GRUPO DATA
ASESORAMIENTO Y MEDIACIÓN EN SEGUROS, S.L.
C/ Periodista Sánchez Asensio, 5
10200 Cáceres
Teléfono:+34 927600000 www.grupodata.es

Grupo Data

LIMPIAR FORMULARIO
SE VAN A BORRAR TODOS LOS DATOS ESCRITOS EN EL FORMULARIO
SI NO

Cuestionario de Seguro Ciberriesgo

Por favor responda de forma completa a todas las preguntas de este Cuestionario Solicitud de Seguro y presente toda la información/documentación complementaria solicitada. La información obtenida mediante este Cuestionario Solicitud de Seguro y mediante toda la información/documentación complementaria será confidencial.

Este cuestionario se aplicará a aquellas Pymes y/o Autónomos cuyo Volumen de Facturación sea menos de 5 Millones.

Información General

Datos del Tomador

Nombre o Razón Social	
NIF / CIF	
Domicilio Social	
Localidad	
C. Postal	
Provincia	
País	
Teléfono de Contacto	
Email	
Dirección Página Web	
Fecha de Creación de la Empresa	

Datos del Riesgo

1.	**Detalle la actividad de su negocio**	
2.	**El Tomador lleva realizando la actividad de este negocio (indicar fecha)**	
3.	**Número de empleados actuales**	
4.	**Ingresos Brutos Anuales**	_____€ (Año Pasado) _____€ (Año Actual) _____€ (Próximo Año)

Gestión de Riesgos Privados

1.	**¿Acepta el Tomador pagar bienes o servicios con tarjetas de crédito?**	☐ Si	☐ No
	En caso afirmativo, **Por favor, indique el porcentaje aproximado de ingresos procedentes de operaciones con tarjetas de crédito en los últimos doce (12) meses.**	%	
	Si el Tomador acepta pagar bienes o servicios con tarjetas de crédito, ¿cumple el Tomador con la normativa aplicable de seguridad de datos emitida por las instituciones financieras para efectuar transacciones?	☐ Si	☐ No
	Si el Tomador no cumple con la normativa aplicable de seguridad de datos, por favor, describa el estado actual de algún trabajo realizado y la fecha estimada de finalización del mismo.	☐ Si	☐ No
2	**¿Tienen los empleados el acceso restringido a la Información No Pública y Relativa a Personas Físicas Identificables?**	☐ Si	☐ No
3	**¿Comparte el Tomador con terceros la Información No Pública y Relativa a Personas Físicas Identificables o la información confidencial, lo que puede conllevar a que el Tomador resulte indemnizado por divulgación de información o negligencia incurrida por ese tercero?**	☐ Si	☐ No

GRUPO DATA
ASESORAMIENTO Y MEDIACIÓN EN SEGUROS, S.L.
C/ Periodista Sánchez Asensio, 5
10200 Cáceres
Teléfono:+34 927600000 www.grupodata.es

Grupo Data

Control de los Sistemas Informáticos

1. ¿El Tomador hace copias de seguridad al menos cada 7 días de los datos confidenciales o sensibles en una ubicación "fría" u "offline" que no se vería afectada por un problema en el sistema operativo, y se comprueba que esas copias de seguridad son recuperables?	☐ Si	☐ No
2. En caso negativo, por favor, indique las excepciones		
3. ¿Utiliza el Tomador sistemas de protección cortafuegos disponibles en el mercado para prevenir el acceso no autorizado a las redes internas o a los Sistemas Informáticos?	☐ Si	☐ No
4. Utiliza MFA (autenticación multifactor) para el acceso al email en la nube y para todos los accesos remotos a su red	☐ Si	☐ No
5. ¿Permite el acceso remoto a su entorno de red sin una VPN (red privada virtual)?	☐ Si	☐ No
6. ¿Subcontrata el Tomador algunas de las operaciones o seguridad de sus Sistemas Informáticos?	☐ Si	☐ No
En caso afirmativo: **Por favor, especifique las operaciones subcontratadas y los vendedores**		
¿Requiere el Tomador a los vendedores que demuestren políticas y procedimientos de seguridad adecuados?	☐ Si	☐ No
7. ¿El Tomador realiza procesos de actualización de software, incluyendo instalaciones de servicios antivirus?	☐ Si	☐ No
En caso afirmativo, **– ¿Se instalan los servicios antivirus dentro de los treinta (30) días desde la cesión?**	☐ Si	☐ No
– Aplica parches críticos	☐ Si	☐ No
– Utiliza software con soporte y que no estén en el final de su vida útil (EOL, fin de vida)	☐ Si	☐ No
8. Protege todos tus dispositivos con antivirus, antimalware y/o software de protección de puntos finales (endpoint protection software)	☐ Si	☐ No
9. Analiza los correos electrónicos entrantes en busca de archivos adjuntos y/o enlaces maliciosos	☐ Si	☐ No
10. Imparte periódicamente (al menos una vez al año) una formación de concienciación en materia de ciberseguridad, incluida la lucha contra la suplantación de identidad (anti-phising), a todas las personas que tienen acceso a la red de su empresa o a los datos confidenciales/personales	☐ Si	☐ No