CAPACITACIÓN

La Certificación de **Computer Hacking Forensic Investigator** (**CHFI**) está diseñada para todos los profesionales de TI involucrados con la seguridad del sistema de información y respuesta a incidentes. **CHFI** presenta un enfoque metodológico detallado y el análisis de evidencia que abarca escenarios principales que permiten a los estudiantes adquirir experiencia práctica en diversas técnicas de investigación **forense** y herramientas estándar necesarias para llevar a cabo con éxito una investigación.

OBJETIVOS:

- Proveer al participante los conocimientos de ciencia forense, delito cibernético y pasos en la investigación forense.
- Conocer las leyes involucradas y trabajar en consecuencia para buscar y confiscar las computadoras con una orden judicial.
- Enumerar los roles del primer respondedor, evaluar la escena del crimen electrónico, realizar entrevistas, recoger, preservar y transportar evidencia electrónica junto con información completa.
- Documentar y definir diferentes tipos de evidencia digital, reglas de evidencia digital, proceso de examen de pruebas y delitos electrónicos.
- Configuración del laboratorio de informática forense Recuperar archivos existentes y eliminados de diferentes sistemas operativos que utilizan diferentes procesos como **Access Data FTK**, Encase, Esteganografía y otras técnicas. Sistema de **crack** y aplicaciones de contraseñas.
- Realice la captura de registros para establecer la correlación de eventos.

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- Investigue el tráfico de red, correos electrónicos y ataques.

- Practique el proceso forense en dispositivos móviles con diferentes sistemas operativos.

DIRIGIDO A:

- Cualquier persona interesada en **Computo Forense**, Investigadores, Asesores legales
- Oficiales de la ley y Militares
- Agentes federales, Gubernamentales
- Detectives, investigadores
- Miembros del equipo de respuesta a incidentes
- gerentes de seguridad de la información
- Hackers éticos
- profesionales de TI, Directores, Gerentes de TI
- Ingenieros de Sistemas, Redes
- Analista de Seguridad, Arquitectos, Auditores, Consultores

DURACIÓN: 40 Hrs.

REQUISITOS:

- Conocimientos básicos en plataforma **Microsoft Windows®** y **Linux**
- Conocimientos en **Hacking Ético**

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

INCLUYE:

- Instalaciones adecuadas
- Material y manuales de cursos
- Instructores Certificados
- Examen de Certificación **Computer Hacking Forensic Investigator 312-49**

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

Reconocimientos

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Temario:

- Fundamentos de las redes computaciones y la defensa
- Amenazas, Vulnerabilidades y Ataques a la Seguridad de las Redes
- Controles, Protocolos y Dispositivos de Seguridad de las Redes
- Diseño e Implementación de la Política de Seguridad de las Redes
- Seguridad Física
- Seguridad del Host
- Configuración y Administración del **Firewall** Seguro
- Configuración y Administración de **IDS** Seguro
- Configuración y Administración de **VPNs** Seguros
- Defensa de Redes Inalámbricas
- Monitoreo y Análisis del Tráfico de las Redes
- Gestión de Riesgos y Vulnerabilidades de las Redes
- Respaldo y Recuperación de Datos
- Respuesta y Administración de Incidentes de las Redes

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Informática forense en el mundo de hoy

- Ciencia forense
- Informática forense
- Informe de incidentes de seguridad
- Aspectos de la seguridad organizacional
- Objetivo de Informática Forense
- Preparación Forense
- Objetivos y planeación de la preparación forense
- Tipos de delitos informáticos
- Delincuencia Cibernética Organizada: Organigrama
- Incidentes disruptivos al negocio
- Pasos clave en la investigación forense
- Papel del investigador forense
- Acceso a los recursos informáticos forenses
- Papel de la evidencia digital
- Enfoque a la investigación forense: un estudio de caso

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- Instrucciones para que el investigador forense se acerque a la escena del crimen
- Asuntos legales
- Informar sobre un delito cibernético
- Persona asignada para reportar el crimen
- Contacto de Agentes Locales Federales

Proceso de Investigación de Informática Forense

- Investigando el crimen informático
- Construyendo el equipo de investigación
- Personas involucradas en informática forense
- Revisar políticas y leyes Forenses
- Notificar a los responsables de la toma de decisiones y adquirir la autorización
- Evaluación de riesgos
- Construir un kit de herramientas de investigación informática
- Pasos para prepararse para una investigación forense informática
- Metodología de Investigación Forense Informática
- Búsquedas sin orden
- Evaluar y asegurar la escena

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- Reunir la información preliminar en la escena
- Formulario de recolección de evidencia
- Recopilar evidencia electrónica
- Asegurar y manejo de la Evidencia
- Cadena de custodia
- Duplicar los datos (**Imaging**)
- Verificar la integridad de la imagen con **MD5 Hash Calculators** (**HashCalc**, **MD5 Calculator** y **HashMyFiles**)
- Recuperar datos perdidos o eliminados
- Software de recuperación de datos
- Evaluar Evidencia y Caso
- Preparar el informe final
- Testificando como un testigo experto
- Cerrando el caso

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Buscando y aprovechando computadoras

- Buscar y confiscar computadoras sin una orden
- Expectativa razonable de privacidad de la Cuarta Enmienda en casos que involucran computadoras
- Búsqueda de un incidente para un arresto legal
- Búsquedas en el lugar de trabajo del sector público y privado
- Buscando y confiscando computadoras con una orden
- Vigilancia Electrónica en Redes de Comunicaciones
- Contenido frente a información de direccionamiento

Evidencia digital

- Aspectos desafiantes de la evidencia digital
- Análisis forense anti-digital (**ADF**)
- Organización Internacional de Pruebas Informáticas (**IOCE**)
- Principios Internacionales de la **IOCE** para Evidencia Digital
- Grupo de trabajo científico sobre evidencia digital (**SWGDE**)
- Proceso de examen de evidencia digital
- Recopilación de evidencia de la memoria **RAM**
- Recopilación de evidencia de una computadora de red independiente

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- Cadena de custodia
- Informe Final de Conclusiones
- Crimen electrónico y consideración de evidencia digital por categoría de crimen

Procedimientos de primera respuesta

- Evidencia electrónica
- Roles de Primera Respuesta
- Dispositivos electrónicos: tipos y recopilación de evidencia potencial
- Kit de herramientas de primera respuesta
- Herramientas y equipo de recolección de evidencia
- Fundamentos de Primera Respuesta
- Asegurando y evaluando la escena electrónica del crimen: una lista de verificación
- Asegurando la escena del crimen
- Documentando la escena del crimen electrónico
- Fotografiando y dibujando la escena
- Video filmando la escena del crimen
- Tratar con las computadoras encendidas, apagadas y en red
- Tratar con archivos abiertos y archivos de inicio
- Procedimiento de apagado del sistema operativo
- Errores comunes de primera respuesta

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Laboratorio de informática forense

- Configuración de un laboratorio de informática forense
- Condiciones ambientales
- área de trabajo de un laboratorio de informática forense
- Investigador Forense Informático
- Oficial de la ley
- Equipo requerido en un laboratorio forense
- Kit de primera respuesta de mano
- Caja de herramientas de incautación de dispositivos

Entendiendo los discos duros y los sistemas de archivos

- Descripción general de la unidad de disco duro
- Unidad de estado sólido (**SSD**)
- Estructura lógica y física de un disco duro
- Interfaces de disco duro: **ATA**, **SCSI**, **IDE/EIDE**, **USB**, **Fibre Channel**
- **Tracks**: **Track Numbering**
- **Sector**: **Advanced Format**: **Sectors**, **Sector Addressing**
- **Cluster** y **Bad Sector**
- Direccionamiento de datos del disco duro

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- Cálculo de la capacidad del disco y rendimiento del disco duro
- Particiones de disco y proceso de arranque
- Proceso de arranque de **Windows** y **Macintosh**
- Tipos de sistemas de **File System**
- Lista de **Network File System**
- **File Allocation Table** (**FAT**) y estructura
- Sistema de archivos de nueva tecnología (**NTFS**) y estructura
- Sistemas de cifrado de archivos (**EFS**)
- Componentes de **EFS** y atributos
- Agente de clave de recuperación de **EFS**
- Herramienta: Recuperación avanzada de datos **EFS**
- Sistemas de archivos populares de **Linux**
- Arquitectura del sistema de archivos de **Linux**: **Ext2** y **Ext3**
- Sistema de archivos **Mac OS X** y **CDFS**
- Sistema de almacenamiento **RAID** y niveles
- Análisis del sistema de archivos usando el kit de **Sleuth** (**TSK**)

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Windows Forensics

- Recopilación de información volátil
- Información volátil, Hora del sistema, Usuarios logeados
- Utilerías: **PsFile** y **OpenFiles**
- Información de la red, Conexiones y puertos
- Estado de la red y Recopilación de información no volátil
- Examinación de **File Systems**, **Registry Settings**, **Microsoft Security** y **ID Event Logs**
- Análisis de memoria de **Windows** y registros
- Análisis de caché, **cookie** e historia en: **IE**, **Firefox**, **Chrome**
- Vista de **cookies**, **caché**, historial de **IE**
- Análisis de archivos de Windows y Papelera de reciclaje
- Puntos de restauración del sistema (archivos **Rp.log** y **Change.log.x**)
- Herramienta: analizador de metadatos
- Análisis de registros **IIS**, **FTP** y **DHCP**
- Análisis de los registros de Firewall de Windows
- Uso de **EnCase** para examinar los archivos de registro de eventos de **Windows**
- Herramienta de **Windows Forensics**: **SO Forensics**
- Herramienta Forense de **Windows**: **Helix3 Pro**

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- Explorador del sistema
- **Secret Explorer**: Explorador secreto
- Herramientas: **Registry Viewer**, **Reg Scanner**, **Alien Registry Viewer**
- Administrador de tareas de seguridad
- **PrcView**, **ProcHeapViewer**
- Visor de memoria
- Herramienta: **PMDump**

Adquisición y duplicación de datos

- Adquisición de datos y conceptos de duplicación
- Principios forenses y procesales
- Tipos de sistemas de adquisición de datos
- **Bit Stream** vs. **Backups**
- Porqué crear una imagen duplicada?
- Métodos de adquisición de datos
- Tipos de adquisición de datos
- Proceso de recopilación de datos estáticos y en vivo
- Porqué los datos volátiles son importantes?
- Metodología de recolección de datos volátiles
- Métodos de validación de **Linux** y **Windows**

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- Adquisición remota de datos
- Adquirir datos en **Windows** y **Linux**
- Comandos: **dd**, **dcfldd** y **Netcat**
- Extracción de **MBR**
- **EnCase Forensic**
- Software de análisis: **DriveSpy**
- Recuperación de **RAID** para **Windows**
- Hardware forense de inteligencia digital: **UltraKit**

Recuperar archivos borrados y particiones eliminadas

- Recuperar los archivos borrados
- Papelera de reciclaje en **Windows**
- Ubicaciones de almacenamiento de la papelera de reciclaje en sistemas **FAT** y **NTFS**
- Archivos dañados en carpeta reciclada
- Recuperación de archivos en **MAC OS X**, **Linux** y **Windows**
- Recuperación de archivos **PC INSPECTOR**
- **Stellar Phoenix Windows Data Recovery**

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- Adición y procesamiento de pruebas estáticas, en vivo y remotas
- Agregar evidencia a un caso
- Selección de las opciones de salida del informe
- Personalización del formato de informes
- Ver y distribuir un informe

Investigación forense utilizando EnCase

- Descripción general de **EnCase Forensic**
- Configuración de **EnCase**: pestaña **EnScript** y pestaña rutas de almacenamiento
- Recuperar carpetas en volúmenes **FAT**
- Creación de un trabajo de análisis y un informe
- Analizando y buscando archivos
- Viendo el directorio de firmas de archivos
- Realizar un análisis de firmas
- Análisis de **hash**
- Visualización de archivos codificados en **base64** y **UUE**
- Creación de un informe utilizando la pestaña Informe

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Esteganografía y archivos de imagen forense

- Cómo funciona la esteganografía y uso legal
- Técnicas y Aplicación de esteganografía
- Herramienta de **esteganografía**: **S-Herramientas**
- Herramientas de **esteganografía**: **ImageHide**, **Mp3stegz**, **MSU StegoVideo**
- Algoritmo de codificación de **Huffman** y **Lempel-Ziv**

Aplicaciones Crackers para contraseña

- Conceptos de crackeo de contraseñas
- Cómo se almacenan las contraseñas de hash en **Windows SAM**
- Tipos de ataques de contraseña
- Ataque pasivo en línea: ataque de hombre en el medio y de repetición
- Ataque activo en línea: Adivinar contraseña
- Ataque activo en línea: **Trojan/Spyware/keylogger**
- Ataque activo en línea: ataque de inyección de hash
- Ataques de **rainbow table**: **Pre-Computed Hash**
- Recuperación de contraseña distribuida de **Elcomsoft**
- Ataque manual de contraseñas

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- Herramientas para descifrar contraseñas: **L0phtCrack**, **OphCrack**, **Caín** y **Abel**, **RainbowCrack**, **SAMInside**, **PWdump7** y **Fgdump**
- Almacenamiento protegido **PassView**
- Recuperación de contraseña de red

Captura de registro y correlación de eventos

- Registros de seguridad informática
- Registros del sistema operativo y aplicaciones
- Archivos de registro del enrutador y **Honeypot**
- Configurando y analizando el registro de **Windows**
- Archivo de registro de **Windows**: Registros del sistema y aplicaciones
- Eventos de inicio de sesión que aparecen en el registro de eventos de seguridad
- Registros de **IIS**, **DHCP** y **ODBC**
- Afrontar los desafíos en la gestión de registros
- Registro centralizado y **Syslogs**
- Pasos para configurar un servidor **Syslog** para sistemas **Unix**
- Sincronización de tiempo con N**TP**
- Configurando **Time Server** en **Windows Server**
- Analizador **EventLog**
- Explorador de registro de eventos

Informática Integrada Internetworking

EC-Council TRAINING PARTNER

PEARSON VUE-Authorized Test Center

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

- **WebLog Expert**
- Monitor de registro de eventos de **ELM**

Análisis forense de redes, investigación de registros e investigación del tráfico de red

- Mecanismo de análisis forense de redes
- Descripción general de la capa física y de enlace de datos del modelo **OSI**
- Visión general de la red y la capa de transporte del modelo **OSI**
- Modelo de referencia **OSI** y protocolo **TCP/IP**
- Sistemas de detección de intrusos (**IDS**), **Firewall** y **Honeypot**
- Ataques de red: **IP Address Spoofing**, **Man-in-the-Middle Attack**, **Packet Sniffing**, **How a Sniffer Works**, **Enumeration**, **Denial of Service Attack**, **Session Sniffing**, **Buffer Overflow**, **Trojan HorseLog Injection Attacks**
- Herramienta de captura de registro: **ManageEngine EventLog Analyzer**
- Manejo de registros como evidencia
- Investigando el tráfico de red usando **Wireshark**
- Adquirir tráfico usando técnicas de envenenamiento de **DNS**
- Servidor proxy de envenenamiento de **DNS**
- Envenenamiento de caché de **DNS**
- Recolección de evidencia de la tabla **ARP**, **DHCP** y **IDS**

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Investigando Ataques Inalámbricos

- Tipos de redes inalámbricas
- Filtrado **MAC** e Identificador de conjunto de servicios (**SSID**)
- Tipos de cifrado inalámbrico: **WEP, WPA** y **WPA2**
- Ataques inalámbricos y Símbolos **Chalking Wi-Fi**
- Ataques de control de acceso
- Ataques de integridad, confidencialidad, disponibilidad y autentificación
- Metodologías para detectar conexiones inalámbricas
- Herramienta de descubrimiento de **Wi-Fi**: **inSSIDer**
- Herramienta de mapeo **GPS**: **WIGLE** y **Skyhook**
- Cómo descubrir redes **Wi-Fi** usando **Wardriving**
- Compruebe el filtrado de **MAC** y Cambio de la dirección **MAC**
- Qué es el análisis de espectro?
- La generación del informe
- Herramientas forenses inalámbricas
- Analizador de paquetes de red

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Seguimiento de correos electrónicos e investigación de delitos de correo electrónico

- Sistema de correo electrónico
- Clientes y Servidor de correo electrónico
- Servidores **POP3** e **IMAP**
- Email **Spamming** y **Spoofing**
- Crimen a través de la sala de chat
- Cabeceras de correo electrónico
- Investigando el crimen por correo electrónico y la violación
- Visualización de encabezados de correo electrónico en **Microsoft Outlook**
- Visualización de encabezados de correo electrónico en **AOL**, **Hotmail**, **Gmail**, **Yahoo**
- Examinar archivos adicionales (archivos .**pst** o .**ost**)
- Comprobando la validez del correo electrónico
- Examine la dirección IP de origen y rastreo
- Herramientas forenses de correo electrónico
- Kit de herramientas forenses (**FTK**)
- Leyes y actos contra delitos de correo electrónico

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Forense móvil

- Diferentes dispositivos móviles y características
- Características de hardware y software de los dispositivos móviles
- Tipos de sistemas operativos móviles
- Arquitectura del sistema **WebOS**
- Arquitectura de sistemas operativos: **Android**, **BlackBerry**, **OS Windows**, **Phone 7, Apple iOS**
- Forense móvil
- Recolectando la Evidencia
- Recopilación de **iPod/iPhone** conectado con la computadora
- Documentar la escena y preservar la evidencia
- Generar informe
- Herramientas de software forense móvil
- Informe de escritura utilizando **FTK** y **ProDiscover**

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815

CAPACITACIÓN

Convertirse en un testigo experto

- Papel del experto en informática forense
- Expertos en litigios civiles y litigios penales
- Alcance del testimonio de testigos expertos
- Testigo técnico frente a testigo experto
- Preparándose para el testimonio
- Preparación de evidencia y documentación
- Presentación de evidencia
- Reglas para el testigo experto
- Reglas relativas a la calificación de un testigo experto
- La orden de los procedimientos de prueba
- ética general al testificar
- Ayudando a su abogado

Informática Integrada Internetworking, SA de CV
informes@informaticaintegrada.com.mx
Tels. 55 5639 6518 y 55 5639 5815