Cuestionario de seguridad y protección de datos para proveedores de software de atención al cliente

Lo que va entre corchetes se sustituye por los datos de la empresa. El proveedor responde en la última columna y adjunta la prueba de cada fila.

EMPRESA
[Nombre de la empresa]

PROVEEDOR
[Nombre del proveedor]

RESPUESTA ANTES DEL
[fecha]

EL CUESTIONARIO, EN CIFRAS

40	9	1	2 semanas
Preguntas	Bloques	Prueba por pregunta	Plazo de respuesta propuesto

00 Datos de la evaluación

Empresa que evalúa [Nombre]. Proveedor [Nombre]. Producto y plan [nombre y plan]. Datos que tratará [contacto, conversaciones, adjuntos, datos de cuenta, otros]. Si pueden llegar datos de salud o financieros [sí / no]. Fecha de envío [fecha]. Respuesta antes del [fecha].

Cada respuesta va con la prueba que se pide en su fila, o con un enlace a ella. Lo que no aplica se marca como «No aplica» con el motivo.

01 Datos y ubicación

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
DAT-1. ¿En qué país se guardan los datos, los adjuntos y las copias?	Un país o región concretos	Contrato y lista de subencargados	
DAT-2. ¿Esa ubicación vale en todos los planes o depende de un complemento?	Plan y coste dichos	Precios u oferta	
DAT-3. ¿Qué categorías de datos trata el servicio?	Lista cerrada	Anexo de tratamiento	
DAT-4. ¿Cómo se separan nuestros datos de los de otros clientes?	Separación descrita	Descripción técnica	
DAT-5. ¿Qué dice el contrato si llegan datos de salud u otras categorías especiales?	Una cláusula concreta	Contrato	

02 Inteligencia artificial

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
IA-1. ¿Dónde corren los modelos de IA y de qué proveedor son?	Región y proveedor nombrados	Lista de subencargados	
IA-2. ¿Entrenan ustedes o el proveedor del modelo con nuestras conversaciones?	No, o sí y desactivable	Cláusula del contrato	
IA-3. Si hay entrenamiento, ¿viene activado y quién lo desactiva?	Lo desactiva la empresa	Ajuste o cláusula	
IA-4. ¿Cuánto guarda el proveedor del modelo lo que se le envía?	Plazo concreto o nada	Contrato del proveedor	
IA-5. ¿Qué gestiones hace la IA sin una persona? ¿Queda registro?	Lista de acciones, las delicadas con aprobación	Registro en la demo	
IA-6. ¿Puede pasar siempre a una persona las conversaciones con datos sensibles?	Sí, con una regla	Configuración en la demo	

03 Contrato y subencargados

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
CON-1. ¿Firman un contrato de encargo con el contenido del artículo 28 del RGPD?	Sí, antes de empezar	El contrato	
CON-2. ¿Dónde está la lista de subencargados, con finalidad y ubicación?	Pública y fechada	Enlace a la lista	

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
CON-3. ¿Cuántos días antes avisan de un cambio y qué podemos hacer si nos oponemos?	Días concretos y derecho a resolver	Cláusula de subencargados	
CON-4. ¿Sale algún dato del Espacio Económico Europeo? ¿Con qué garantía?	No, o con adecuación o cláusulas tipo	Cláusula de transferencias	
CON-5. ¿Cómo podemos auditarles?	Informes a petición y auditoría con preaviso	Cláusula de auditoría	

04 Accesos y permisos

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
ACC-1. ¿Qué roles hay y qué puede hacer cada uno?	Roles descritos, con mínimo privilegio	Configuración en la demo	
ACC-2. ¿Se puede exigir el doble factor a todo el equipo?	Sí, desde la configuración	Ajuste en la demo	
ACC-3. ¿Hay inicio de sesión único? ¿En qué plan?	Sí o no, con plan	Precios	
ACC-4. ¿Quién del proveedor puede ver nuestros datos? ¿Queda registrado?	Personas concretas, con registro	Política de accesos	
ACC-5. ¿Hay registro de accesos del equipo? ¿Cuánto se guarda?	Sí, con plazo y exportable	Registro en la demo	

05 Cifrado y copias

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
CIF-1. ¿Se cifran los datos en tránsito y en reposo?	TLS 1.2 o superior y cifrado en reposo	Página de seguridad	
CIF-2. ¿Cómo se guardan las contraseñas?	Con un algoritmo de derivación, nunca en claro	Página de seguridad	
CIF-3. ¿Cada cuánto se hacen copias y cuándo se probó restaurarlas?	Frecuencia y fecha de la última prueba	Política de copias	
CIF-4. ¿Dónde están las copias y cuánto se guardan?	Misma región y plazo dicho	Política de copias	

06 Incidentes y brechas

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
INC-1. ¿En cuántas horas avisan de una brecha de datos personales?	Un plazo en horas	Cláusula de brechas	
INC-2. ¿Qué incluye ese aviso?	Naturaleza, afectados, consecuencias y medidas	Cláusula de brechas	
INC-3. ¿Hay contacto de seguridad y vía para avisar de vulnerabilidades?	Un correo publicado	Página de seguridad	
INC-4. ¿Han tenido alguna brecha con datos de clientes en los últimos tres años?	Sí o no, con explicación	Respuesta firmada	

07 Conservación y borrado

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
BOR-1. ¿Podemos fijar cuánto se guardan las conversaciones?	Plazo configurable o borrado a petición	Ajuste en la demo	
BOR-2. ¿Se borran todos los datos de una persona, conversaciones incluidas?	Sí, desde la app o con plazo	Demo y cláusula de derechos	
BOR-3. Al terminar, ¿cuántos días hay para exportar y cuándo se borra todo?	Días concretos, copias incluidas	Cláusula de devolución	
BOR-4. ¿En qué formato se exportan los datos?	Formato abierto y completo	Exportación de prueba	

08 Continuidad

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
CNT-1. ¿Qué disponibilidad se compromete y qué pasa si no se cumple?	Porcentaje mensual y compensación	Acuerdo de nivel de servicio	
CNT-2. ¿Cuánto tardan en responder a una incidencia crítica?	Horas, por escrito	Acuerdo de nivel de servicio	
CNT-3. ¿Cómo se avisa de una caída?	Página de estado o correo	Enlace o ejemplo	
CNT-4. ¿Qué pasa con nuestros datos si el servicio cierra o cambia de dueño?	Devolución y borrado garantizados	Contrato	

09 Certificaciones

Pregunta	Qué respuesta vale	Prueba que se pide	Respuesta
CER-1. ¿Qué certificaciones tienen como empresa?	Nombre, alcance y fecha	Certificado o informe	
CER-2. ¿Cuáles son de su infraestructura y no suyas?	Separadas	Informe del proveedor de nube	
CER-3. ¿Cuándo fue la última prueba de intrusión?	Fecha y resumen	Resumen del informe	

10 Registro y decisión

Un bloque está cerrado cuando todas sus filas tienen respuesta y prueba. Sin prueba, la fila queda pendiente.

Bloque	Estado	Pendiente	Responsable y fecha
1. Datos y ubicación	[Cerrado / Pendiente]		
2. Inteligencia artificial	[Cerrado / Pendiente]		
3. Contrato y subencargados	[Cerrado / Pendiente]		
4. Accesos y permisos	[Cerrado / Pendiente]		
5. Cifrado y copias	[Cerrado / Pendiente]		
6. Incidentes y brechas	[Cerrado / Pendiente]		
7. Conservación y borrado	[Cerrado / Pendiente]		
8. Continuidad	[Cerrado / Pendiente]		
9. Certificaciones	[Cerrado / Pendiente]		