EJEMPLO SINTÉTICO — NO ES LA EVALUACIÓN DE UN CLIENTE

Europe Cyber-Safe

Pasaporte de Despliegue de IA — declaración de autoevaluación

Organización	Agencia Creativa Ejemplo S.L. (15 empleados)	**Referencia**	SAMPLE-0002
Completada el	2026-10-30	**Completada por**	director@example.com
Cuestionario	v1.1-EU-es (EU, es) · `050a3330a65081dc`		

> **Autoevaluación realizada por la organización. Ni Europe Cyber-Safe ni ninguna otra persona han examinado las respuestas. Este informe no constituye asesoramiento jurídico.**

El informe describe la situación únicamente en la fecha en que se completó.

Calificaciones por área

Cada área se califica a partir de las respuestas dadas: rojo si alguna respuesta activa el rojo; si no, ámbar si alguna respuesta es ámbar o está sin responder; en otro caso, verde. No se genera ninguna puntuación global.

Área	Calificación
D1 Inventario de IA	ROJO
D2 Protección de datos	ROJO
D3 Gobernanza y política	ROJO
D4 Supervisión humana	ÁMBAR
D5 Control de proveedores	ÁMBAR
D6 Respuesta a incidentes de IA	ÁMBAR

Acciones

Primero las áreas en rojo y, después, las más rápidas.

#	Área	Acción	Esfuerzo
1	D1	Designe un responsable del inventario y hágalo constar en la política de uso de la IA.	una hora
2	D1	Programe un control trimestral del inventario en la agenda del responsable designado.	una hora
3	D2	Añada a la política de privacidad una sección sobre el uso de la IA que indique los fines y las categorías de proveedores; publíquela e informe al personal.	una hora
4	D2	Difunda la lista de datos prohibidos a todo el personal y colóquela a la vista allí donde se utilizan las herramientas.	una hora

EJEMPLO SINTÉTICO — NO ES LA EVALUACIÓN DE UN CLIENTE

5	D2	Registre, a partir de la documentación del proveedor, la ubicación de los datos y el mecanismo de transferencia de cada herramienta; cuando los datos salgan del EEE, confirme el mecanismo (una decisión de adecuación, o cláusulas contractuales tipo de la UE con una evaluación de la transferencia).	una hora
6	D2	Para cada herramienta, localice el control de supresión o el compromiso contractual de supresión; retire las herramientas que no ofrezcan ninguno de los dos cuando haya datos personales en juego.	una hora
7	D3	Designe un responsable de las decisiones sobre IA y anote las tres preguntas que se plantea antes de autorizar una herramienta (qué datos, qué condiciones, quién revisa los resultados).	una hora
8	D1	Complete el inventario de IA con la plantilla; pregunte a cada responsable de equipo qué herramientas utilizan él y su equipo, incluidas las extensiones del navegador y las aplicaciones del móvil.	un día
9	D1	Deje de introducir ya datos personales en herramientas con condiciones para consumidores o desconocidas. Traslade ese uso a un plan empresarial con contrato de encargo del tratamiento, o suprima ese uso.	un día
10	D1	Compruebe la configuración de IA de cada producto importante (transcripción de reuniones, resúmenes, autocompletado) y añádala al inventario; decida cuáles desactivar.	un día
11	D2	Aplique la plantilla de análisis previo de EIPD a cada herramienta que trate datos personales; realice una EIPD completa cuando el análisis así lo indique.	un día
12	D3	Adopte la plantilla de política de uso de la IA (dos páginas), haga que la firme el propietario de la empresa, difúndala a todo el personal y registre quién la ha leído.	un día
13	D3	Organice una sesión de sensibilización sobre IA de una hora para todo el personal (presentación modelo) y conserve la lista de asistencia.	un día
14	D3	Examine los cinco contratos de clientes más importantes y las orientaciones sobre IA de su colegio u organización profesional en busca de cláusulas de confidencialidad y de IA; registre el resultado.	un día
15	D4	Informe al personal sobre los modos de fallo de la IA con la nota de una página; incluya un ejemplo real de su propio sector.	una hora
16	D4	Acuerde una convención sencilla (un pie de página, un campo, una carpeta) para marcar los resultados relevantes elaborados con ayuda de la IA.	una hora
17	D5	Consulte la declaración de uso de datos de cada proveedor; active la exclusión o pase a un plan que excluya el entrenamiento; registre el resultado en el inventario.	una hora
18	D5	Recopile la evidencia de la página de seguridad o del centro de confianza (trust centre) de cada proveedor y guárdela junto al inventario.	una hora
19	D5	Designe quién recibe los avisos de los proveedores; redacte una nota de salida de un párrafo para cada herramienta crítica (cómo exportar, cómo dejar de usarla).	una hora

20	D6	Incorpore los incidentes de IA al procedimiento existente de incidentes o de reclamaciones, con tres ejemplos y un contacto designado.	una hora
21	D6	Designe a la persona que decide sobre las brechas y tenga a mano el formulario de notificación de brechas de su autoridad de protección de datos y una plantilla de registro de brechas (el art. 33 del RGPD exige documentar toda brecha).	una hora
22	D6	Active el registro de actividad en las herramientas de plan empresarial; cuando no esté disponible, lleve un registro compartido sencillo para los usos que impliquen datos personales o confidenciales.	una hora
23	D4	Introduzca un paso de revisión a cargo de una persona designada para todos los resultados de IA dirigidos a clientes o que afecten a registros; inclúyalo en el visto bueno habitual.	un día
24	D5	Obtenga las condiciones de plan empresarial o el contrato de encargo del tratamiento de cada proveedor; si no existen, deje de enviar datos personales a ese proveedor.	un día
25	D5	Traslade las herramientas de IA a cuentas gestionadas por la empresa con MFA; añádalas a la lista de comprobación de bajas.	un día
26	D6	Para cada herramienta crítica, pruebe una vez la exportación y anote cómo desactivar el acceso; conserve los registros esenciales fuera de la herramienta.	un día
27	D4	Documente el paso de revisión, la base jurídica y los controles de sesgo realizados; determine si el uso entra en el anexo III del Reglamento de Inteligencia Artificial y planifique las obligaciones de los responsables del despliegue aplicables a partir del 2 de diciembre de 2027.	una semana

Respuestas dadas

D1 Inventario de IA — ROJO

ID	Pregunta	Respuesta	Nivel
D1-1	¿Ha elaborado una lista de todas las herramientas de IA que se utilizan en la empresa, incluidas las cuentas gratuitas que el personal usa en sus propios dispositivos o con sus propias credenciales?	No hay lista	rojo
D1-2	¿Alguna herramienta del inventario recibe datos personales de clientes, pacientes o empleados?	Sí - en al menos una herramienta con condiciones para consumidores, o cuyas condiciones se desconocen	rojo
D1-3	¿Hay una persona designada responsable de mantener actualizado el inventario y de autorizar nuevas herramientas?	No	ámbar
D1-4	¿Se incluyen en el inventario las funciones de IA integradas en productos que ya utiliza (correo electrónico, CRM, contabilidad, navegadores, herramientas de reuniones, teléfonos)?	No estamos seguros	ámbar

D1-5	¿Cuándo se contrastó por última vez el inventario con lo que el personal utiliza realmente?	Nunca, o no hay inventario	rojo

D2 Protección de datos — ROJO

ID	Pregunta	Respuesta	Nivel
D2-1	¿Informa su política de privacidad a clientes y personal de que se utilizan herramientas de IA, con qué fines y con qué proveedores?	No	rojo
D2-2	Para las herramientas que tratan datos personales, ¿ha realizado una evaluación de impacto relativa a la protección de datos (EIPD) o un análisis previo documentado que concluya que no es necesaria?	No	rojo
D2-3	¿Dispone el personal de una lista escrita de lo que nunca debe introducirse en una herramienta de IA (por ejemplo, datos de pacientes, números de tarjeta, identificadores de clientes, contraseñas)?	Se comunicó verbalmente, nada por escrito	ámbar
D2-4	¿Sabe dónde almacena y trata sus datos cada proveedor, y si salen del Espacio Económico Europeo (EEE)?	Para algunas herramientas	ámbar
D2-5	¿Puede suprimir, o hacer que el proveedor suprima, los datos conservados en cada herramienta de IA cuando deje de utilizarla o cuando una persona lo solicite?	No estamos seguros	ámbar

D3 Gobernanza y política — ROJO

ID	Pregunta	Respuesta	Nivel
D3-1	¿Existe una política escrita de uso de la IA que el personal conozca y que indique qué está permitido y qué no?	Redactada pero no difundida	ámbar
D3-2	¿Quién decide si una nueva herramienta o función de IA puede utilizarse con fines empresariales?	La dirección, de manera informal	ámbar
D3-3	¿Enumera la política los usos prohibidos - por ejemplo, tomar decisiones sobre personas sin revisión humana, o generar contenidos presentados como escritos por una persona cuando ello induciría a error?	Sí	verde

D3-4	¿Ha recibido todo el personal que utiliza herramientas de IA, en los últimos 12 meses, una formación de sensibilización sobre los límites a la introducción de datos, los modos de fallo y la política?	Parte del personal	ámbar
D3-5	¿Restringen sus contratos con clientes, sus normas profesionales o su organismo regulador la forma en que puede utilizar la IA con la información de esos clientes, y las está cumpliendo?	Existen restricciones y no estamos seguros de cumplirlas	rojo

D4 Supervisión humana — ÁMBAR

ID	Pregunta	Respuesta	Nivel
D4-1	¿Comprueba una persona competente los resultados de la IA antes de que lleguen a un cliente, a un registro o a una decisión sobre una persona?	Normalmente	ámbar
D4-2	¿Conoce el personal que utiliza herramientas de IA los tipos de errores que cometen estas herramientas - hechos y citas inventados, información desactualizada, errores afirmados con seguridad, sesgos?	Parte del personal	ámbar
D4-3	¿Puede saber a posteriori qué documentos, correos electrónicos o registros se elaboraron con ayuda de la IA?	A veces	ámbar
D4-4	¿Responde una persona designada de una decisión asistida por IA exactamente igual que de una decisión humana?	Sí	verde
D4-5	¿Utiliza la IA para la selección de personal, la concesión de crédito, la fijación de precios, la determinación de la elegibilidad, la evaluación del desempeño u otras decisiones sobre personas?	Sí, con una revisión humana efectiva y una base documentada	ámbar

D5 Control de proveedores — ÁMBAR

ID	Pregunta	Respuesta	Nivel
D5-1	Para cada proveedor de IA que trata sus datos, ¿dispone de un contrato o unas condiciones que incluyan un contrato de encargo del tratamiento (art. 28 RGPD)?	Para algunos	ámbar

D5-2	¿Sabe si cada proveedor utiliza los datos que usted introduce para entrenar o mejorar sus modelos, y ha ejercido la exclusión cuando es posible?	Se desconoce	ámbar
D5-3	¿Ha visto alguna evidencia de seguridad independiente de cada proveedor (por ejemplo, certificación ISO/IEC 27001, informe SOC 2, un esquema nacional de referencia, resumen de una prueba de penetración)?	No	ámbar
D5-4	¿Se controla el acceso a cada herramienta de IA con cuentas empresariales, autenticación multifactor y retirada del acceso cuando una persona deja la empresa?	En parte	ámbar
D5-5	Si un proveedor cambiara sus condiciones, sufriera una brecha de seguridad o cerrara, ¿se enteraría, y tiene forma de dejar de utilizarlo rápidamente?	No	ámbar

D6 Respuesta a incidentes de IA — ÁMBAR

ID	Pregunta	Respuesta	Nivel
D6-1	¿Sabe el personal qué se considera un incidente de IA (por ejemplo, datos personales pegados en una herramienta, un resultado perjudicial o erróneo sobre el que se ha actuado, un aviso de brecha de un proveedor) y cómo comunicarlo?	De manera informal	ámbar
D6-2	¿Podría cumplir el plazo de notificación de 72 horas del RGPD ante su autoridad de protección de datos si se expusieran datos personales a través de una herramienta de IA?	No estamos seguros	ámbar
D6-3	¿Ha sufrido un incidente de IA, o ha realizado un ejercicio de simulación sobre uno, en los últimos 12 meses?	Sí	verde
D6-4	¿Conserva suficientes registros (quién usó qué herramienta, cuándo y para qué) para investigar después un incidente de IA?	En parte	ámbar
D6-5	¿Podría dejar de utilizar una herramienta de IA concreta en un día laborable si se viera comprometida, sin perder registros esenciales de la empresa?	En parte	ámbar

Referencias citadas

- Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689), art. 26 (obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo) y anexo III; para los usos del anexo III se aplican a partir del 2 dic. 2027 en

virtud del Reglamento (UE) 2026/1744
- Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689), art. 4 (alfabetización en materia de IA), aplicable desde el 2 feb. 2025 y modificado por el Reglamento (UE) 2026/1744: los proveedores y los responsables del despliegue deben adoptar medidas para favorecer la alfabetización en materia de IA de su personal y de otras personas que utilicen sistemas de IA en su nombre
- Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689), art. 50 (transparencia: informar a las personas de que interactúan con un sistema de IA; revelar los contenidos generados o manipulados por IA), aplicable desde el 2 ago. 2026
- ISO/IEC 27001:2022; esquemas nacionales de referencia (por ejemplo, Esquema Nacional de Seguridad (ENS) / guías de INCIBE, BSI IT-Grundschutz, CyberFundamentals); autenticación multifactor y controles de altas y bajas
- Comisión Europea, Alfabetización en materia de IA - Preguntas y respuestas (2025)
- Dictamen 28/2024 del CEPD sobre determinados aspectos de protección de datos relacionados con el tratamiento de datos personales en el contexto de los modelos de IA (dic. 2024); orientaciones sobre IA de su autoridad nacional de protección de datos (por ejemplo, la Agencia Española de Protección de Datos (AEPD) u otra autoridad nacional)
- Legislación laboral nacional y normas sobre los comités de empresa en materia de vigilancia y de IA en la selección y la gestión de personal; Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689), anexo III, punto 4 (los usos en el ámbito del empleo son de alto riesgo)
- ENISA, Multilayer Framework for Good Cybersecurity Practices for AI (2023); NCSC/CISA y agencias asociadas, Guidelines for secure AI system development (nov. 2023)
- Directivas de la UE sobre igualdad de trato (2000/43/CE, 2000/78/CE, 2006/54/CE) y legislación nacional contra la discriminación (discriminación directa e indirecta)
- RGPD, art. 22 (decisiones individuales automatizadas); directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles (WP251 rev.01)
- RGPD, arts. 33-34 (notificación a la autoridad de control en un plazo de 72 horas cuando exista un riesgo para las personas; registro de toda brecha); Directrices 9/2022 del CEPD sobre la notificación de violaciones de la seguridad de los datos personales
- RGPD, art. 35 (evaluación de impacto relativa a la protección de datos); directrices sobre la EIPD del Grupo de Trabajo del Artículo 29 (WP248 rev.01, respaldadas por el CEPD); lista de su autoridad nacional de tratamientos que requieren una EIPD
- RGPD, capítulo V (arts. 44-49): decisiones de adecuación; cláusulas contractuales tipo (Decisión 2021/914 de la Comisión); Recomendaciones 01/2020 del CEPD sobre medidas complementarias
- Reglamento General de Protección de Datos (RGPD), arts. 12-14 (información que debe facilitarse a los interesados)
- Orientaciones de ENISA sobre gestión de incidentes; orientaciones de notificación de su CSIRT nacional; notificación conforme al art. 23 de NIS2 (para las entidades incluidas en su ámbito)
- ISO/IEC 42001:2023, sistemas de gestión de la inteligencia artificial (funciones, evaluación de impacto, ciclo de vida, proveedores)
- ISO/IEC 27001:2022, anexo A 8.15 (registro) y 8.16 (actividades de seguimiento)
- NIST AI Risk Management Framework 1.0 (Govern, Map, Measure, Manage) y su perfil de IA generativa (NIST AI 600-1)
- OWASP Top 10 for LLM Applications 2025 (inyección de prompts, divulgación de información sensible, cadena de suministro)
- Orientaciones de ENISA sobre la seguridad de la cadena de suministro de las TIC; Directiva NIS2, art. 21(2)(d), seguridad de la cadena de suministro (para las entidades incluidas en su ámbito)

Las referencias son fuentes públicas que se indican por comodidad; consulte la versión vigente antes de basarse en ellas. Esta declaración no constituye asesoramiento jurídico ni tiene valor de certificación.