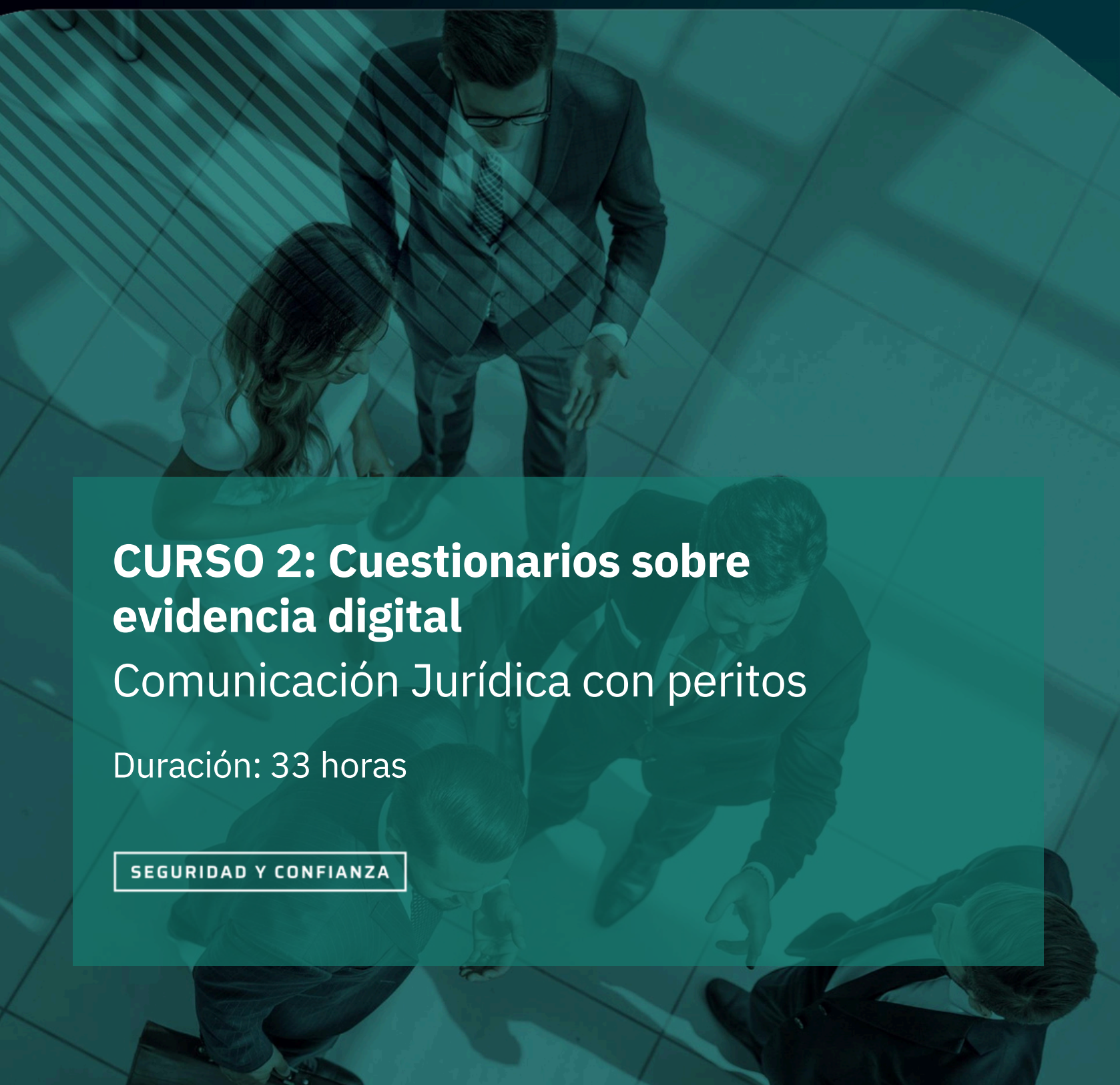
CERTIFICACIÓN

Competencias jurídicas en litigio de medios digitales y peritaje

Estructurada de acuerdo a ISO 17024



CURSO 2: Cuestionarios sobre evidencia digital

Comunicación Jurídica con peritos

Duración: 33 horas

SEGURIDAD Y CONFIANZA

Introducción:

La transformación digital ha cambiado radicalmente el panorama legal. La evidencia digital ya no es una excepción: es una constante en litigios civiles, mercantiles, penales y laborales. Esta realidad exige abogados capaces de comprender, cuestionar y utilizar técnicamente esta evidencia en juicio. Por ello, desarrollamos la **Certificación de Competencias Jurídicas en Litigio Digital**, un programa innovador compuesto por tres cursos en serie especializados que fortalecen la interacción efectiva entre el abogado litigante y el perito informático, con enfoque práctico, normativo y estratégico. ***Este temario corresponde al CURSO 2: Cuestionario sobre evidencia digital.***

Objetivo:

Desarrollar en los abogados la habilidad para formular cuestionamientos técnicos y jurídicos precisos y pertinentes dirigidos a peritos informáticos respecto a la evidencia digital obtenida de diversas fuentes tecnológicas. Esto se logrará mediante la comprensión de los conceptos técnicos esenciales, el reconocimiento de los formatos comunes de presentación de evidencia para cada tecnología, y la práctica intensiva en la creación de cuestionarios para el interrogatorio y contrainterrogatorio del perito.

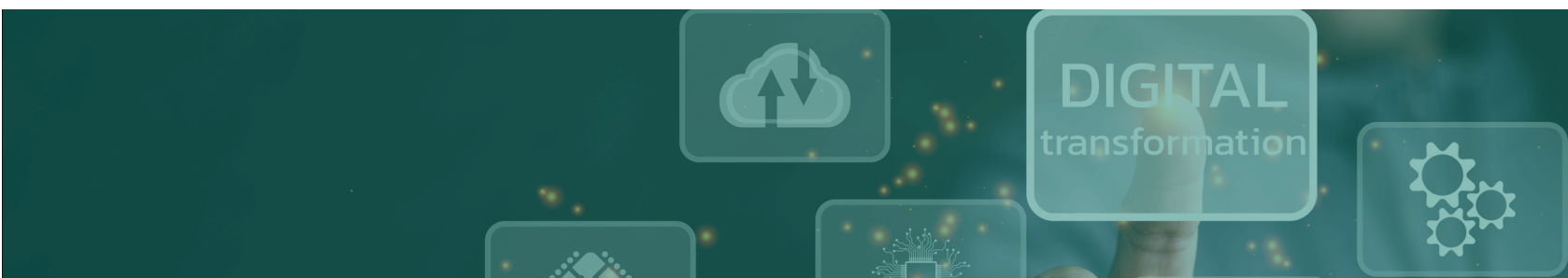
Al finalizar el curso el participante:

- Comprender los conceptos técnicos fundamentales asociados a la evidencia digital de las principales tecnologías (Sistemas Operativos, Móviles, Redes, Nube, Comunicaciones, etc.) necesarios para un interrogatorio informado.

- Identificar los formatos típicos en que se presenta la evidencia digital y los reportes periciales para cada tipo de tecnología.

- Formular preguntas específicas, basadas en los conceptos y formatos aprendidos, para el interrogatorio y contrainterrogatorio del perito informático sobre metodología, autenticidad, integridad, interpretación, alcance y limitaciones de los hallazgos .

- Adaptar estratégicamente los cuestionarios al tipo específico de tecnología y al contexto del caso.



¿Para quién es este programa?

- Abogadas y Abogados litigantes.
- Autoridades jurisdiccionales (Juezas, Jueces, Magistradas y Magistrados).
- Profesionales del derecho interesados en actualizar sus competencias frente a la transformación tecnológica del sistema judicial.
- Servidores públicos, ministerios públicos y defensores que desean reforzar su capacidad para valorar evidencia digital.
- Estudiantes y pasantes de derecho.

Requisitos

Para tomar este curso el participante deberá de cumplir con al menos uno de estos puntos:

- Abogados que hayan completado el Curso 1: "Introducción a la Prueba Digital".
- Demostrar conocimientos equivalentes sobre los fundamentos de la prueba digital, cadena de custodia y la estructura básica del dictamen pericial.

Contenido Temático

Tema 1: OSINT y Evidencia Web/Redes Sociales

a. Conceptos Clave para el Interrogatorio: OSINT (Definición, fuentes públicas), búsqueda avanzada (operadores, dorks), autenticación de perfiles, preservación web (volatilidad, métodos), scraping (límites).
b. Formatos Comunes de Evidencia y Reportes Periciales: capturas de pantalla certificadas/con metadatos, archivos WARC (Web ARChive), reportes de herramientas OSINT, exportaciones de datos de redes sociales (vía API o herramientas), registros WHOIS/DNS.
c. Desarrollo de Cuestionarios para Peritos: aplicación de cuestionamientos clave

i. Validación de la metodología .
ii. Confirmación de la cadena de custodia e integridad .
iii. Clarificación de hallazgos técnicos .
iv. Exploración de limitaciones o interpretaciones alternativas .
v. Vinculación con los hechos del caso.

Tema 2: Sistemas Operativos de Escritorio

a. Conceptos Clave para el Interrogatorio: sistema de archivos NTFS, registro de Windows (función, claves relevantes: USBs, programas instalados), logs de eventos EVTX (tipos de eventos: login, ejecución), metadatos MACB (significado de fechas), artefactos de ejecución (LNK, Jump Lists, Prefetch).
b. Formatos Comunes de Evidencia y Reportes Periciales: exportaciones del Registro (ej. claves específicas en .reg o reportes), archivos EVTX, archivos LNK/Jump Lists, archivos Prefetch/Superfetch, reportes de timelines forenses .
c. Desarrollo de Cuestionarios para Peritos: aplicación de cuestionamientos clave:

i. Validación de la metodología .
ii. Confirmación de la cadena de custodia e integridad .
iii. Clarificación de hallazgos técnicos .
iv. Exploración de limitaciones o interpretaciones alternativas .
v. Vinculación con los hechos del caso.

Tema 3: Dispositivos Móviles (iOS/Android)

a. Conceptos Clave para el Interrogatorio: diferencias iOS/Android relevantes, tipos de extracción (Lógica, Sistema Archivos, Física, Cloud) y qué obtiene cada una, cifrado y bloqueos (impacto en acceso), bases de datos SQLite (comunes en apps), fuentes de geolocalización (GPS, Wi-Fi, celdas, metadatos fotos).
b. Formatos Comunes de Evidencia y Reportes Periciales: reportes de herramientas forenses (Cellebrite, Magnet AXIOM - PDF, HTML), bases de datos SQLite, archivos de configuración (plist en iOS), exportaciones de llamadas/SMS/chats, datos de geolocalización (KML, GPX), archivos multimedia con metadatos.
c. Desarrollo de Cuestionarios para Peritos: aplicación de cuestionamientos clave:

i. Validación de la metodología .
ii. Confirmación de la cadena de custodia e integridad .
iii. Clarificación de hallazgos técnicos .
iv. Exploración de limitaciones o interpretaciones alternativas .
v. Vinculación con los hechos del caso.

Tema 4: Evidencia de Red y Tráfico de Datos

a. Conceptos Clave para el Interrogatorio: direcciones IP (públicas vs. privadas, DHCP), protocolos TCP/UDP (diferencia básica), DNS (traducción nombre-IP), capturas de tráfico PCAP (qué contienen), logs de Firewall/Proxy (qué registran), NetFlow/IPFIX (metadatos de comunicación), impacto del cifrado (TLS/SSL).
b. Formatos Comunes de Evidencia y Reportes Periciales: archivos PCAP, reportes de análisis (Wireshark, NetworkMiner), logs exportados (Firewall, Proxy, IDS/IPS - texto, CSV, syslog), registros NetFlow/IPFIX, diagramas de red.
c. Desarrollo de Cuestionarios para Peritos: aplicación de cuestionamientos clave:

i. Validación de la metodología .
ii. Confirmación de la cadena de custodia e integridad .
iii. Clarificación de hallazgos técnicos .
iv. Exploración de limitaciones o interpretaciones alternativas .
v. Vinculación con los hechos del caso.

Tema 5: Evidencia en la Nube (Cloud Forensics) y SaaS

a. Conceptos Clave para el Interrogatorio: modelos IaaS/PaaS/SaaS y Responsabilidad Compartida, principales proveedores (AWS, Azure, GCP), logs de proveedor (CloudTrail, Azure Monitor, etc. - qué registran), snapshots (qué son, para qué sirven), jurisdicción y acceso a datos (MLATs, CLOUD Act).
b. Formatos Comunes de Evidencia y Reportes Periciales: logs exportados (JSON, CSV), logs de aplicaciones SaaS (formatos específicos), snapshots (formatos de imagen virtual), reportes de herramientas de adquisición cloud, correspondencia con proveedores, contratos de servicio .
c. Desarrollo de Cuestionarios para Peritos: aplicación de cuestionamientos clave:

i. Validación de la metodología .
ii. Confirmación de la cadena de custodia e integridad .
iii. Clarificación de hallazgos técnicos .
iv. Exploración de limitaciones o interpretaciones alternativas .
v. Vinculación con los hechos del caso.

Tema 6: Correos Electrónicos y Mensajería Instantánea

a. Conceptos Clave para el Interrogatorio: encabezados de email (qué información contienen, rastreo de ruta), spoofing (falsificación de remitente), autenticación (SPF, DKIM, DMARC - propósito), formatos (PST, MBOX, EML), cifrado de extremo a extremo (limitaciones), Legal Hold / eDiscovery (qué es).
b. Formatos Comunes de Evidencia y Reportes Periciales: correos en formato EML o contenedores PST/MBOX, análisis de encabezados (en reportes), reportes de herramientas forenses de email, exportaciones de chats (formatos variables, bases de datos SQLite), capturas certificadas (como último recurso), documentación de Legal Holds.
c. Desarrollo de Cuestionarios para Peritos: aplicación de cuestionamientos clave:

i. Validación de la metodología .
ii. Confirmación de la cadena de custodia e integridad .
iii. Clarificación de hallazgos técnicos .
iv. Exploración de limitaciones o interpretaciones alternativas .
v. Vinculación con los hechos del caso

Tema 7: IoT, Forense Vehicular y Criptomonedas

a. Conceptos Clave para el Interrogatorio: IoT (fuentes de evidencia: dispositivo, app, nube), forense vehicular (Sistemas Infotainment, EDR, CAN bus), cripto (Blockchain, wallets, transacciones, exploradores), anonimato/Pseudonimato en cripto y rastreo.
b. Formatos Comunes de Evidencia y Reportes Periciales: logs de IoT, firmware extraído, datos de apps móviles, datos de EDR, datos de infotainment, reportes de análisis de blockchain (diagramas), información de exchanges (si se obtiene legalmente).
c. Desarrollo de Cuestionarios para Peritos: aplicación de cuestionamientos clave:

i. Validación de la metodología .
ii. Confirmación de la cadena de custodia e integridad .
iii. Clarificación de hallazgos técnicos .
iv. Exploración de limitaciones o interpretaciones alternativas .
v. Vinculación con los hechos del caso

Tema 8: Inteligencia Artificial

a. Conceptos Clave para el Interrogatorio: IA vs. ML (básico), datos de entrenamiento vs. Inferencia, logs de inferencia (qué registran), sesgo (Bias) en modelos, ataques adversariales y Prompt Injection, explicabilidad (XAI - por qué es importante).
b. Formatos Comunes de Evidencia y Reportes Periciales: logs de inferencia, reportes de análisis de seguridad del modelo (sesgos, vulnerabilidades), datos de entrenamiento (si accesibles), código fuente (si aplica), dictámenes explicando funcionamiento / fallos / manipulación.
c. Desarrollo de Cuestionarios para Peritos: aplicación de cuestionamientos clave:

i. Validación de la metodología .
ii. Confirmación de la cadena de custodia e integridad .
iii. Clarificación de hallazgos técnicos .
iv. Exploración de limitaciones o interpretaciones alternativas .
v. Vinculación con los hechos del caso

Tema 9: Audio y Video

a. Conceptos Clave para el Interrogatorio: formatos y Calidad (Audio/Video), metadatos (Audio/Video), autenticación (detección ediciones/manipulación), análisis ENF (Electric Network Frequency - audio), mejora (límites y documentación), identificación de Locutor (limitaciones), deepfakes (qué son, detección).
b. Formatos Comunes de Evidencia y Reportes Periciales: archivo original (audio/video), copia trabajada (mejorada), reporte análisis autenticidad/integridad, reporte ENF, reporte mejora, dictamen identificación locutor, reporte análisis deepfake, transcripciones, fotogramas clave.
c. Desarrollo de Cuestionarios para Peritos: Aplicación de Cuestionamientos Clave:

i. Validación de la metodología .
ii. Confirmación de la cadena de custodia e integridad .
iii. Clarificación de hallazgos técnicos .
iv. Exploración de limitaciones o interpretaciones alternativas .
v. Vinculación con los hechos del caso

Evaluación:

Dos casos prácticos simulados donde los participantes deberán:

1.Analizar un informe pericial (provisto) que involucre una o más tecnologías vistas en el curso, identificando conceptos clave y formatos de evidencia presentados.

2.Elaborar un cuestionario detallado y estructurado (preguntas para interrogatorio y contrainterrogatorio) dirigido al perito informático, basado en los hallazgos del informe y aplicando las técnicas aprendidas.

Para mayor información, contáctenos:
contacto@nyce.org.mx
(55) 12045190