CERTIFICACIÓN
Cómputo Forense y Ciberseguridad
Nivel 1

Dirigido a:

El curso está orientado a profesionales de informática que desean aprender cómo realizar investigaciones sobre delitos relacionados con las TI.

Para aprovechar el curso es importante contar con conocimientos básicos de redes y sistemas operativos, en caso de que apenas comiences, es importante que asistas a los webinarios gratuitos que ya están incluidos en el costo del curso, en ellos se te darán los temas más importantes, para que al iniciar el diplomado puedas obtener el mayor provecho de las cátedras.

Objetivo:

Al finalizar el curso los alumnos tendrán 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.

Policías de México hasta Argentina han tomado la certificación.

http://www.pgjebcs.gob.mx/noticias/2017/01/31/inician-pgje-curso-en-computo-forense-para-peritos-y-agentes-de-investigacion/

http://policia.chaco.gov.ar/index.php/ecmPagesView/view/id/12349

Duración: 45 Horas.

Facilidades: Curso propedéutico, coffee break, internet y conexiones eléctricas. (en las sedes presenciales)

Valor Curricular: Curso registrado ante la Secretaría de Estado de México STPS, se puede consultar el registro bajo el RFC CID1107146P8
http://agentes.stps.gob.mx:141/Buscador/BuscadorAgente.aspx

STPS
SECRETARÍA DEL TRABAJO Y PREVISIÓN SOCIAL

Valor Curricular: El Latin American Council For Cybersecurity And Computer Forensic © LACCCF 2019 otorga la certificación: Computing Analysis Forensics Specialized Certification (CAFSC)

Requerimientos RECOMENDADOS de equipo de cómputo:

- 160 Gb de espacio en disco duro
- 4 GB en RAM
- Procesador Intel i3 o superior

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.

Propedéutico Conceptos básicos (10 horas en video)

- Introducción y administración de maquinas virtuales Vmware y VirtualBox
- Introducción, manejo y administración de sistemas Linux
- Introducción a redes
- Ciber patrullaje en la red
- Nmap desde 0, descubriendo sistemas, puertos y vulnerabilidades.

Resumen del cronograma de actividades

Día 1	Módulo I.- Metodología Jurídica De La Investigación Pericial. (3 horas)
	Módulo II.- Juicios orales en México relacionados con ciberbullying, sexting, grooming, robos a tarjetas y cuentas bancarias.

	Módulo III.- Ataques Web/Red (3.5 horas)
Día 2	Módulo IV.- Evidencia Física (3 horas)
	Módulo V.- Sistemas de Archivos (2 horas)
	Módulo VI.- Análisis Forense A Sistemas Operativos Windows 1° parte (3 horas)
Día 3	Módulo VI.- Análisis Forense A Sistemas Operativos Windows 2° parte (3 horas)
	Módulo VII.- Sistemas Virtuales (2 horas)
	Módulo VIII.- Evidencia Digital (2.5 horas)
Día 4	Módulo IX.- Análisis Forense A Sistemas Operativos Linux (8 horas)
Día 5	Módulo X.- Análisis Forense en Dispositivos Móviles

* Los tiempos señalan sólo las horas de cátedras, se añaden tiempos extras para realizar ejercicios de todos los temas vistos en el día.

TEMARIO:

Propedéutico Conceptos básicos (10 horas)

- Introducción al manejo y configuración de Maquinas 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
- Cardin, tarjetas de crédito
- Propiedad intelectual
- Delitos en materia de derechos de autor
- Phishing
- Spoofing
- The National Center for Missing & Exploited NCMEC
- Análisis y procesamiento de la información relacionada a la pornografía infantil y trata de personas

DÍA 1

Módulo I.- Metodología Jurídica De La Investigación Pericial. (3 horas)

- 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 III.- Juicios orales en México relacionados con ciberbullying, sexting, grooming, robos a tarjetas y cuentas bancarias.

Módulo III.- Ataques Web/Red (3.5 horas)

- 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

DÍA 2

Módulo IV.- Evidencia Física (3 horas)

- 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 RAID 0+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 (2 horas)

- 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 (8 horas)

- 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

DÍA 3

- 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 (2 horas)

- 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 (4 horas)

- 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

DÍA 4

Módulo IX.- Análisis Forense A Sistemas Operativos Linux (8 horas)

- 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

DÍA 5

Módulo X.- Análisis Forense en Dispositivos Móviles (8 horas)

- 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

Al finalizar los diez módulos, los participantes recibirán un diploma con valor curricular y reciben un código para aplicar el examen de certificación.