

# Análisis forense en plataformas Windows

## \* OBJETIVOS:

Proporcionar a los asistentes conocimientos básicos de análisis forense en plataformas MS Windows tanto en parada como en caliente.

## \* ORIENTADO A:

Responsables de seguridad, consultores, jefes de proyecto y administradores de redes y sistemas.

## \* REQUISITOS:

Conocimientos de Windows, Networking y Seguridad.

## \* TEMARIO:

- **Localización de información en Windows.**
  - Sistema operativo funcionando.
  - Sistema operativo apagado.
- El visor de eventos, acceso a objetos.
- El registro de Windows.
- Procesos activos en el sistema.
- Puertos abiertos TCP y UDP, ¿que servicios esconden?
- Revisión de la partición con el sistema parado.
- Herramientas: Análisis de memoria y de disco.