

INTELIGENCIA ARTIFICIAL DESDE CERO

Lección 3. Seguridad, privacidad y uso responsable

Duración sugerida	1 hora y 30 minutos a 2 horas.
Modalidad	Presencial, virtual o semipresencial.
Dirigido a	Personas bachilleres y público general que inician su formación en inteligencia artificial.
Tema central	Cómo proteger datos, cuidar la privacidad y usar la IA con criterio y responsabilidad.
Producto esperado	Reconocer riesgos básicos y aplicar buenas prácticas en situaciones cotidianas.

Presentación. La seguridad y la privacidad no son temas lejanos: aparecen cada vez que usamos el celular, compartimos información, aceptamos permisos o consultamos una herramienta de IA. En esta lección se busca que el participante aprenda a identificar riesgos sencillos y a usar la inteligencia artificial de manera responsable, sin miedo, pero con criterio.

1. Propósitos de aprendizaje

1	Identificar riesgos básicos de seguridad y privacidad al usar internet y herramientas de IA.
2	Reconocer buenas prácticas para proteger datos personales, contraseñas y documentos.
3	Comprender que el uso responsable de la IA exige revisar, verificar y pensar antes de compartir o decidir.

2. Punto de partida

Cuando una persona envía una foto, comparte un documento, acepta condiciones sin leer o escribe datos sensibles en una herramienta digital, deja una huella. Con la inteligencia artificial esto exige todavía más cuidado, porque muchas plataformas procesan grandes cantidades de información. Usar IA no solo es pedir respuestas; también implica saber qué compartir, qué verificar y qué proteger.

3. Riesgos frecuentes

Entre los riesgos más comunes están compartir datos personales sin necesidad, usar contraseñas débiles, confiar en enlaces o mensajes falsos, copiar información privada en asistentes de IA y publicar contenido sin verificar. También existe el riesgo de creer que toda respuesta automática es correcta. La IA puede ayudar mucho, pero no garantiza verdad absoluta ni reemplaza la responsabilidad humana.

Situación	Riesgo principal	Buena práctica
Enviar la cédula o datos bancarios por un chat cualquiera.	Exponer información sensible.	Compartir solo por canales seguros y cuando sea realmente necesario.
Usar la misma contraseña en todo.	Facilitar accesos no autorizados.	Crear contraseñas distintas y más fuertes.
Pegar un contrato o historia clínica en una IA pública.	Perder control sobre información privada.	Evitar subir datos confidenciales o anonimizarlos.
Reenviar noticias o imágenes sin revisar.	Difundir información falsa o dañina.	Verificar fuente, fecha y contexto antes de compartir.

4. Uso responsable de la IA

Usar la IA responsablemente significa pensar antes de escribir, revisar antes de creer y decidir antes de publicar. Conviene hacer preguntas claras, no compartir datos privados, contrastar respuestas con otras fuentes y recordar que la decisión final debe seguir siendo humana. La IA puede ahorrar tiempo y apoyar el trabajo, pero siempre necesita supervisión, especialmente cuando se trata de salud, dinero, estudio o documentos importantes.

5. Actividad breve de aplicación

Lea cada caso y escriba qué haría para actuar con seguridad y responsabilidad.

Caso	¿Qué haría?
Una aplicación le pide acceso a contactos, cámara, ubicación y micrófono para una función sencilla.	_____
Un compañero le envía un enlace sospechoso diciéndole que es urgente abrirlo.	_____
Una herramienta de IA le da una respuesta muy segura sobre un tema importante, pero usted no conoce la fuente.	_____

6. Evaluación breve

1	¿Por qué seguridad y privacidad no significan exactamente lo mismo?
2	Mencione dos datos que no conviene compartir en una herramienta pública de IA.
3	Explique una buena práctica para manejar contraseñas.
4	¿Por qué no se debe copiar y pegar cualquier respuesta de IA sin revisar?

7. Síntesis final

La seguridad, la privacidad y el uso responsable forman parte del aprendizaje básico sobre inteligencia artificial. Una persona que usa IA con criterio no solo busca respuestas rápidas: también protege sus datos, revisa la información y piensa en las consecuencias de lo que comparte. La mejor relación con la tecnología combina utilidad con prudencia.

Orientación para el facilitador. Trabaje con ejemplos cotidianos: contraseñas, permisos del celular, cadenas falsas, fotografías y uso de asistentes de IA. Promueva una actitud equilibrada: aprovechar la tecnología sin entregar información ni confianza de manera automática.