, puede presentar una reclamación ante la Agencia de Protección de Datos (www.aepd.es).

No se entregará documentación del cliente a terceros no autorizados.

☐ NO DESEO RECIBIR INFORMACIONES COMERCIALES

Declaración

Declaro/Declaramos que (a) este formulario ha sido completado tras 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 propuesta de seguro han sido comunicados. Asimismo, acuerdo/acordamos que este formulario y toda la información proporcionada será incorporada al contrato de seguro y formarán parte del mismo.

Firma:	
Nombre:	
Cargo:	
Fecha:	