

## CCFI

### Objetivo:

Este curso está diseñado para darle al estudiante las herramientas y los conocimientos básicos para iniciarse en el mundo Forense Informático. Busca que el estudiante entienda con detalle cómo identificar las posibles fallas de seguridad, como se generan, como encontrar evidencia de brechas de seguridad, ataques, estrategias para el manejo de evidencia. En este escenario, el curso ofrece la Metodología Forense y un marco conceptual de análisis que oriente a los alumnos ante una situación en la que se encuentre comprometida la seguridad informática de una organización.

Nuestros CCFI tendrán los elementos necesarios para abordar posibles situaciones de fraude realizados a través de computadoras, sabrán identificar evidencia digital relevante y presentar una aproximación desde la perspectiva legal en conjunto con las especificaciones técnicas que reviste el hecho.

### Dirigido a:

Profesionales de la seguridad de negocios, administradores de sistemas, auditores, profesionales legales, entidades bancarias, seguros y otros profesionales.

### Forma de evaluación:

La certificación CCFI representa un esquema diferente en las certificaciones actuales ya que el proceso de examen se divide en 2 partes:

Fase I: Examen en línea (1032V1). El estudiante deberá contestar diversas preguntas teórico/prácticas de manejo de diferentes escenarios para la aplicación forense.

Fase II: Examen práctico. Se le otorgará al estudiante acceso a un servidor virtual a través de internet, que contará con las herramientas para el análisis y procedimiento que se exigirán en la entrega del informe, el cual se llenará en línea a medida que avanza en las etapas descritas en la documentación; al finalizar la documentación se le entregará a los jueces que analizarán cada una de las pautas respondidas por el estudiante.

Al finalizar el informe durante un período de evaluación aproximado de 24 horas se entregan los resultados y se procederá a la entrega del certificado a través del correo internacional.

La puntuación mínima para la aprobación de cada Fase deberá ser de 700 / 1000 Puntos.

### Requisitos del participante:

El alumno debe poseer fuertes conocimientos técnicos en Redes, Hardware, Sistemas Operativos GNU/Linux y Microsoft Windows, Programación y Seguridad Informática en general.

### Duración:

La capacitación tendrá una duración de 40 hs

Informes: [www.arcanus.com.uy](http://www.arcanus.com.uy)

[info@arcanus.com.uy](mailto:info@arcanus.com.uy)

## Temario:

### **Módulo 1: La informática Forense en el Mundo de Hoy**

- Introducción
- Definición de Ciencia Forense
- Definición de Informática Forense
- ¿Qué es la Informática Forense?
- Breve reseña histórica
- Ámbito de actuación
- Principios de la Informática Forense
- Principio de intercambio de Locard
- Objetivos de la Informática Forense
- Necesidad de la Informática Forense
- Fallas y riesgos de la informática forense
- Papel de la Informática Forense en el seguimiento de los ciberdelincuentes
- Cibercrimen
- Ejemplos de crímenes cibernéticos
- Motivos del crimen cibernético
- Reglas del forense informático
- Metodología del forense informático
- Recursos del forense informático
- Manteniendo una conducta profesional
- Evidencia digital
- Tipos de evidencia digital
- Forense Digital
- El proceso de investigación

### **Módulo 2: Leyes e Informática Forense**

- ¿Qué es un cibercrimen?
- ¿Qué es la informática forense?
- ¿Por qué ocurren los cibercrimenes?
- Leyes informáticas
- Enfoques para formular ciberleyes
- Las ciberleyes están relacionadas con...
- FBI
- Scientific Working Group on Digital Evidence (SWGDE)
- USA Patriot Act, 2001
- Construcción de un caso de Cibercrimen
- Como investiga el FBI un Cibercrimen
- ¿Cómo iniciar una investigación?
- Cuestiones legales en la incautación de equipos
- Cuestiones internacionales relacionadas con la informática forense
- Investigación de un cibercrimen

### **Módulo 3: Proceso Investigativo Forense**

- Metodología del Proceso Investigativo Forense
- Fases del Proceso Investigativo

**Módulo 4: Procedimiento de Respuesta Inicial**

- Introducción
- Concepto de Vulnerabilidad
- Estadísticas
- Concepto de Incidente
- Reporte de Incidentes
- Categoría de los Incidentes
- Incidentes de Bajo Nivel
- Incidentes de Nivel Medio
- Incidentes de Alto Nivel
- Manejo de Incidentes
- Procedimiento
- Preparación
- Identificación
- Contención
- Extracción
- Recuperación
- Seguimiento
- Documentar la Calidad de Respuesta a un Incidente

**Módulo 5: Laboratorio de Informática Forense**

- Asignación presupuestaria para un Laboratorio Forense.
- Área de trabajo de un Laboratorio Forense.
- Configuración general de un Laboratorio Forense.
- Equipo necesario para un Laboratorio Forense.
- Ambiente de un Laboratorio Forense.
- Condiciones ambientales.
- Consideraciones estructurales.
- Comunicaciones.
- Requisitos básicos de una estación de trabajo en un laboratorio forense.
- Inventario de aplicaciones y sistemas operativos.
- Recomendaciones para la seguridad física del laboratorio forense.
- Mantenimiento.
- Auditando un laboratorio de informática forense.
- Requisitos legales de un Laboratorio Forense.
- Responsabilidades del director de un laboratorio forense.

**Módulo 6: Adquisición y Duplicación de Datos**

- Determinando los mejores métodos de adquisición.
- Contingencias en la Recuperación de Datos.
- Adquisición de datos en MS-DOS.
- Adquisición de datos en Windows.
- Adquisición de datos en Linux.
- Otras herramientas de adquisición de datos.
- Necesidad de la duplicación de datos.
- Herramientas de Duplicación de Datos

**Módulo 7: Investigación Forense de Sistemas Windows**

- Introducción

- Buenas prácticas para la recogida y análisis de datos
- Cuentas y Perfiles de Usuario
- Tipos de Logon en sistemas Windows
- La Papelera de Reciclaje. Estructura y funcionamiento
- Archivos de Registro de Windows. Estructura
- Index.dat e Internet Explorer. Estructura y funcionamiento
- Recogida de archivos Log del sistema
- Ntuser.dat y archivos de Registro de Windows

#### **Módulo 8: Análisis Forense de Sistemas UNIX/Linux**

- Uso de Linux como herramienta forense.
- Entendiendo las particiones en Linux
- Montando particiones.
- Estructura de directorios en Linux.
- Secuencia de inicio de Linux.
- Análisis forense en Linux.
- Utilidades de análisis forense en Linux.
- Copia del disco rígido y sistema de archivos.
- Acceso a los datos del sistema de archivos.
- Distros Linux especializadas en forense.
- Herramientas forenses para Linux.

#### **Módulo 9: Aplicando las Ciencia Forense a las Redes**

- Modelo OSI
- Reunión de Pruebas sobre una Red
- Herramienta Wireshark
- Snort
- Documentación de Evidencias de Red
- Reconstrucción de pruebas para la investigación.

#### **Módulo 10: Algunas Técnicas Relevantes**

- Introducción a los archivos de imagen.
- Reconociendo un archivo de imagen.
- Entendiendo las imágenes bitmap y vectoriales.
- Gráficos Metafile.
- Distintos formatos de imágenes.
- Entendiendo la compresión de datos.
- Entendiendo la compresión Lossless y Lossy.
- Reparar encabezados dañados.
- Reconstruir los fragmentos de un archivo.
- Esteganografía.
- Estegoanálisis.

#### **Módulo 11: Análisis de Correos Electrónicos**

- Fundamentos de Internet.
- Funcionamiento de un servidor de correo.
- Crímenes mediante el correo electrónico.

- Spam.
- Mail Bombing y Mail Storm.

- Phishing.
- Hoax.
- Enviando correos falsos.
- Investigando crímenes relacionados con el correo electrónico.
- Viendo el encabezado del mensaje.
- Examinando archivos de correos.
- Rastreando un correo electrónico.
- Algunas consideraciones en el rastreo de correos.
- Herramientas forenses para correos electrónicos.

**Módulo 12: Password Cracking de Aplicaciones**

- Que es una contraseña.
- Tipos de contraseñas.
- ¿Cómo los hackers obtienen contraseñas?
- ¿Qué es un Password Cracker?
- Modus operandi de un atacante utilizando un Password Cracker.
- Como trabaja un Password Cracker.
- Clasificación del software de cracking.
- Sitios con base de datos de contraseñas.
- Herramientas de password cracking.
- Contramedidas.

**Módulo 13: Recuperando Archivos y Particiones Eliminadas**

- Eliminación de archivos en Windows
- Estructura y funcionamiento de la Papelera de Reciclaje
- Recuperación de archivos eliminados
- Recuperación de particiones eliminadas
- Herramientas para recuperar archivos eliminados
- Herramientas para recuperación de particiones borradas.

**Módulo 14: Forense en PDA y Móviles**

- Tecnologías actuales de telefonía móvil.
- Evidencia en dispositivos móviles.
- Metodología de examinación forense de teléfonos móviles.
- Personal Digital Assistant (PDA).
- Análisis Forense en PDA.
- Herramientas para realizar análisis forense en móviles y PDA.
- Puntos para recordar mientras se conduce la investigación.