DigiLatam

by AMD Tech®

ACADEMIA MEXICANA DE DERECHO DIGITAL Y TECNOLÓGICO, AC

Los Mejores TECHNOLAWYERS y Especialistas Digitales de Iberoamérica 2025

Año 2 - Número 3

DigiLatam
by AMDTech®
ACADEMIA MEXICANA DE DERECHO DIGITAL Y TECNOLÓGICO, AC

Directorio Editorial

Del Director:

Para nosotros es un gusto editar este, nuestro tercer número de tu revista DIGILATAM, en el que podrás encontrar interesantes temas referentes al E-Commerce, la Inteligencia Artificial en los ámbitos de la Justicia y del Empresariado y de Valoración de Evidencias Digitales.

En nuestras secciones de Perfiles y Organizaciones Destacadas conocerás a personalidades del entorno digital, así como a organismos que aportan conocimiento al mismo.

Como eje de este número te presentamos el listado de los “Mejores Technolawyers 2025”.

También encontrarás nuestras secciones de la Academia, donde presentamos diversidad de información relacionada con este entorno digital.

Agradecemos el apoyo que al momento nos has brindado, el cual nos compromete a que este medio continúe siendo el enlace entre las diversas instancias que conforman nuestro ecosistema.

Gracias por ser parte de AMDTech.

Dr. David E. Merino Téllez.

Contenido

ANÚNCIATE CON NOSOTROS

AUDIENCIA

+11,500
Usuarios Únicos

+99,500
Page Views

+93,000
Usuarios Alcanzados

+17,900
Usuarios Alcanzados

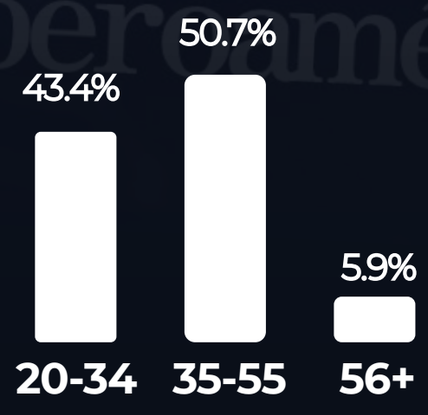
+11,000
Usuarios Alcanzados

TOTAL:
+232,900

PASS ALONG
4

45.8%
MUJERES

54.2%
HOMBRES



EDAD

Para mayores informes:
+52 56 3704 6926
dvaldes@amdtech.mx

E-Commerce vs Estado

Por: Lic. Jerónimo Ocejo Torres.

La República de los Algoritmos: Cuando la Plataforma Sustituye a la Ley

En buena parte de América Latina, las plataformas digitales ya cumplen funciones que antes solo realizaba el Estado. Organizan mercados, generan confianza entre desconocidos, procesan pagos, otorgan crédito y resuelven conflictos. No es una provocación ni una exageración intelectual: es una descripción de la vida económica cotidiana de millones de personas.

Para muchos ciudadanos, la primera experiencia con reglas claras, pagos confiables y mecanismos de protección no ocurre frente a un banco, un juzgado o una autoridad fiscal. Ocurre dentro de una plataforma.

El comercio electrónico dejó de ser un canal de ventas. Se convirtió en infraestructura económica. Y como toda infraestructura, distribuye poder.

Cuando la confianza deja de venir de la ley

En América Latina, el problema central del comercio nunca fue el precio ni la oferta. Fue la desconfianza.
Desconfianza en que el producto llegue.
Desconfianza en que el pago sea reconocido.
Desconfianza en que alguien responda cuando algo sale mal.
Durante décadas, el Estado no logró resolver este problema de forma eficiente. Las plataformas sí.
Mercado Libre construyó reputación donde no existía.
Amazon impuso estándares logísticos que ningún sistema público logró escalar.
En México, Brasil o Colombia, resolver un conflicto dentro de una plataforma suele ser más rápido, más barato y efectivo que acudir a un tribunal.

La consecuencia es profunda y rara vez se nombra:
La confianza dejó de ser un bien público y se convirtió en un servicio privado.
La informalidad no fue el problema, fue el punto de partida.
Más de la mitad de la fuerza laboral latinoamericana opera en esquemas informales. Las plataformas no intentaron eliminar esa realidad. La ordenaron.
En México, miles de pequeños vendedores descubrieron que era más sencillo cumplir con las reglas de una plataforma que con las reglas fiscales. No por evasión deliberada, sino porque el sistema digital ofrecía algo que el sistema formal no: claridad, previsibilidad y respuesta.
Las llamadas “Nenis” no son una anomalía digital ni un fenómeno marginal. Son la expresión más clara de cómo el comercio electrónico absorbió una realidad económica que el Estado nunca logró formalizar del todo.
Las plataformas no formalizan por decreto. Formalizan por incentivos:
Reputación, pagos garantizados, acceso a demanda, logística confiable.
Para muchos pequeños vendedores, la plataforma es el primer espacio donde existen reglas estables, aunque esas reglas no sean públicas ni negociables.

La plataforma ve todo. El vendedor, no.

Aquí aparece el núcleo del poder.
La plataforma conoce el mercado completo: precios, rotación, elasticidad, comportamiento del consumidor y riesgos. Ajusta reglas en tiempo real. Define visibilidad.
El vendedor solo ve su vitrina.
Esta diferencia no es un error del sistema. Es su diseño.
Mientras el mercado crece, esta asimetría se tolera. Cuando el

crecimiento se desacelera, se convierte en una forma silenciosa de disciplina económica. El que no se adapta desaparece del radar.
No hay castigo explícito. Solo invisibilidad.
Pagos y logística: decisiones políticas disfrazadas de técnica
Hablar de comercio digital sin hablar de pagos y logística es hablar de marketing, no de economía.
En Brasil, Pix demostró que cuando el Estado decide intervenir en una capa estratégica, puede alterar el equilibrio completo del sistema. Pagos instantáneos, interoperables y accesibles redujeron dependencia y reequilibraron poder frente a bancos y fintechs.
En México, el avance fue fragmentado pero revelador. SPEI, OXXO Pay y esquemas híbridos tradujeron el efectivo al mundo digital. No fue una estrategia explícita de soberanía digital, pero sí una respuesta pragmática a una realidad concreta.
Donde el Estado no asumió el control, el mercado decidió por él.
Y cada decisión técnica terminó siendo una decisión política, aunque nadie la llamara así.

El crédito como herramienta de disciplina

El crédito embebido es uno de los mecanismos más influyentes del comercio digital, pero rara vez se analiza por lo que realmente es: una herramienta de disciplina económica.
Para millones de vendedores y consumidores, el primer acceso al financiamiento no vino de un banco, sino de una plataforma.
No se evaluaron ingresos formales ni historiales tradicionales.
Se evaluó comportamiento.
Cumplir tiempos.
Mantener reputación.
No generar reclamos.
Rotar inventario.
Quien se comporta “bien” accede a crédito. Quien no, queda fuera.
Es eficiente.
También es opaco.
Nadie sabe con claridad cómo se decide el acceso ni cómo se corrige una exclusión. El crédito deja de ser solo inclusión financiera y se convierte en un mecanismo silencioso de control.

Cuando el algoritmo sustituye al criterio

Las plataformas reemplazaron criterios humanos por decisiones algorítmicas. No por malicia, sino por eficiencia.
Estas decisiones no responden a conspiraciones ni agendas ocultas. Son decisiones empresariales legítimas. El riesgo aparece cuando su impacto es sistémico y no existe ningún mecanismo externo de rendición de cuentas.
Millones de decisiones económicas se toman sin explicación ni posibilidad real de apelación. Cuando eso ocurre a escala, ya no estamos ante un problema tecnológico, sino ante un problema de poder.

Cuando la plataforma sustituye a la ley

Las plataformas crearon regímenes normativos privados. Términos de uso, sanciones automáticas y resolución interna de disputas funcionan mejor que la ley formal en muchos casos.
El problema no es su eficacia, sino la ausencia de contrapesos.
Cuando una cuenta es suspendida, no hay juez independiente, ni debido proceso, ni autoridad externa. La plataforma legisla, juzga y ejecuta al mismo tiempo.

En contextos de debilidad institucional, esta sustitución se vuelve estructural. Y cuanto más fuerte se vuelve la plataforma, menos incentivos existen para fortalecer al Estado.

Datos: el recurso que gobierna sin cotizar
En el comercio tradicional, el recurso crítico era el capital. En el comercio digital, el recurso decisivo son los datos.
América Latina exporta comportamiento e importa decisiones.
Los datos se generan localmente, pero se procesan y monetizan fuera de la región.
Quien controla los datos controla el conocimiento del mercado. Y sin marcos claros sobre su uso y protección, la dependencia se profundiza.

Soberanía digital: capacidad, no consigna
La soberanía digital no es aislamiento tecnológico ni nacionalismo digital. Es capacidad de decisión.
Capacidad de decidir: qué capas son estratégicas, dónde se procesan los datos, qué reglas no pueden quedar completamente privatizadas.
Pix demuestra que esto es posible. El problema es que sigue siendo la excepción y no la norma.

El punto de no retorno
Toda infraestructura llega a un momento en el que cambiarla se vuelve extraordinariamente costoso.
Cuando los usuarios ya no conciben alternativas.
Cuando los negocios dependen completamente del sistema.
Cuando los estándares se consolidan.
América Latina se acerca a ese umbral.

La decisión que seguimos postergando
El comercio digital funciona. Negarlo sería absurdo.
Lo que sigue sin discutirse es quién gobierna ese funcionamiento.

Regular con entendimiento.
Competir en capas estratégicas.
O abdicar.
No asumir el control no es neutral. Significa aceptar que otros gobiernen la infraestructura económica.
La discusión sobre comercio digital no es tecnológica. Es política.
Si las reglas las define el código, si los conflictos los resuelven términos de uso, si el acceso al mercado depende de algoritmos y si la confianza es un servicio privado, entonces la pregunta no admite rodeos:

¿Queremos ciudadanos con derechos o usuarios con condiciones de uso?

LIC. JERÓNIMO OCEJO TORRES.

Abogado con Experiencia Global en Compliance, Gobierno Corporativo e Infraestructura.
Coordinador de la Comisión de E-Commerce de la AMDTech.

Inteligencia Artificial en la Justicia:

Cinco Ejes para un Modelo de Regulación Algorítmica Judicial

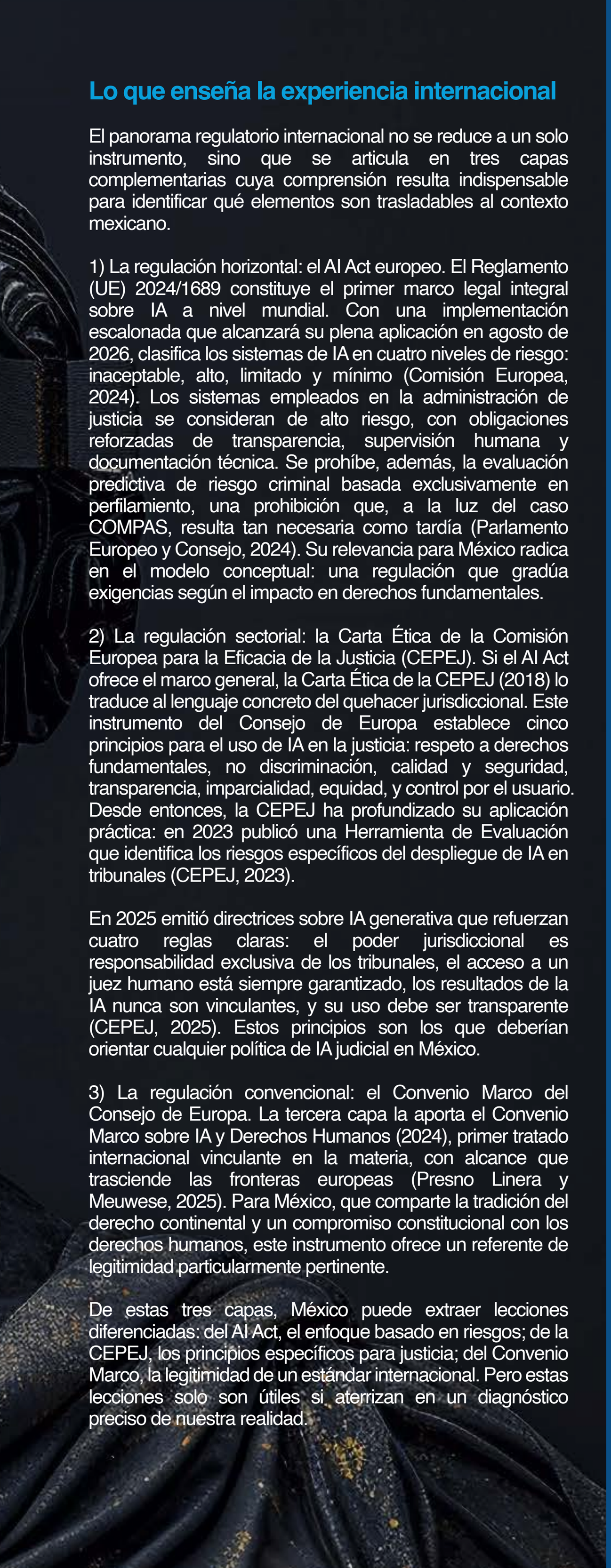
Por: Lic. Jorge Antonio Montiel Romero.

Introducción

¿Puede un algoritmo recomendar la prisión preventiva de una persona con base en patrones estadísticos? ¿Su código postal, su edad, su historial familiar? No es ciencia ficción. En Estados Unidos, el sistema COMPAS fue diseñado precisamente para predecir la probabilidad de reincidencia delictiva (Angwin et al., 2016). En 2016, una investigación de ProPublica reveló que el algoritmo etiquetaba erróneamente a personas afrodescendientes como de alto riesgo con el doble de frecuencia que a personas blancas (Angwin et al., 2016). Esta es la advertencia más elocuente de lo que ocurre cuando la Inteligencia Artificial (IA) opera en el sistema de justicia sin marcos de gobernanza adecuados.

Ahora bien, este escenario distópico no le es ajeno a América Latina. En Argentina, Prometea redujo de 190 días a menos de una hora la elaboración de dictámenes en la Fiscalía de Buenos Aires (Corvalán, 2018). En Colombia, PretorIA asiste a la Corte Constitucional en la gestión de más de 600,000 acciones de tutela anuales, priorizando las que exigen atención urgente (Saavedra y Upegui, 2021). Y en 2023, un juez del Juzgado Primero Laboral de Cartagena utilizó ChatGPT para complementar la motivación de una sentencia de tutela, generando un caso que la Corte Constitucional revisó en su Sentencia T-323 de 2024, estableciendo los primeros principios éticos para el uso de IA generativa en la justicia colombiana (Corte Constitucional de Colombia, 2024). La tecnología ya está aquí. La pregunta es si nuestros marcos normativos están a la altura.

Este artículo propone que México puede y debe construir un modelo de regulación algorítmica judicial propio, informado por la experiencia internacional pero enraizado en la realidad institucional del sistema de justicia nacional.



Lo que enseña la experiencia internacional

El panorama regulatorio internacional no se reduce a un solo instrumento, sino que se articula en tres capas complementarias cuya comprensión resulta indispensable para identificar qué elementos son trasladables al contexto mexicano.

1) La regulación horizontal: el AI Act europeo. El Reglamento (UE) 2024/1689 constituye el primer marco legal integral sobre IA a nivel mundial. Con una implementación escalonada que alcanzará su plena aplicación en agosto de 2026, clasifica los sistemas de IA en cuatro niveles de riesgo: inaceptable, alto, limitado y mínimo (Comisión Europea, 2024). Los sistemas empleados en la administración de justicia se consideran de alto riesgo, con obligaciones reforzadas de transparencia, supervisión humana y documentación técnica. Se prohíbe, además, la evaluación predictiva de riesgo criminal basada exclusivamente en perfilamiento, una prohibición que, a la luz del caso COMPAS, resulta tan necesaria como tardía (Parlamento Europeo y Consejo, 2024). Su relevancia para México radica en el modelo conceptual: una regulación que gradúa exigencias según el impacto en derechos fundamentales.

2) La regulación sectorial: la Carta Ética de la Comisión Europea para la Eficacia de la Justicia (CEPEJ). Si el AI Act ofrece el marco general, la Carta Ética de la CEPEJ (2018) lo traduce al lenguaje concreto del quehacer jurisdiccional. Este instrumento del Consejo de Europa establece cinco principios para el uso de IA en la justicia: respeto a derechos fundamentales, no discriminación, calidad y seguridad, transparencia, imparcialidad, equidad, y control por el usuario. Desde entonces, la CEPEJ ha profundizado su aplicación práctica: en 2023 publicó una Herramienta de Evaluación que identifica los riesgos específicos del despliegue de IA en tribunales (CEPEJ, 2023).

En 2025 emitió directrices sobre IA generativa que refuerzan cuatro reglas claras: el poder jurisdiccional es responsabilidad exclusiva de los tribunales, el acceso a un juez humano está siempre garantizado, los resultados de la IA nunca son vinculantes, y su uso debe ser transparente (CEPEJ, 2025). Estos principios son los que deberían orientar cualquier política de IA judicial en México.

3) La regulación convencional: el Convenio Marco del Consejo de Europa. La tercera capa la aporta el Convenio Marco sobre IA y Derechos Humanos (2024), primer tratado internacional vinculante en la materia, con alcance que trasciende las fronteras europeas (Presno Linera y Meuwese, 2025). Para México, que comparte la tradición del derecho continental y un compromiso constitucional con los derechos humanos, este instrumento ofrece un referente de legitimidad particularmente pertinente.

De estas tres capas, México puede extraer lecciones diferenciadas: del AI Act, el enfoque basado en riesgos; de la CEPEJ, los principios específicos para justicia; del Convenio Marco, la legitimidad de un estándar internacional. Pero estas lecciones solo son útiles si aterrizan en un diagnóstico preciso de nuestra realidad.

México: avance legislativo acelerado, pendiente el enfoque judicial

México se encuentra en un momento legislativo decisivo. Tras diversas iniciativas en 2025, el Senado tenía previsto votar el 25 de febrero de 2026 una Ley General de Inteligencia Artificial (Observatorio IA México, 2026), respaldada por una reforma al Artículo 73 constitucional (Senado, 2026). La propuesta, elaborada por la Comisión de IA del Senado a partir de 34 recomendaciones de 72 especialistas (Comisión de IA del Senado, 2025), adopta una arquitectura en tres niveles: reformas constitucionales, ley general con enfoque basado en riesgos, y armonización de al menos 17 leyes sectoriales. Se contempla un Consejo Mexicano de Ética para la IA, una Agencia para el Desarrollo de la IA, un registro de sistemas de alto riesgo y sandboxes regulatorios.

Estas iniciativas representan avances sustanciales, pero comparten una limitación que merece señalarse ahora que la votación es inminente: adoptan el enfoque de riesgos inspirado en el AI Act europeo sin incorporar la granularidad sectorial que la CEPEJ ha demostrado indispensable para el ámbito judicial. La Ley General contempla un registro de sistemas de alto riesgo y evaluaciones de impacto (Observatorio IA México, 2026), pero no distingue entre la IA que optimiza una cadena de suministro y la que asiste a un juzgador en la determinación de una medida cautelar.

Y es que, a diferencia de otros sectores, en el sistema de justicia las decisiones asistidas por algoritmos inciden directamente en la libertad, el patrimonio y los derechos fundamentales de las personas. Una encuesta de la UNESCO a operadores judiciales de 96 países reveló que el 44% ya utiliza herramientas de IA generativa como ChatGPT en sus funciones, pero el 91% reporta que su institución no les proporciona capacitación ni lineamientos para su uso responsable (UNESCO, 2024).

Por otro lado, la creación del Órgano de Administración Judicial, en sustitución del ya extinto Consejo de la Judicatura Federal, ha generado un rediseño institucional que permite incorporar la gobernanza algorítmica como componente estructural, no como añadido posterior. Los proyectos tecnológicos que no cuentan con políticas de gobernanza desde su concepción terminan generando resistencias institucionales que dificultan su adopción y comprometen su sostenibilidad. La regulación no puede llegar después de la tecnología, debe ser parte de su diseño.

Cinco ejes para un modelo de regulación algorítmica judicial

1) Clasificación de riesgos contextualizada. No es lo mismo un chatbot que informa al ciudadano sobre el estado de su expediente que un sistema que sugiere al juzgador si procede una medida cautelar. Tratar ambos con las mismas reglas produce uno de dos resultados igualmente dañinos: o se asfixia la innovación con requisitos desproporcionados, o se desprotege al justiciable con controles insuficientes. La salida es una gradación: las herramientas de búsqueda jurisprudencial pueden situarse en riesgo limitado; los

sistemas de apoyo a la decisión judicial deben clasificarse como de alto riesgo, con exigencias reforzadas de explicabilidad y supervisión.

2) Supremacía del juicio humano. Ningún sistema de IA sustituye la función jurisdiccional. Los resultados algorítmicos son orientativos, es decir, la persona juzgadora conserva la responsabilidad última y la obligación de fundamentar y motivar conforme a derecho. Este principio es la condición de legitimidad de toda la empresa de digitalización judicial. El caso COMPAS muestra qué ocurre cuando ese límite se difumina: jueces que consideraron puntuaciones algorítmicas que ni ellos ni los acusados podían verificar o impugnar, y un sistema que, según reveló una investigación periodística, producía tasas de falsos positivos significativamente más altas para acusados afroamericanos (Angwin et al., 2016).

3) Transparencia y trazabilidad. Afirmar la supremacía humana sin mecanismos para verificarla es retórica. Todo sistema de IA judicial debe documentar sus datos de entrenamiento, lógica de funcionamiento, limitaciones conocidas y criterios de diseño. Sin esa información, la auditoría algorítmica es imposible y el debido proceso, inverificable.

Prometea, desarrollado en el Ministerio Público Fiscal de Buenos Aires, ofrece un referente concreto: su algoritmo es abierto, auditable y trazable (Corvalán, 2018), lo que inspiró el desarrollo de PretorIA en la Corte Constitucional colombiana (Saavedra y Upegui, 2021) y facilitó su despliegue como asistente en la Corte Interamericana de Derechos Humanos (Estévez et al., 2020).

4) Evaluaciones de impacto algorítmico. La transparencia describe el sistema tal como es; la evaluación de impacto anticipa lo que puede producir. Son complementarias y ninguna sustituye a la otra. Antes de desplegar cualquier sistema de IA en el ámbito judicial, debe evaluarse el riesgo de discriminación, sesgo, vulneración de datos personales y afectación a la independencia judicial. Siguiendo la metodología de la CEPEJ, estas evaluaciones deben ser periódicas y no pueden diseñarse desde un escritorio: requieren incorporar la perspectiva de los operadores jurídicos que interactuarán cotidianamente con la herramienta (CEPEJ, 2023).

5) Gobernanza institucional y competencias digitales. Ningún modelo regulatorio funciona sin una estructura que lo sostenga. Dentro del Poder Judicial de la Federación, esto implica designar áreas responsables de la supervisión de sistemas de IA, crear protocolos de adquisición y evaluación tecnológica, desarrollar programas de alfabetización en IA para personal jurisdiccional y administrativo. Los marcos ISO 42001 y el AI Risk Management Framework del NIST ofrecen referentes metodológicos para esta tarea (ISO, 2023; NIST, 2023). La mayor resistencia a la transformación digital no proviene de limitaciones tecnológicas, sino de la falta de competencias y marcos institucionales claros. La construcción de estas capacidades es lo que convierte los cuatro ejes anteriores en prácticas efectivas.

Conclusiones

La regulación algorítmica judicial es una dimensión esencial de la protección de derechos fundamentales en la era digital. Esta experiencia internacional, articulada en las tres capas analizadas, sugiere que los marcos más robustos combinan un enfoque graduado de riesgos con principios específicos para el sector justicia. La experiencia latinoamericana añade una lección adicional: la tecnología avanza con o sin regulación, y la ausencia de marcos normativos no impide su adopción, solo la vuelve riesgosa.

Con la votación de la Ley General de IA prevista para el 25 de febrero de 2026, el país está a punto de contar con su primer marco regulatorio integral. Los cinco ejes propuestos ofrecen una hoja de ruta complementaria para el ámbito judicial. La nueva ley general es un paso necesario, pero no suficiente: el Poder Judicial requiere políticas sectoriales propias. La transformación digital solo será verdaderamente transformadora si coloca a la persona y sus derechos en el centro de toda decisión algorítmica. Y esa gobernanza debe construirse desde el corazón mismo de la institución judicial.

Bibliografía:

Angwin, J., Larson, J., Mattu, S. y Kirchner, L. (2016, 23 de mayo). Machine Bias. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Cámara de Diputados. (2025, 22 de abril). Iniciativa con proyecto de decreto por el que se expide la Ley Federal para el Desarrollo Ético, Soberano e Inclusivo de la Inteligencia Artificial. Gaceta Parlamentaria, núm. 6768-II-4. https://sitl.diputados.gob.mx/LXVI_leg/cuadros_comparativos/2PO1/1005-2PO1-25.pdf

Comisión de IA del Senado de la República. (2025). Hacia un marco normativo para la Inteligencia Artificial (IA): Informe 2024-2025. https://comisiones.senado.gob.mx/inteligencia_artificial/images/noticias/Informe_2024-2025.pdf

Comisión Europea para la Eficiencia de la Justicia [CEPEJ]. (2018, 4 de diciembre). Carta Ética Europea sobre el uso de la inteligencia artificial en los sistemas judiciales y su entorno. Consejo de Europa. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

CEPEJ. (2023). Herramienta de evaluación para la operacionalización de la Carta Ética Europea sobre el uso de la IA en los sistemas judiciales, CEPEJ(2023)16final. Consejo de Europa. https://rm.coe.int/cepej-2023-16final-operationalisation-ai-ethical-charter-en/1680adcc9c

CEPEJ. (2025, 19 de diciembre). Directrices sobre el uso de la IA generativa para profesionales judiciales, CEPEJ(2025)18Final. Consejo de Europa. https://rm.coe.int/cepej-2025-18final-en-draft-guidelines-on-the-use-of-generative-ai-for/48802a4ad1

Consejo de Europa. (2024, 5 de septiembre). Convenio Marco sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho, CETS n.º 225. https://rm.coe.int/1680afae3c

Corte Constitucional de Colombia. (2024). Sentencia T-323/24 (M.P. Juan Carlos Cortés González). https://www.corteconstitucional.gov.co/relatoria/2024/t-323-24.htm

Corvalán, J. G. (2018). Inteligencia artificial: retos, desafíos y oportunidades — Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia. Revista de Investigações Constitucionais, 5(1), 295-316. https://doi.org/10.5380/rinc.v5i1.55334

Estevez, E., Fillottrani, P. y Linares Lejarraga, S. (2020). PROMETEA: Transformando la administración de justicia con herramientas de inteligencia artificial. Banco Interamericano de Desarrollo. https://doi.org/10.18235/0002378

ISO. (2023). ISO/IEC 42001:2023. Tecnología de la información — Inteligencia artificial — Sistema de gestión. Organización Internacional de Normalización. https://www.iso.org/standard/42001

National Institute of Standards and Technology [NIST]. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Diario Oficial de la UE, L 2024/1689. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L_202401689

Observatorio IA México. (2026, febrero). Proceso legislativo: Ley General de Inteligencia Artificial. https://www.observatorio-ia-mexico.com/proceso-legislativo

Presno Linera, M. Á. y Meuwese, A. (2025). Regulating AI from Europe: A joint analysis of the AI Act and the Framework Convention on AI. The Theory and Practice of Legislation, 13(3), 292-311. https://doi.org/10.1080/20508840.2025.2492524

LIC. JORGE ANTONIO MONTIEL ROMERO

Subdirector de Políticas y Estrategias para la Transformación Digital Consejo de la Judicatura Federal.
Coordinador de la Comisión de Transformación Digital de la AMDTech.

TOP COMPLIANCE
AND RISK MANAGEMENT COMMUNITY®

¡AFÍLIATE A TOP COMPLIANCE!

Somos la asociación gratuita de profesionales de cumplimiento más grande de Iberoamérica.

BENEFICIOS:

- Bolsa de Trabajo Especializada
- Revista Digital
- Alianzas Estratégicas
- Grupos Especializados de WhatsApp
- Hasta 40% de Descuento en Cursos Seleccionados
- Mentorías Gratuitas
- Programa de Actualización Continua
- Eventos Especializados

SOMOS EL ECOSISTEMA DE CUMPLIMIENTO MÁS GRANDE DE IBEROAMÉRICA CON

+ 14,700 PROFESIONALES, CON PRESENCIA EN 11 PAÍSES.

¡AFILIACIÓN GRATUITA!

REGISTRO EN: TOPCOMPLIANCE.ORG

TOP COMPLIANCE · TOPCOMPLIANCE · @_TOPCOMPLIANCE · TOP COMPLIANCE

Desafíos del Uso de la Inteligencia Artificial en la Práctica Legal

Por: Mtro. Patricio González Granados.

La práctica legal contemporánea atraviesa una de las transformaciones más profundas de su historia. La irrupción de la Inteligencia Artificial (IA) no solo ha modificado la forma en que los abogados trabajan, sino también la velocidad y profundidad con la que se analizan los asuntos jurídicos. Hoy, las herramientas de IA permiten revisar y analizar contratos extensos en minutos, redactar correspondencia legal con mayor precisión, identificar jurisprudencia relevante mediante búsquedas inteligentes y realizar análisis predictivos.

La promesa de la IA es eficiencia, reducción de costos y rapidez. Sin embargo, detrás de esa eficiencia surgen dilemas éticos, de cumplimiento normativo y de responsabilidad profesional que no pueden ignorarse, incluso en escenarios tecnológicos aún no regulados.

La incorporación de la IA al ejercicio del derecho no exime al abogado de su responsabilidad profesional. Por el contrario, la amplía. Naturalmente, el hecho de que una redacción, un análisis o una recomendación sea generada parcialmente por una herramienta tecnológica no traslada la carga ética o jurídica al proveedor del software. El resultado final, y las consecuencias que de él se deriven, siguen siendo responsabilidad del profesional que firma o valida el documento.

Riesgos inherentes

Delegar tareas críticas sin supervisión, confiar ciegamente en un algoritmo o utilizar sin criterio los resultados generados por IA puede constituir una forma moderna de negligencia profesional. El abogado debe comprender, al menos en términos generales, cómo funcionan las herramientas que incorpora en su práctica, así como sus límites, posibles sesgos y márgenes de error. La responsabilidad profesional, en la era de la inteligencia artificial, consiste precisamente en mantener el control humano sobre el proceso.

Uno de los riesgos más críticos es la divulgación no autorizada de información. Cargar datos confidenciales de clientes o estrategias jurídicas a plataformas de IA puede tener consecuencias imprevisibles si los sistemas almacenan información o la utilizan para aprendizaje automático. Distintos casos en sectores tecnológicos han evidenciado cómo la introducción de datos sensibles en herramientas públicas generó filtraciones fuera del control corporativo.

Estos precedentes muestran que la automatización sin control humano puede amplificar errores y vulnerar derechos fundamentales. Para la práctica legal, las lecciones son claras: no delegar decisiones críticas únicamente a la IA, validar manualmente la información procesada y documentar cada revisión humana.

Otro riesgo importante es el sesgo algorítmico. La IA aprende de los datos con los que se alimenta y puede reproducir injusticias o errores preexistentes. En despachos legales, podría traducirse en análisis contractuales defectuosos o estrategias procesales que omiten riesgos críticos. A ello se suman los errores de generación de contenido, como citas inexistentes o referencias fabricadas, que han obligado a firmas internacionales a implementar nuevas políticas internas y capacitación obligatoria.

Estos ejemplos subrayan que la supervisión humana no es opcional, sino una obligación profesional.

Autorregulación de la abogacía

Ante el desarrollo acelerado de la tecnología, los colegios y asociaciones profesionales han asumido un papel central en la autorregulación. En México, la Barra Mexicana, Colegio de Abogados (BMA) ha elaborado lineamientos éticos para el uso responsable de la Inteligencia Artificial, enfatizando la supervisión directa del abogado, la verificación humana de la información generada, la transparencia con clientes y tribunales y la protección del secreto profesional.

En el plano internacional, la International Bar Association (IBA) ha promovido principios orientados a preservar la independencia profesional, la confidencialidad y la responsabilidad humana frente al uso de tecnologías emergentes, mientras que asociaciones como la American Bar Association y la Law Society of England and Wales han publicado opiniones formales y guías que insisten en tres obligaciones centrales: comprender la tecnología, supervisar su uso y garantizar la confidencialidad de los datos.

Estos ejemplos reflejan una tendencia clara: la profesión jurídica está respondiendo mediante mecanismos de autorregulación que buscan integrar la innovación sin comprometer los valores esenciales de la abogacía.

Integración tecnológica a la práctica

La integración de la Inteligencia Artificial en despachos y departamentos legales requiere mucho más que experimentar con nuevas herramientas: implica repensar los procesos internos, la gestión de información y, sobre todo, la responsabilidad profesional de cada abogado frente a sus clientes. Por ello, establecer políticas internas claras es esencial para asegurar un uso de la IA que sea responsable, seguro y eficiente.

La formación continua de todos los miembros del despacho es esencial: abogados y personal administrativo deben comprender los riesgos de la IA, las mejores prácticas para manejar información sensible y los procedimientos internos de supervisión. La auditoría periódica y los indicadores de desempeño, como porcentaje de revisiones humanas, cantidad de incidentes y cumplimiento de protocolos, permiten medir la efectividad de estas medidas, fortaleciendo una cultura organizacional responsable y consciente de los riesgos tecnológicos.

En suma, la integración de la IA combina eficiencia y prudencia, políticas internas sólidas, supervisión humana rigurosa y adaptación contractual. Este enfoque protege al cliente, resguarda la reputación del despacho y establece una base ética que permite aprovechar la innovación sin comprometer la integridad profesional.

Conclusión

La incorporación de la IA en la práctica legal representa un cambio profundo, que va mucho más allá de la simple eficiencia. Nos coloca ante una oportunidad histórica: aprovechar herramientas que permiten analizar grandes volúmenes de información, detectar patrones, anticipar riesgos y optimizar procesos que antes demandaban semanas de trabajo. Pero, al mismo tiempo, nos recuerda que toda innovación viene acompañada de responsabilidad. La tecnología nunca sustituye el juicio, la ética y la diligencia profesional del profesionista.

El camino hacia un uso responsable de la IA requiere establecer políticas internas sólidas, definir protocolos claros para la gestión de información sensible y crear una cultura de supervisión y verificación. La formación continua y la auditoría periódica no son un lujo: son instrumentos esenciales para garantizar que cada “output” generado por la IA sea revisado, comprendido y validado antes de llegar al cliente o a un tribunal. Asimismo, documentar cada decisión y cada interacción con la tecnología protege tanto a la firma como a quienes dependen de su asesoría.

Mirando al futuro, el desafío no es solo tecnológico, sino cultural y estratégico. La adopción responsable de la IA permitirá a los abogados concentrarse en la creatividad jurídica, el análisis crítico y la resolución de problemas complejos, mientras la tecnología asume tareas repetitivas o analíticas. Los despachos que logren integrar esta visión serán capaces de ofrecer un servicio más preciso, ágil y confiable, fortaleciendo la relación con sus clientes y consolidando su reputación.

En definitiva, la IA en la práctica legal no es un riesgo que deba evitarse, sino una oportunidad que debe gestionarse con rigor, ética y visión de futuro. El verdadero valor reside en combinar la inteligencia humana con la artificial de manera equilibrada, transformando la práctica del derecho en un espacio donde la innovación y la responsabilidad caminan de la mano. Adoptar este enfoque no solo asegura el cumplimiento normativo y la protección de la información, sino que también marca la diferencia entre un despacho reactivo y uno preparado para liderar la abogacía del siglo XXI.

MTRO. PATRICIO GONZÁLEZ GRANADOS
Socio de NEREO – IP & TECH
Coordinador del Comité de I. A. del capítulo México de la WCA.

INACIEP®

INSTITUTO DE ALTA DIRECCIÓN EN CIENCIAS EMPRESARIALES Y PATRIMONIALES

INVESTIGACIÓN Y CAPACITACIÓN EN DIVERSAS ÁREAS EMPRESARIALES

"CON MÁS DE 15 AÑOS DE EXPERIENCIA"

"Contamos con los expositores más destacados en las materias que se imparten".

www.inaciep.mx

Talleres, seminarios, diplomados y conferencias de manera:

- Presencial
- En Línea

INACIEP, contribuye al desarrollo, fortalecimiento y mejora continua del ámbito empresarial de nuestro país.

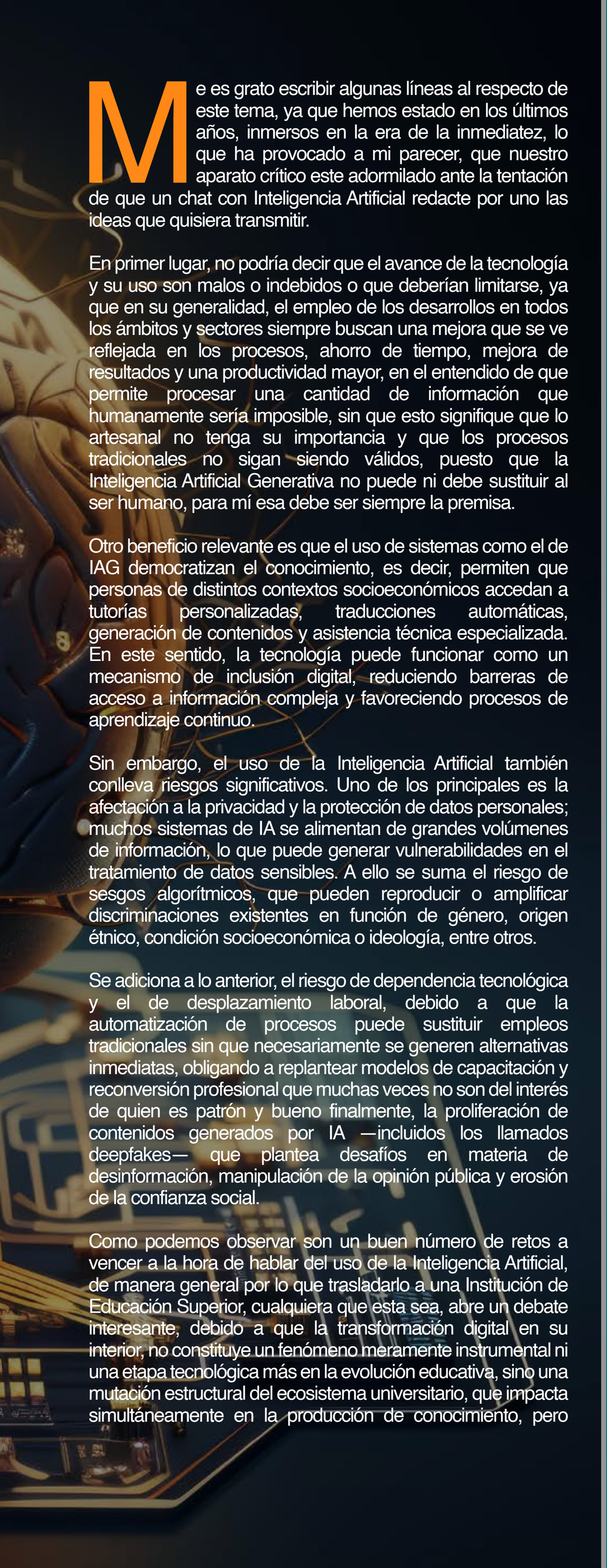
INACIEP @InaciepMX INACIEP @inaciep

Universidad Pública e Inteligencia Artificial:

Ética Estudiantil, Gobernanza Digital y Autonomía

Por: Mtra. Claudia I. Llanos Argüello.

¿Formar o delegar? Autonomía Universitaria, Inteligencia Artificial y Crisis de Autoría Académica.



Me es grato escribir algunas líneas al respecto de este tema, ya que hemos estado en los últimos años, inmersos en la era de la inmediatez, lo que ha provocado a mi parecer, que nuestro aparato crítico este adormilado ante la tentación de que un chat con Inteligencia Artificial redacte por uno las ideas que quisiera transmitir.

En primer lugar, no podría decir que el avance de la tecnología y su uso son malos o indebidos o que deberían limitarse, ya que en su generalidad, el empleo de los desarrollos en todos los ámbitos y sectores siempre buscan una mejora que se ve reflejada en los procesos, ahorro de tiempo, mejora de resultados y una productividad mayor, en el entendido de que permite procesar una cantidad de información que humanamente sería imposible, sin que esto signifique que lo artesanal no tenga su importancia y que los procesos tradicionales no sigan siendo válidos, puesto que la Inteligencia Artificial Generativa no puede ni debe sustituir al ser humano, para mí esa debe ser siempre la premisa.

Otro beneficio relevante es que el uso de sistemas como el de IAG democratizan el conocimiento, es decir, permiten que personas de distintos contextos socioeconómicos accedan a tutorías personalizadas, traducciones automáticas, generación de contenidos y asistencia técnica especializada. En este sentido, la tecnología puede funcionar como un mecanismo de inclusión digital, reduciendo barreras de acceso a información compleja y favoreciendo procesos de aprendizaje continuo.

Sin embargo, el uso de la Inteligencia Artificial también conlleva riesgos significativos. Uno de los principales es la afectación a la privacidad y la protección de datos personales; muchos sistemas de IA se alimentan de grandes volúmenes de información, lo que puede generar vulnerabilidades en el tratamiento de datos sensibles. A ello se suma el riesgo de sesgos algorítmicos, que pueden reproducir o amplificar discriminaciones existentes en función de género, origen étnico, condición socioeconómica o ideología, entre otros.

Se adiciona a lo anterior, el riesgo de dependencia tecnológica y el de desplazamiento laboral, debido a que la automatización de procesos puede sustituir empleos tradicionales sin que necesariamente se generen alternativas inmediatas, obligando a replantear modelos de capacitación y reconversión profesional que muchas veces no son del interés de quien es patrón y bueno finalmente, la proliferación de contenidos generados por IA —incluidos los llamados deepfakes— que plantea desafíos en materia de desinformación, manipulación de la opinión pública y erosión de la confianza social.

Como podemos observar son un buen número de retos a vencer a la hora de hablar del uso de la Inteligencia Artificial, de manera general por lo que trasladarlo a una Institución de Educación Superior, cualquiera que esta sea, abre un debate interesante, debido a que la transformación digital en su interior, no constituye un fenómeno meramente instrumental ni una etapa tecnológica más en la evolución educativa, sino una mutación estructural del ecosistema universitario, que impacta simultáneamente en la producción de conocimiento, pero también en los procesos de enseñanza, los modelos de evaluación, la gestión institucional y la configuración ética del sujeto universitario, situaciones que no son menores pues hay que replantear los modelos, técnicas y procesos tradicionales para lograr salir de la caja y alcanzar la realidad actual, es decir una reconfiguración total. En este marco, la incorporación de Inteligencia Artificial (IA), analítica de datos y plataformas digitales no solo plantea desafíos pedagógicos, sino también dilemas que impactan las esferas constitucionales y éticas.

Las Instituciones de Educación Superior (IES), como entes históricos de producción y transmisión del conocimiento, han experimentado una mutación profunda en el contexto del entorno digital y más ahora con la expansión de plataformas virtuales, sistemas de gestión del aprendizaje y herramientas de inteligencia artificial puesto que han traído como consecuencia una redefinición de los procesos formativos y administrativos.

Puedo afirmar que, en el ámbito universitario, la Inteligencia Artificial Generativa (IAG) representa una herramienta con enorme potencial transformador que trae aparejados beneficios que no podemos evitar ver y querer como podrían destacarse, la personalización del aprendizaje capaz de adaptarse al ritmo, estilo y necesidades de cada estudiante, proporcionando retroalimentación inmediata y recursos complementarios específicos lo que favorecería procesos formativos más inclusivos y eficientes, hablando de la planta académica la IAG puede apoyar en actividades como la evaluación automatizada, el diseño de contenidos, el análisis de desempeño académico y la detección temprana de rezago o abandono escolar. Desde el lado, de la investigación, la IAG podría ser una herramienta de apoyo que facilitaría el análisis masivo de datos, la identificación de patrones complejos y la revisión automatizada de literatura científica, lo que permitiría a un investigador acelerar sus procesos de descubrimiento fortaleciendo su producción académica. Y bueno hablando de la administración central de una IES, podría ser utilizada para optimizar la gestión universitaria mediante sistemas predictivos que mejoren la asignación de recursos, la planeación institucional, la optimización de sus procesos y la toma de decisiones estratégicas.

No obstante, no todo es color de rosa por supuesto y los riesgos en el entorno universitario son igualmente relevantes y tampoco podemos omitirlos de esta lectura. Uno de los principales y del que se han hecho foros y charlas en sinnúmero de sedes universitarias en los últimos dos años aproximadamente, es la posible afectación a la integridad académica, de la producción científica y cultural universitaria, esto debido a que el uso indiscriminado de herramientas generativas puede fomentar el uso indebido de obras o mejor conocido como plagio, la simulación de aprendizaje o la pérdida de habilidades críticas como la argumentación, la investigación autónoma y la escritura analítica, por lo que académicos de todas las áreas del conocimiento nos vemos obligados a replantear los modelos de enseñanza y de evaluación, evitando satanizar a las herramientas pero si haciendo un trabajo de sensibilización al estudiantado, para procurar fortalecer la formación ética en el uso responsable de la tecnología, cualquiera que esta sea.

La brecha digital entre estudiantes con distinto acceso a recursos tecnológicos avanzados, es un tema que también preocupa debido a que podría profundizar desigualdades existentes. No es unicamente de conectividad, sino un fenómeno estructural que incide directamente en la calidad del aprendizaje, la autonomía intelectual y las oportunidades futuras, si lo vemos en el contexto actual, donde herramientas basadas en Inteligencia Artificial, bases de datos especializadas, software de análisis y plataformas colaborativas forman parte del ecosistema educativo, quienes carecen de dispositivos adecuados, acceso estable a internet o alfabetización digital avanzada parten de una desventaja acumulativa. Esta disparidad no solo limita la adquisición de competencias técnicas, sino que podría afectar la capacidad crítica, la producción académica y la inserción en entornos profesionales cada vez más digitalizados. Por último, si hablamos desde una perspectiva institucional, el uso de IA implica desafíos en materia de gobernanza de datos, transparencia algorítmica y responsabilidad ante decisiones automatizadas que afecten trayectorias académicas.

En consecuencia, mi opinión es que el debate no debe centrarse en la aceptación o rechazo de tecnologías como lo es la Inteligencia Artificial, sino en el diseño de marcos normativos, éticos y pedagógicos que permitan maximizar sus beneficios y mitigar sus riesgos. En el contexto universitario, esto implica integrar la alfabetización digital crítica como parte esencial de la formación profesional, garantizando que la IA sea una herramienta de fortalecimiento del conocimiento y no un sustituto acrítico del pensamiento humano.

Para el caso de la Universidad Nacional Autónoma de México (UNAM), en México, representa un caso paradigmático debido a su tamaño, su autonomía constitucional y su papel histórico en la democratización del conocimiento, y no solo eso sino también debido a la manera en que esta institución trabaja la gobernanza digital, y donde está muy consciente que su manera de abordar estos temas, tendrá efectos normativos y simbólicos regionales, debido a que su actuar es replicado a nivel Latinoamérica por las demás universidades.

Debido a esto es importante tener mucho cuidado sobre los pasos que se vayan dando sin que esto signifique quedarse estáticos, ya que nosotros como parte de esta comunidad debemos impulsar a que las universidades transiten hacia un modelo de gobernanza algorítmica participativa, en el que la regulación del uso de IA por parte del estudiantado se base en principios de autonomía, integridad académica, proporcionalidad y justicia distributiva.

Para el caso de las IES públicas en su generalidad, y en particular el de la UNAM, se resalta la idea de que no son únicamente una entidad educativa, sino una institución constitucionalizada, basada en el reconocimiento de la autonomía, su rol como motor de desarrollo social y su financiamiento por parte del Estado, frecuentemente blindados a nivel constitucional o mediante leyes de rango constitucional. Tal es el caso de la autonomía universitaria de la UNAM que es reconocida y que implica capacidad normativa interna, autogobierno y libertad de cátedra señalados en su Ley Orgánica. Sin embargo, esta autonomía no excluye la transformación digital; por el contrario, exige que la universidad diseñe su propio modelo de integración tecnológica conforme a sus principios fundacionales.

Ahora bien, la pregunta a realizarse es ¿qué ha hecho la UNAM, en estos temas?, bueno, ha adoptado un enfoque proactivo y plural para incorporar la inteligencia artificial en sus procesos académicos, a nivel organizativo se han creado espacios institucionales dedicados al estudio, experimentación y evaluación de la IA: entre ellos figuran laboratorios especializados (por ejemplo, el Laboratorio de Inteligencia Artificial, Información y Datos del IIBI) y grupos académicos centrados en la IA generativa que organizan jornadas, cursos y redes de colaboración para difundir buenas prácticas. Estas instancias no solo fomentan la innovación técnica, sino que promueven la reflexión crítica sobre los efectos sociales de la tecnología. En el terreno educativo, la UNAM ha publicado lineamientos y guías dirigidas a profesorado y estudiantado para el uso responsable de herramientas generativas. Documentos institucionales (recomendaciones pedagógicas y guías para estudiantes) señalan que la IAG debe emplearse como herramienta de apoyo —no como sustituto del trabajo intelectual— y recomiendan prácticas concretas: declarar el uso de IA en entregables, contrastar información con fuentes verificadas, y diseñar actividades de evaluación que privilegien la producción original y el razonamiento crítico. Estas guías evidencian que la Universidad busca integrar la IAG sin sacrificar la rigurosidad académica. En investigación y validación científica, la UNAM combina capacidades de cómputo con controles metodológicos para evitar sesgos y sobreconfianza en modelos automáticos. Iniciativas como la afiliación de laboratorios a metodologías de evaluación (por ejemplo, Z-inspection® para la auditoría holística de sistemas de IA) muestran un interés explícito por evaluar la fiabilidad técnica y los riesgos éticos en cada etapa del ciclo de vida de los proyectos. También, la Universidad también mantiene mesas y conversatorios sobre ética e IA para enlazar recomendaciones globales como las de la UNESCO con criterios locales de transparencia y responsabilidad.

Por último, siempre es necesario comentar que la Universidad Nacional Autónoma de México (UNAM) ha reconocido que, junto a beneficios como los que ya detallamos, también existen retos significativos relacionados con el uso responsable por parte de estudiantes e investigadores; y que entre los desafíos más visibles está la superación del desconocimiento y el temor que aún rodea el funcionamiento de estas herramientas, lo cual puede llevar a un uso superficial o improductivo de la tecnología si no se acompaña de formación sólida y acompañamiento pedagógico, la fuerte posibilidad de que estudiantes deleguen en la máquina tareas que requieren pensamiento profundo, debilitando el desarrollo de habilidades críticas si no se diseña con claridad el propósito educativo de su uso.

Asimismo, la existencia de desafíos éticos y de evaluación académica: tanto docentes como investigadores enfrentan la necesidad de diferenciar el trabajo genuino del producido parcialmente con IA, lo que exige como ya mencioné, nuevos criterios de evaluación y estrategias pedagógicas que reconozcan el rol de estos sistemas sin permitir prácticas de plagio o sustitución de procesos cognitivos propios. El reto de garantizar la equidad en el acceso y la alfabetización digital entre la comunidad estudiantil, ha sido abatida por la UNAM promoviendo espacios como el Grupo Académico de Inteligencia Artificial Generativa (GAIA-GEN), cursos masivos abiertos en línea (MOOCs) como IA generativa en el aula,

recursos formativos especializados y guías para docentes y estudiantes diseñadas para orientar el uso pedagógico y ético de la IA. A pesar de que estas iniciativas buscan capacitar a la comunidad universitaria, fomentar una adopción crítica y pedagógicamente informada de las tecnologías, y alinear su uso con los principios de rigor científico, integridad académica y respeto a los derechos de autor y a la privacidad de datos no significa que sea una actividad acabada sino que debemos verla como trabajo y actualización constante pues los diversos desarrollos que contienen inmersa la IAG son vastos y se van moviendo con una rapidez que es difícil alcanzar y que nos obliga ir modificando y adecuando los criterios a su alrededor de manera constante; los retos de la UNAM también se reflejan en el contexto de la investigación ya que mientras la IA puede acelerar procesos analíticos y abrir nuevas líneas de exploración científica, los investigadores deben balancear la eficiencia que aporta la IA con la necesidad de transparencia metodológica, control de sesgos algorítmicos y validación humana de resultados, de manera que el conocimiento generado conserve su calidad y confianza.

CONCLUSIONES

En definitiva, la Inteligencia Artificial no constituye una amenaza en sí misma para la universidad pública, sino una prueba de su madurez institucional. El verdadero riesgo no radica en su existencia, sino en su adopción acrítica o en su prohibición reactiva. Para una institución como la UNAM, cuya autonomía no es privilegio sino responsabilidad histórica, el desafío consiste en demostrar que es posible integrar innovación tecnológica sin abdicar del rigor académico, la formación ética ni la justicia social. Formar sin delegar, innovar sin sustituir, regular sin censurar: ahí se juega el futuro de la universidad en la era algorítmica.

La discusión sobre Inteligencia Artificial en las IES públicas revela que la autonomía universitaria ya no puede entenderse únicamente como autogobierno administrativo o libertad de cátedra, sino también como capacidad de gobernanza digital. En este nuevo escenario, la UNAM y las universidades públicas están llamadas a diseñar marcos propios de regulación, evaluación y uso ético de la IA que respondan a su misión social. No se trata de delegar la producción del conocimiento a sistemas automatizados, sino de formar sujetos capaces de dialogar críticamente con ellos. La universidad que preserve su autonomía será aquella que, frente al algoritmo, no renuncie a su función formadora ni a su responsabilidad pública.

Y, por último, es que si algo debe quedar claro es que la discusión sobre Inteligencia Artificial no es meramente tecnológica, sino profundamente humana. La crisis de autoría académica, la brecha digital y los dilemas de evaluación no son problemas técnicos aislados, sino síntomas de una transformación cultural más amplia. En este contexto, el centro no debe ser la herramienta, sino el sujeto universitario: su capacidad de pensar, cuestionar, crear y asumir responsabilidad ética por su producción intelectual. La universidad pública del siglo XXI no puede formar operadores de sistemas, sino ciudadanos críticos capaces de utilizar la inteligencia artificial sin convertirse en dependientes de ella.

MTRA. CLAUDIA I. LLANOS ARGÜELLO

Directora Legal Propiedad Intelectual y Transferencia de Tecnología para la UNAM y Profesora de Propiedad Intelectual en División de Estudios de Posgrado de la Facultad de Derecho UNAM. Coordinadora Comisión de Vinculación Universitaria de la AMDTech.

De la Dispersión a la Homologación.

El Nuevo Estándar Transversal de Valoración de Evidencias Digitales en México

Por: Lic. David Pizaña Rito.

Introducción

La valoración de evidencias digitales en el sistema jurídico mexicano transitó, durante más de dos décadas, por un escenario de dispersión normativa. Materias como la Mercantil, Fiscal, Administrativa, Financiera y de Propiedad Intelectual desarrollaron lineamientos propios para el reconocimiento de información en medios electrónicos, mientras que otras carecían por completo de disposiciones específicas.

Los litigantes fundamentaban sus argumentos exclusivamente desde la ley especial de cada materia, y los órganos jurisdiccionales valoraban sin un estándar transversal, produciendo criterios dispares ante evidencias de naturaleza similar. Si bien ordenamientos como el Código de Comercio incorporaron desde hace más de veinticinco años principios para la valoración de evidencias digitales, la ausencia de un criterio unificador dejaba lagunas significativas.

El decreto publicado en el Diario Oficial de la Federación el 14 de noviembre de 2025, mediante el cual se reforman sesenta y ocho ordenamientos legales federales, constituye la respuesta institucional a esta fragmentación. En materia de evidencias digitales, el decreto homologa el criterio de valoración remitiéndolo a los artículos 348, 349 y 350 del Código Nacional de Procedimientos Civiles y Familiares (CNPCyF).

El presente artículo analiza el alcance de esta homologación, los mecanismos a través de los cuales opera, y las herramientas técnicas y tecnológicas que los profesionales del derecho deben conocer para su aplicación efectiva.

1 El panorama previo de dispersión normativa y lagunas

Previo al decreto, el panorama normativo se caracterizaba por una marcada asimetría respecto a la admisión y valoración de pruebas en medios electrónicos. Ordenamientos como el Código de Comercio, el Código Fiscal de la Federación y la Ley Federal de Procedimiento Contencioso Administrativo incorporaban disposiciones para la valoración de información electrónica, cada uno con criterios propios. La materia financiera contaba con lineamientos particulares a través de diversas leyes sectoriales. Sin embargo, estos marcos funcionaban de forma aislada, sin articulación entre sí. Frente a ellos, ámbitos como el derecho familiar, la propiedad intelectual o la protección de datos personales carecían por completo de criterios expresos, generando que la admisibilidad y el valor de una misma evidencia digital variaran según la materia, no por su naturaleza intrínseca ni por su confiabilidad técnica, sino por la existencia o inexistencia de disposiciones en el ordenamiento aplicable.

El marco jurídico mexicano ya contemplaba los principios esenciales de fiabilidad, integridad, atribución y equivalencia funcional, pero la ausencia de un criterio unificador impedía que trascendieran el ámbito de cada ordenamiento particular. El resultado era un sistema fragmentado donde la experiencia acumulada durante décadas no lograba articularse en un estándar coherente, dejando a la práctica forense sin un marco común que respondiera a la realidad transversal del uso de tecnologías digitales.

2 El alcance y mecánica del decreto de homologación

El decreto del 14 de noviembre de 2025 modifica sesenta y ocho ordenamientos legales federales. Si bien su alcance abarca múltiples áreas del derecho, en lo que concierne a la valoración de evidencias digitales opera a través de tres vías diferenciadas que configuran un sistema de homologación que permea la totalidad del orden jurídico federal.

La primera vía es la homologación directa, la cual se refiere a los ordenamientos reformados para remitir expresamente a los artículos 348, 349 y 350 del CNPCyF. Entre ellos, el Código de Comercio (arts. 1054, 1061 Bis y 1063), el Código Fiscal de la Federación (art. 130), la Ley Federal de Procedimiento Contencioso Administrativo (arts. 10 y 46) y la Ley Federal para el Control de Sustancias Químicas Susceptibles de Desviar para la Fabricación de Armas Químicas (arts. 4 y 71).

La segunda vía opera mediante la supletoriedad del CNPCyF, extendiendo la homologación a materias que carecían de referente normativo como eran la Ley Federal de Protección a la Propiedad Industrial (art. 3), Ley Federal del Derecho de Autor (arts. 10 y 213), leyes de protección de datos personales, Ley de Firma Electrónica Avanzada (art. 6), Ley Federal de Procedimiento Administrativo (art. 2) y Ley de Navegación y Comercio Marítimos (arts. 6 y 264).

La tercera vía se configura por remisión específica en materia de pruebas en el sector financiero, Ley de Instituciones de Crédito, Ley del Mercado de Valores, Ley para Regular las Instituciones de Tecnología Financiera, Ley de Ahorro y Crédito Popular, Ley de Fondos de Inversión, Ley de Instituciones de Seguros y de Fianzas, entre otras.

Es fundamental subrayar que el decreto no crea principios nuevos, sino que homologa los existentes bajo un criterio unificado. Los conceptos de fiabilidad, integridad, atribución y equivalencia funcional encuentran ahora en los artículos 348, 349 y 350 su punto de convergencia normativa, configurando un mecanismo de tres vertientes que garantiza que ninguna materia federal quede al margen de un criterio común.

3 El estándar unificado de valoración en los artículos 348, 349 y 350

El estándar unificado se articula en tres disposiciones que conforman un sistema integral como es el reconocimiento de la información en medios electrónicos como prueba, los criterios para valorar su fuerza probatoria y las condiciones de integridad que garantizan su confiabilidad.

El artículo 348 reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos, digitales, en una cadena de bloques o en cualquier otra tecnología. La expresión “o en cualquier otra tecnología” refleja un enfoque de neutralidad tecnológica que permite incorporar desarrollos futuros sin reformas adicionales. Este artículo resuelve la cuestión de la admisibilidad de la información en cualquier medio electrónico, la cual es por mandato legal, un medio de prueba reconocido en todas las materias alcanzadas por la homologación.

El artículo 349 establece los parámetros para valorar la fuerza probatoria de dicha información, como es la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada; la posibilidad de atribuir a las personas obligadas el contenido y la accesibilidad para ulterior consulta. Estos tres parámetros configuran un criterio concurrente de valoración. En el plano práctico, el requisito de fiabilidad del método encuentra un referente técnico fundamental en la NOM-151-SCFI-2016, norma oficial mexicana que establece los requisitos para la conservación de mensajes de datos y la digitalización de documentos. La NOM-151 define los estándares que un Prestador de Servicios de Certificación (PSC) debe cumplir para garantizar la integridad, autenticidad y disponibilidad de la información en medios electrónicos a lo largo del tiempo. Para los profesionales del derecho, esta norma constituye el puente entre el requisito legal del artículo 349 y su materialización técnica: una evidencia digital conservada conforme a la NOM-151 cuenta con un respaldo objetivo que fortalece su fiabilidad ante cualquier órgano jurisdiccional.

El artículo 350 aborda la integridad y el tratamiento probatorio de la cadena de bloques (blockchain). En su primer supuesto, cuando la ley requiera que un documento sea conservado en su forma original, el requisito queda satisfecho si la información se ha mantenido íntegra e inalterada desde su forma definitiva y es accesible para consulta ulterior. En su segundo supuesto, otorga a la información contenida en cadena de bloques el valor de prueba plena, que representa el máximo valor probatorio que la legislación procesal reconoce, siempre que no existan circunstancias fehacientes de vulneración o manipulación. Esto obedece a que las características intrínsecas de la tecnología blockchain, su arquitectura descentralizada y distribuida, sus métodos de consenso, cifrado y su diseño orientado a evitar la modificación no autorizada, tal como el propio CNPCyF la define en su artículo 3, fracción VII, hacen que la información allí registrada satisfaga, por su propia naturaleza, los requisitos de fiabilidad, integridad y trazabilidad. Los profesionales del derecho deben comprender que la blockchain no es una tecnología ajena a su ejercicio, ya que es a partir de esta reforma, el medio probatorio digital más robusto reconocido por la ley, y su conocimiento resulta indispensable para el diseño de estrategias probatorias eficaces en el entorno digital.

4 Los principios rectores y la nueva dimensión de los acuerdos digitales

La homologación impacta de manera directa la práctica jurídica, al imponer que quienes ejercen el derecho adopten y apliquen como base los principios rectores del CNPCyF. El principio de equivalencia funcional (art. 936) establece que la información en un mensaje de datos tiene la misma eficacia probatoria que la contenida en documentos impresos; la firma electrónica avanzada satisface el requisito de firma autógrafa, y ninguna autoridad puede negar efectos jurídicos a información por estar en un medio electrónico. El principio de no discriminación de mensajes de datos (art. 936, fracc. I, y art. 347) complementa lo anterior, no se negarán efectos jurídicos a información por la sola razón de estar contenida en un mensaje de datos, siempre que se haya generado, archivado o conservado en un medio fiable.

El principio de neutralidad tecnológica (art. 937) dispone que el CNPCyF no impone preferencias en favor o en contra de determinada tecnología, garantizando que el estándar mantenga vigencia ante la evolución tecnológica. Los principios de fiabilidad y atribución (art. 349) y de integridad (art. 350 y art. 3, fracc. XXIII) completan el marco, y encuentran sus herramientas de materialización más sólidas en la conservación conforme a la NOM-151 y en el registro en blockchain: la NOM-151 como estándar técnico de conservación certificada que respalda la fiabilidad del método y la cadena de bloques como tecnología que satisface los requisitos de integridad con la máxima fuerza probatoria reconocida por la ley.

Estos cinco principios obligan a replantear la visión del contrato formal como único instrumento generador de derechos y obligaciones exigibles. Los acuerdos celebrados a través de mensajería instantánea, correo electrónico, plataformas digitales y redes sociales constituyen medios idóneos para la creación de derechos cuyo cumplimiento puede ser exigido judicialmente, siempre que las evidencias digitales cumplan los requisitos de fiabilidad, atribución, integridad y accesibilidad. El criterio homologado confirma que la vía por la que se expresó la voluntad como lo puede ser un contrato digital, una cadena de mensajes de WhatsApp, un intercambio de correos electrónicos o una transacción en plataforma digital, no determina por sí misma su validez probatoria; lo que la determina es el cumplimiento de los principios que ahora rigen transversalmente.

Conclusiones

El decreto del 14 de noviembre de 2025 marca el tránsito de la dispersión normativa a la homologación transversal.

No introduce nuevos principios, sino que los unifica bajo un estándar articulado en los artículos 348, 349 y 350 del CNPCyF. Las tres vías de alcance probatorio garantizan que prácticamente ninguna materia federal quede al margen de este criterio. Los cinco principios rectores como son equivalencia funcional, no discriminación de mensajes de datos, neutralidad tecnológica, fiabilidad y atribución, e integridad, conforman el marco bajo el cual toda evidencia digital debe ser valorada.

Su aplicación efectiva exige que los profesionales del derecho no solo conozcan el fundamento legal, sino también las herramientas que materializan estos principios: la NOM-151, en tanto estándar de conservación certificada que respalda la fiabilidad del método y la cadena de bloques como la tecnología a la que el legislador otorgó expresamente el valor de prueba plena. La visión del contrato como único instrumento generador de derechos debe ampliarse hacia los acuerdos digitales. La entrada en vigor gradual del CNPCyF, con plazo máximo al 1º de abril de 2027, ofrece la ventana para que los operadores jurídicos internalicen estos principios, se familiaricen con la normativa técnica y comprendan el alcance probatorio de las tecnologías emergentes. El estándar transversal no admite ya la valoración desde la exclusiva óptica de la ley especial de la materia; exige certeza jurídica uniforme para quienes ofrecen estas pruebas y para quienes las valoran.

Bibliografía

Código Nacional de Procedimientos Civiles y Familiares [CNPCyF]. Arts. 3, 308, 335, 347, 348, 349, 350, 936 y 937. Diario Oficial de la Federación, última reforma 15 de enero de 2026 (México).
Decreto por el que se reforman, adicionan y derogan diversas disposiciones de sesenta y ocho ordenamientos legales federales. Diario Oficial de la Federación, 14 de noviembre de 2025 (México).
Código de Comercio. Arts. 1054, 1061 Bis y 1063. Diario Oficial de la Federación, última reforma 14 de noviembre de 2025 (México).
Código Fiscal de la Federación. Art. 130. Diario Oficial de la Federación, última reforma 14 de noviembre de 2025 (México).
Ley Federal de Procedimiento Contencioso Administrativo. Arts. 10 y 46. Diario Oficial de la Federación, última reforma 14 de noviembre de 2025 (México).
Norma Oficial Mexicana NOM-151-SCFI-2016. Prácticas comerciales — Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos. Diario Oficial de la Federación (México).

LIC. DAVID PIZAÑA RITO

Abogado y Empresario Especializado en Tecnología, Propiedad Intelectual e Inteligencia Artificial. Coordinador de Operaciones de la AMDTech.

¡HAZTE MIEMBRO DE

AMDTech®

ACADEMIA MEXICANA DE DERECHO DIGITAL Y TECNOLÓGICO, AC

y recibe grandes beneficios!

- **Descuento del 40%** en nuestros cursos, eventos y seminarios abiertos al público en general.
- **Capacitación y eventos gratuitos** exclusivos para la membresía.
- **Recepción y posibilidad de ser articulista** de la Revista Digital IBLATAM.
- **Posibilidad de representar a la AMDTech** y al sector en foros nacionales e internacionales en la materia.
- **Networking** con distinguidos actores de la industria.
- **Beca** del 20% sobre el pago de inscripciones y beca del 10% sobre el pago de colegiaturas a los miembros afiliados y empleados de "AMDTech" así como a sus familiares en línea directa en los niveles **de posgrado, así como en diplomados y talleres**, en los diversos campos del Instituto de Especialización para Ejecutivos (IEE).
- **Ópticas Lux otorga en pago de contado un 15% de descuento** en anteojo graduado, lentes de contacto, anteojos solares y auxiliares auditivos a los miembros afiliados de "AMDTech".

Hazte miembro, es gratis.

Conoce más detalles: amdtech.mx

AMDTech amdtechmx @AMDTechMx AMDTech, A.C.

Los Mejores TECHNOLAWYERS y Especialistas Digitales de Iberoamérica 2024

Nombre	Profesión	País
Alda Rodríguez	Abogada	Andorra
Claudia Alonso	Abogada	Andorra
Diana Garmón	Administradora	Andorra
Jennifer Rubio	Abogada	Andorra
Jonathan Hinkson	Abogado	Andorra
Oriol Giró	Abogado	Andorra
Pau Augé	Abogado	Andorra
Pere Cristofol	Abogado	Andorra
Víctor Rosello	Abogado	Andorra
Ariel J. Ibáñez	Abogado	Argentina
David Mielnik	Abogado	Argentina
Daniel Monastersky	Abogado	Argentina
Ezequiel Braun Pellegrini	Abogado	Argentina
Gustavo Ariel Atta	Abogado	Argentina
J. Darío Veltani	Abogado	Argentina
Juan Pablo Gallego	Abogado	Argentina
María Raquel Burgueño	Abogada	Argentina
Matías Santiago Vallejos	Consultor /Abogado	Argentina
Mónica Fernández Campero	Abogada	Argentina
Pablo Balancini	Contador	Argentina
Roberto Arturo Docimo	Abogado	Argentina
Romina Iannello	Abogada	Argentina
Mariana Avilés Roja	Abogada	Bolivia
Ana Paula Martínez	Abogada	Brasil
Caroline Teófilo	Abogada	Brasil
Daniela Cristina Ito	Abogada	Brasil
Daniela Lin	Abogada	Brasil
David Britain	Licenciado en Economía	Brasil
Harry Duran	Analista	Brasil
Henrique Rocha	Abogado	Brasil
Isa Gabriela Stefano	Abogada	Brasil
Jamila Venturini	Periodista	Brasil
Leandro Bissoli	Abogado	Brasil
Leticia Gerard Tavares Málaga	Abogada	Brasil
Luana Cristina Romero de Souza	Licenciada en Ciencias Contables	Brasil
Patricia Peck Pinheiro	Abogada	Brasil
Rómulo Pinheiro	Abogado	Brasil
Washington Fonseca	Abogado	Brasil
Alberto Pulido A	Abogado	Chile
Andrés Jara	Abogado	Chile
Antonia San Martín Sola	Ingeniera Comercial	Chile
Eduardo Esclona	Abogado	Chile

Juan Carlos Lara Gálvez	Abogado	Chile
Katherina Canales Madrid	Abogada	Chile
Paula Jaramillo	Abogada	Chile
Ignacio Canals	Emprendedor	Chile
Adriana Peñaranda	Abogada	Colombia
Catalina Castellanos Rubio	Abogada	Colombia
David Andrés Zambrano Méndez	Abogado	Colombia
Efrén Porras	Abogado	Colombia
Jacobo A. González Cortés	Abogado	Colombia
Jhohan Sanabri De Luque	Abogado	Colombia
José Antonio Pulido Murcia	Diseñador	Colombia
José Fernando Torres Varela	Abogado	Colombia
Juan David Cardona Pérez	Abogado	Colombia
Juan Felipe Torres	Abogado	Colombia
Juan Manuel Pacheco	Abogado	Colombia
Juan Nicolás Laverde	Abogado	Colombia
Marcil Ortiz	Abogado	Colombia
Natalia Ospina Díaz	Abogada	Colombia
Nicolle Rojas Tamayo	Abogado	Colombia
Rafael H. Gamboa Bernate	Abogado	Colombia
Sergio Michelson Jaramillo	Abogado	Colombia
Adrián Obando	Abogado	Costa Rica
Alex Thompson	Abogado	Costa Rica
Alexander Cortés	Abogado	Costa Rica
Augusto R. Arce	Abogado	Costa Rica
Carlos Solan	Abogado	Costa Rica
Christine Brown Ledezma	Mercadóloga	Costa Rica
Eugenia Vízquez Rodríguez	Abogada	Costa Rica
Juan Esteban Durango	Abogado	Costa Rica
Rodrigo Castro	Abogado	Costa Rica
María Encalada	Ingeniera	Ecuador
María Gabriela Galeas Castrillón	Abogada	Ecuador
Martín Burbano de Lara	Abogado	Ecuador
Nicolás Castillo Castelo	Abogado	Ecuador
Oscar Montezuma Panez	Analista	Ecuador
Rafael Bonifaz	Administrador	Ecuador
Sofía Vintimilla	Abogada	Ecuador
Marta Cadavid	Contadora	Estados Unidos
Gerardo Cuchillas	Abogado	El Salvador
Ingrid Gamboa Rozo	Ciencias Políticas y Gobierno	Guatemala
Luis Abundio Maldonado	Abogado	Guatemala
Pablo Cordón Barrientos	Administrador de Negocios	Guatemala
Aimed Pimentel	Licenciada en Informática	México
Alejandra Lagunes Soto Ruiz	Lic. en Ciencias de la Comunicación	México

Alejandro Celorio Alcántara	Abogado	México
Alejandro Galván Illanes	Abogado	México
Alexei Pinal	Ing. en Comunicaciones y Elect.	México
Alfredo Bazúa Witte	Abogado	México
Alfredo Reyes Krafft	Abogado	México
Aline Arbesú Ovín	Abogada	México
Amando Mastachi Aguario	Abogado	México
Ana Claudina García Allende	Abogada	México
Ana Teresa Sáenz Hernández	Lic. en Relaciones Internacionales	México
Andrés Velázquez Olavarrieta	Ing. en Ciber. y Sist. de Cómputo	México
Ángel Sumano Correa	Abogado	México
Begoña Cancino Garín	Abogada	México
Berenice Dávalos	Abogada	México
Bernardo Álvarez del Castillo Vargas	Abogado	México
Bernardo Fernández del Castillo Quintana	Abogado	México
Carlos Alberto Pérez Macías	Abogado	México
Carlos Pérez de la Sierra	Abogado	México
Carlos David Pérez Retes	Abogado	México
Carlos Mora Villalpando	Abogado	México
Carlos Roberto García Ángeles	Abogado	México
Carlos Valderrama Narváez	Abogado	México
Carmen Calderón Infante	Lic. en C. Políticas y Admin. Pública	México
Cesar Augusto Giovenile López	Ing. en Tel. Sistemas y Electrónica	México
Christian Paredes González	Abogado	México
Ciro Humberto Ortiz Estrada	Ingeniero Químico Industrial	México
Claudia Alin Escoto Velázquez	Lic. en C. de la Com. C. Políticas y Gob.	México
Claudia I. Llanos Argüello	Abogada	México
Claudia Gabriela González Morón	Abogada	México
Cynthia Gabriela Solís Arredondo	Abogada	México
Daniel Ackerman	Abogado	México
Daniel Martínez Serrano	Abogado	México
Daniel Quintero Chávez	Abogado	México
Daniel Sánchez y Bejar	Abogado	México
Danixa Fabiola Chavero Ramírez	Abogada	México
David Enrique Merino Téllez	Abogado	México
David Pizaña Rito	Abogado	México
Diana Peza Iniestra	Abogada	México
Diego Ramos Castillo	Abogado	México
Dulce María Cipatli Naranjo Sánchez	Abogada	México
Dulcina Álvarez Domínguez	Abogada	México
Edgar L. Espejel	Abogado	México
Eduardo Manuel Ruiz Orozco Pérez	Abogado	México
Elena Estavillo	Licenciada en Economía	México

Elier Cruz	Ingeniero	México
Elizabeth Argüello Maya	Economista	México
Eloísa Cadenas Morales	Ingeniera	México
Elsa Bibiana Peralta Hernández	Abogada	México
Edgar Salinas	Lic. en Ciencias de la Comunicación	México
Edgar Sandoval Monroy	Ingeniero	México
Eileen Matus Calleros	Abogada	México
Erick Tavares Robledo	Abogado	México
Erika Mata Sánchez	Ciberseguridad	México
Ernesto Ibarra Sánchez	Abogado	México
Ernesto López Medina	Abogado	México
Etienne Luquet Farías	Abogado	México
Faviola Martínez Juárez	Lic. en Ciencias de la Informática	México
Federico Hernández Arroyo	Abogado	México
Fernando Caballero	Ciberseguridad	México
Francisco Javier Careaga Franco	Abogado	México
Geraldine Loaeza	Abogada	México
Gerardo Ambrosio González	Abogado	México
Gina Gallegos García	Ingeniera	México
Gonzalo Manuel Araujo Cabarcas	Licenciado en Ciencias	México
Graciela Castro González	Abogada	México
Graciela Robles Espinosa	Abogada	México
Guillermo Amezcua	Licenciado en Administración	México
Guillermo Ucha Cabadas	Abogado	México
Gustavo Guillén	Ingeniero en Sistemas y Abogado	México
Ignacio Bermeo Juárez	Abogado	México
Indira Rivero Alfaro	Abogada	México
Inna Makhniboroda	Abogada	México
Irving Gerardo Peña López	Lic. en Administración de Empresas	México
Isabel Davara Fernández de Marcos	Abogada	México
Itzú Martínez Calva	Abogada	México
Ivan Díaz González	Ingeniero en Sistemas y Abogado	México
Jacobo Apichoto Palermo	Abogado	México
Jaime Díaz Limón	Abogado	México
Jaime Olmos de la Cruz	Licenciado en Informática	México
Janet Huerta Estefan	Abogada	México
Javier Augusto Téllez Navarro	Abogado	México
Javier Joaquín López Casarín	Lic. en D. y en C. Política y Admin. P.	México
Javier Villanueva Walbey	Abogado	México
Jenny M.Hernández Rodríguez	Abogada	México
Jersain Z. Llamas Covarrubias	Abogado	México
Jerónimo Ocejo Torres	Abogado	México
Jesús Alfredo Ramírez Ramírez	Analista en Sistemas	México
Jesús Edmundo Coronado C.	Abogado	México

Jesús Roberto Briano Borunda	Ingeniero	México
Jimena Chi Barrales	Abogada	México
Joel A. Gómez Treviño	Abogado	México
Jonatan Elias Ojeda Serdan	Abogado	México
Jorge Andrés Cervantes Aguirre	Abogado	México
Jorge A. Claret C. Diego de Arribbas	Ing. en Cibernética y Computación	México
Jorge Fernando Negrete P.	Abogado	México
Jorge Maximino Cuahuey Santiago	Sistemas	México
Jorge Antonio Montiel Romero	Abogado	México
Jorge Munguía Hernández	Ingeniero	México
Jorge Tavares Robledo	Abogado	México
José Antonio Arochi de la Torre	Abogado	México
José Antonio Peña Merino	Lic. en C. Política y R. Internacionales	México
José Díaz Cuadra	Abogado	México
José Luis García Méndez	Ingeniero	México
José Manuel Magaña Rufino	Abogado	México
José Mario de la Garza Marroquín	Abogado	México
José Palomar Duclaud	Abogado	México
José Patricio González Granados	Abogado	México
José Renato Meléndez Galván	Ingeniero	México
Josel Hernández Barroso	Abogado	México
Juan Carlos Luna	Abogado	México
Juan Luis Hernández Conde	Abogado	México
Juana Cynthia Rojas Magaña	Ingeniera	México
Julia I. Rodríguez Morales	Ingeniera Industrial y de Sistemas	México
Julio Alejandro Durán Gómez	Abogado	México
Karla Islas	Química	México
Karla Ramírez García	Ingeniera Industrial y de Sistemas	México
Karla Verónica Ortiz Robles	Abogada	México
Kiyoshi Tsuru Alberú	Abogado	México
Laura Elena Herrera Bravo	Licenciada en Informática	México
Laura Lizette Enríquez Rodríguez	Licenciada en Ciencias Políticas	México
Leticia Stephanie Enríquez Valerio	Abogada	México
Ligia González Lozano	Abogada	México
Lorena Bravo	Ingeniera en Sistemas	México
Lourdes Mancillas Esquivel	Lic. en Administración de Empresas	México
Luis Alfonso Cervantes Rivera	Ingeniero en Finanzas	México
Luis Cárdenas Ibarra	Abogado	México
Luis Fernando Osuna Márquez	Abogado	México
Luis Javier Pérez del Real	Ingeniero Cibernético	México
Manuel Díaz Franco	Ingeniero	México
Manuel Pliego Ramos	Abogado	México
Marco V. Herrera	Ciencias de la Comunicación	México
Marcos Javier Rubio Molina	Abogado	México

María Ariza García Migoya	Ingeniera Industrial	México
María Elena Fernández González	Abogada	México
Mario Alberto Rodríguez Vargas	Abogado	México
Mariza De La Mora Mondragón	Abogada	México
Martha Ruth Celis Jiménez	Abogada	México
Martín Alejandro Levenson	Ingeniero	México
Mauricio Ocampo Villaseñor	Abogado	México
Miguel Pinodueñas Rodulfo	Abogado	México
Mireya Valverde Okón	Abogada	México
Mónica María Serralde Vera	Abogada	México
Natalia Mendoza Servín	Abogada	México
Nuhad Ponce Kuri	Abogada	México
Octavio de la Torre de Stéfano	Abogado	México
Odracir Ricardo Espinoza Valdez	Abogado	México
Oliver González Barrales	Ing. en Sistemas Computacionales	México
Omar Gabriel Soto Tabares	Abogado	México
Oscar Andrés Castillo Caamal	Abogado	México
Paola Rivera Zavala	Abogada	México
Paulo Magaña Rodríguez	Abogado	México
Patricia Ramírez	Abogada	México
Patricio González Granados	Abogado	México
Paulina Islas Huacuja	Abogada	México
Pepe Toriello Martínez	Abogado	México
Philippe Boulanger	Licenciado en Mercadotecnia	México
Raúl Valencia del Toro	Abogado	México
Raymundo Espinoza Hernández	Abogado	México
Ricardo Alkins Villarroel	Ingeniero	México
Ricardo Andrés Cacho García	Abogado	México
Roberto Arochi Escalante	Abogado	México
Rocío Yánez Pérez	Abogada	México
Rodolfo Enrique Martínez Gutiérrez	Abogado	México
Rodrigo Gómez Olivar	Lic. en Comunicación, Publi. y Mark.	México
Rosa Aidé Fabela Valdez	Abogada	México
Salma Leticia Jalife Villalón	Ingeniera en Computación	México
Salvador Camacho Hernández	Abogado	México
Salvador Mejía Álvarez	Abogado	México
Sergio F. Aguilar Montaño	Abogado	México
Shadia Ponce Kuri	Abogada	México
Sissi de la Peña	Ingeniera Civil	México
Valeria Amparano López	Abogada	México
Vanessa Díaz Rodríguez	Abogada	México
Vanessa Solís Caballero	Contadora	México
Wensllei José Sulbarán Matos	Ingeniero en Informática	México
Ximena Puente de la Mora	Abogada	México

Yaritza Rodelo García	Abogada	México
Alexander Mendoza	Contador	Panamá
Alexandra Ruiloba	Abogada	Panamá
Ana Graciela Medina	Abogada	Panamá
Celso Córdoba	Abogado	Panamá
David Sucre Levy	Abogado	Panamá
Gabriela Tejada de Britton	Abogada	Panamá
Juan Ramón Anria Jaén	Lic. en Ciencias Tecnológicas	Panamá
Lia Hernández Pérez	Abogada	Panamá
Mariela I. de la Guardia Oteiza	Abogada	Panamá
Moisés Iván Rivera A.	Abogado	Panamá
Abel Revoredo	Abogado	Perú
Erik Iriarte Ahon	Abogado	Perú
Diego Cabrera	Abogado	Perú
Francisco Gálvez Ruiz Huidobro	Abogado	Perú
Jessica Valdivia Amayo	Abogada	Perú
José Miguel Porto	Abogado	Perú
Mayra Alejandra Ariñez Vera	Abogada	Perú
Verónica Vergaray	Abogada	Perú
Joana Duarte	Abogada	Portugal
Madalena Barradas	Abogada	Portugal
Maria João Escudeiro	Abogada	Portugal
Teresa Delgado	Abogada	Portugal
Alejandro Guanes	Abogado	Uruguay
Alejandro Piera	Abogado	Uruguay
Carolina Bañales	Ingeniera	Uruguay
Fernando Heisecke	Abogado	Uruguay
Lucia Aguerre Cazes	Abogada	Uruguay
Alejandra Morilo	Abogado	Venezuela
Celis Guevara Wazzan	Abogado	Venezuela
Christ Villalobos	Abogada	Venezuela
José Luis Tamayo Rodríguez	Abogado	Venezuela
Marcelo Enriquez Díaz Cabral	Ingeniero	Venezuela
Miguel Antonio Rodriguez	Abogado	Venezuela
Raymond Orta Martínez	Abogado	Venezuela

Perfiles Destacados

MARCELA GONZÁLEZ RIVERO

Actualmente desempeña la posición de presidenta del Sector de Tecnologías para la Información en CANACINTRA, desde donde lidera iniciativas estratégicas para fortalecer la transformación digital, la innovación tecnológica y la competitividad de las pymes con impacto en la industria mexicana.

Encabeza programas de inclusión, asesoría y vinculación orientados a fomentar la participación de niñas y jóvenes en áreas STEM, como parte del compromiso institucional de CANACINTRA.

Consultora especializada en tecnología, estrategias ESG y responsabilidad social empresarial. Abogada con formación complementaria en gestión de proyectos y actualmente en formación como oficial de cumplimiento normativo.

Empresaria con más de 15 años de trayectoria en el sector de Tecnologías de la Información, ha coordinado proyectos nacionales consolidando alianzas intersectoriales para el desarrollo tecnológico, aportando experiencia en innovación, transformación digital y vinculación estratégica.

PHILIPPE BOULANGER

Vicepresidente de Salud Empresarial en la CONCANACO SERVYTUR México
Director de Innovación en VitâgeLab

Nacido en el norte de Francia en 1976, Philippe Boulanger ha forjado una trayectoria internacional en París, España, Miami y México. Con formación en Marketing, identificó tempranamente oportunidades en la adopción de tecnologías clave: de las TI y el comercio electrónico a la integración de finanzas digitales, así como la innovación en salud y bienestar como pilares de productividad empresarial.

Inició su carrera en editoriales especializadas como VNU e IDG, liderando estrategias comerciales y expansión en Europa y Latinoamérica. Su visión de interacción bidireccional lo impulsó a fundar el primer evento eShow en México y la Academia Digital PYMES, además de co-fundar Sinestesia.Digital.
Fue Vicepresidente de Comercio Electrónico y Presidente de la Asociación de Internet MX (2019-2022), y posteriormente Vicepresidente de Economía Digital en CONCANACO, colaborando con la Secretaría de Economía, PROFECO y COFECE en diagnósticos de digitalización para PYMES.

Hoy, como Vicepresidente de Salud Empresarial en CONCANACO SERVYTUR, promueve el bienestar integral —físico, mental y económico— de empresarios y colaboradores, incorporando data, IA y Blockchain para fortalecer la resiliencia y competitividad de las empresas mexicanas. Paralelamente, en VitâgeLab dirige innovación en medicina de precisión, laboratorio clínico avanzado, programas de hábitos y conciencia para la longevidad, elevando la calidad de vida, el rendimiento empresarial mediante enfoques personalizados y basados en evidencia.

LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ

Tiene estudios doctorales en Administración Pública, maestría en Gestión Pública Aplicada, y es politóloga por el Instituto Tecnológico Autónomo de México. Es especialista en partidos políticos y transparencia por la Universidad Autónoma Metropolitana, Oficial de Cumplimiento en Inteligencia Artificial y está certificada en Gestión de Riesgos de Inteligencia Artificial ISO 37301 por NYCE y White Box Project.

Cuenta con más de un centenar de publicaciones y una trayectoria profesional de más de 15 años, desempeñándose en cargos de alta dirección en los Poderes Ejecutivo y Legislativo, y en organismos constitucionalmente autónomos, como el INAI y el INE en el que también fue designada Consejera Electoral en el ámbito local. Fue directora en una Cámara Industrial Nacional y Vicepresidenta de Transparencia en la Asociación Mexicana de Integridad y Compliance.

Es colaboradora de diversos medios de comunicación, entre los que destacan El Heraldo de México, El Universal, ContraRéplica, La Silla Rota, entre otros. Asimismo, es docente de diversas materias y módulos en la UNAM, Anáhuac, Escuela Libre de Derecho y Universidad Panamericana. Es profesora de asignatura en el Tecnológico de Monterrey. De igual manera ejerce como catedrática y coordinadora académica del Diplomado Combate a la Corrupción: Integridad y Rendición de Cuentas, del Instituto Nacional de Administración Pública (INAP), y de la Especialización en Derecho Europeo de Protección de Datos Personales, de la Universidad de Barcelona.

En 2025, fue nominada al Premio Giovanni Butarelli, de la Asamblea Global de la Privacidad.

Actualmente es Consejera del Consejo Directivo del INAP, Líder del Capítulo Ciudad de México de la Alianza México CiberSeguro y Comisionada Presidenta del Instituto de Transparencia y Protección de Datos Personales de la Ciudad de México (INFO CDMX).

Organizaciones
Destacadas

JAAK

Empresa mexicana especializada en verificación de identidad digital y biometría, anunció la incorporación de su nueva solución de Firma Electrónica, fortaleciendo su ecosistema tecnológico para la digitalización de procesos críticos de negocio. Esta integración permite a las organizaciones verificar la identidad de sus usuarios y formalizar acuerdos con validez legal plena dentro de un mismo flujo automatizado.

La solución de Firma Electrónica de JAAK cumple con la NOM-151-SCFI-2016, otorgando validez jurídica equivalente a la firma autógrafa en México, e incluye además firma electrónica simple para operaciones globales, adaptándose a distintos tipos de transacción e industrias.

De acuerdo con Arianna Quezada, fundadora y CEO de JAAK, la verificación de identidad y la firma electrónica son componentes inseparables de la confianza digital: primero se valida quién es la persona mediante biometría, y posteriormente se formaliza el acuerdo con certeza jurídica, todo en una experiencia digital continua.
El portafolio integrado de JAAK ofrece un flujo completo que incluye verificación biométrica facial con liveness avanzado, análisis de documentos oficiales mediante OCR, consulta en listas restrictivas para cumplimiento PLD, firma electrónica con trazabilidad completa y gestión de expedientes digitales auditables. Esto resulta especialmente relevante para sectores altamente regulados como el inmobiliario, financiero y de salud, donde las obligaciones de identificación, conservación de evidencia y formalización contractual son críticas.

La plataforma permite reducir procesos que antes tomaban días a cierres digitales en minutos, eliminando fricción operativa, errores manuales y riesgos de incumplimiento normativo. Su tecnología ha sido entrenada específicamente para población latinoamericana, alcanzando precisiones superiores al 99.5% en reconocimiento facial, y ofreciendo despliegues flexibles en modalidad SaaS, on-premise o híbrida.

Con más de 15 millones de verificaciones de identidad procesadas, certificaciones como ISO/IEC 27001, ISO 9001, iBeta nivel 2 y estándares NIST, JAAK refuerza su posición como proveedor confiable de infraestructura de confianza digital. La compañía proyecta que la incorporación de firma electrónica duplicará su volumen de operaciones, al permitir que los mismos procesos de verificación deriven directamente en acuerdos legalmente vinculantes.

Asociación Latinoamericana de Profesionales en Seguridad Informática, A.C. (ALAPSI).

La actual mesa directiva para el periodo 2025 – 2028, que coincide con el treinta aniversario de la organización, es presidida por Sergio Reynoso Pérez y un grupo de profesionales reconocidos en el ámbito profesional.

A mediados de la década de los 90, se constituye la ALAPSI, por la inquietud y preocupación de un grupo de profesionales del área de Informática para mitigar y reducir los riesgos generados por el uso de la tecnología de la información en las organizaciones privadas y públicas en México y Latinoamérica.

ALAPSI desde su fundación se ha encargado de promover las mejores prácticas, normas, estándares y capacitación en seguridad de la información, así como las certificaciones internacionales de la especialidad, con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de los recursos informáticos de las organizaciones.

Actualmente la capacitación y certificación en seguridad de la información no es solamente para los profesionales de la materia. Nos encontramos ante un panorama en el cual la tecnología está presente en todos los ámbitos de las personas no solamente de las organizaciones, por lo que se vuelve necesario acercar el conocimiento de los riesgos y amenazas a los que están expuestos en el ciberespacio al público en general.

Promovemos el crecimiento, la profesionalización de la Seguridad de la Información, así como las prácticas que apoyen a las Organizaciones públicas y privadas para asegurar la confidencialidad, integridad, disponibilidad de los recursos y servicios informáticos, con apego a principios y valores en la vida profesional o personal de cada uno de sus miembros.

Las certificaciones de ciberseguridad validan las habilidades y conocimientos de los profesionales en el desarrollo de su trabajo, no solo mejoran sus credenciales, también aumentan la confianza de las organizaciones en sus capacidades para salvaguardar la información crítica de las organizaciones.

Desde su origen, ALAPSI ha dado acompañamiento a un gran número de profesionales que eligieron desarrollarse en el campo de la ciberseguridad logrando que consiguieran obtener su respectiva certificación.

Regcheq: Tecnología que impulsa el cumplimiento en el ecosistema PLD.

En un entorno regulatorio cada vez más complejo, las empresas necesitan soluciones que les permitan cumplir de forma ágil, segura y automatizada. Regcheq es una plataforma tecnológica especializada en Prevención de Lavado de Dinero y Financiamiento al Terrorismo (PLD/FT), diseñada para apoyar a entidades financieras y actividades vulnerables en el cumplimiento de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI) y la Comisión Nacional Bancaria y de Valores (CNBV).

Con más de una década de experiencia en Latinoamérica, Regcheq ayuda a automatizar procesos clave, como la gestión de expedientes, la elaboración de avisos, el monitoreo de operaciones y la identificación de beneficiarios controladores. Su objetivo es reducir riesgos, optimizar tiempos y ofrecer un cumplimiento normativo eficiente y confiable.

La plataforma permite personalizar criterios, flujos de trabajo y mecanismos establecidos por cada empresa, de esta manera se ofrece un sistema adaptable que se integra fácilmente con otros sistemas mediante la integración con APIs.

En un entorno regulatorio cada vez más exigente, automatizar el cumplimiento en materia de PLD es clave para reducir riesgos y optimizar la labor de los oficiales de cumplimiento. Con Regcheq, las empresas pueden garantizar procesos más ágiles, seguros y alineados con la normativa vigente.

Conoce más en www.regcheq.com.mx.

Sección:
MINUTOS MILLONARIO$

Compliance y Tecnología
¿Binomio reactivo o estratégico?

Por: M. SC. Juan Fernando Castillejos Echandi.

El cumplimiento normativo ha evolucionado de ser una función reactiva y administrativa para convertirse en un pilar estratégico para la gestión de riesgos y la integridad organizacional en el siglo XXI. Esta transformación se ha acelerado notablemente por la digitalización de procesos, la globalización de los mercados y la creciente complejidad de los marcos regulatorios, tanto en el sector público como en el privado. En este contexto, la tecnología emerge como un catalizador fundamental, redefiniendo la manera en que las organizaciones diseñan, implementan y supervisan sus programas de cumplimiento.

La integración de herramientas como la Inteligencia Artificial (IA), el Big Data, la tecnología Blockchain y los Sistemas de Gestión de Cumplimiento (como la norma ISO 37301) han permitido a las organizaciones anticipar riesgos, automatizar controles, garantizar la trazabilidad de las operaciones y fortalecer la transparencia. Sin embargo, estos avances también plantean desafíos éticos, legales y de privacidad, exigiendo una revisión constante de los marcos regulatorios y una gobernanza robusta que equilibre la innovación con la protección de los derechos fundamentales.

Tradicionalmente, el cumplimiento se gestionaba mediante auditorías manuales, controles documentales y capacitaciones periódicas. Ahora, la digitalización y la automatización han revolucionado este paradigma, permitiendo una gestión más proactiva, integral y basada en datos.

En el sector público, la Estrategia Digital Nacional de México ejemplifica cómo la tecnología puede ser un motor de transformación institucional, promoviendo la interoperabilidad, la transparencia y la eficiencia operativa en la administración pública. En el sector privado, la adopción de soluciones tecnológicas de RegTech (Tecnología Regulatoria) y GovTech han permitido a las empresas responder ágilmente a los cambios regulatorios, reducir costos operativos y fortalecer la confianza de los stakeholders.

La convergencia entre compliance y tecnología no solo responde a la necesidad de cumplir con la normativa, también se convierte en un diferenciador competitivo y un elemento clave para la sostenibilidad y la reputación corporativa.

La Inteligencia Artificial ha irrumpido con fuerza en el ámbito del cumplimiento normativo, ofreciendo capacidades avanzadas para el procesamiento de grandes volúmenes de datos, la detección de patrones anómalos y la automatización de tareas repetitivas. Los sistemas de IA se utilizan para:

- Monitoreo continuo de transacciones y comunicaciones: Algoritmos de machine learning analizan operaciones financieras en tiempo real para identificar posibles fraudes, lavado de dinero o conflictos de interés.
- Análisis predictivo de riesgos: La IA permite anticipar escenarios de incumplimiento mediante la evaluación dinámica de riesgos y la simulación de impactos.
- Automatización de auditorías y revisiones documentales: Los sistemas de IA pueden revisar contratos, políticas y registros para detectar cláusulas o prácticas no conformes.
- Gestión de canales de denuncia y whistleblowing: Chatbots y asistentes virtuales facilitan la recepción y clasificación de denuncias, mejorando la accesibilidad y la protección del informante.

No obstante, la integración de IA en compliance plantea desafíos significativos. Entre los principales riesgos destacan:

- Sesgo algorítmico y discriminación: Si los datos de entrenamiento contienen sesgos, los sistemas de IA pueden perpetuar prácticas discriminatorias, afectando la equidad y la reputación de la organización.
- Falta de transparencia y explicabilidad: Muchos modelos funcionan como "cajas negras", dificultando la trazabilidad y la justificación de las decisiones automatizadas.
- Responsabilidad penal y civil: La autonomía de la IA genera interrogantes sobre la imputación de responsabilidades en caso de daños o delitos cometidos por o a través de sistemas inteligentes.

El Big Data ha transformado la gestión del cumplimiento normativo al permitir el procesamiento y análisis de grandes volúmenes de información estructurada y no estructurada. Las principales aplicaciones de esta en compliance incluyen:

- Evaluación y gestión de riesgos: El análisis de datos provenientes de múltiples fuentes (transacciones, correos electrónicos, redes sociales) permite identificar riesgos emergentes y mitigar amenazas antes de que se materialicen.
- Monitoreo y vigilancia en tiempo real: Los sistemas de big data detectan anomalías y patrones sospechosos en operaciones financieras, facilitando la prevención de delitos como el lavado de dinero o la manipulación de mercados.
- Automatización de reportes regulatorios: La recopilación y análisis automatizado de datos agiliza la elaboración de informes exigidos por autoridades, reduciendo errores y tiempos de respuesta.
- Debida diligencia y conocimiento del cliente (KYC): Permite construir perfiles de riesgo más completos y dinámicos, mejorando la efectividad de los procesos de onboarding y monitoreo continuo.

Sin embargo, el uso intensivo de Big Data en compliance también implica desafíos en materia de privacidad, seguridad de la información y calidad de los datos. La protección de datos personales y la gestión ética de la información son aspectos críticos, especialmente bajo marcos regulatorios como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en nuestro país.

La tecnología blockchain se ha consolidado como una herramienta disruptiva para el cumplimiento normativo, especialmente en lo que respecta a la trazabilidad, la transparencia y la inmutabilidad de los registros. Sus principales aplicaciones en compliance se ven reflejadas en:

- Registro y auditoría de transacciones: Ya que permite crear registros indelebles y verificables de operaciones, facilitando la auditoría y la detección de fraudes.
- Contratos inteligentes (smart contracts): Estos algoritmos autoejecutables automatizan el cumplimiento de condiciones contractuales, reduciendo la intervención humana y el riesgo de manipulación.
- Gestión de identidades digitales: Blockchain puede utilizarse para crear sistemas de identidad digital soberana, mejorando la seguridad y la privacidad en procesos de autenticación y autorización.
- Evidencia digital y validez legal: En México, la legislación reconoce la validez probatoria de documentos y contratos digitales firmados electrónicamente y respaldados por blockchain, siempre que cumplan con los requisitos de integridad y atribución.

No obstante, la adopción de blockchain en el sector público y privado enfrenta retos regulatorios, técnicos y organizacionales. Entre los principales desafíos podemos destacar:

- Interoperabilidad y escalabilidad: La integración de blockchain con sistemas legados y la gestión de grandes volúmenes de datos requieren soluciones técnicas avanzadas.
- Privacidad y protección de datos: La inmutabilidad de la cadena puede entrar en conflicto con derechos como el "derecho al olvido" y la gestión de datos sensibles.
- Jurisdicción y reconocimiento legal: La naturaleza descentralizada de blockchain plantea interrogantes sobre la aplicabilidad de las leyes y la resolución de disputas transfronterizas.

En América Latina, países como México, Colombia y Panamá han avanzado en la regulación y adopción de blockchain para la gestión pública, la identidad digital y la trazabilidad de activos, aunque persisten desafíos en la consolidación de marcos normativos comunes.

El auge de la Tecnología Regulatoria (RegTech) ha revolucionado la manera en que las organizaciones abordan el cumplimiento normativo, especialmente en sectores altamente regulados como el financiero, el asegurador y el tecnológico. Las soluciones RegTech más destacadas incluyen:

- Plataformas de gestión de riesgos y cumplimiento (GRC): Integran la gestión de políticas, riesgos, controles y auditorías en una sola plataforma, facilitando la centralización y la trazabilidad.
- Sistemas de monitoreo transaccional y prevención de lavado de dinero (AML): Utilizan IA y machine learning para detectar operaciones sospechosas y cumplir con regulaciones internacionales como la FATF y la Ley Fintech.
- Herramientas de verificación de identidad y KYC: Incorporan biometría, análisis de datos y listas de sanciones para fortalecer los procesos de onboarding y debida diligencia.
- Automatización de reportes regulatorios y gestión documental: Facilitan la generación, almacenamiento y presentación de informes exigidos por autoridades, asegurando la integridad y la validez legal de los documentos digitales.

En México y América Latina, empresas diversas ofrecen soluciones adaptadas a las necesidades locales, permitiendo a las organizaciones cumplir con normativas nacionales e internacionales de manera eficiente y escalable.

La Ciberseguridad se ha convertido en un componente esencial del compliance, especialmente ante el aumento de ciberataques y la sofisticación de las amenazas digitales. Las mejores prácticas en cibercompliance incluyen:

- Evaluación y gestión de riesgos de seguridad: Identificación de vulnerabilidades, implementación de controles y monitoreo continuo de incidentes.
- Desarrollo de políticas y procedimientos de seguridad: Definición de normas internas sobre acceso, cifrado, respaldo y respuesta a incidentes.
- Capacitación y concientización del personal: Formación regular sobre buenas prácticas de seguridad y cumplimiento normativo.
- Auditorías y monitoreo continuo: Evaluación periódica de la eficacia de las medidas de seguridad y adaptación a nuevas amenazas.

El cibercompliance no solo protege la información confidencial y la reputación de la organización, sino que también es un requisito legal bajo normativas como el Reglamento General de Protección de Datos (GDPR) europeo, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) a nivel nacional y estándares internacionales como la ISO/IEC 27001.

Podemos concluir que la tecnología está transformando radicalmente el cumplimiento normativo en organizaciones públicas y privadas, ofreciendo herramientas avanzadas para la gestión de riesgos, la automatización de controles, la trazabilidad de operaciones y la transparencia institucional. La integración de Inteligencia Artificial, Big Data, Blockchain y Sistemas de Gestión de Cumplimiento permite a las organizaciones anticipar amenazas, optimizar procesos y fortalecer la confianza de los stakeholders.

Sin embargo, estos avances tecnológicos también plantean desafíos éticos, legales y de privacidad que exigen una gobernanza robusta, marcos regulatorios adaptativos y una cultura organizacional basada en la integridad y la responsabilidad. La protección de datos personales, la ciberseguridad, la transparencia algorítmica y la protección del informante son aspectos críticos que deben ser gestionados de manera proactiva y alineada con los estándares internacionales.

El éxito de la transformación digital del compliance depende del compromiso de la alta dirección, la integración de sistemas interoperables, la formación continua del talento y la adaptación ágil a los cambios regulatorios. La evaluación de riesgos, el uso de KPIs y la gestión del cambio son elementos clave para garantizar la efectividad y la sostenibilidad de los programas de cumplimiento en la era digital.

En definitiva, la tecnología no solo es un habilitador del cumplimiento normativo, sino también un motor de innovación, transparencia y legitimidad institucional. Las organizaciones que logren equilibrar la innovación tecnológica con la ética, la legalidad y la protección de los derechos fundamentales estarán mejor preparadas para enfrentar los desafíos y aprovechar las oportunidades de la economía digital.

M. SC. JUAN FERNANDO CASTILLEJOS E.
Director Ejecutivo de la AMDTech.

Juan Fernando Castillejos Echandi
@jfcastillejos
l.a.juanfdocastillejoechandi

ALKINS
PRODUCCIONES

Globoflexia
para:

- Arreglos
- Eventos
- Detalles
- Regalos
- Decoraciones

Solicita tu cotización al:

55 2277 9270

Desarrollo Humano Integral por:

curet plus

BIENESTAR EMPRESARIAL

Bienestar Laboral y Salud Organizacional

Por: Mtra. Yadira García Ruiz.

El bienestar laboral es un factor fundamental para fortalecer equipos de trabajo productivos, motivados, y, sobre todo, comprometidos, impactando de manera positiva en el desempeño y el éxito de las organizaciones.

En un entorno de alta competitividad y crecientes exigencias, la salud organizacional se refleja en la cultura, el liderazgo, el clima laboral y en cómo estos influyen de manera significativa en la motivación, el desempeño y en los aspectos emocionales, mentales y sociales que impactan directamente en el día a día de los colaboradores.

Por estas razones, en la actualidad las organizaciones buscan crear entornos con programas orientados a la reducción del estrés, fortalecimiento de un clima laboral y estimular las relaciones interpersonales, entre otros, con la finalidad de que los colaboradores se sientan valorados.

Además, se consigue que la producción sea más eficiente y que el trabajo resulte de mayor calidad.

¿Qué son los programas de bienestar laboral?
Los colaboradores representan el activo más importante dentro de una empresa, por lo que estos programas de bienestar laboral están orientados a cuidar el bienestar integral tanto dentro como fuera del entorno de trabajo.

Su objetivo es promover la calidad de vida de los colaboradores, impulsando acciones que fortalezcan su salud física, emocional, mental y social. De esta manera, las organizaciones invierten en su talento humano, fortaleciendo equipos de trabajo, productivos y comprometidos con la organización.

Ventajas de programas de bienestar en la organización:

Mejora la reputación de la empresa: las organizaciones que promueven este tipo de iniciativas son mejor valoradas, atrayendo candidatos con alto potencial.
Impacto económico positivo: reducen costos a largo plazo en temas de salud laboral, es decir, reducción de rotación de personal y formación.

Trabajo en equipo: se establecen relaciones empáticas y propician la colaboración alcanzando los objetivos.
Productividad: los colaboradores tienen mejores resultados y, por ende, mejor desempeño.

Colaboradores eficientes: los trabajadores se sienten comprometidos si las condiciones laborales son adecuadas, eso los motiva y surge el interés de contribuir con la organización.

Desarrollo profesional: impulsa la dedicación y el empeño de seguir adquiriendo nuevos conocimientos, capacitándose y creciendo dentro de la empresa.

Reduce el riesgo de enfermedades y ausentismo: promueven hábitos saludables, una mejor calidad de vida y un mayor rendimiento laboral.

Equilibrio personal y laboral: reduce el agotamiento y permite armonizar las responsabilidades reduciendo el estrés y el desgaste laboral.

Tipos de programas de bienestar laboral:
Hoy en día existen múltiples opciones para canalizar este tipo de programas desde alimentación sana, actividad física, pasando por formación continua, hasta programas de salud mental, por ejemplo:
• Salud emocional y mental: apoyo y asistencia psicológica, manejo del estrés, programas de meditación o mindfulness.
• Salud física: campañas de actividad física, prevención de enfermedades, alimentación balanceada y revisiones médicas periódicas.
• Desarrollo profesional: programas de aprendizaje o capacitación, mentorías y sucesión de carrera.
• Equilibrio personal, laboral y social: gestión del tiempo, flexibilidad en horarios laborales, teletrabajo.
• Clima organizacional: comunicación, relaciones interpersonales, trabajo de equipo y eventos o celebraciones.
• Asistencia a las familias: programas de descuentos en seguros médicos, sala de lactancia, entre otras.

El bienestar laboral ha ido evolucionando de tal manera que las organizaciones implementan herramientas tecnológicas para mejorar la vivencia de sus colaboradores. Actualmente, las plataformas digitales juegan un papel muy importante, ya que permite integrar soluciones de bienestar laboral accesibles, como asesorarías de nutrición y actividades orientadas al bienestar. Esto ayuda a las empresas a innovar formas de trabajo más flexibles, saludables y alineadas a las necesidades de estos tiempos.

En resumen, los programas de bienestar laboral son una estrategia para las empresas, por tanto, es importante conocer las necesidades de los colaboradores y proporcionarles los beneficios que permitan cultivar un ambiente sólido, saludable e inclusivo.

Estos proyectos, si se promueven y desarrollan correctamente, pueden ser muy beneficiosos para cualquier organización. A futuro, una cultura organizacional enfocada en el bienestar laboral será determinante para atraer y retener talento, además de permitir a las empresas enfrentar con mayor solidez los cambios constantes.

MTRA. YADIRA GARCÍA RUIZ
Psicología en el Desarrollo Humano.
Directora de Capital Humano de Top Compliance.

COMPLIANCE 4.0:
Cómo la tecnología está redefiniendo la prevención del lavado de dinero en México

Por: Mtra. Katherine Leal López.

La Prevención de Lavado de Dinero y Financiamiento al Terrorismo (PLD/FT) atraviesa una transformación silenciosa pero profunda. Lo que antes dependía de revisiones manuales, expedientes físicos y controles periódicos, hoy exige monitoreo en tiempo real, análisis de datos masivos y decisiones automatizadas. En un entorno digital, donde las transacciones ocurren en segundos y los riesgos evolucionan constantemente, el Compliance "tradicional" simplemente ya no es suficiente.

Las organizaciones en México; bancos, fintechs, SOFOMES, casas de cambio e incluso empresas no financieras vulnerables enfrentan un escenario más complejo: mayores exigencias regulatorias de la CNBV y la UIF, clientes digitales y nuevas tipologías de fraude que combinan la tecnología y crimen financiero. La pregunta ya no es si deben modernizarse, sino qué tan rápido pueden hacerlo.

Uno de los problemas más comunes es el exceso de alertas generadas por los sistemas de monitoreo, las instituciones financieras medianas pueden producir miles de alertas mensuales, de las cuales la gran mayoría resultan ser falsos positivos.

El resultado, analistas revisando operaciones legítimas mientras los riesgos reales pueden pasar desapercibidos.

En México, donde las transferencias electrónicas vía SPEI y CoDi han incrementado el volumen y la velocidad de las operaciones, este reto se ha intensificado. Por ello, muchas entidades están implementando modelos de analítica avanzada y machine learning para priorizar clientes y transacciones de mayor riesgo. La automatización ya no es innovación, es supervivencia operativa.

Hablemos del onboarding digital y del robo de identidad, hoy día las aperturas de cuentas a distancia se aceleraron con la digitalización de los servicios financieros. Sin embargo, también creció el uso de identidades falsas, documentos alterados e incluso datos robados para crear cuentas que posteriormente se utilizan para dispersar recursos ilícitos.

Fintechs mexicanas y bancos digitales han tenido que reforzar sus procesos de KYC con biometría facial, pruebas de vida y validaciones contra bases oficiales como INE o CURP. Además, el monitoreo continuo del cliente se ha vuelto indispensable. Hoy, conocer al cliente no es un evento único al inicio de la relación, sino un proceso totalmente permanente.

Cada vez es más común que los clientes envíen o reciban recursos desde exchanges de criptomonedas, aunque estas operaciones no siempre son ilícitas, la trazabilidad del origen de los fondos se vuelve más compleja.

Las áreas de cumplimiento ahora deben analizar direcciones blockchain, identificar vínculos con billeteras de alto riesgo o mercados ilegales, y documentar adecuadamente el origen de recursos. Algunas instituciones mexicanas ya integran herramientas de blockchain analytics para complementar sus investigaciones, ampliando el alcance del monitoreo más allá del sistema bancario tradicional.

Por ello, también es importante hablar de otro foco rojo como lo son los terceros: proveedores, distribuidores, comisionistas o aliados comerciales. En México, las empresas también deben considerar riesgos derivados de listas restrictivas, sanciones internacionales o incluso la inclusión de terceros en los listados como el 69-B del SAT, que identifica presuntas operaciones inexistentes.

Hoy, muchas organizaciones realizan screening automatizado y monitoreo continuo de terceros, no solo al inicio de la relación, la debida diligencia dejó de ser un trámite para convertirse en un control preventivo clave. Los fraudes electrónicos, el phishing y el ransomware también impactan directamente a Compliance. Los recursos obtenidos se dispersan rápidamente a través de múltiples cuentas o activos virtuales para dificultar su rastreo. Por lo que esto ha obligado a una mayor colaboración entre áreas de ciberseguridad, fraude y PLD. Detectar un ataque ya no es solo un incidente tecnológico, sino un posible evento de lavado de dinero que puede requerir reportes regulatorios.

El cumplimiento normativo está dejando de ser un área operativa para convertirse en un habilitador estratégico del negocio. Las organizaciones que adoptan soluciones RegTech, monitoreo en tiempo real y automatización no solo cumplen mejor con la regulación, sino que reducen costos, mejora la experiencia del cliente y fortalecen su reputación.

En el contexto mexicano, donde la supervisión es cada vez más estricta y las operaciones más digitales, el mensaje es claro: el Compliance no puede mirar al pasado, debe anticiparse al riesgo en el presente.

La prevención de lavado de dinero ya no se trata de revisar expedientes, sino de interpretar datos y en esta nueva era, la tecnología es el principal aliado para proteger a las organizaciones y al sistema financiero.

MTRA. KATHERINE LEAL LÓPEZ

Maestra en Juicios Orales y en Cumplimiento Corporativo. Especialista en Compliance, Ética y Anticorrupción. Oficial de Cumplimiento certificada por el GIAO. Consultora de Compliance independiente, Jefa de Ética y Compliance en IGSA, Función de Cumplimiento en IGSA Medical.

Katherine Leal

Lo Tecnológico por:

AMD Tech
ACADEMIA MEXICANA DE DERECHO DIGITAL Y TECNOLÓGICO, AC

Lentes Ray-Ban Meta

Por: Ing. Ricardo Stephen Alkins Villarroel.

La tecnología que convierte la mirada en contenido

Durante años, la evolución del smartphone giró en torno a una pregunta: ¿cómo capturar mejor el momento? Más resolución, más estabilización, más inteligencia artificial. Sin embargo, el siguiente paso ya no está en el bolsillo, sino en el rostro.

Los Ray-Ban Meta Smart Glasses representan un cambio silencioso pero profundo: la cámara deja de ser un dispositivo que sostenemos y se convierte en una extensión natural de nuestra visión. Meta no lanzó simplemente unos lentes inteligentes. Introdujo una nueva interfaz entre el mundo físico y el digital.

Diseño y especificaciones

Uno de los grandes aciertos del dispositivo es su estética. A diferencia de intentos anteriores en el mercado de gafas inteligentes, el diseño conserva el ADN icónico de Ray-Ban.

La tecnología está integrada de forma casi imperceptible:

- Cámara ultra gran angular de 12 MP
- Grabación de video en 1080p en primera persona
- Micrófonos mejorados para audio espacial
- Bocinas abiertas en las varillas
- Control por voz con IA integrada
- Sincronización con smartphone y redes sociales

La experiencia es clara: grabar sin interrumpir la experiencia.

Estos lentes no están pensados únicamente para entusiastas tecnológicos. Su mercado natural es el creador de contenido. Con transmisión en vivo directa a plataformas sociales, los Ray-Ban Meta convierten cualquier momento cotidiano en una experiencia compartida en tiempo real. Desde un concierto hasta una reunión profesional, el usuario puede capturar exactamente lo que ve, sin levantar un teléfono. El impacto aquí es estratégico: la tecnología wearable deja de ser accesorio y se convierte en plataforma de comunicación.

El asistente por voz integrado permite comandos simples como:

- “Hey Meta, toma una foto”
- “Hey Meta, graba un video”
- “Hey Meta, transmite en vivo”

La verdadera apuesta de Meta no es solo la cámara, sino la integración progresiva de inteligencia artificial contextual en dispositivos ambientales. Es el inicio de una computación menos visible y más integrada al entorno humano.

Los Ray-Ban Meta no reemplazarán al smartphone de inmediato. Pero sí anticipan una tendencia inevitable: dispositivos cada vez más integrados al cuerpo y menos visibles.

Más que un accesorio tecnológico, estos lentes representan un cambio cultural. La pregunta ya no es si podemos grabar todo lo que vemos. La verdadera pregunta es si estamos listos para vivir en un mundo donde todos puedan hacerlo.

Sin duda, este será uno de los productos más significativos en la evolución de la tecnología wearable en la última década. No por su potencia técnica, sino por lo que simbolizan: el inicio de una nueva etapa donde la mirada se convierte en medio digital y cuando la tecnología se vuelve invisible, su impacto se vuelve inevitable.

Fuentes:
ChatGPT
COPILOT

ING. RICARDO STEPHEN ALKINS VILLARROEL
Especialista en Ciberseguridad y Transformación Digital
Coordinador de la Comisión de Jovenes de la AMDTech.

@ricardoalkins

IMAGEN ESTRATÉGICA

EL ESCUDO INVISIBLE:

Imagen Estratégica y Gestión de Crisis ante el Incidente Digital

Por: Mtro. Román Trejo Gómez.

Introducción

En un ecosistema de dependencia tecnológica absoluta, la vulnerabilidad digital ha dejado de ser una posibilidad remota para convertirse en una certeza estadística. Sin embargo, cuando una organización enfrenta una brecha de seguridad, el daño técnico es apenas la punta del iceberg; el verdadero impacto se mide en la erosión de la confianza y el colapso de la percepción pública. La imagen estratégica en la gestión de crisis no es un accesorio estético, sino el componente crítico de la resiliencia corporativa. En un entorno donde el vacío de información es reclamado rápidamente por la especulación, la capacidad de una entidad para proyectar control, transparencia y cumplimiento legal determina si el incidente será un bache operativo o el fin de su prestigio reputacional.

Para que esta resiliencia no sea solo un concepto abstracto, la imagen estratégica debe materializarse en acciones concretas que blinden la credibilidad de la institución. No basta con "parecer" bajo control; es necesario ejecutar una arquitectura de comunicación que responda con precisión técnica y sensibilidad humana. Esta estructura se sostiene sobre tres pilares fundamentales que transforman la vulnerabilidad en una demostración de integridad institucional:

1. Transparencia Dirigida:

El equilibrio entre información y seguridad bajo este primer pilar, en el cual la organización enfrenta el dilema de qué decir y cuándo decirlo. En el marco del Derecho Digital, la transparencia no significa sobreexposición, sino comunicación de mitigación. Informar de manera errática solo genera pánico; por el contrario, explicar qué medidas se están tomando para proteger al usuario refuerza la ética corporativa. Cumplir con los protocolos de notificación que exige la ley no es solo un trámite, es un mensaje potente que posiciona a la empresa como un ente responsable ante el mercado.

2. Liderazgo Visible:

La autoridad frente al caos como extensión de esa transparencia, este segundo pilar exige que la respuesta tenga un rostro humano y autorizado. Ante un ciberataque, el silencio se traduce como negligencia. La imagen estratégica requiere de un vocero que proyecte serenidad: la elección entre el CEO o el Director Legal no es trivial, pues su lenguaje no verbal debe transmitir que la situación está bajo una gestión experta. Una organización que "da la cara" de manera estructurada reduce drásticamente el impacto negativo en su valor intangible.

3. Coherencia de Marca y Resiliencia Visual:

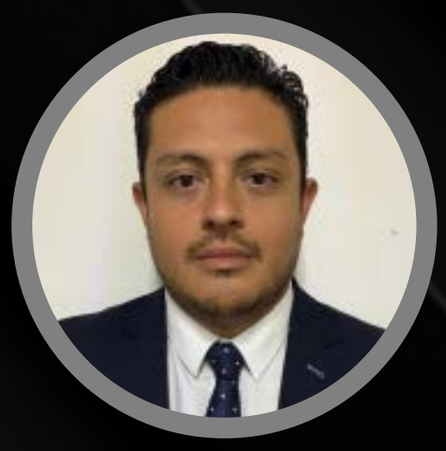
Finalmente, la respuesta debe ser estéticamente coherente con la identidad de la organización. Si una marca vende "seguridad", sus comunicados de crisis deben evitar la sobreactuación y mantener una sobriedad impecable. La resiliencia visual consiste en demostrar que, a pesar del ataque, los valores de la institución siguen intactos. La meta es que, una vez superada la contingencia, la narrativa dominante sea la profesionalidad de la respuesta y no la vulnerabilidad del sistema.

La "Hora de Oro" y el Factor Tiempo

En la comunicación estratégica, los primeros sesenta minutos tras la detección son vitales. Si la organización no ocupa el espacio informativo con su propia versión de los hechos, el vacío será llenado por especulaciones de terceros o, peor aún, por la narrativa de los propios atacantes. Una respuesta rápida y profesional no solo detiene la hemorragia reputacional, sino que posiciona a la entidad como un referente en gestión de incidentes.

Conclusión: La Reputación como Activo Digital

La crisis, por naturaleza, es transitoria; sin embargo, la percepción que deje a su paso es permanente. Integrar la imagen estratégica dentro de los planes de respuesta a incidentes de ciberseguridad ya no es opcional para el abogado digital o el consultor tecnológico moderno. Al final del día, las organizaciones no son juzgadas únicamente por las vulnerabilidades de sus sistemas, sino por la integridad y la profesionalidad de su respuesta humana. La imagen estratégica es, en última instancia, el escudo más resistente contra la desconfianza digital.



MTRO. ROMÁN TREJO GÓMEZ
Director de Enlace y Relaciones Institucionales
Grupo Atelier Patrimonial.

Sección:

Nuevas Generaciones

Ius Ex Machina:
El Derecho Global y la Reconfiguración de la Justicia en la Era del Algoritmo

Mazatzin Quintanar Gómez.

Lo aplicamos, lo defendemos y lo estudiamos mientras la realidad jurídica se reconfigura en tiempo real, mediada por tecnología, datos y algoritmos. No es una crisis: es una mutación. Esta columna existe para nombrar ese desplazamiento silencioso: cuando la justicia deja de escribirse y empieza a ejecutarse.

I. El horizonte 2026: ¿hacia una lex informática soberana?

Si el lector ha llegado hasta aquí, probablemente comparte una intuición fundamental: el Derecho ya no habita exclusivamente en códigos impresos ni en bibliotecas silenciosas. Actualmente, el fenómeno jurídico se manifiesta como una arquitectura dinámica de datos, protocolos y decisiones automatizadas que condicionan —muchas veces de forma invisible— la vida cotidiana de individuos, empresas y Estados.

Nos encontramos en el punto de inflexión de una transformación profunda: el tránsito de la norma escrita a la norma programada. Durante siglos, la soberanía jurídica se entendió como una potestad territorialmente delimitada. Hoy, sin embargo, dicha noción se ve tensionada por la ubicuidad del código, por sistemas tecnológicos que operan de manera transnacional y cuyos efectos no reconocen fronteras políticas.

Litigar en Ciudad de México, asesorar en Madrid o diseñar esquemas de Compliance en Seúl implica interactuar, directa o indirectamente, con sistemas de inteligencia artificial que responden a estándares técnicos globales. En este contexto emerge con fuerza la llamada Lex informática: un conjunto de reglas técnicas, normativas y prácticas que, sin ser producidas exclusivamente por los Estados, regulan conductas y generan consecuencias jurídicas reales.

Tal como advirtió Lawrence Lessig hace ya dos décadas, el código no solo ejecuta instrucciones, sino que regula comportamientos y distribuye poder (Lessig, 2006). Si el siglo XX fue el siglo de las constituciones nacionales, el XXI parece consolidarse como el de los marcos regulatorios transnacionales, donde instrumentos como la Ley de Inteligencia Artificial de la Unión Europea (AI Act) se convierten en estándares de facto para actores globales, incluso fuera del territorio europeo.

Para la abogacía de las nuevas generaciones, el campo de batalla ya no es únicamente el diario oficial local, sino la interacción compleja entre derecho interno, regulación supranacional y arquitectura tecnológica.

II. La opacidad algorítmica y el juicio de la "caja negra"

Uno de los mayores desafíos jurídico-tecnológicos de nuestro tiempo es la llamada opacidad algorítmica, comúnmente descrita como el problema de la black box. En la teoría general del derecho, cualquier acto de autoridad debe estar debidamente fundado y motivado; este principio constituye un pilar del debido proceso y de la legitimidad del poder.

No obstante, en la práctica contemporánea, sistemas algorítmicos —incluidos modelos de Inteligencia Artificial con capacidad de aprendizaje autónomo— toman decisiones que afectan derechos fundamentales: acceso a créditos hipotecarios, determinación de primas de seguros, selección de candidatos laborales e incluso evaluación del riesgo de reincidencia penal.

El problema no radica únicamente en la automatización, sino en la imposibilidad práctica de explicar cómo y por qué se llegó a un resultado específico. En muchos casos, ni siquiera los propios desarrolladores pueden reconstruir el razonamiento interno del sistema. Esta situación genera

una vulnerabilidad jurídica inédita: decisiones con efectos normativos sin una motivación comprensible.

De ahí surge el llamado derecho a la explicabilidad (right to explanation), desarrollado ampliamente en la doctrina contemporánea (Wachter & Mittelstadt, 2019). No se trata solo de exigir transparencia técnica, sino de garantizar que los resultados algorítmicos sean inteligibles para los seres humanos afectados por ellos. La justicia no puede sostenerse sobre decisiones inexplicables.

Como ha señalado Frank Pasquale, la opacidad tecnológica no es neutral; constituye una nueva forma de poder que escapa al escrutinio democrático (Pasquale, 2015). En este escenario, la labor del jurista se expande: ya no basta con interpretar normas, es necesario auditar procesos de tratamiento de datos y exigir responsabilidad en sistemas automatizados.

III. Sesgo algorítmico y la nueva discriminación sistémica

Uno de los compromisos más fuertes de las nuevas generaciones jurídicas es la defensa de la equidad y la justicia social. En el ámbito del derecho tecnológico, este compromiso se traduce en la lucha contra el sesgo algorítmico.

Existe una narrativa tecnocrática que sostiene que la tecnología es neutral por ser matemática. Esta premisa es profundamente engañosa. Los sistemas de Inteligencia Artificial aprenden a partir de datos históricos; si dichos datos reflejan desigualdades estructurales —de género, raza o nivel socioeconómico— el algoritmo no corrige esas injusticias: las reproduce y amplifica.

Así, estamos transitando de formas clásicas de discriminación directa, fácilmente identificables en un tribunal, hacia una discriminación por diseño, más sutil, más difícil de probar y potencialmente más dañina. Un criterio aparentemente neutro, como el código postal o el historial de consumo digital, puede funcionar como un proxy discriminatorio que excluye sistemáticamente a grupos vulnerables.

Diversos países han comenzado a reconocer este fenómeno como una amenaza a los derechos fundamentales. Iniciativas legislativas y jurisprudenciales en América Latina y Europa buscan tipificar la discriminación algorítmica como una forma de violación estructural de derechos humanos. En este contexto, la abogacía contemporánea debe dominar el concepto de discriminación algorítmica indirecta y desarrollar herramientas probatorias adecuadas para enfrentarla.

El reto consiste en evitar que el ius sea reemplazado por un utilitarismo estadístico que sacrifique a las minorías en nombre de la eficiencia.

IV. La geopolítica del dato y el Compliance transfronterizo

Para quienes buscan especialización en el mercado jurídico internacional de 2026, el mensaje es claro: la demanda de auditores de algoritmos y expertos en protección de datos crece exponencialmente. El Compliance ya no es una lista burocrática de requisitos, sino una estrategia geopolítica.

Actualmente, el mundo puede entenderse dividido —con matices— en tres grandes modelos regulatorios: el europeo, centrado en derechos humanos y ética tecnológica; el estadounidense, caracterizado por un federalismo digital fragmentado; y el asiático, donde la seguridad nacional y el control estatal de los datos ocupan un lugar central.

El abogado global debe ser capaz de navegar este mosaico normativo. Una base de datos alojada en la nube puede estar sujeta simultáneamente a múltiples jurisdicciones, con obligaciones contradictorias. Ignorar esta realidad hoy equivale a no saber leer un contrato hace medio siglo.

V. La transformación del ejercicio profesional: del litigio a la auditoría

La automatización no reemplazará a los abogados, pero sí desplazará a quienes se nieguen a comprenderla. La ventaja competitiva de la abogacía contemporánea no será la velocidad, sino el criterio ético y la capacidad de intervención humana.

La noción de human-in-the-loop se vuelve central: en decisiones de alto riesgo, debe existir siempre una supervisión humana efectiva y una vía clara de impugnación. El derecho de daños y la responsabilidad civil están siendo reconfigurados para responder a una pregunta clave: ¿quién responde cuando un sistema de IA causa un perjuicio?

Programadores, proveedores de datos y empresas usuarias entran en un nuevo esquema de corresponsabilidad que exige marcos normativos innovadores.

VI. Conclusión: Reclamando el humanismo en el bit

El Derecho no está desapareciendo; se está transformando en una capa de software que envuelve a la sociedad. Pero el software carece de conciencia. Esa es, precisamente, la función irrenunciable del jurista.

La generación que hoy se forma tiene la responsabilidad histórica de garantizar que, en un mundo gobernado por algoritmos, la dignidad humana siga siendo el principio rector. El código puede ser ley, pero la Ley —con mayúscula— debe ser siempre el límite del código.

Bibliografía

Código Nacional de Procedimientos Civiles y Familiares [CNPCyF]. Arts. 3, 308, 335, 347, 348, 349, 350, 936 y 937. Diario Oficial de la Federación, última reforma 15 de enero de 2026 (México).

Decreto por el que se reforman, adicionan y derogan diversas disposiciones de sesenta y ocho ordenamientos legales federales. Diario Oficial de la Federación, 14 de noviembre de 2025 (México).

Código de Comercio. Arts. 1054, 1061 Bis y 1063. Diario Oficial de la Federación, última reforma 14 de noviembre de 2025 (México).

Código Fiscal de la Federación. Art. 130. Diario Oficial de la Federación, última reforma 14 de noviembre de 2025 (México).

Ley Federal de Procedimiento Contencioso Administrativo. Arts. 10 y 46. Diario Oficial de la Federación, última reforma 14 de noviembre de 2025 (México).

Norma Oficial Mexicana NOM-151-SCFI-2016. Prácticas comerciales — Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos. Diario Oficial de la Federación (México).

MAZATZIN QUINTANAR GÓMEZ

Recomendaciones del Mes

INTELIGENCIA ARTIFICIAL PARA ABOGADOS

Autor: Lumaira Fedriani
Amazon México

¿Qué es la Inteligencia Artificial y cómo impacta a los abogados?
En este texto, se nos presenta que la Inteligencia Artificial es una rama de la ciencia de la computación que busca dotar a las máquinas de habilidades humanas, como el aprendizaje, la percepción y la toma de decisiones. En el contexto legal, la IA se ha convertido en un aliado invaluable para los abogados, transformando la forma en que investigamos, analizamos datos y resolvemos casos.

EL DERECHO Y LA TECNOLOGÍA EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

Autor: Yanina Paula
Editorial: Autores de Argentina

Este libro ofrece una visión integral de los desafíos y oportunidades que la IA presenta para el marco jurídico actual. Analiza casos reales y teorías legales emergentes, proponiendo un diálogo entre expertos en derecho y tecnología para encontrar soluciones equilibradas y justas. Desde la responsabilidad legal de los algoritmos hasta la protección de datos personales y los derechos digitales, cada capítulo aborda un aspecto crucial del impacto de la IA en la sociedad.

EL PODER DE LOS CENTAVOS

Plataforma: Netflix

Basada en la historia real de gente corriente que se enfrentó a Wall Street y ganó dinero convirtiendo GameStop (una tienda de videojuegos) en una empresa muy atractiva para los inversores novatos. En medio de todo estaba Keith Gill, un tipo normal, analista y youtuber aficionado que lo apostó todo invirtiendo los ahorros de su vida en las acciones de Gamestop, y publicando online sobre dichas inversiones en un famoso foro de reddit. Cuando sus comentarios en las redes sociales revolucionan el sector, comienza a cambiar su vida y la de todos los que le siguieron comprando acciones en Robinhood, una app de trading sin comisiones.

NUESTROS
SERVICIOS

Agencia Creativa

MAGNITUD
CREATIVA

DESARROLLO
AUDIOVISUAL

GESTIÓN DE
MEDIOS

COMUNICACIÓN
GRÁFICA

AMBIENTACIÓN Y
DISEÑO DE PRODUCTOS

LIVE
EVENTS

Magnitud Creativa

contacto@magnitudcreativa.com

www.magnitudcreativa.com