FORMACIÓN PROFESIONAL FLDM

FACULTAD LIBRE DE DERECHO DE MONTERREY
Formación Integral de Profesionales del Derecho

CURSO

Ciberseguridad e inteligencia artificial para abogados

Criterio jurídico para gobernar el riesgo digital: regulación, contratos, gobernanza e incidentes

10 horas · En línea · Del 12 de noviembre al 10 de diciembre de 2026

Descripción del programa

Las brechas de datos, el ransomware y la adopción acelerada de la inteligencia artificial generativa dejaron de ser asuntos exclusivos del área de tecnología: hoy son materia de gobierno corporativo, de responsabilidad profesional y de cláusulas que se negocian en cada contrato relevante. A las personas abogadas, dentro y fuera de la empresa, se les pide opinar sobre incidentes, transferencias de datos, herramientas de IA y decisiones automatizadas, con frecuencia sin un marco jurídico ordenado para hacerlo y con consecuencias directas en materia de responsabilidad civil, penal y regulatoria.

Este curso entrega ese marco. En cinco sesiones en vivo, complementadas con material asíncrono, recorre el panorama regulatorio global y el marco legal mexicano aplicable, para después analizar el riesgo desde las dos trincheras del ejercicio profesional, la abogacía in-house y la de despacho, y cerrar con la respuesta a incidentes desde la función legal, incluido un simulacro de brecha de datos. Cada sesión concluye con un ejercicio aplicado, de modo que las personas participantes conviertan el contenido en criterio y herramientas utilizables desde el día siguiente.

Información general

Duración	10 horas (5 sesiones)
Modalidad	En línea
Plataforma	Teams (sesiones en vivo) y Canvas (material asíncrono)
Fechas	Jueves 12, 19 y 26 de noviembre y 3 y 10 de diciembre de 2026
Horario	6:00 a 8:00 p. m.
Costo regular	$8,160 MXN
Pronto pago (10%)	$7,344 MXN
Inscripción	www.fldm.mx/products/ciberseguridad

Objetivo general

Que las personas participantes evalúen y mitiguen los riesgos legales derivados de vulnerabilidades de ciberseguridad y del uso de inteligencia artificial, como asesores internos de una empresa o como consejeros externos de clientes, con criterio aplicable a contratos, gobernanza corporativa y respuesta a incidentes.

¿A quién va dirigido?

- Abogadas y abogados in-house responsables de cumplimiento, gobernanza de datos y de la relación con las áreas de tecnología (IT/CISO).
- Abogadas y abogados de despacho que asesoran en due diligence, contratación tecnológica, protección de datos y litigio post-incidente.
- Personas directivas no abogadas con responsabilidad jurídica sobre datos, tecnología o riesgos corporativos.
- Profesionales que participan en operaciones de M&A y en transferencias de datos en contextos de nearshoring.
- Perfiles con o sin formación técnica: el curso traduce el riesgo tecnológico a lenguaje y criterio jurídico.

Estructura del programa

Módulo 1 · Noviembre 12 El entorno global: ciberseguridad e inteligencia artificial como riesgo sistémico	
Objetivo	Que las personas participantes analicen por qué la ciberseguridad y la inteligencia artificial se convirtieron en asuntos de gobierno corporativo y dimensionen el alcance extraterritorial del panorama regulatorio global sobre las empresas mexicanas.
Contenidos clave	– De tema de IT a asunto de gobierno corporativo: por qué la ciberseguridad y la IA llegaron al consejo de administración. – Estadísticas y tendencias globales: costo promedio de las brechas de datos, crecimiento del ransomware y adopción acelerada de la IA generativa en el entorno corporativo. – Casos emblemáticos internacionales. – El binomio IA y ciberseguridad: la IA como amplificador del riesgo (phishing generado con IA, deepfakes) y de la defensa (detección de amenazas).

	– Panorama regulatorio comparado: EU AI Act, GDPR y marcos sectoriales de EE. UU., y su efecto extraterritorial sobre empresas mexicanas. – Ejercicio de cierre: mapeo rápido de exposición de la organización o del cliente frente a datos sensibles y sistemas de IA.

Módulo 2 · Noviembre 19 El marco legal mexicano aplicable	
Objetivo	Que las personas participantes evalúen las obligaciones y responsabilidades que el orden jurídico mexicano impone en materia de datos personales, ciberseguridad e inteligencia artificial.
Contenidos clave	– La Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su reglamento. – Iniciativas y anteproyectos de regulación de la IA en México: estado actual del debate legislativo. – Normativa sectorial relevante: disposiciones de ciberseguridad de la CNBV y criterios de la CONDUSEF para instituciones financieras. – Responsabilidad civil y penal: delitos informáticos del Código Penal Federal y daños derivados de sistemas de IA. – Intersección con la normativa laboral: vigilancia algorítmica y uso de IA en procesos de contratación. – Ejercicio de cierre: comparativo de la LFPDPPP frente al GDPR en una transferencia de datos matriz-subsidiaria, típica del nearshoring.

Módulo 3 · Noviembre 26 Riesgos para la empresa: la perspectiva in-house	
Objetivo	Que las personas participantes diseñen las políticas internas mínimas viables y el esquema de gobernanza de IA que una organización requiere para operar con riesgo jurídico controlado.
Contenidos clave	– Ransomware y extorsión de datos: impacto legal, obligaciones de notificación e implicaciones jurídicas de pagar un rescate. – Riesgo de terceros y cadena de suministro, crítico en la manufactura orientada al nearshoring. – Uso no gobernado de IA generativa por el personal (shadow AI) y fuga de información confidencial.

	– Responsabilidad por decisiones automatizadas sin supervisión humana; propiedad intelectual y contenido generado con IA. – El abogado in-house en el comité de gobernanza de IA: políticas mínimas viables (uso aceptable, clasificación de datos, gestión de accesos) y lenguaje común con el CISO y las áreas de IT. – Ejercicio de cierre: diseño de una política de uso aceptable de IA generativa para una empresa manufacturera con matriz extranjera.

Módulo 4 · Diciembre 3 Riesgos para el cliente: la perspectiva de despacho	
Objetivo	Que las personas participantes estructuren procesos de due diligence, cláusulas contractuales y estrategias de asesoría que protejan a clientes de distintos sectores frente a riesgos de ciberseguridad e IA.
Contenidos clave	– Due diligence de ciberseguridad e IA en operaciones de M&A: qué preguntar, qué documentos solicitar y qué red flags atender. – Cláusulas de protección de datos y ciberseguridad en contratos comerciales. – Cláusulas específicas para el uso de IA: representaciones y garantías, límites de responsabilidad y propiedad de los outputs. – SLAs con proveedores de tecnología y nube y su intersección con las obligaciones regulatorias del cliente. – Asesoría multisectorial y litigio post-incidente: fintech, manufactura e instituciones de ahorro; gestión de crisis legal. – Ética profesional: confidencialidad del cliente al usar herramientas de IA en la práctica legal propia. – Ejercicio de cierre: revisión y marcado de una cláusula contractual de IA y datos con errores comunes, para identificarlos y corregirlos.

Módulo 5 · Diciembre 10 Respuesta a incidentes desde la función legal	
Objetivo	Que las personas participantes formulen el protocolo de actuación legal ante un incidente de ciberseguridad, desde la detección hasta la remediación.
Contenidos clave	– Anatomía de un incidente: detección, contención, notificación y remediación, y el rol de la función legal en cada fase.

	– Plazos y destinatarios de la notificación: autoridades, personas afectadas y contrapartes contractuales. – Preservación del privilegio abogado-cliente durante la investigación forense. – Coordinación con aseguradoras: coberturas y exclusiones de las pólizas de ciberseguridad. – Ejercicio de cierre: simulacro tabletop guiado de una brecha de datos con toma de decisiones en tiempo real.

Metodología y experiencia formativa

- Sesiones en vivo con exposición conceptual orientada a la toma de decisiones, a cargo de personas docentes practicantes.
- Análisis de casuística real: casos internacionales y mexicanos, criterios regulatorios y precedentes relevantes.
- Un ejercicio aplicado por sesión (mapeo de exposición, comparativo normativo, política de uso aceptable, marcado de cláusulas y simulacro de brecha) con retroalimentación de la persona docente.
- Material asíncrono y recursos descargables en Canvas para profundizar entre sesiones, con seguimiento académico de Formación Profesional.

Resultados de aprendizaje

Al finalizar el programa, las personas participantes serán capaces de:

- Analizar el panorama regulatorio global y mexicano en materia de ciberseguridad e inteligencia artificial, su interacción y sus efectos sobre organizaciones mexicanas.
- Evaluar los riesgos de ciberseguridad e IA más relevantes según el rol profesional, in-house o de despacho, y el sector del cliente.
- Redactar y revisar cláusulas contractuales que atiendan riesgos de ciberseguridad, protección de datos y uso de IA.
- Diseñar políticas internas y esquemas de gobernanza de IA, incluida la participación en comités de riesgos.
- Estructurar procesos de due diligence de ciberseguridad e IA en operaciones de M&A.
- Formular protocolos de respuesta a incidentes desde la óptica legal y asesorar de manera preventiva y reactiva a consejos de administración.

Persona docente



Mtro. David Ricardo Morales Sánchez

Profesor de la Facultad Libre de Derecho de Monterrey

Egresado de Tulane University Law School con una Maestría en Comercio Internacional y Licenciado por la Facultad Libre de Derecho de Monterrey (FLDM). Posee experiencia en multinacionales como Heineken y Grupo AlEn. Es profesor de la FLDM, donde integra conocimientos jurídicos tradicionales con una comprensión avanzada de LegalTech, contratos inteligentes, automatización de procesos legales y tecnologías emergentes.

Constancia

Se otorgará Constancia de Participación con valor curricular, emitida por Formación Profesional de la Facultad Libre de Derecho de Monterrey, a quienes cumplan con al menos el 80% de asistencia y los requisitos académicos del programa.

Los programas de Formación Profesional no cuentan con reconocimiento de validez oficial de estudios otorgado por la Secretaría de Educación Pública, ni conducen a la obtención de título o grado académico con efectos oficiales.

Informes e inscripción

Formación Profesional – Facultad Libre de Derecho de Monterrey

Correo: profesional@fldm.edu.mx · WhatsApp: 81-2201-6771

Inscripción: www.fldm.mx/products/ciberseguridad

Morones Prieto 1000 Pte., esquina Alfonso Reyes, Valle Poniente, Santa Catarina, N.L., C.P. 66197, México.