COMPUTING
ANALYSIS FORENSICS
SPECIALIZED CERTIFICATION

duriva

Certifícate como Perito en Informática Forense con la oferta más completa de Latinoamérica.

Los fraudes digitales, estafas comerciales y bancarias, robo y manipulación de datos, usurpación de identidad, espionaje industrial, ataques contra la protección de datos personales y phishing, son hoy los **principales delitos** en entornos tanto empresariales como personales.

Por ello, en Duriva formamos expertos en ciberseguridad e informática forense, con **más de 16 años** liderando el sector en México y América Latina. Nuestras certificaciones, actualizadas al contexto del 2025, cuentan con reconocimiento judicial y te permitirán integrarte a una red profesional internacional que impulsará tu carrera.

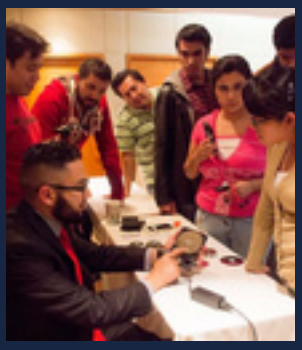
Con **104 generaciones certificadas** desde Tijuana hasta Buenos Aires, actualizamos continuamente nuestros temarios para adaptarlos a la realidad y los desafíos del 2025. Con más de 16 años dedicados completamente a la informática forense, te proporcionará conocimientos prácticos, actualizados y enfocados a tu beneficio profesional.

En Duriva no solo recibirás una certificación especializada y prestigiosa, también formarás parte de una red profesional internacional que te ayudará a destacar en tu carrera.

¿Por qué elegir Duriva?

Empresa líder en América Latina.

Con más de 16 años de experiencia y reconocimiento judicial contamos con el mayor número de expertos capacitados, aportando formación de vanguardia.



Temario más amplio.

Cubrimos una mayor cantidad de temas y profundizamos en ellos, ofreciendo una formación completa e integral que supera lo habitual en el mercado.

Experiencia con policías cibernéticas.

El mismo nivel de excelencia que ofrecemos a cuerpos de seguridad se extiende a nuestros cursos abiertos al público.

Más de 100 generaciones satisfechas

Avalan la calidad de nuestros cursos y nuestra experiencia formando a profesionales en Cómputo Forense y Ciberseguridad.

Reconocimiento internacional.

Somos parte del American Council for Cybersecurity and Computer Forensic (ACCCF), lo que respalda el prestigio de nuestros programas.

Instructor pionero.

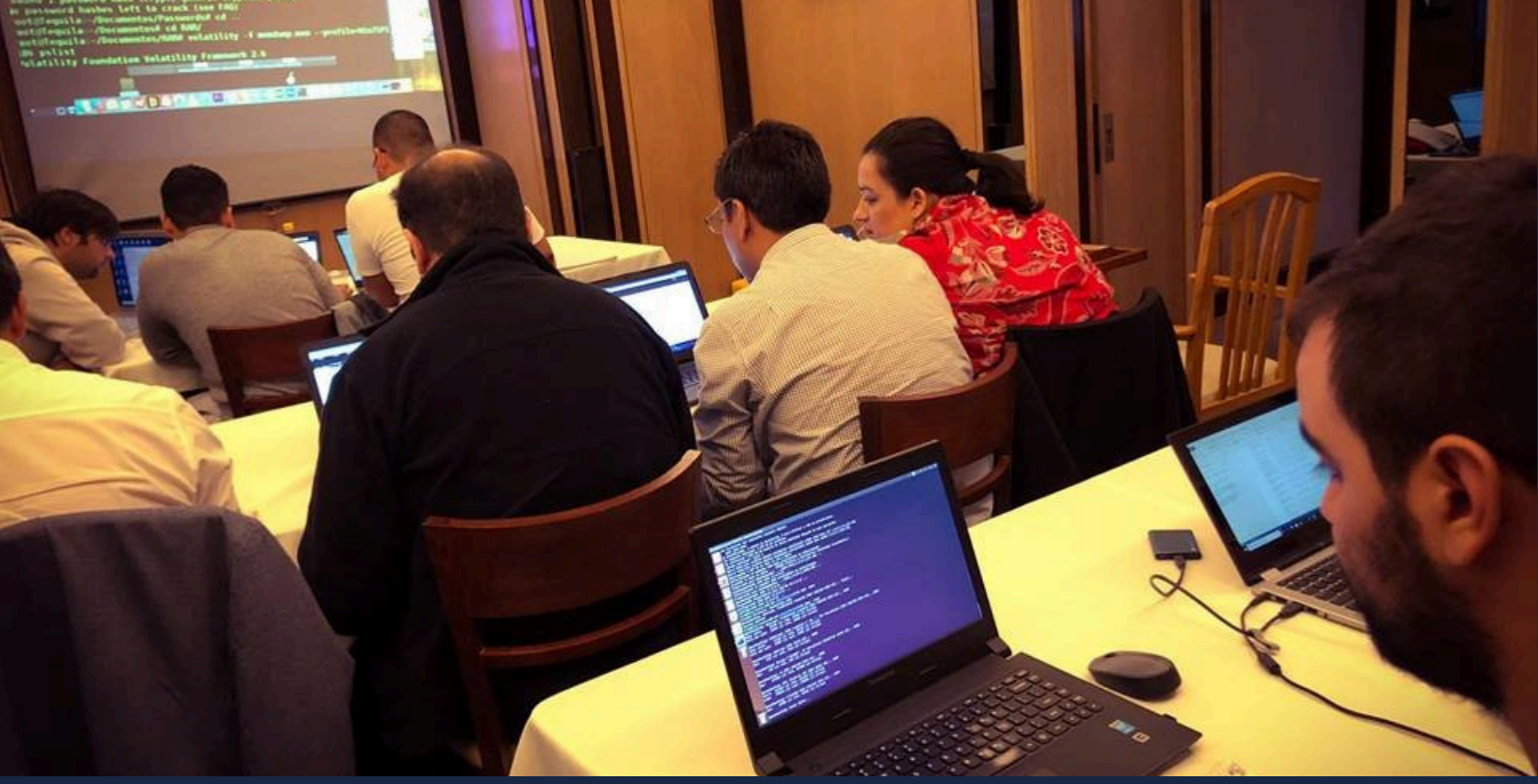
Nuestro docente cuenta con amplia trayectoria y ha desarrollado metodologías que hoy sirven de referente para otras instituciones.

Red internacional de contactos.

Formamos parte de una comunidad global que promueve colaboraciones y alianzas, facilitando oportunidades de networking y conexión con expertos en distintos países.

Valor curricular en México.

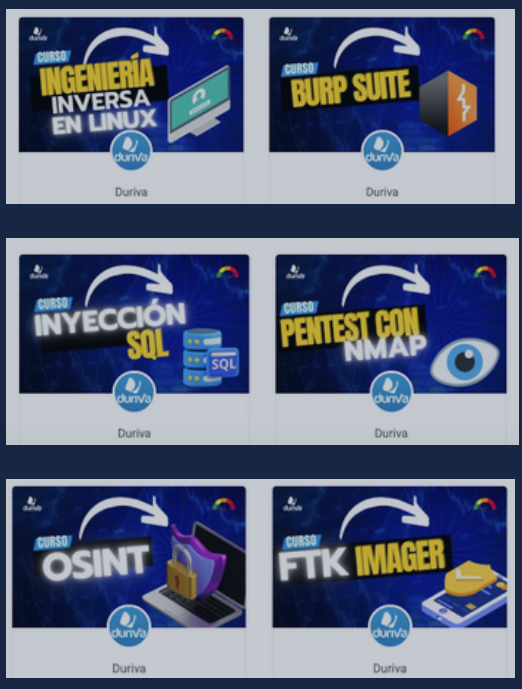
Registrados ante la Secretaría del Trabajo y Previsión Social (STPS) con el número CID1107146P8-0015, lo cual otorga una sólida validez oficial.



"Desde 2008, nuestra meta ha sido desarrollar futuros líderes en peritaje informático. Por ello, nuestros cursos y certificaciones cuentan con valor curricular ante la STPS y la ACCCF."

A través de **Duriva University,** los alumnos obtienen acceso a un curso propedéutico y disfrutan de 6 meses de acceso a contenidos exclusivos, donde se profundiza en los temas más relevantes de la industria.

duriva.university



Resumen del Temario

Contamos con un **propedéutico** y **9 módulos** diseñados para abordar desde las bases legales y técnicas del cómputo forense hasta las metodologías avanzadas de ciberseguridad. Además, en cada módulo se incluye **un caso práctico** que permite aplicar de forma inmediata los conocimientos adquiridos.

Módulos:

1. **Fundamentos Operativos de la Investigación Digital.**
2. **Adquisición y Preservación de Evidencia Digital.**
3. **Sistemas de Archivos.**
4. **Análisis Forense en Windows.**
5. **Análisis Forense en Entornos Linux.**
6. **Evidencia Volátil, Memoria y Respuesta Rápida.**
7. **Forense en Dispositivos Móviles y Registros Telefónicos.**
8. **Análisis de Audio, Video y Fuentes Multimediales**
9. **Integración Global de Evidencias y Presentación Final.**

¿A QUIÉN VA DIRIGIDO?

Este curso es para cualquier persona interesada en ciberseguridad e informática forense, sin importar su experiencia. Con un enfoque práctico desde cero, es ideal para quienes buscan aprender y aplicar estos conocimientos.

Especialmente dirigido a:

- **Profesionales en informática** que buscan especializarse en auditoría, gestión y consultoría en ciberseguridad y peritaje informático.

- **Técnicos informático**s de empresas y organismos públicos que desean aplicar sus conocimientos en investigación forense digital.

- **Abogados y especialistas en criminología** interesados en comprender la evidencia digital y su impacto en investigaciones legales.
- **Policías y fuerzas del orden** que requieren formación en análisis forense digital para fortalecer su labor en investigaciones. (Descuento especial para agentes de policía).
- **Responsables de seguridad informática** en entidades públicas y privadas que buscan reforzar sus competencias y compartir experiencias.

- **Estudiantes y recién titulados** que desean adquirir una ventaja competitiva con formación práctica y actualizada.

Si te apasiona la ciberseguridad y la investigación digital, este curso es para ti. **No necesitas experiencia previa, solo ganas de aprender**

MÓDULO I.

Fundamentos Operativos de la Investigación Digital.

Sienta las bases para reconocer escenarios forenses domésticos y empresariales, así como la forma de gestionar información crítica. Se estudia la trazabilidad de distintos dispositivos y la manera de abordar las exigencias legales.

1. Reconocimiento del Entorno Forense

- Diferencias de escenarios: entorno doméstico vs. entorno empresarial.
- Trazabilidad de dispositivos (PC, laptop, móviles, sistemas embebidos).

2. Requisitos Legales y Admisibilidad de la Evidencia

- Peticiones de datos a terceros (proveedores de telefonía, ISP, redes sociales).
- Respuestas típicas y cómo interpretarlas (logfiles, metadatos, registros transaccionales…).
- Validación de la información: sellos, firmas, acuses de recibo.

3. Gestión de la Evidencia Compleja

- Casos con múltiples soportes (varios discos, USB, teléfonos, tablets…).
- Herramientas de etiquetado automatizado y tracking (códigos QR, software de inventario).

4. Estrategias de Coordinación Multidisciplinaria

- Cooperación con departamentos legales, recursos humanos o directivos.
- Manejo de documentación compartida y cronogramas de intervención.

5. Caso Práctico

- Diseño de un plan de recolección simultánea en distintos puntos de una empresa, con preparación de la documentación y comunicaciones previas.

MÓDULO II.

Adquisición y Preservación de Evidencia Digital.

Aborda las técnicas y herramientas para clonar y conservar evidencia, desde pequeños dispositivos hasta altos volúmenes de datos. Se explica cómo verificar la integridad de la información y organizarla de forma sistemática.

1. Hardware y Configuraciones Avanzadas de Clonación

- Adaptadores (SAS, NVMe, eMMC…) y sus usos forenses.
- Protocolos de interfaz menos comunes (PCIe, Thunderbolt).
- Empleo de duplicadores forenses especializados (Tableau, Logicube…).

2. Automatización en la Duplicación

- Scripting para clonaciones masivas (bash, PowerShell…).
- Integraciones con herramientas como Belkasoft Evidence Center o Autopsy para generación automática de reportes de hash.

3. Verificaciones de Integridad y Criptografía

- Uso de hashes múltiples (MD5, SHA-1, SHA-256, SHA-3) para mayor robustez
- Almacenamiento de claves y contraseñas en entornos seguros (HSM, cofres digitales).

4. Organización de Grandes Volúmenes

- Estrategias de particionado y segmentación de imágenes cuando el disco es muy grande
- Metodologías de archivado en servidores forenses (NAS, SAN) para equipos con decenas de TB.

5. Caso Práctico

- Clonación simultánea de varios discos duros con adaptadores diferentes, creando registros detallados y aplicando verificación con hashes avanzados.

MÓDULO III.
Sistemas de Archivos.

Presenta en detalle la estructura interna de los sistemas de archivos, tanto en entornos Windows como Linux. Se analizan las principales técnicas de recuperación de datos borrados y la interpretación de metadatos relevantes para la investigación.

1. Estructura General y Tipos de Partición
- MBR y GPT: diferencias y espacios de arranque.
- Sectores, clústeres, asignaciones y metadatos.

2. Principales Sistemas de Archivos en Entornos Windows
- FAT, exFAT, NTFS: características, journaling, recuperación de archivos borrados.
- Flujos alternos de datos (ADS) y su relevancia en investigaciones.

3. Sistemas de Archivos en Entornos Linux
- ext2, ext3, ext4: inodos, journaling, permisos.
- Manejo de directorios y reservas de bloques.

4. Búsqueda y Recuperación de Información Específica
- Identificación de archivos eliminados o fragmentados.
- Comparación de hashes e integridad a nivel de archivo.

5. Caso Práctico
- Análisis de una unidad con múltiples particiones (NTFS y ext) donde se localizan datos eliminados para su posterior documentación forense.

MÓDULO IV.
Análisis Forense en Windows.

Examina artefactos clave del sistema operativo Windows, cubriendo también la investigación de correos criminales. El módulo enfatiza la correlación de eventos en entornos empresariales y la búsqueda de flujos alternos de datos que puedan ocultar evidencia.

1. Artefactos Profundos de Windows
- Profundización en “Registry Hives” (SYSTEM, SAM, SECURITY, SOFTWARE, NTUSER…).
- Logs avanzados: Sysmon, PowerShell logs, rastreo de ejecutables (.evtx).

2. Análisis en Entornos Empresariales
- Detección de uso de Windows Server (Active Directory, GPO, roles…).
- Escenarios con múltiples usuarios y perfiles.
- Scripts de administración y sus impactos en la seguridad.

3. Investigación de Correos Criminales
- Autenticación de correos (encabezados, DKIM, SPF, DMARC).
- Detección de correos falsificados y phishing.
- Extracción de buzones (PST/OST) y correlación con la actividad del equipo.

4. Recuperación y Análisis de Datos Ocultos
- Investigaciones de flujos alternos (ADS).
- Búsqueda de copias sombras (Shadow Copy) y volúmenes anteriores.
- Desensamblado básico de ejecutables sospechosos.

5. Caso Práctico
- Análisis de un sistema Windows Server 2019 con varios usuarios, donde se detectan patrones de acceso anómalo y modificaciones en directivas de grupo, así como correos manipulados.

MÓDULO V.

Análisis Forense en Entornos Linux.

Detalla la investigación de logs y configuraciones en servidores Linux. Se muestran métodos para detectar intrusiones, localizar rootkits y correlacionar eventos en servicios web y bases de datos, elaborando líneas de tiempo coherentes.

1. Manejo Avanzado de Logs y Configuraciones
- Revisión de systemd journals, logs rotados y archivados.
- Detección de configuraciones personalizadas.
- Identificación de contenedores (Docker).

2. Persistencia y Revisiones de Seguridad
- Comprobación de binarios críticos con checksums.
- Revisión de permisos suid/sgid, parches del kernel instalados.
- Identificación de rootkits a nivel kernel.

3. Trazado de Redes Internas en Linux
- Comandos ip, ss, netstat, lsof para análisis forense.
- Registro y mapeo de puertos abiertos, servicios en segundo plano.

4. Correlación Multilog
- Integración de logs de Apache/Nginx, MySQL/MariaDB y correos.
- Generación de timelines al unificar varios orígenes.

5. Caso Práctico
- Análisis de un servidor Linux que aloja un servicio web y base de datos, con indicios de intrusiones repetidas y manipulación de configuraciones.

MÓDULO VI.

Evidencia Volátil, Memoria y Respuesta Rápida.

Explica la toma de datos en sistemas en funcionamiento, aprovechando herramientas para capturar memoria y conexiones de red al momento. Se aprende a realizar una respuesta inmediata ante incidentes y documentar la información de forma efectiva.

1. Herramientas Estructuradas de Respuesta a Incidentes
- LiME, Volatility, Rekall para Linux y Windows.
- Scripts de “live response” que recolectan datos clave (PSRecon, LiveResponse, etc.).

2. Examinando la RAM en Búsquedas Complejas
- Identificación de strings relevantes (contraseñas, tokens, llaves).
- Comparación de direcciones de memoria con binarios en disco.
- Reconocimiento de inyecciones de proceso, hooking, etc.

3. Mapeo de Conexiones de Red en Memoria
- Localización de sockets ocultos o puertos no oficiales.
- Trazas en la tabla ARP, DNS cache y conexiones salientes.

4. Gestión Inmediata de la Escena
- Elaboración de mini-laboratorios portátiles para capturar la evidencia.
- Técnicas de priorización: qué tomar primero (logs, RAM, disco) según el caso.

5. Caso Práctico
- Aplicación de un guion de respuesta a incidentes en un sistema “comprometido” en tiempo real, recolectando datos de RAM y correlacionándolos con registros del disco.

MÓDULO VII.

Forense en Dispositivos Móviles y Registros Telefónicos.

Explica la toma de datos en sistemas en funcionamiento, aprovechando herramientas para capturar memoria y conexiones de red al momento. Se aprende a realizar una respuesta inmediata ante incidentes y documentar la información de forma efectiva.

1. Extracciones Avanzadas en Android y iOS
- Manejo de bootloaders y utilidades de root/jailbreak (sólo a nivel forense).
- Extracción de volúmenes cifrados, coping BFS (Block File System).

2. Aplicaciones de Mensajería
- Recuperación de bases de datos SQLite en WhatsApp, Telegram, Signal.
- Identificación de archivos multimedia y duplicados en la memoria del teléfono.

3. Correlación de Sábanas de Llamadas
- Lectura detallada de antenas, celdas, triangulación.
- Cruce con datos de geolocalización en el móvil (GPS interno, WiFi).
- Detección de puntos críticos (noches, horarios laborales, etc.).

4. Herramientas Móviles Avanzadas
- Cellebrite UFED, Magnet AXIOM Mobile, Oxygen Forensic Detective.
- Scripts de Python para parseo rápido de logs en masa.

5. Caso Práctico
- Se recibe un smartphone con respaldo en la nube (sin tratar la temática de cloud). Con la extracción, se cruza con sábanas de llamadas del operador, hallando incongruencias de horarios.

MÓDULO VIII.

Análisis de Audio, Video y Fuentes Multimediales

Enseña la validación de contenidos audiovisuales para identificar ediciones, superposiciones o modificaciones. El estudiante integra metadatos y analiza cada fotograma o muestra de audio, corroborando la autenticidad de lo presentado.

1. **Procesamiento Forense de Audio**
   a. Herramientas específicas (Audacity, Adobe Audition, Ocenaudio).
   b. Estructura interna de WAV, MP3, FLAC, manipulación de bitrate.
   c. Filtrado de ruido y segmentación de canales.
2. **Video y Metadatos Detallados**
   a. Contenedores (MKV, MP4, AVI), codecs (H.264, HEVC).
   b. Revisión de timestamps, fotogramas insertados, saltos sospechosos.
   c. Extracción de metadatos en software como FFmpeg, Avidemux.
3. **Edición, Superposiciones y Sintetizaciones**
   a. Ajustes de color o transiciones para disimular cortes.
   b. Audio superpuesto, mezcla de conversaciones en un solo track.
   c. Validación de la fuente original con checksums y secuencias de fotogramas.
4. **Integración en la Narrativa Forense**
   a. Enlace con registros telefónicos o informáticos para corroborar tiempos.
   b. Formato de documentación para clips de audio y video.
5. **Caso Práctico**
   a. Se suministra un archivo de video con edición sospechosa y un audio con supuestas conversaciones. El alumno debe detectar las inconsistencias y presentarlas en un miniinforme forense.

MÓDULO IX.

Integración Global de Evidencias y Presentación Final.

Concluye unificando las distintas fuentes de evidencia (Windows, Linux, móviles, multimedia). Se crea un informe integral y se practica la exposición ante instancias legales o de auditoría, resolviendo objeciones y preguntas técnicas.

1. **Unión de Hallazgos Complejos**
   - Técnicas de timeline avanzado para unificar registros de Windows, Linux, móviles, audio y video.
   - Categorización de hallazgos según relevancia para la investigación.
2. **Redacción de Informes Forenses Exhaustivos**
   - Estructura: objetivos, metodología aplicada, evidencia analizada, conclusiones parciales.
   - Incluir representaciones gráficas (mapas, cronogramas, correlaciones).
3. **Gestión de Información Masiva**
   - Procesamiento big data en la forense.
   - Casos con decenas o cientos de dispositivos involucrados.
   - Herramientas para indexar y buscar de forma distribuida (p.ej. Splunk).
4. **Simulación de Presentación Ante Autoridades**
   - Preparar discurso conciso para clientes, auditores o tribunales.
   - Preguntas frecuentes y objeciones más comunes.
5. **Caso Práctico Integral**
   - Los participantes reciben un caso con evidencias de disco Windows, logs de Linux, dispositivos móviles y archivos multimedia. Deben elaborar un informe final unificado considerando que es un caso real.

SOBRE EL INSTRUCTOR

El curso es impartido por **Jocsan Laguna Romero**, pionero en **Cómputo Forense en América Latina.** Fue el creador de la primera distribución de Cómputo Forense de la región, la cual presentó en el auditorio de la **Facultad de Ingeniería de la UNAM**. Su innovación tuvo un gran impacto, siendo ampliamente difundida en medios de circulación nacional como Aristegui Noticias, Excélsior, El Financiero, la Gaceta de la UNAM y CONACYT, entre otros..

SESIONES ONLINE EN DIRECTO

Podrás seguir e intervenir en las sesiones desde cualquier lugar, sin necesidad de desplazarte.

NETWORKING INTERNACIONAL

Podrás conocer e interactuar con otros participantes de toda Latinoamérica, estableciendo contacto tanto de forma virtual como presencial a lo largo del curso.

Como alumno adquirirás las competencias necesarias para:

- Dominar los conocimientos esenciales para llevar a cabo investigaciones sobre delitos relacionados con las Tecnologías de la Información (TI), aplicando técnicas avanzadas de Cómputo Forense.
- Adquirir noción sobre los aspectos legales necesarios para presentar adecuadamente los resultados de la evidencia digital en procesos judiciales.
- Gestionar y organizar un análisis informático de manera eficiente y estructurada.
- Abordar sistemas Windows, Linux y Android desde un enfoque altamente especializado, permitiendo la recuperación de información incluso cuando el software comercial presenta limitaciones.

DATOS CLAVE

Duración

- 40 horas de formación principal.[1]
- 10 horas adicionales de curso propedéutico, diseñado para nivelar conocimientos y maximizar el aprendizaje.

Requerimientos

- Espacio en disco duro: 160 GB
- Memoria RAM: 8 GB
- Procesador: Intel i7 o equivalente superior.
- Si usas Mac: Para garantizar una experiencia óptima, avísanos con anticipación. Debido a la arquitectura de los procesadores Mac, la virtualización estándar de Windows no es compatible con algunas herramientas. Te proporcionaremos una máquina virtual preconfigurada para que puedas seguir el curso sin inconvenientes.

Beneficios al completar el curso

- Al finalizar y aprobar la evaluación, los alumnos podrán desempeñarse como analistas de riesgos informáticos y especialistas en la detección de intrusos en redes corporativas.[2]
- Obtendrán **doble constancia** con valor curricular avalada por la Secretaría del Trabajo y Previsión Social (STPS) y el American Council for Cybersecurity and Computer Forensic (ACCCF).[3]

Curso Propedéutico

- Sabemos que no todos los participantes cuentan con el mismo nivel de conocimiento previo. Por ello, hemos desarrollado un curso propedéutico de 10 horas, diseñado para garantizar que todos los alumnos aprovechen al máximo la formación principal.

1.-El temario del contenido de curso, como el uso de nuevas versiones de aplicaciones o sistemas operativos más actualizados.
2.-La constancia con valor curricular ante la STPS, así como la del ACCCF, se obtiene una vez que el alumno aprueba la evaluación de conocimientos.
3.- Al finalizar cada uno de los temas se realizan ejercicios para poner en práctica lo aprendido, además, se añaden laboratorios con distintos niveles de complejidad, desde básico a avanzado, que en el último modulo serán resueltos en su totalidad por los instructores.
Puede llegar a tener modificaciones siempre que sean para mejorar el temario del curso.

CAFSC

COMPUTING
ANALYSIS FORENSICS
SPECIALIZED
CERTIFICATION

Duriva® 2025

Consultoría Integral en Desarrollo Mecatrónico SA de CV

informaticaforense

Duriva

@duriva

@duriva

Av Patriotismo 201, piso 4, San Pedro de los Pinos,
Benito Juárez, 03800 Ciudad de México, CDMX

consulta@duriva.com | **52 (55) 8852 7509**