DIPLOMADO EN EL NUEVO SISTEMA DE JUSTICIA CIVIL Y FAMILIAR.
JUICIOS DIGITALES

José Pablo Vidal Araya
Socio
Fortis Consultoría
México, Junio 2025

OBJETIVOS DEL CURSO

- Comprender los conceptos generales sobre expediente electrónico y juicios digitales.
- Entender las aplicaciones, limitantes y alcances del uso de las tecnologías en la labor jurisdiccional.
- Conocer de los beneficios y riesgos del uso de la tecnología en los juicios digitales.

AGENDA DEL TRABAJO DEL PRIMER DÍA

Primer bloque

- Evolución del expediente electrónico

Segundo bloque

- Expediente digital

AGENDA DEL TRABAJO DEL SEGUNDO DÍA

Tercer bloque

- Expediente digital
- Firma electrónica
- Audiencias a distancia

Cuarto bloque

- Seguridad digital
- Inteligencia Artificial en justicia

Quinto bloque

- Repaso general de lo visto
- Reflexiones finales

2. EXPEDIENTE DIGITAL

¿QUÉ ES UN EXPEDIENTE DIGITAL?

Conjunto de documentos electrónicos vinculados a un proceso judicial, con validez legal equivalente al papel.

- Documentos electrónicos
- Metadatos obligatorios
- Estructura jerárquica
- Interfaces de acceso

SELLADO DE TIEMPO

Certificación que prueba la existencia e integridad de un documento en un momento exacto.

Definición: base de datos descentralizada que registra transacciones en bloques encadenados y cifrados.

Características:

- Inmutable
- Descentralizado
- Transparente

FIRMA ELECTRÓNICA Y VALIDEZ LEGAL

Regulación:

1. Ley de firma electrónica
2. eIDAS UE
3. LFPDPPP

Tipos de firma electrónica:

1. Simple
2. Avanzada
3. Cualificada

ERRORES QUE SE PUEDEN PRESENTAR EN UN EXPEDIENTE ELECTRÓNICO

- Firma electrónica ausente o inválida
- Documentos alterados
- Formatos no compatibles o corruptos
- Falta de metadatos
- Almacenamiento inadecuado
- Escaneo de baja calidad

ACTIVIDAD GRUPAL: ORGANIZAR EL FLUJO DE UN EXPEDIENTE DIGITAL

T1: El sistema envía notificación electrónica al demandado.

T2: El sistema asigna un número de expediente único y lo registra en la plataforma.

T3: El juez/a dicta sentencia electrónica con firma digital.

T4: El abogado/a firma la demanda con firma electrónica.

T5: Se programa una audiencia por videoconferencia.

T6: La sentencia se imprime y firma en papel.

T7: El abogado/a redacta la demanda en formato digital.

T8: El expediente se archiva en la nube con cifrado.

T9: Se adjuntan pruebas digitales: videos, mails, documentos escaneados.

T10: La plataforma aplica un sello de tiempo para certificar la fecha/hora exacta

T11: El demandado/a acepta/rechaza la demanda digitalmente.

T12: El abogado envía la demanda por WhatsApp al juzgado.

T13: El juzgado verifica que la demanda cumpla con los requisitos legales y la radica.

T14: Las partes en audiencia suben pruebas adicionales a la plataforma.

ACTIVIDAD GRUPAL: ORGANIZAR EL FLUJO DE UN EXPEDIENTE DIGITAL (SOLUCIÓN)

T6

T12

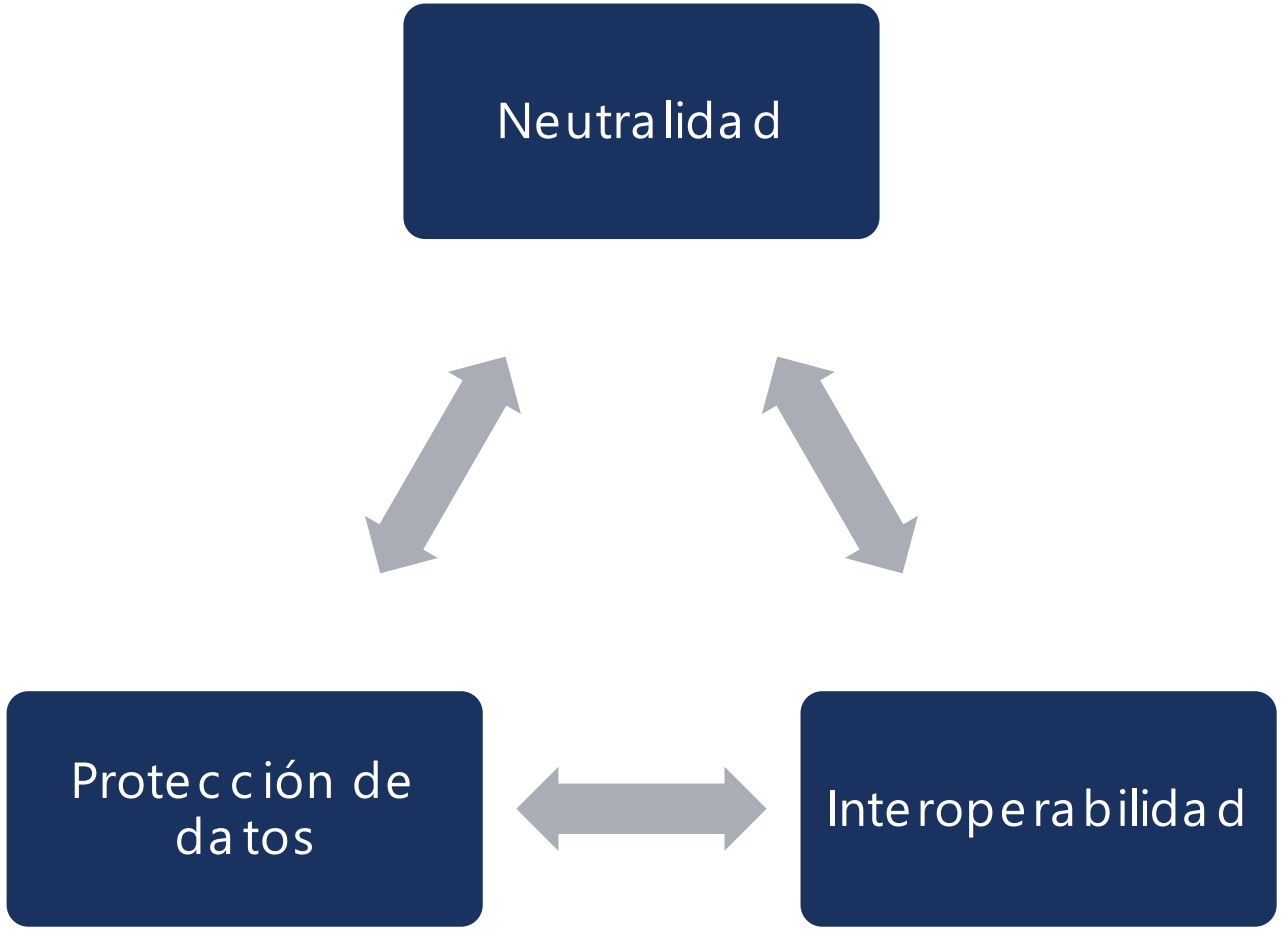
3. PRINCIPIOS TIC EN JUSTICIA

PRINCIPIOS TIC EN JUSTICIA

"El 73% de los tribunales en América Latina aún no cumplen con estándares de interoperabilidad"

Fuente: CEJA – Revistas Judiciales.

PRINCIPIOS TIC EN JUSTICIA

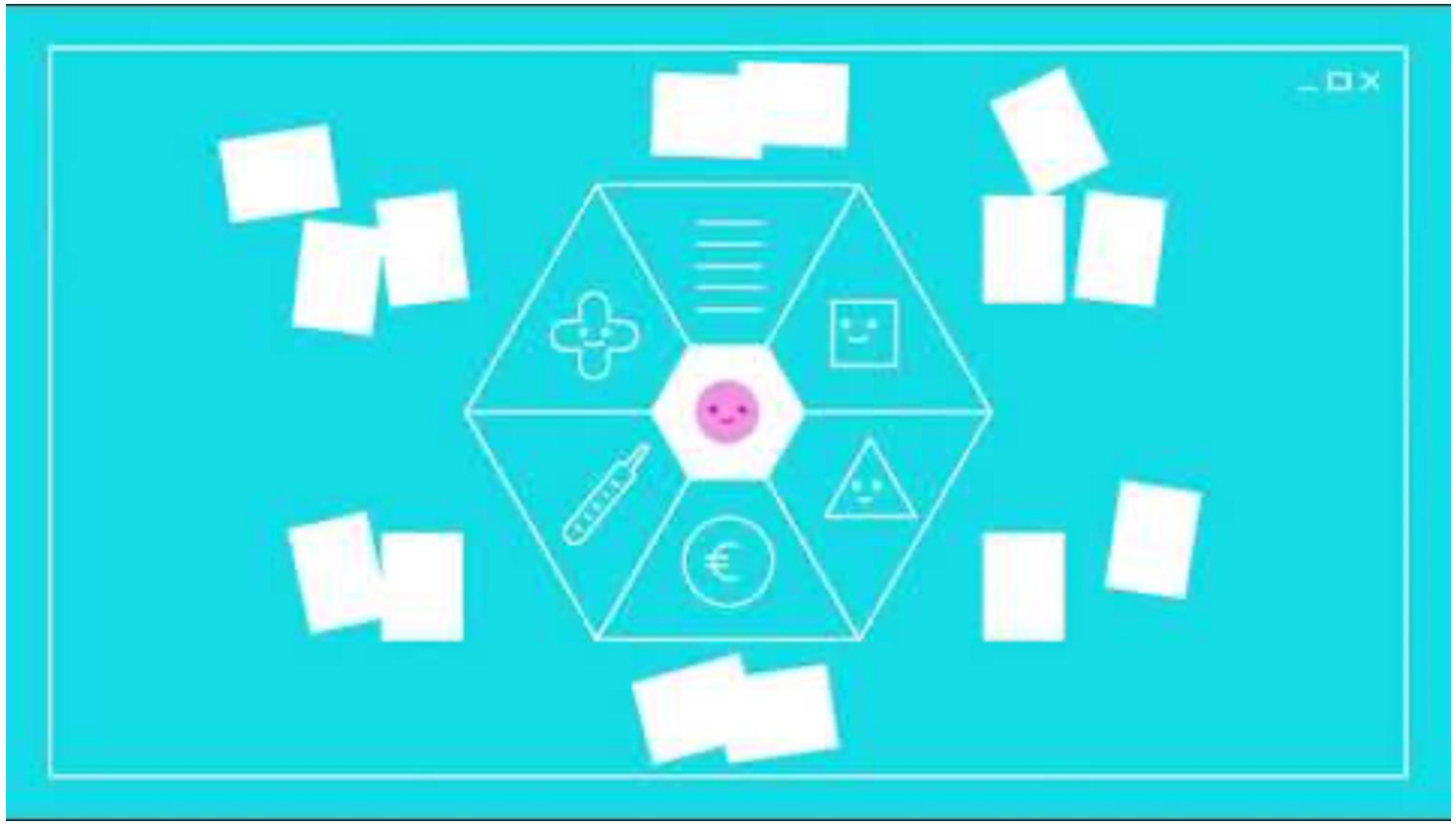


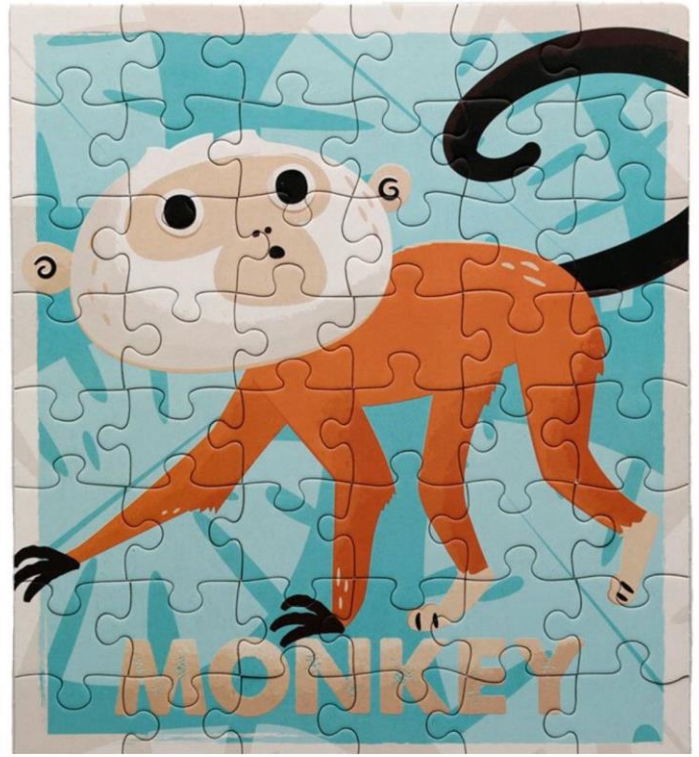
NEUTRALIDAD TECNOLÓGICA

Principio que garantiza que ninguna tecnología, marca o software específico sea obligatorio para acceder a servicios o derechos, asegurando igualdad de condiciones.

1. **Libertad de elección:** los sistemas deben funcionar con cualquier herramienta
2. **Sin monopolios:** evitar que un proveedor controle procesos críticos.
3. **Accesibilidad:** acceso desde cualquier tipo de equipo y sistema operativo.
4. **Riesgos de exclusión social:** no puede ser la única alternativa de uso.
5. **Riesgos de costos:** tener que incurrir en costos de acceso o licencias.

INTEROPERABILIDAD





"Sistemas que hablan entre sí"

¿CUÁLES SON LOS DESAFÍOS DE LA INTEROPERABILIDAD EN MÉXICO/SLP?

Ve a

www.menti.com

Introduce el código

8140 8541

O usa el código QR

PROTECCIÓN DE DATOS: ESTÁNDAR GLOBAL EN PROTECCIÓN DE DATOS PERSONALES (GDPR)

Principios Clave

- Licitud, transparencia y minimización: Solo recoger datos necesarios.
- Limitación de plazo: Conservar datos solo el tiempo estrictamente necesario.
- Seguridad: Cifrado y medidas técnicas/organizativas.

Derechos de los Ciudadanos

- Acceso, rectificación y portabilidad de sus datos.
- Derecho al olvido: Solicitar eliminación de datos obsoletos.
- Oposición al procesamiento (ej: marketing no deseado).

Objetivo: proteger los datos personales de ciudadanos de la UE, incluso si el tratamiento ocurre fuera de Europa.

Aplicable desde mayo 2018.

PROTECCIÓN DE DATOS EN MÉXICO (LFPDPPP)

Principios Clave

- Consentimiento: Los datos solo pueden tratarse con autorización (tácita o expresa).
- Finalidad: Uso limitado a lo declarado al recabar los da
- Confidencialidad: Obligación de guardar secreto sobre

Derechos ARCO

- Acceso, Rectificación, Cancelación y Oposición (ARC
- Plazo de respuesta: 20 días hábiles para atender solicitu

Sanciones

- Multas hasta ~$3.4 MDP (ajustadas en 2023).
- No requiere notificación inmediata de brechas (solo ante INAI si hay riesgo significativo).

PROTECCIÓN DE DATOS

Aspecto	GDPR (UE)	LFPDPPP (México)
Ámbito territorial	Aplica a todo el mundo si trata datos de ciudadanos UE.	Solo aplica en México.
Consentimiento	Debe ser **explícito e informado**.	Puede ser **tácito** en algunos casos.
Derechos	Acceso, rectificación, portabilidad, olvido.	Solo **ARCO** (sin portabilidad u olvido).
Multas máximas	**4% ingresos globales** o **20M€**.	**~$3.4 MDP** (en UMA).
Notificación de brechas	**72 horas** desde el descubrimiento.	Solo si el INAI lo determina necesario.
Figura clave	**Delegado de Protección de Datos (DPO)** obligatorio en algunos casos.	**No requiere DPO**.

PROTECCIÓN DE DATOS: HERRAMIENTAS Y RECOMENDACIONES

- Clasificación de datos
- Minimización de datos
- Capacitación continua
- Evaluaciones de riesgo
- Proveedores seguros
- Cifrado de datos
- Control de accesos
- Protección de BD

ORGANIZA EN ORDEN DE PRIORIDAD LOS PRINCIPIOS SEGÚN EL NIVEL DE URGENCIA EN SU IMPLEMENTACIÓN

Ve a

www.menti.com

Introduce el código

8140 8541

O usa el código QR

"Sin neutralidad, interoperabilidad y protección de datos, la justicia digital es solo papel electrónico"

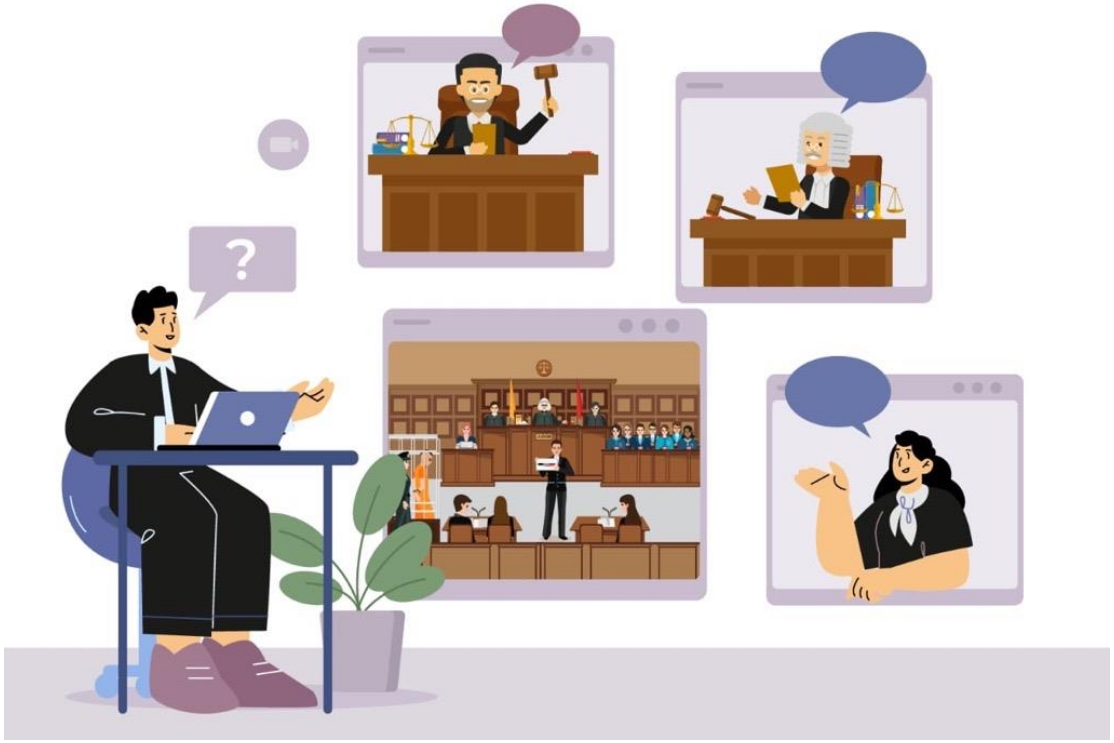
BREAK (20 MIN)

TIMER ONLINE

RELAJEMOS UN POCO LA MAÑANA

4. AUDIENCIAS A DISTANCIA

PANORAMA ACTUAL



"El 85% de los tribunales en América Latina usan audiencias remotas post-pandemia"

Fuente: CEJA, 2023.

PANORAMA ACTUAL: COVID E IMPULSO DIGITAL

América Latina (México, Colombia, Argentina):

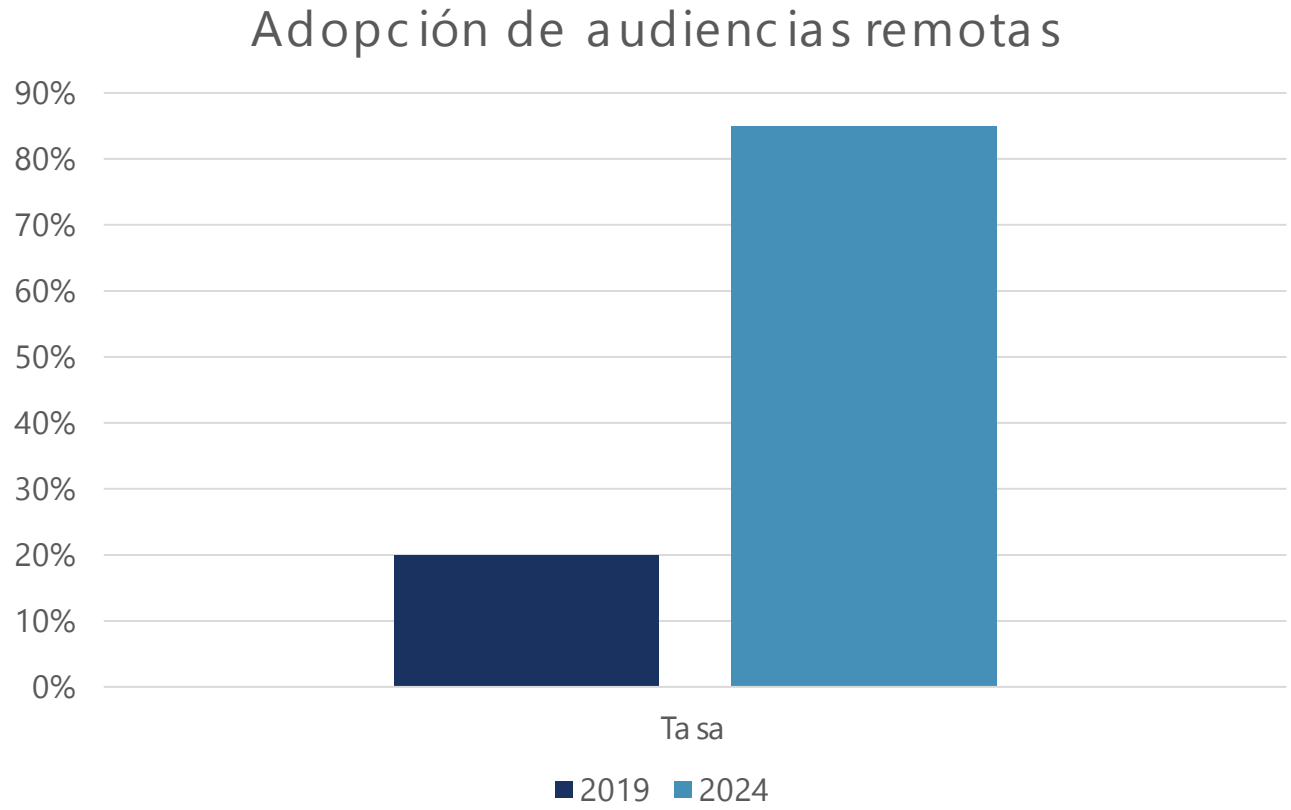
- 2019: 10-15% (solo en grandes ciudades).
- 2024: 70-80% (incluso en zonas rurales).

Europa (UE):

- 2019: 25-30% (países nórdicos líderes).
- 2024: 90-95% (estándar en todos los Estados miembros).

EE.UU./Canadá:

- 2019: 35-40% (cortes federales).
- 2024: 85-90% (adopción en 50 estados).



PLATAFORMAS UTILIZADAS

¿QUÉ TANTO DOMINO ESTAS PLATAFORMAS?

Ve a

www.menti.com

Introduce el código

8140 8541

O usa el código QR

PROTOCOLO A CONSIDERAR PARA UNA AUDIENCIA REMOTA

1. **Vestimenta:** Toga o formal (evitar fondos distractores).
2. **Silenciar micrófono** cuando no se hable.
3. Uso de **"levantar mano"** para intervenir.
4. **Prueba técnica previa** (audio, cámara, luz).

ESTUDIO MÉXICO EVALÚA

Adopción Acelerada:

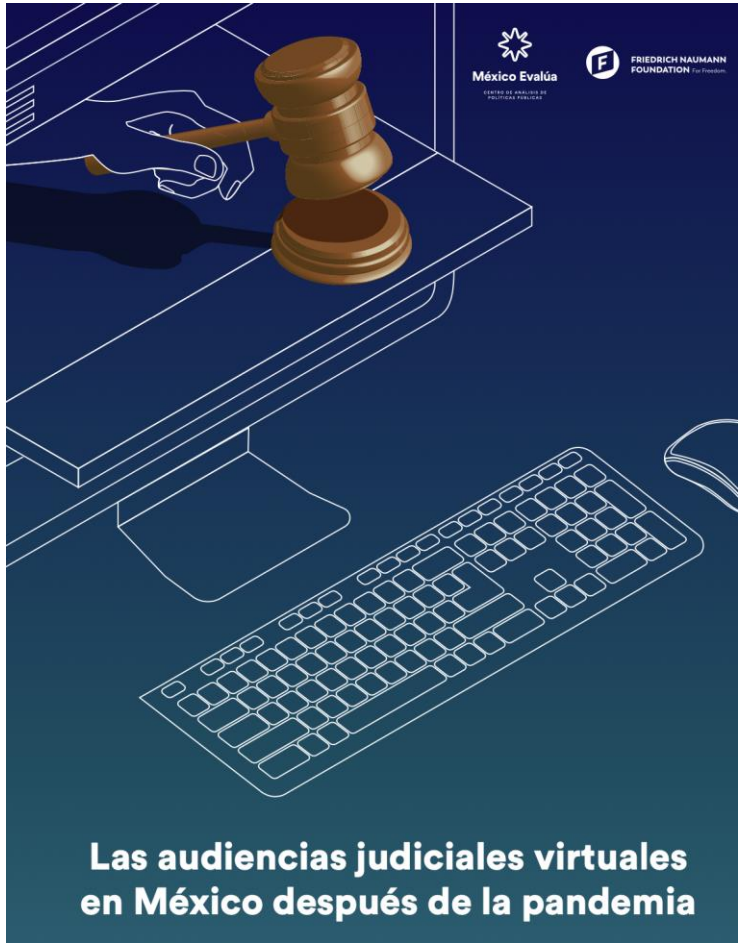
1. Antes de 2020: <10% de audiencias virtuales.
2. 2023: 70-80% en tribunales federales y 50% en estatales.
3. Jurisdicciones líderes: CDMX, Nuevo León y Jalisco.

Beneficios:

1. Eficiencia: Reducción del 40% en tiempos de resolución de casos.
2. Ahorros: Disminución de costos operativos (traslados, papel, almacenamiento).
3. Acceso a justicia: Mayor participación de víctimas y testigos en zonas remotas.

Desafíos:

1. Brecha digital: 30% de tribunales en zonas rurales carecen de infraestructura (internet, hardware).
2. Capacitación insuficiente: 45% de jueces y abogados reportan dificultades técnicas.
3. Seguridad y privacidad: Riesgos de filtración de datos en plataformas no especializadas (ej: Zoom).



5. SEGURIDAD DIGITAL

RIESGOS DE SEGURIDAD

"El 60% de los ataques a instituciones judiciales son por phishing"

Fuente: Interpol, 2023.

ATAQUES DE SEGURIDAD

TIPOS DE RIESGOS DE SEGURIDAD

Phishing (Suplantación de Identidad)

- Qué es: Correos, mensajes o llamadas falsas que imitan instituciones legítimas (ej: bancos, tribunales).
- Objetivo: Robar credenciales, datos sensibles o instalar malware.
- Ejemplo: "Su cuenta del Poder Judicial será suspendida. Ingrese aquí [enlace falso]".
- Impacto: Pérdida de datos, acceso no autorizado a sistemas.

Ransomware (Secuestro de Datos)

- Qué es: Malware que cifra archivos y exige rescate (generalmente en criptomonedas).
- Objetivo: Extorsión económica o sabotaje.
- Ejemplo: Ataque al Tribunal de Justicia de CDMX (2023), que paralizó audiencias por días.
- Impacto: Pérdida de información crítica, costos de recuperación.

TIPOS DE RIESGOS DE SEGURIDAD

Suplantación (Spoofing)

- Qué es: Falsificación de identidades (ej: emails, números de teléfono o perfiles de redes sociales).
- Objetivo: Engañar a víctimas para transferencias fraudulentas o filtraciones.
- Ejemplo: Un abogado recibe un email del "juez" pidiendo documentos confidenciales.
- Impacto: Fraude financiero, violación de confidencialidad.

Fugas de Información

- Qué es: Exposición accidental o intencional de datos (ej: nubes públicas sin cifrar, USB perdidos).
- Objetivo: Acceso a información privilegiada.
- Ejemplo: Expedientes judiciales subidos a Google Drive sin restricciones.
- Impacto: Multas por incumplimiento de GDPR/LFPDPPP, daño reputacional.

TIPOS DE RIESGOS DE SEGURIDAD

Ataques a Cadenas de Suministro

- Qué es: Compromiso de proveedores externos (ej: software judicial vulnerado).
- Objetivo: Infectar sistemas legítimos a través de terceros.
- Ejemplo: Ataque a SolarWinds (2020), que afectó a gobiernos.
- Impacto: Brechas masivas, espionaje.

Ingeniería Social

- Qué es: Manipulación psicológica para obtener información (ej: llamadas falsas de "soporte técnico").
- Objetivo: Bypass de controles de seguridad.
- Ejemplo: "Soy del área de TI. Necesito su contraseña para actualizar el sistema".
- Impacto: Acceso no autorizado a redes internas.

¿HE SIDO VÍCTIMA DE ALGÚN INTENTO O AMENAZA DE SEGURIDAD?

Ve a

www.menti.com

Introduce el código

8140 8541

O usa el código QR

6. INTELIGENCIA ARTIFICIAL EN JUSTICIA

¿QUÉ ES LA INTELIGENCIA ARTIFICIAL?

Sistemas que simulan inteligencia humana mediante algoritmos (aprendizaje automático, redes neuronales).

Principales hitos de desarrollo:

- 1950: Alan Turing y el "Test de Turing".
- 1997: IBM Deep Blue vence al campeón de ajedrez.
- 2016: AlphaGo de Google gana en Go.
- 2020s: ChatGPT, modelos de lenguaje (GPT-4).
- 2024: IA predictiva (ej: Loomis en EE.UU.).
- 2025: IA generativa.

Crecimiento de inversión en IA (2010: $1B → 2024: $500B).

APLICACIONES DE IA EN JUSTICIA

Automatización de procesos

- Chatbot judicial.

IA predictiva

- Caso: Nijeer Parks (EE.UU.) análisis de identidad (controversia por sesgos raciales).
- Dato: "En Estonia, los jueces usan IA para sugerir sentencias en casos menores".

Análisis de evidencias

- Herramientas: Reconocimiento facial (con límites éticos), minería de textos en expedientes.

Asistencia a jueces

- Ejemplo: Plataforma Lex Machina (analiza jurisprudencia en segundos).

DESAFÍOS ÉTICOS Y NORMATIVOS

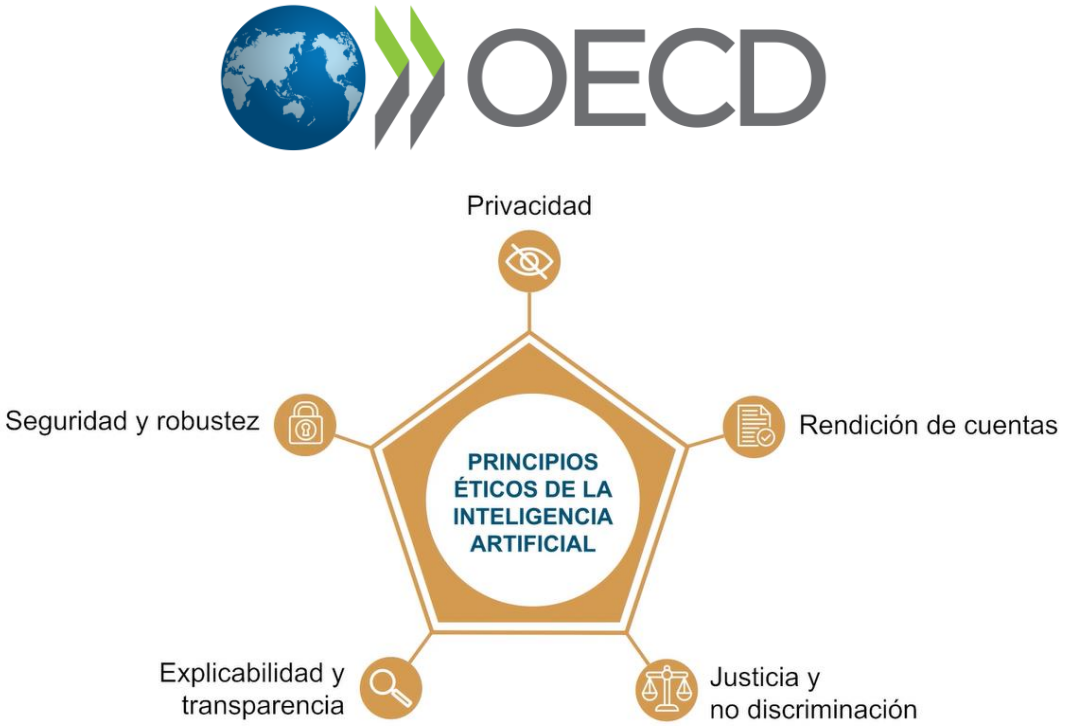
- Uso irresponsable de IA: Caso Nijeer Parks

- Sesgos que perpetúan desigualdades, racismo, estereotipos de género, etc.
- Falta de transparencia en la generación y entrenamiento del algoritmo

DESAFÍOS ÉTICOS Y NORMATIVOS

¿Cómo funciona?	Calidad de los datos	Soluciones
• Aprendizaje supervisado • Aprendizaje no supervisado	• Sesgos en los datos de entrada: Descarte de variables & distribución de categorías	• Análisis previo de los datos • Datos representativos • Crear datos • Transparencia • Implementación de principios éticos y monitoreo

DESAFÍOS ÉTICOS Y NORMATIVOS



APLICACIONES ACTUALES

Caso Colombia: es un sistema de Inteligencia Artificial que busca mejorar el proceso de selección de tutelas en la Corte Constitucional.

1. Búsqueda
2. Categorización
3. Estadística

¿REEMPLAZARÁ LA IA LA LABOR JURISDICCIONAL?

Ve a

www.menti.com

Introduce el código

8140 8541

O usa el código QR

BREAK (20 MIN)

TIMER ONLINE

¿DE QUÉ HABLAMOS EN ESTOS DÍAS?

Expediente electrónico

Firma electrónica

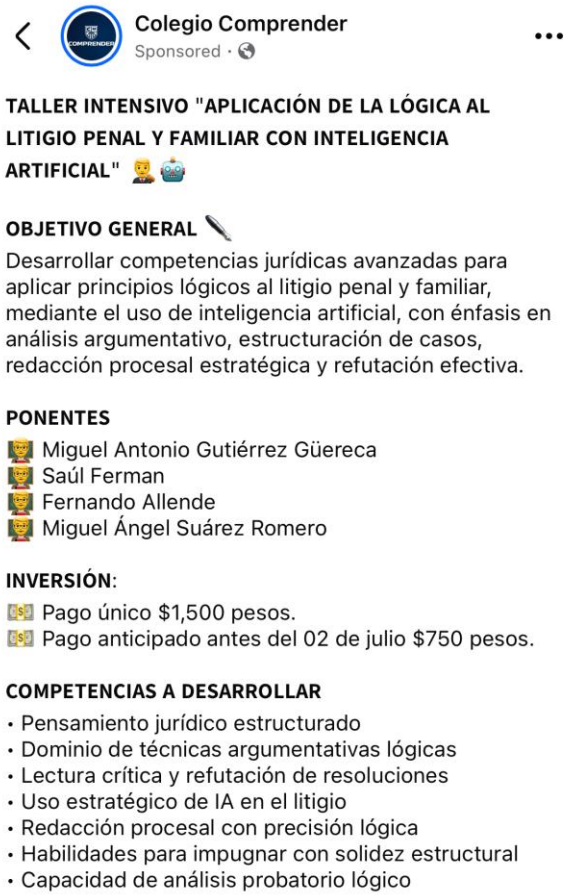
Audiencias a distancia

Seguridad digital

Inteligencia Artificial

REFLEXIONES FINALES

- La tecnología es un medio y no un fin.
- Requerimos de despojarnos de prejuicios y paradigmas para poder dar un salto de fe y evolucionar.
- No todo lo que brilla es oro.
- Recuerden: el desafío no está en obtener información, sino que está en determinar qué información nos es útil.



Colegio Comprender
Sponsored ·

TALLER INTENSIVO "APLICACIÓN DE LA LÓGICA AL LITIGIO PENAL Y FAMILIAR CON INTELIGENCIA ARTIFICIAL" 👨‍⚖️🤖

OBJETIVO GENERAL 🔪

Desarrollar competencias jurídicas avanzadas para aplicar principios lógicos al litigio penal y familiar, mediante el uso de inteligencia artificial, con énfasis en análisis argumentativo, estructuración de casos, redacción procesal estratégica y refutación efectiva.

PONENTES

🏆 Miguel Antonio Gutiérrez Güereca
🏆 Saúl Ferman
🏆 Fernando Allende
🏆 Miguel Ángel Suárez Romero

INVERSIÓN:

💵 Pago único $1,500 pesos.
💵 Pago anticipado antes del 02 de julio $750 pesos.

COMPETENCIAS A DESARROLLAR

- Pensamiento jurídico estructurado
- Dominio de técnicas argumentativas lógicas
- Lectura crítica y refutación de resoluciones
- Uso estratégico de IA en el litigio
- Redacción procesal con precisión lógica
- Habilidades para impugnar con solidez estructural
- Capacidad de análisis probatorio lógico

EVALUACIÓN DEL CUMPLIMIENTO DE LOS OBJETIVOS

Ve a

www.menti.com

Introduce el código

8140 8541

O usa el código QR

¡GRACIAS!