



www.eysglobal.com



MÓDULO 1

TEMA 17: PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANALISIS FORENSE

PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANÁLISIS FORENSE



Los objetivos principales de todo análisis forense son:

- Recrear lo que ha ocurrido en un dispositivo digital durante el incidente de seguridad.
- Analizar las incidencias para impedir que se repitan en el futuro.



PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANÁLISIS FORENSE



La metodología empleada para alcanzar estos objetivos de estar compuesta al menos de los siguientes pasos:

- Analizar el funcionamiento del sistema para extraer toda la información posible sobre el mismo.
- Respetar rigurosamente el marco legal establecido.
- Recopilar todas las evidencias posibles.
- Autenticar las evidencias recogidas.
- Proteger las evidencias para que no se alteren, si es posible, realizar copias para poder trabajar con ellas y así preservar las originales.
- Analizar las evidencias.
- Presentar el informe final lo más detallado posible.
- Destruir la información duplicada si es necesario.

PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANALISIS FORENSE

Las evidencias digitales respecto a las evidencias físicas tienen tres ventajas muy importantes:

- Pueden ser duplicadas con total exactitud.
- Existen herramientas para verificar si la evidencia ha sido modificada.
- Se pueden recuperar, en la mayoría de los casos, después de un borrado.



PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANÁLISIS FORENSE



El resultado del análisis de la información puede ser **prueba determinante en un proceso judicial**.

Actualmente existen herramientas específicas para el **análisis de discos duros**, dispositivos móviles o correos electrónicos, al servicio de la informática forense. Se trata de herramientas especializadas en una capa concreta de la infraestructura en la que se ha podido realizar un ataque.

Pese a todo lo expuesto, lo único que se puede asegurar es que los datos en la red no son completamente seguros y se deben implantar por parte de las administraciones sistemas capaces de **perseguir el cibercrimen de forma efectiva**.

PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANALISIS FORENSE

Presentación e informe de resultados finalizado el análisis forense se debe redactar un informe pericial con conclusiones y justificación del sistema de trabajo empleado. El informe debe ser claro y conciso ya que puede terminar como prueba en los tribunales.



PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANÁLISIS FORENSE



Es la fase final y la mas delicada e importante la cual será el documento que sustentara una prueba en un proceso legal, básicamente tener en cuenta estos dos pasos:

Organización de la Información:

Retomemos toda la documentación generada en las fases de la metodología e igual cualquier información anexa como notas, antecedentes o informe policial.

Identifiquemos lo mas importante y pertinente de la investigación

Realizar conclusiones (tenga en cuenta los hechos) y crear una lista de las pruebas para presentar en el informe.

PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANÁLISIS FORENSE



Escribir el Informe Final:

Debe ser claro, conciso y escrito en un lenguaje entendible para gente común (no tan técnico).

Debe contener como mínimo:

Propósito del Informe. Explicar claramente el objetivo del informe, el público objetivo, y por qué se preparó el informe.

Autor del informe. Todos los autores y co-autores del informe, incluyendo sus posiciones, las responsabilidades durante la investigación, y datos de contacto.



PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANÁLISIS FORENSE



Resumen de Incidentes. Introducir el incidente y explicar su impacto. El resumen deberá estar escrito de manera que una persona no técnica, como un juez o jurado sería capaz de entender lo que ocurrió y cómo ocurrió.

Pruebas. Proporcionar una descripción de las pruebas de que fue adquirido durante la investigación. Cuando el estado de la evidencia que describen la forma en que fue adquirida, cuándo y quién lo adquirió.

PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANÁLISIS FORENSE



Detalles . Proporcionar una descripción detallada de lo que la evidencia se analizó y los métodos de análisis que se utilizaron. Explicar los resultados del análisis. Lista de los procedimientos que se siguieron durante la investigación y de las técnicas de análisis que se utilizaron. Incluir una prueba de sus resultados, tales como los informes de servicios públicos y las entradas de registro..

PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANÁLISIS FORENSE



Conclusión. Resumir los resultados de la investigación. La conclusión debe ser específico de los resultados de la investigación. Citar pruebas concretas para demostrar la conclusión, pero no dan excesivos detalles acerca de cómo se obtuvieron las pruebas (tal información debe estar en la sección “Detalles”). Incluir una justificación para su conclusión, junto con las pruebas y la documentación. La conclusión debe ser lo más clara y sin ambigüedades como sea posible. En muchos casos, se declaró cerca del comienzo del informe, porque representa la información procesable.



PRESENTACIÓN DE RESULTADOS Y OBJETIVOS DEL PROCESO DE ANÁLISIS FORENSE



Los documentos justificativos. Incluya cualquier información de antecedentes a que se refiere en todo el informe, tales como diagramas de red, los documentos que describen los procedimientos de investigación de equipos usados, y un panorama general de las tecnologías que intervienen en la investigación. Es importante que los documentos justificativos proporcionar información suficiente para que el lector del informe para comprender el incidente tan completamente como sea posible.