www.eysglobal.com

MÓDULO 1

TEMA 3: FINALIDAD DE UN ANALISIS FORENSE

FINALIDAD DE UN ANALISIS FORENSE

FINALIDAD DE UN ANALISIS FORENSE

El **análisis forense digital** es muy importante no solamente en los casos de **ciberdelitos**, sino también para detectar fallos en los **sistemas de seguridad informáticos** con lo que se solucionan los problemas entes de que ocurran.

Los **peritos informáticos forenses** utilizan un software especializado para acceder a la información independientemente del dispositivo en el que se encuentre.

FINALIDAD DE UN ANALISIS FORENSE

Pautas para el análisis forense informático

•El primer paso para llevar a cabo un análisis forense informático es comprobar el estado del dispositivo electrónico, para conocer si está dañado o se han eliminado datos.

•Tras esto se realiza una **copia** de la información extraída y se almacena en un soporte seguro. Es necesario tener cuidado al manejar el dispositivo de origen ya que es preciso dejarlo exactamente igual que antes de comenzar el análisis.

•La siguiente fase consiste en conservar de forma segura el contenido que se ha extraído. Por ello el **soporte** en el que se encuentre almacenado debe estar en perfectas condiciones hasta que se termine el trabajo.

FINALIDAD DE UN ANALISIS FORENSE

•Aquí es cuando viene el auténtico **análisis del software y hardware** filtrando los datos importantes, pero sin borrar nada.

•La analítica observa todos los parámetros posibles: **contraseñas, usuarios, archivos, mensajes, conversaciones, documentos encriptados, los contenidos** subidos a la nube y cualquier detalle que pueda significar algo.

•Por último, se realiza un informe en el que se recoge toda la información lograda, de una forma objetiva, así como los pasos que se han seguido durante la investigación.

POR QUÈ ES NECESARIO EN UN ANALISIS FORENSE DIGITAL

Las nuevas tecnologías se encuentran en pleno auge, principalmente aquellas que incluyen información y comunicación, las cuales contienen una grandísima cantidad de datos privados almacenados en la red. Esto ha dado lugar a ataques informáticos a través de Internet, o también conocidos como ciberdelitos.

DATOS ADQUIRIDOS EN EL ANÁLISIS

En el análisis forense digital se extrae gran cantidad de información, parte de ella podemos calificarla en dos grupos:
•Información volátil: Este tipo de información es aquella que, tras apagar el dispositivo electrónico se pierde. Aunque no es completamente cierto, ya que es posible recuperarla a través del almacenamiento RAM.

DATOS ADQUIRIDOS EN EL ANÁLISIS

•Información no volátil: Por el contrario este tipo de información permanece en el disco duro incluso cuando el aparato electrónico se apaga indebidamente.
El perito informático debe realizar una imagen del disco duro a través de herramientas especializadas. Si se emplean herramientas conocidas como tipo Ghost, se podrá perder información de bajo nivel y será prácticamente irrecuperable.

LO QUE DEBEMOS TENER EN CUENTA:

LO QUE DEBEMOS TENER EN CUENTA:

Tener una copia exacta de un disco permite al investigador acceder al **sistema de archivos** e inspeccionar las **cuentas de usuario** existentes, los **documentos** asociados a un usuario, y los **programas** instalados, entre otras cosas. Sin embargo, mediante la utilización de herramientas y **suites forenses**, se puede buscar una gran variedad de información que es difícil de encontrar por simple inspección. En primera instancia, se puede **indexar** el contenido del disco de acuerdo con ciertas **palabras clave**, pudiendo realizar luego **búsquedas** de esas palabras, visualizando los archivos donde se encuentran y su contenido. Por ejemplo, si se quiere encontrar evidencia de un fraude, se pueden buscar palabras como “fraude”, “robo” o “soborno”.