



EDUCACIÓN

Comisión de la RED NACIONAL CPC

PRIVACIDAD Y BUENAS PRÁCTICAS



RED NACIONAL
DE COMITÉS DE PARTICIPACION
CIUDADANA



Comité de
Participación Social
JALISCO



INKLUDERING

ANTES DE PEGAR, PENSEMOS

¿Pegarías un expediente ciudadano en una aplicación que no conoces?

Usar IA puede ahorrar tiempo. También puede exponer a una persona en segundos.



EMPECEMOS

En la era actual de la transformación digital, los datos tienen tanto valor como el petróleo, garantizar la privacidad e implementar una gobernanza de datos sólida son fundamentales para establecer una IA confiable.

Se recopila y utiliza información confidencial para crear y ajustar (fine-tune) sistemas de IA y aprendizaje automático.



PRIVACIDAD

La privacidad en la IA es la práctica de proteger la información personal o sensible que los sistemas de IA recopilan, utilizan, comparten o almacenan.

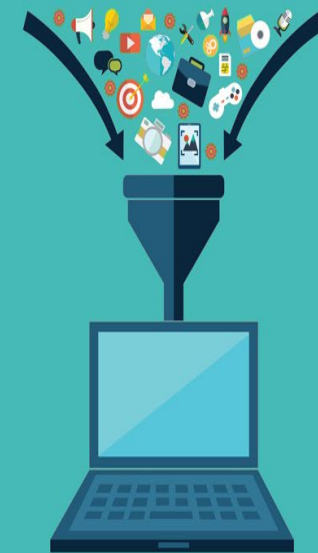
Es el principio de que una persona debe tener control sobre sus datos personales.



RECOLECCIÓN DE DATOS

El concepto de privacidad de los datos es anterior a la IA, y la forma en que las personas conciben la privacidad de los datos ha evolucionado con el advenimiento de la inteligencia artificial.

Está relacionado con capacidad de decidir cómo las organizaciones recopilan, almacenan y utilizan sus datos.



LEVANTA LA MANO

¿Has usado IA para redactar un oficio?

¿Para resumir un documento?

¿Has subido una foto, PDF o Excel?

¿Sabes si esa herramienta está autorizada?



[Esta foto](#) de Autor desconocido está bajo licencia [CC BY-ND](#)

RIESGOS A LA PRIVACIDAD EN LA ERA DE LA IA

Recopilación de datos confidenciales.

Recopilación de datos sin consentimiento.

Uso de datos sin permiso.

Vigilancia y sesgo sin control.

Exfiltración de datos (transferencia deliberada de datos hacia el exterior, es decir un ataque).

Filtración de datos.



VOLUMEN DE DATOS

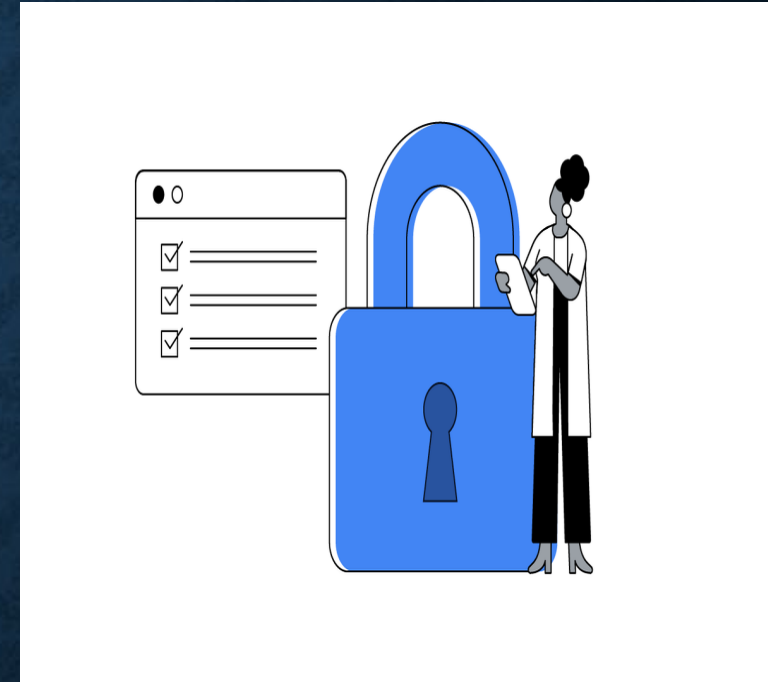
Se incluyen terabytes o petabytes de texto, imágenes o video como datos de entrenamiento, e inevitablemente parte de esos datos son datos sensibles: salud, orientación sexual, origen étnico entre otros.

Mayor probabilidad de que queden expuestos.



ENFOQUES DE PRIVACIDAD

- Evaluar los riesgos durante todo el ciclo de vida de la IA.
- Recopilar únicamente los datos necesarios y permitidos legalmente.
- Solicitar consentimiento y permitir el acceso y control de los datos.
- Aplicar medidas de seguridad: cifrado, anonimización y control de acceso.
- Proteger especialmente los datos sensibles y limitar estrictamente su uso.



CADA DATO REPRESENTA A UNA PERSONA

- Una queja tiene una persona detrás.
- Una nómina afecta el patrimonio de alguien.
- Un expediente de salud revela intimidad.
- Un dato de una víctima puede ponerla en riesgo.
- Una filtración también rompe la confianza pública.



GOBERNANZA DE DATOS

La gobernanza de datos establece reglas, responsables y controles sobre cómo se recopilan, utilizan, protegen, comparten y eliminan los datos.

En los sistemas de IA también busca:

- Garantizar datos precisos, íntegros y confiables.
- Controlar quién puede acceder a ellos.
- Proteger los datos utilizados para entrenar, dar contexto y operar la IA.
- Convertir la privacidad en una obligación clara y exigible.



ARTÍCULO 16



El artículo 16 constitucional reconoce el derecho a la protección de datos personales.

“Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”.

Usar IA no elimina ninguna de estas obligaciones.



ARTÍCULO 66

El artículo 66 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados permite adoptar esquemas de mejores prácticas para:

Elevar la protección de los datos personales.

Armonizar su tratamiento dentro de cada sector.

Facilitar el ejercicio de los derechos ARCO.

Facilitar las transferencias de datos.

Complementar la normativa y demostrar su cumplimiento.

DERECHOS ARCO

Facultad que otorga la Ley para que el titular de los datos personales, pueda decidir a quién proporciona su información, cómo y para qué.

- Acceso: Derecho de acceder a información personal en posesión de terceros.
- Rectificación: Rectifica tu información en caso de estar incompleta o inexacta.
- Cancelación: Solicita que eliminen tus datos cuando lo desees.
- Oposición: Derecho a oponerte al uso de tu información personal.



PEGAR O SUBIR ES COMPARTIR

Un prompt, una foto, un audio, un PDF o un Excel pueden salir del control institucional.

No significa que todo se vuelva público automáticamente. Significa que ya depende de otra herramienta, sus permisos, su configuración y sus reglas.

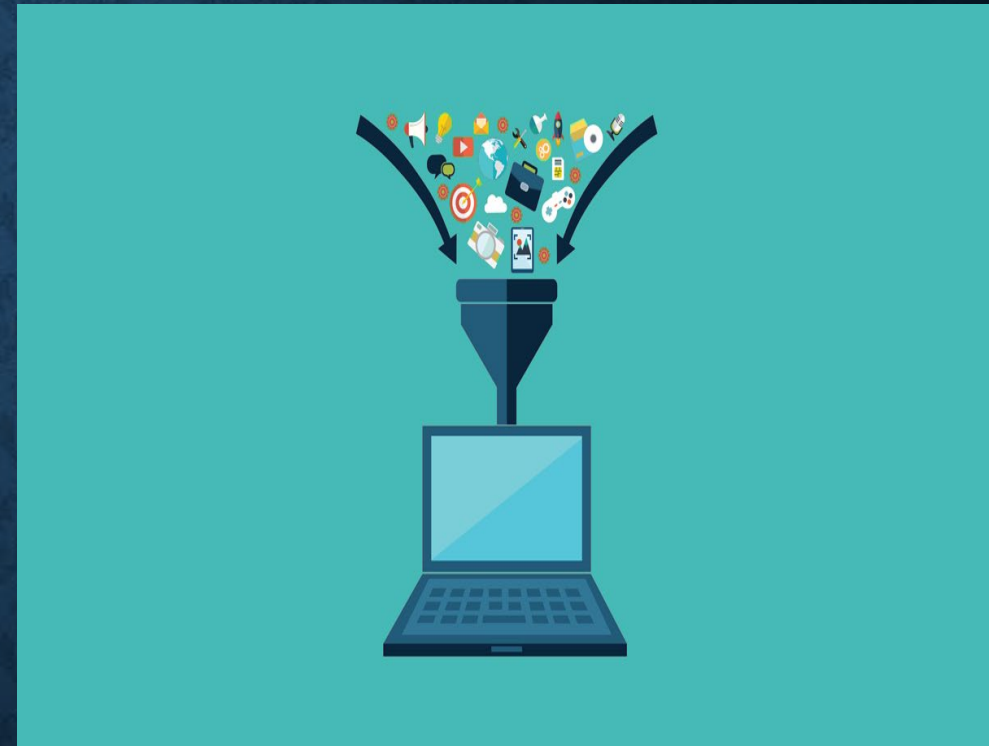
Si no conoces esas condiciones, no compartas información real.



OBJETIVO USAR IA SIN EXPONER DATOS

Al terminar podrás:

- Reconocer información delicada.
- Decidir qué no compartir.
- Transformar una tarea en un prompt seguro.
- Actuar si ocurre un error.



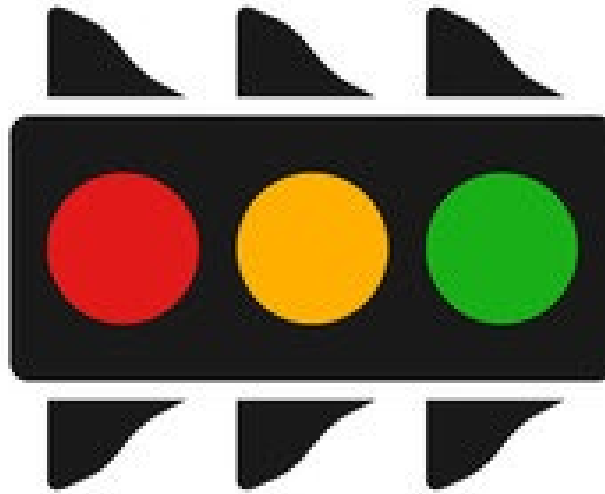
PRINCIPIOS DE LA GOBERNANZA DE DATOS

- Calidad e integridad: utilizar datos correctos, completos y actualizados.
- Acceso, privacidad y seguridad: definir quién puede acceder a los datos y bajo qué condiciones.
- Linaje y trazabilidad: conocer el origen y las transformaciones de los datos.
- Responsabilidad: establecer quién responde por los datos, las políticas y sus resultados.



EL SEMÁFORO ANTES DE USAR IA

ROJO: no
compartir.



VERDE: usar solo
información pública,
genérica o inventada,
y revisar el resultado.



AMARILLO:
detenerse, anonimizar
y consultar.



ROJO: NUNCA LO PEGUES NI LO SUBAS

- Contraseñas, accesos, tokens o llaves.
- CURP, RFC, INE, domicilio o teléfono.
- Datos de salud, biométricos, bancarios o de nómina.
- Expedientes de víctimas, menores o beneficiarios.
- Información confidencial, reservada o de seguridad.



AMARILLO: DETENTE Y CONSULTA

- Borradores internos.
- Informes todavía no publicados.
- Fragmentos anonimizados.
- Datos agregados de trabajo.

Úsalos solo si existe autorización, son necesarios y ya eliminaste identificadores.



VERDE: PÚBLICO O INVENTADO

- Leyes y reglas ya publicadas.
- Formatos genéricos sin datos reales.
- Ejemplos ficticios.
- Estadísticas públicas y agregadas.

Aun en verde: revisa exactitud, fuentes y tono antes de usar el resultado.



ACTIVIDAD 1: LA QUEJA CIUDADANA

Quieres usar IA para contestar una queja.
El expediente incluye:

Nombre, domicilio, teléfono, folio y
detalles de salud.

¿Rojo, amarillo o verde?

¿Qué información necesita realmente la IA
para ayudarte?



LA TAREA SÍ; LOS DATOS NO

NO: “Resume esta queja” + expediente completo.

SÍ: “Redacta una respuesta institucional sobre un retraso. Usa [NOMBRE] y [FOLIO]. No inventes hechos.”

Después completa los campos dentro del sistema institucional y revisa el texto.



ANONIMIZAR NO ES PONER INICIALES

Eliminemos también:

- Folios, teléfonos, correos y domicilios.
- Fechas y combinaciones que identifican.
- Fotos, firmas, placas, QR y códigos de barras.
- Comentarios, propiedades y metadatos del archivo.

Si todavía puedes reconocer a la persona, no está anonimizado.



ACTIVIDAD 2: EL EXCEL DE NÓMINA

Necesitas detectar duplicados. El archivo contiene nombres, RFC, cuentas bancarias y salarios.

- A) Subir todo a una IA.
- B) Quitar solo los nombres.
- C) Usar un método interno autorizado o consultar a TI y protección de datos.



LA HERRAMIENTA TAMBIÉN IMPORTA

Antes de usarla, confirma:

- ¿Está autorizada por la institución?
- ¿Uso la cuenta correcta?
- ¿Está permitida para esta tarea y estos datos?
- ¿Sé a quién consultar?

“Temporal”, “privado” o “incógnito” no sustituyen la autorización.



MENOS DATOS = MENOS RIESGO

- Usa un fragmento, no el expediente completo.
- Prefiere cantidades agregadas.
- Sustituye casos reales por ejemplos inventados.
- No adjuntes un archivo si una instrucción genérica basta.

Comparte únicamente lo necesario para la tarea autorizada.



UNA FOTO TAMBIÉN CONTIENE DATOS

Una captura puede mostrar nombres, notificaciones o pestañas.

Una foto puede revelar rostros, gafetes, placas, documentos o códigos QR.

Un Word, Excel o PDF puede contener comentarios, hojas ocultas, autor y metadatos.

Revisa el archivo completo, no solo lo que ves en pantalla.



LA IA TAMBIÉN PUEDE INVENTAR

Antes de firmar, enviar o publicar:

- Confirma nombres, fechas y cantidades.
- Abre las fuentes originales.
- Verifica leyes, artículos y procedimientos vigentes.
- Corrige tono, contexto y posibles sesgos.

La responsabilidad no se transfiere a la herramienta.



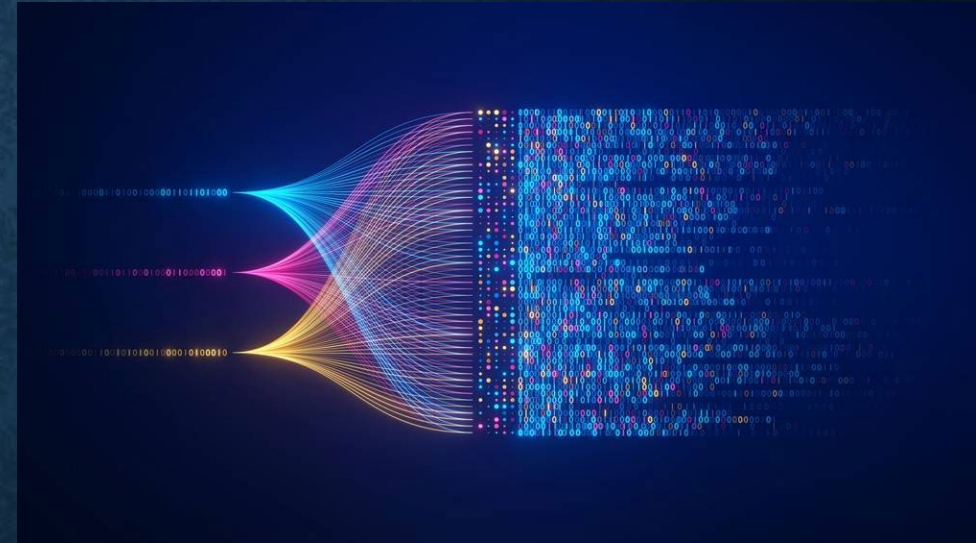
LA DECISIÓN FINAL ES HUMANA

La IA puede apoyar la redacción, organización o búsqueda.

No debe decidir por sí sola sobre:

- Beneficios o apoyos.
- Sanciones.
- Contratación.
- Salud, seguridad o atención a víctimas.

Una persona responsable debe revisar contexto, evidencia y reglas.



MITO O REALIDAD

1. "Si borro el chat, desaparece el riesgo."
2. "Si está en internet, puedo pegarlo."
3. "Una cuenta institucional permite subir cualquier archivo."
4. "Quitar el nombre siempre anonimiza."

¿Verdadero o falso?



SI YA COMPARTISTE INFORMACIÓN...

1. Detén el envío o uso.
2. Anota qué compartiste, dónde y cuándo.
3. Reporta de inmediato por el canal institucional.
4. Sigue las instrucciones para contener, eliminar o preservar evidencia.
5. No ocultes el incidente ni sigas “probando”.

Reportar temprano ayuda a reducir el daño.



ANTES DE PEGAR, HAZ ALTO

A - Antes de pegar, detente.

L - Limita: usa solo lo necesario.

T - Tapa datos, metadatos y pistas.

O - Ocupa solo herramientas autorizadas y revisa el resultado.

Si hay duda, no lo compartas: consulta.



PARA TOMAR EN CUENTA



POSIBLE ATAQUE CON IA



En 2026 se reportó que un atacante habría utilizado Claude y GPT para explotar vulnerabilidades en sistemas del SAT, el INE y otras instituciones.

Aunque las dependencias negaron que existiera una filtración confirmada, el caso deja una advertencia: la IA no crea las vulnerabilidades, pero permite explotarlas con mayor rapidez y escala.

Por eso necesitamos controles de acceso, monitoreo y responsabilidades claras.

PEGASUS

Pegasus demuestra hasta dónde puede llegar el uso indebido de la tecnología. Una vez comprometido el teléfono, puede acceder a mensajes, ubicación, cámara y micrófono, incluso mediante ataques que no requieren que la persona haga clic.

En México se confirmaron infecciones de periodistas y defensores de derechos humanos. El problema no es solamente la falta de consentimiento, sino la ausencia de legalidad, supervisión y rendición de cuentas.





EDUCACIÓN

Comisión de la RED NACIONAL CPC

¡MUCHAS GRACIAS!



RED NACIONAL
DE COMITÉS DE PARTICIPACIÓN
CIUDADANA



Comité de
Participación Social
JALISCO



INKLUDERING