

LISTA DE CONTROL

Seguridad de los usos de la IA

Controles que deben realizarse antes y durante el uso de herramientas de IA generativa

La presente lista ordena los controles de seguridad propios de las herramientas de IA generativa: cuentas, datos, documentos tratados, extensiones, acciones automatizadas e incidentes. Complementa la política de seguridad de la organización sin sustituirla.

1. Cuentas y accesos

- ☐ Inventariar las cuentas que dan acceso a herramientas de IA, incluidas las cuentas personales utilizadas para el trabajo.
- ☐ Activar la autenticación de dos factores en cada cuenta.
- ☐ Vincular las cuentas profesionales a la organización y no a direcciones personales.
- ☐ Retirar los accesos cuando un colaborador deje la organización.

2. Datos

- ☐ Definir los datos cuya introducción está prohibida en una herramienta de gran público y difundirlos entre los usuarios.
- ☐ Verificar, para cada herramienta, el uso de los intercambios para el entrenamiento, la revisión humana y el plazo de conservación.
- ☐ Desactivar el uso de los intercambios para la mejora de los modelos cuando la herramienta lo permita.
- ☐ Reservar los datos personales y confidenciales a las ofertas regidas por un contrato de tratamiento.

3. Documentos e instrucciones ocultas

- ☐ Tratar los documentos, páginas web y correos electrónicos sometidos a una herramienta como material que debe analizarse, no como instrucciones.
- ☐ No someter documentos de origen desconocido a una herramienta que disponga de permisos de acción.
- ☐ Controlar los enlaces y archivos adjuntos producidos por una herramienta antes de abrirlos o transmitirlos.

4. Extensiones, conectores y acciones automatizadas

- ☐ Someter a autorización la instalación de extensiones de navegador y de aplicaciones de IA.
- ☐ Limitar los conectores (correo electrónico, almacenamiento, agenda) a los accesos estrictamente necesarios.
- ☐ Exigir una validación humana antes de cualquier acción con efecto externo: envío, publicación, pago, supresión.
- ☐ Conservar un registro de las acciones ejecutadas por una herramienta automatizada.

Documento de información general; no constituye ni asesoramiento jurídico ni un dictamen sobre una situación particular. Las referencias a los textos deben comprobarse en su redacción vigente en la fecha de utilización.

Firma de consultoría no inscrita en el Colegio de Abogados; ninguna representación ante los tribunales ni acto reservado a las profesiones jurídicas reguladas.

5. Incidentes

- ☐ Designar a la persona a la que debe notificarse una introducción accidental de datos, una fuga o un contenido erróneo difundido.
- ☐ Consignar cada incidente: fecha, herramienta, datos afectados, medidas adoptadas.
- ☐ Examinar, cuando haya datos personales afectados, las obligaciones derivadas de la Ley n.º 09-08.
- ☐ Examinar, para las entidades sujetas a ella, las obligaciones de declaración previstas por la Ley n.º 05-20.

Referencias

- Ley n.º 09-08 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, promulgada por el dahir n.º 1-09-15 de 22 de safar de 1430 (18 de febrero de 2009), Boletín Oficial n.º 5711 de 23 de febrero de 2009 (edición general) y n.º 5714 de 5 de marzo de 2009 (edición de traducción oficial), artículo 23.
- Ley n.º 05-20 relativa a la ciberseguridad, promulgada por el dahir n.º 1-20-69 de 4 de hiya de 1441 (25 de julio de 2020), Boletín Oficial n.º 6904 de 30 de julio de 2020 (edición general), p. 4160, y n.º 6906 de 6 de agosto de 2020 (edición de traducción oficial), artículos 8, 14, 30 y 33.
- OWASP, «LLM01:2025 Prompt Injection», OWASP Top 10 for LLM Applications 2025, <https://genai.owasp.org/llmrisk/llm01-prompt-injection/> (página consultada el 21 de octubre de 2026).
- OWASP, «LLM06:2025 Excessive Agency», OWASP Top 10 for LLM Applications 2025, <https://genai.owasp.org/llmrisk/llm062025-excessive-agency/> (página consultada el 21 de octubre de 2026).