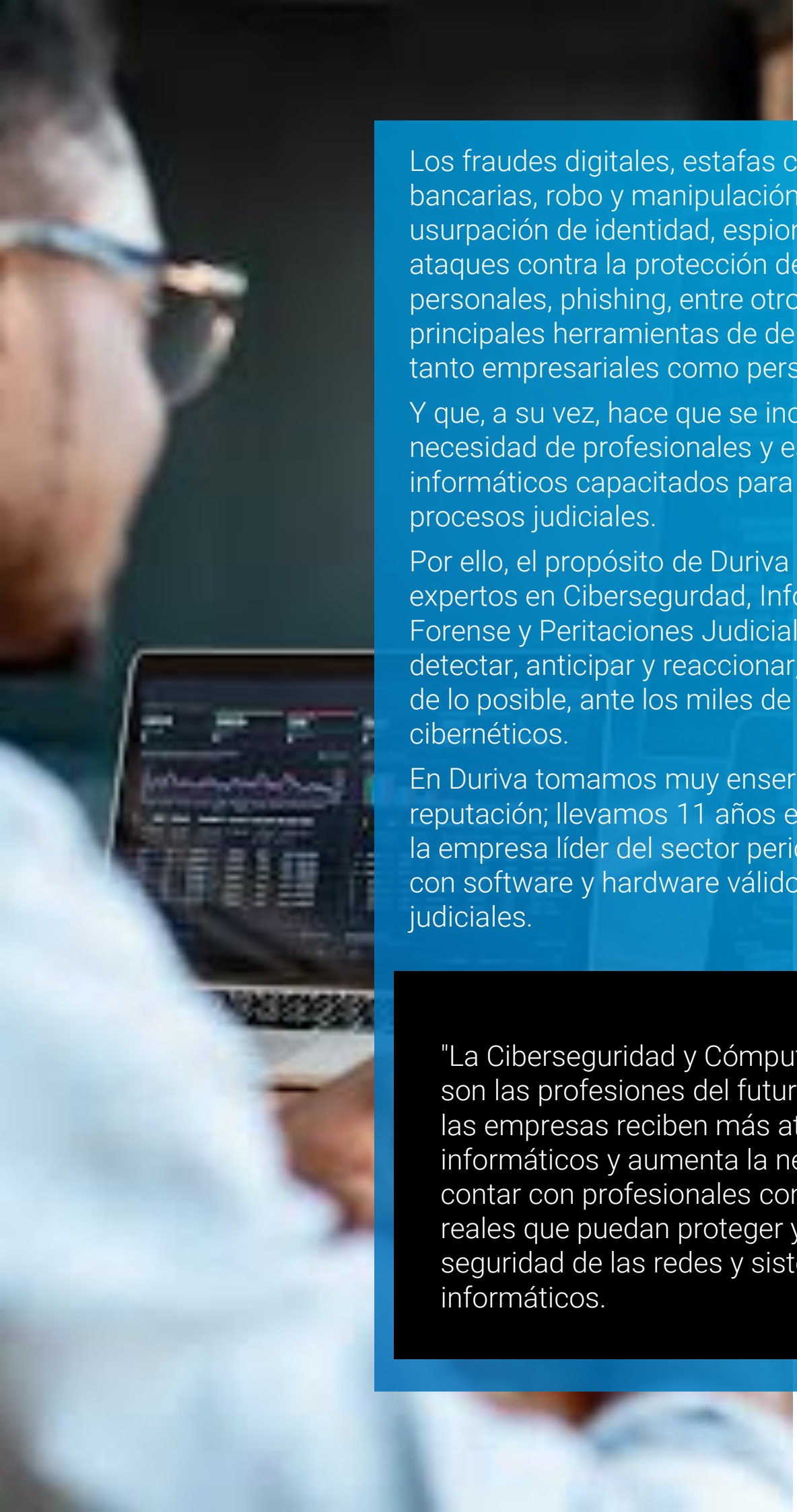
duriva

COMPUTING

ANALYSIS FORENSICS

SPECIALIZED CERTIFICATION



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

Y que, a su vez, hace que se incremente la necesidad de profesionales y especialistas informáticos capacitados para intervenir en procesos judiciales.

Por ello, el propósito de Duriva es formar expertos en Cibersegurdad, Informática Forense y Peritaciones Judiciales capaces de detectar, anticipar y reaccionar, en la medida de lo posible, ante los miles de ataques cibernéticos.

En Duriva tomamos muy enserio nuestra reputación; llevamos 11 años en México siendo la empresa líder del sector pericial informático con software y hardware válido en procesos judiciales.

"La Ciberseguridad y Cómputo Forense son las profesiones del futuro... Cada día las empresas reciben más ataques informáticos y aumenta la necesidad de contar con profesionales con habilidades reales que puedan proteger y auditar la seguridad de las redes y sistemas informáticos.

"Desde el 2008 tenemos la meta de desarrollar futuros líderes en peritaje informático, es por ello por lo que nuestros cursos y certificaciones tienen valor curricular ante la STPS y la ACCCF".

Duriva University, es el campus prestigioso en América Latina para certificarse en temas de Ciberseguridad y Cómputo Forense, debido a la trayectoria internacional.

"Nuestra experiencia es reconocida en toda América Latina, por lo que hemos transmitido nuestros conocimientos a entidades de justicia y fuerzas del orden del continente".

¿Por qué elegir DURIVA?

Somos la empresa de América Latina con más expertos capacitados, 100 generaciones de expertos están satisfechos para la calidad de los cursos.

Con la misma calidad y profesionalismo que adiestramos a distintas policías cibernéticas, impartimos nuestros cursos y certificaciones que son abiertos al público en general.

Al formar parte del American Council For Cybersecurity And Computer Forensic © ACCCF, el respaldo a nuestros cursos está reconocido a nivel internacional.

Así mismo en México, tenemos el registro con valor curricular ante la Secretaría del Trabajo y Previsión Social bajo el número CID1107146P8- 0015

Como alumno adquirirás las competencias necesarias para:

- Dominar los conocimientos generales necesarios para poder llevar a cabo investigaciones sobre delitos relacionados con las TI utilizando técnicas de Cómputo Forense.
- Además de que tendrán noción de los aspectos legales que se deben considerar para presentar adecuadamente los resultados de la evidencia digital.
- Gestionar y organizar un análisis informático.
- Abordar sistemas Windows, Linux y Android desde un enfoque altamente especializado, recuperando información cuando el software comercial queda limitado.

DATOS CLAVE

Duración

40 horas (1)

*10 horas adicionales de propedéutico

Requerimientos

160 Gb de espacio en disco duro

4 GB en RAM Procesador Intel i3 o equivalente superior

- Al cubrir con la totalidad del curso y aprobar la evaluación, los alumnos podrán ejercer como analistas de riesgos informáticos, así como en la detección de intrusos en redes corporativas.
- Doble constancia con valor curricular ante la STPS y el ACCCF (2)
- Sabemos que no todos parten del mismo punto, por ello se desarrolló un **curso propedéutico de 10 horas para que todos los participantes saquen el máximo provecho del curso.**

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.

PROFESSIONAL SPEAKERS

El docente principal es Jocsan Laguna Romero, quien desarrolló la primera distribución de Cómputo Forense de América Latina, haciendo una presentación en el auditorio de la Facultad de Ingeniería de la UNAM, noticia difundida en distintos medios de circulación nacional, como el portal de Aristegui Noticias, Excélsior, El Financiero, la gaceta de la UNAM, CONACYT entre otros.

SESIONES ONLINE EN DIRECTO

Podrás seguir e intervenir en las sesiones estés donde estés, sin necesidad de desplazamientos.

NETWORKING INTERNACIONAL

Podrás conocer al resto de participantes de Latinoamérica con los que te pondremos en contacto de forma presencial y/o virtual a lo largo del curso.

ESTRUCTURA ACADÉMICA

PROPEDÉUTICO

- Introducción y administración de máquinas virtuales VMware y VirtualBox
- Introducción, manejo y administración de sistemas Linux Introducción a redes
- Nmap desde 0, descubriendo sistemas, puertos y vulnerabilidades.
- Introducción al manejo y configuración de Máquinas Virtuales VMware y VirtualBox
- Introducción a Linux
- IP, VLAN, WIFI
- Darknet, Deepweb, TOR, Navegador/buscador TOR "The Onion Router
- Whois
- Maltego
- Aplicaciones para el monitoreo de incidentes: Zona-h, Dark-h, Hootsuite y Pastebin
- Phishing
- Spoofing

MÓDULO I.
Metodología Jurídica De La Investigación Pericial

- Normas internacionales de manejo de evidencia digital.
- Planimetría
- Cadena de Custodia
- Preservación, observación, fijación, levantamiento, etiquetamiento, traslado al laboratorio.
- Dictamen Pericial
- Características del dictamen pericial.
- Método científico y su relación con el dictamen pericial.
- Aplicación del Dictamen pericial en el modelo del juicio penal acusatorio.

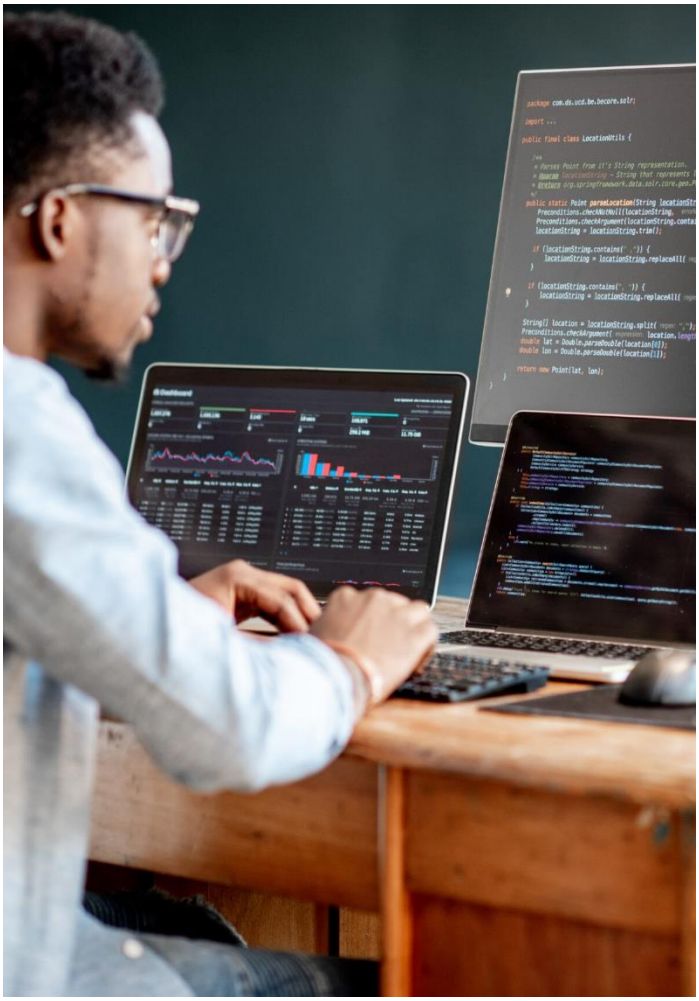
MÓDULO II.
Juicios Orales en México relacionados con Ciberbullying, Sexting, Grooming, robos a tarjetas y cuentas bancarias.

MÓDULO III.
Ataques Web/Red

Técnicas de recolección de tráfico de red	Captura y análisis de paquetes	Extracción de evidencia digital
Análisis de tráfico y detección de anomalías	Explotación de vulnerabilidades	Analizando logs
Creación y detección de Rouge AP	Principales ataques a WHM(Cpanel)/Plesk	Análisis de logs de servidores web
Ataques y análisis de logs de los principales CMS	Registro y recolección de evidencia en Apache	Investigación de correos criminales

MÓDULO IV.
Evidencia Física

- Medios de almacenamiento
- Fases de arranque del disco duro
- Sectores con daños físicos
- Recuperación de Arreglos RAID 0, RAID 1, RAID 5, RAID 10 y RAID0+1 Daños Lógicos más comunes, manejo y recuperación
- Daños Físicos internos más comunes, su manejo correcto y su recuperación
- Recolección manejo y análisis de la evidencia



MÓDULO V.
Sistemas de Archivos

- Organización de los datos
- Particiones de disco
- Capas de sistemas de archivos
- Análisis del MBR
- Datos alojados o sin alojar
- Capas de metadatos
- Apuntadores e inodos
- Sistemas de archivo ext2/3, NTFS y FAT32/16
- Entradas MFT
- Tiempos de accesos
- Esteganografía

MÓDULO VI.

Análisis Forense A Sistemas Operativos Windows

- Etapas del análisis
- Análisis externo
- Análisis de tráfico
- Respuesta en Windows y recolección de evidencia volátil
- Verificación de aplicaciones sospechosas
- Recuperación de contraseñas
- Sistemas de archivos y tiempo MAC
- Flujos alternos de datos
- Analizadores de archivos
- Generación de imágenes bit a bit
- Montaje de imágenes y uso de herramientas automatizadas
- Extracción y análisis de logs
- Manejo, generación y análisis de Shadow Copy
- Documentos cifrados, uso de herramientas gratuitas y comerciales para el acceso a la evidencia

MÓDULO VII.

Sistemas Virtuales

- Máquinas virtuales
- Virtualización de entornos informáticos
- Virtualización de entonos informáticos a partir de copias obtenidas
- Sistemas de la nube
- Sistemas Windows Server
- Sistemas Linux Server

MÓDULO VIII.
Evidencia Digital

- Conceptos generales del análisis de memoria volátil
- Escala de volatilidad
- Análisis de memoria de sistemas Windows
- Análisis de memoria de sistemas GNU/Linux
- Estructura del volcado
- Estructuras de datos en el volcado
- Análisis de memoria RAM, búsqueda de procesos y servicios sospechosos
- Laboratorio de análisis
- Herramientas de análisis
- Diferencias de extracción de en Windows y Linux
- Autentificación de la preservación de la evidencia
- Reconocimiento del tipo de evidencia

MÓDULO IX.

Análisis Forense A Sistemas Operativos Linux

- Selección de sistemas vivos o muertos
- Comandos a ejecutar en un sistema sospechoso
- Volcado de memoria
- Descripción el sistema
- Historial de acciones
- Procesos
- Conexiones de red activas
- Configuración de las interfaces de red
- Tareas programadas
- Módulos del Kernel
- Análisis forense a sistemas (vivos y muertos)
- Montado de imágenes
- Análisis de bitácoras
- Archivos especiales
- Comparación de hashes
- Archivos sospechosos

MÓDULO X.

Análisis Forense en Dispositivos Móviles

- Introducción – ¿Por qué hacer análisis forense digital a un móvil?
- Recomendaciones a tener en cuenta en el análisis forense a móviles
- Analizando los sistemas móviles líderes del mercado
- Análisis forense a dispositivos iOS
- Adquiriendo la evidencia digital
- Adquisición desde un Backup de iTunes Adquisición de copia bit a bit
- Adquisición de copia lógica
- Análisis de la evidencia adquirida
- Análisis de Contactos, Llamadas, Mail, Fotos y Videos, Mensajes de Texto, Notas, Calendario de Eventos, Navegación desde Safari, Spotlight, Mapas, Notas de Voz, Preferencias del Sistema, Logs del Sistema, Diccionarios Dinámicos,

- Análisis Con gratuitas
- Manejo y extracción con Oxygen Forensic ®

  Métodos de extracción. (Datos básicos de extracción: contactos, llamadas, mensajes, calendario, diccionarios.)

  Extracción de datos en dispositivos con protección de contraseña. Formatos de Back Up soportados por Oxygen Forensic Suite.

  Explorador de archivos Recuperación de datos eliminados. Detección de spyware

  Historia Conexiones Web

  Cronología - todos los hechos de la utilización del dispositivo. Contactos todos los contactos obtenidos de diversas fuentes.

  Enlaces y Estadísticas, Social Graph todas las conexiones sociales entre los usuarios de dispositivos y contactos.
- La construcción y personalización de informes forenses.
  - Análisis forense a dispositivos Android Sistema de archivos y arquitectura
  - Configurando el laboratorio forense y los emuladores Acceso a la información de los dispositivos Adquiriendo la evidencia digital
  - Análisis de la evidencia adquirida
  - Análisis de Contactos, Llamadas, Mail, Fotos y Videos, Mensajes de texto, Calendario y demás información almacenada en el dispositivo.
  - Recomendaciones adicionales para la entrega del informe

¿A QUIÉN VA DIRIGIDO?

Profesionales en informática.

Técnicos informáticos de empresas y organismos públicos que desean dirigir sus conocimientos hacia auditorias, gestiones o consultorías en materia de ciberseguridad y peritaje informático.

Estudiantes que deseen adquirir una ventaja competitiva en conocimientos de informática forense.

Recién titulados y estudiantes de últimos cursos que quieran una formación actual práctica que les permita orientarse profesionalmente y entrar a trabajar a un mercado laboral complejo y competitivo.

Responsables de medios de departamento de seguridad, consultoría y asesoría informática de entidades públicas y privadas que deseen apoyarse y compartir la visión de otros profesionales de prestigio e intensa actividad profesional.

informaticaforense

Duriva

@duriva

@duriva

Contacto

52 (55) 3689 1396

Paseo de la Reforma 42 piso oficina A, Colonia Juárez, Cuauhtémoc CDMX C.P. 06600

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