APUNTES 05

DOCUMENTACIÓN Y ELABORACIÓN DE INFORMES DE ANÁLISIS FORENSES

ANÁLISIS FORENSE INFORMÁTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

1.- DOCUMENTACIÓN Y ELABORACIÓN DE INFORMES DE ANÁLISIS FORENSES.

Caso práctico

María después de duras semanas de trabajo, tiene que plasmar todo el trabajo realizado. Desde el análisis y procesado de todas las evidencias hasta la extracción de las debidas conclusiones.

Son muchas evidencias, informes, documentos y datos que necesita reflejar en el informe de forma clara y precisa.

Para ello, y aunque no existe un modelo oficial de informe, se basará en el formato y esquema que se considera dentro de las buenas prácticas del sector.

Sabe que todo su trabajo valdrá de poco si no es capaz de trasladarlo de una manera objetiva tanto a nivel ejecutivo como técnico en el informe.

El informe forense es clave para poner en valor el trabajo realizado. Deberemos de ser capaces de realizar de forma correcta y reproducible la parte más importante de un análisis forense: Explicar que ha sucedido.

Para realizar este punto necesitaremos responder a las preguntas iniciales (5Q) planteadas. Si hay alguna de ellas que no se puede responer porque no se dispone de evidencias o algún otro factor externo se indicará en el informe.

1.1.- OBJETIVO Y ALCANCE.

El objetivo que tenemos llegados a este punto es claro, producir un informe que refleje todo nuestro trabajo, desde un punto de vista ejecutivo y técnico. ¿Qué características tiene que tener nuestro informe?:

- **Reproducible**: Lo primero de todo es que nuestro informe tiene que ser reproducible. Es decir, todas las acciones y conclusiones estarán basadas en hechos de tal manera que otro analista forense partiendo de las mismas evidencias, puede realizar llegaría al mismo resultado.
- **Verdadero**: Todas las afirmaciones que se indican en el informe deberán de ser objetivas y son ciertas, y cuando no haya un grado de certeza alto se hablará de hipótesis y estarán debidamente justificadas.
- **Correcto**: Las afirmaciones y conclusiones del informe deben de responder las preguntas planteadas.
- **Completo**: El informe debe contener todas las evidencias analizadas y las conclusiones para dar respuesta a las preguntas planteadas, en caso de que no se haya podido procesar una evidencia o haya alguna pregunta que no se pueda responder se indicarán los motivos que así lo obligan.
- **Comprensible**: El informe tiene que tener dos vertientes una ejecutiva a través del resumen ejecutivo donde se plasmen las principales conclusiones a alto nivel y por otro lado en el análisis debe estar redactado de forma que sea comprensible para una persona técnica claramente de forma general.

Respecto al alcance, debemos de incluir

- Todas las evidencias identificadas.
- Todas las evidencias procesadas.
- Principales conclusiones.
- Línea temporal que abarque todos los sucesos relacionados y las evidencias que lo sustenten.

1.2.- FORMATO Y ESQUEMA DEL INFORME.

Aunque no existe un modelo unificado y dentro del ámbito forense podremos encontrar desde informes periciales a informes de respuesta ante incidentes. Debemos de hacer constar quien es el autor o autores del informe y qué capacitación tenemos en la materia para ello incluiremos los siguientes punto

Resumen ejecutivo

- Principales conclusiones a alto nivel.

Presentación

- Nombre completo de los autores.
- Número de colegiado o tarjeta profesional de la organización profesional en la que están colegiados los autores.
- Titulación académica.
- Resumen de nuestra capacitación en el área.
- Parte que nos requiere (un juzgado, un cliente, etc)

Alcance

- Ámbito de nuestra investigación
- Motivo o situación de nuestra contratación
- Preguntas específicas que debamos dar respuesta.

Antecedentes

- Plantilla de toma de datos inicial.
- Autorización de acceso.
- Contexto o situación particular de la investigación.

Investigación

- Fuentes de información y datos de partida.
- Estandartes, normas, reglamentos y leyes aplicables citados en los distintos apartados.
- Terminología y abreviatura.
- Herramientas utilizadas.
- Limitaciones.
- Garantía de custodia y salvaguarda de evidencias.
- Extracción de evidencias declaradas en el acta notarial.
- Geolocalización.
- Línea de tiempo. Investigación realizada. Proceso de análisis.

Conclusiones

- Dictamen final.
- Conclusiones finales.
- Hechos que soportan las conclusiones.

Anexos

- Contienen toda la información en bruto necesaria para que el análisis pueda ser reproducible por una tercera parte.
    - Documentos de análisis detallados.
    - Documentos regulatorios o específicos.
    - Documento de garantías de evidencias.

1.3.- NORMAS Y RECOMENDACIONES.

A nivel de recomendaciones generales del informe deberemos de:

- Ser objetivos, evitar opiniones o comentarios no basados en hechos
- Ceñirnos a las evidencias, evitando comentar aspectos no relacionados con las mismas.
- Expresar el resumen ejecutivo con lenguaje formal y directo
- Utilizar un lenguaje técnico en el proceso de análisis.
- Explicar como llegamos de forma reproducible a las conclusiones.
- El informe deberá de ser legible y por tanto deberemos de trabajar la economía del lenguaje (es decir expresar la información con el mínimo de la palabras necesarias pero que sea claro y conciso).
- No mencionar o hacer referencias a aspectos fuera del alcance definido, es decir, ceñirnos al alcance.
- El informe ejecutivo se hace al final, partiendo de las conclusiones finales, siendo directos y con un lenguaje ejecutivo.

A nivel de legislación deberemos de recordar que el peritaje informático se rige por la Ley de Enjuiciamiento Civil recogida aquí.

Este punto también hace que sea recomendable estar al día de cambios legales o de legislación que pudiera afectarnos.

Debes conocer

Uno de los puntos más importantes es conocer el tipo de información que estamos escribiendo, ya que la mayoría de las veces contiene información sensible. Durante los últimos años se ha trabajo en hacer una clasificación o sellado de la información sensible pero no clasificada en el ámbito de la Seguridad de la Información mediante el protocolo TLP. Tiene una excelente guía en la web oficial de INCIBE.

Debes conocer

Uno de los ejemplos de estar al día con los cambios de lesgislación podría ser:

> Artículo 299.2 Ley de Enjuiciamiento Civil: Medios de prueba«También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso»

Por tanto, un medio de prueba puede ser una prueba informática que pueda ser estudiada, almacenada y obtener conclusiones reproducibles.

> Artículo 340 Ley de Enjuiciamiento CivilEl artículo 340.1 de la Ley de Enjuiciamiento Civil (LEC) que determina respecto a las condiciones de los peritos: «los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de este».

Si se tratara de materias que no estén comprendidas en títulos profesionales oficiales, «habrán de ser nombrados entre personas entendidas en aquellas materias». Por otra parte, en el artículo 457 de la Ley de Enjuiciamiento Criminal (LECrm) se incluyen otras consideraciones a tener en cuenta sobre como ser perito judicial al determinar que: Los peritos pueden ser o no titulares. Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentando por la Administración. Son peritos no titulares los que, careciendo de título oficial, tienen sin embargo, conocimientos o práctica especiales en alguna ciencia o arte”

1.4.- CONCLUSIONES

Es el punto más importante de todo el informe, las conclusiones. Aquí trasladamos en valor todo nuestro trabajo realizado y a partir de este punto se construye el resumen ejecutivo.

El punto más importante a remarcar es separar de una manera clara los hechos probados de las conclusiones. Los hechos probados son fehacientes, de una manera clara y objetiva cualquier otro forense llegaría al mismo hecho que nosotros después de procesar las evidencias. El problema surge porque muchas veces podemos testar muy seguros de una conclusión debido a nuestra creencia basada en nuestra experiencia pero no tener la evidencia o prueba fehaciente que lo soporte, por lo que en vez de clasificarlo como hecho lo calificaríamos como hipótesis.

Algunos consejos prácticos para el analista forense:

- Trata de ser claro y directo en las conclusiones.
- Habla de hechos si tienes todas las garantías y puedes dar fe de ellas, sino es así o todavía faltan evidencias que sustenten el hecho, habla de hipótesis.
- Hablar de hipótesis no es algo malo, a veces no podemos garantizar un hecho, trata de darles relevancia aportando datos adicionales (casos similares, otros informes periciales, evidencias que sugieren o dan cuerpo a esa hipótesis).
- Construye el resumen ejecutivo basado en las conclusiones. Intenta resumir en el menor número de palabras los hechos más relevantes siendo claro y coherente.

Autoevaluación

Identifica si las siguientes frases son verdaderas o falsas

1- El resumen ejecutivo expresa las conclusiones y debería ir por tanto con las conclusiones al final del documento.
   a. Verdadero
   b. Falso

2- Se considera buena práctica introducir a los autores y sus capacitaciones para con la materia.
   a) Verdadero
   b) Falso

3- Si las conclusiones son muy extensas se pueden poner como anexo al informe.
   a) Verdadero
   b) Falso

4- Debe de dotarse de contexto la investigación durante la fase de antecendentes.
   a) Verdadero
   b) Falso

TEST I

1- Para realizar el informe no es necesario responder a las preguntas inicialmente planteadas ¿Verdadero o falso?
   a) Verdadero
   b) Falso

2-¿Que necesita un informe para ser correcto?:
   a) Contener todas las evidencias identificadas y procesadas.
   b) Las afirmaciones y conclusiones del informe deben de responder las preguntas planteadas.
   c) Que todas las acciones y conclusiones estarán basadas en hechos.
   d) Es no contenga faltas de ortografía.

3- Teniendo clara la parte más importante de un análisis forense, que debe contener un informe:
   a) Capturas de pantalla.
   b) Explicación de lo sucedido.
   c) Conclusiones del análisis.
   d) Introducción completa.

4-¿Los medios de reproducción de la palabra, el sonido y la imagen son admitidos por la ley de Enjuiciamiento Civil como prueba?:
   a) Si, todos ellos.
   b) Solo los medios de reproducción de la palabra y el sonido.
   c) Solo los medios de imágen y sonido.
   d) Ninguno de ellos.

5- No es recomendable expresar el resumen ejecutivo con lenguaje formal y directo. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

6- Qué punto NO pertenece al apartado de antecedentes:
   a) Plantilla de toma de datos inicial.
   b) Fuentes de información y datos de partida.
   c) Contexto o situación particular de la investigación.
   d) Autorización de acceso.

7- Cuáles son otras consideraciones a tener en cuenta sobre como ser perito judicial:
   a) Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentando por la Administración.
   b) Son peritos no titulares los que, careciendo de título oficial, tienen sin embargo, conocimientos o práctica especiales en alguna ciencia o arte"
   c) Todas son correctas.
   d) Los peritos pueden ser o no titulares.

8- Un informe se considera completo si contiene las conclusiones para dar respuesta a las preguntas planteadas aunque no se hayan podido procesar algunas evidencias. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

9- En el apartado conclusiones de un informe debe incluir:
   a) No es necesario incluir conclusiones si no se ha obtenido ninguna.
   b) Las conclusiones, dictamen y los hechos que soporten a las conclusiones
   c) Únicamente el dictamen final.
   d) Únicamente las conclusiones finales

10- Dentro del alcance, es recomendable:
   a) Mencionar aspectos que puedan ser interesantes pese a no estar en el alcance.
   b) Adaptar el alcance si se cree conveniente.
   c) Hacer referencias a aspectos fuera del alcance definido.
   d) Ceñirnos a dicho alcance.

TEST II

1- Para poner en valor el trabajo realizado, el informe forense es clave. ¿Verdadero o Falso?
   a. Verdadero
   b. Falso

2- Las afirmaciones y conclusiones del informe deben de responder las preguntas planteadas ¿Verdadero o Falso?
   a. Verdadero
   b. Falso

3- Los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de este. ¿Verdadero o Falso?
   a. Verdadero
   b. Falso

4- En un informe es recomendable:
   a) Ser objetivos
   b) Trabajar la economía del lenguaje
   c) Todas las respuestas son correctas
   d) Ceñirnos al alcance.

Respuestas:
Autoevaluación I: 1 b), 2 a), 3 b), 4 a)
TEST I:1 b), 2 b), 3 b), 4 a), 5 b), 6 b), 7 c), 8 a), 9 b), 10 d)
TEST II: 1 a), 2 a), 3 a), 4 c), 5 a), 6 c), 7 b), 8 b), 9 c), 10 a)

5- Es recomendable en un informe trabajar la economía del lenguaje (es decir expresar la información con el mínimo de la palabras necesarias pero que sea claro y conciso).¿Verdadero o Falso?
   a) Verdadero
   b) Falso

6- ¿Qué debe incluir el alcance de un informe?:
   a) Línea temporal que abarque todos los sucesos relacionados y las evidencias que lo sustenten.
   b) Todas las evidencias identificadas y procesadas.
   c) Todas las respuestas son correctas
   d) Principales conclusiones.

7- Es lo mismo una evidencia procesada y una evidencia identificada. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

8- No es importante estar al dia de cambios legales o de legislación ¿Verdadero o falso?
   a) Verdadero
   b) Falso

9- ¿En que punto del informe debe aparecer las principales conclusiones a alto nivel?:
   a) Presentación.
   b) Investigación.
   c) Resumen ejecutivo.
   d) Conclusiones.

10- En un informe, debemos de hacer constar quien es el autor o autores del informe y qué capacitación tienen en la materia ¿Verdadero o Falso?
   a) Verdadero
   b) Falso

Caso práctico
María se enfrenta a la parte final de su trabajo: el informe forense.
Sabe que este informe debe recoger el trabajo de duras semanas de análisis de evidencias y extracción de información. Cualquier actuación realizada relevante debe de estar recogida en el informe, así como las principales conclusiones y análisis técnico realizado. María sabe que si no lo reporta en el informe es como si no se hubiera hecho. Por otra parte sabe que aunque explique técnicamente como se ha llegado a las conclusiones debe también hacer un resumen ejecutivo donde se explique sin tecnicismos las principales conclusiones de la investigación.
Apartado 1: Análisis de Informe Forense.
En esta tarea analizaremos un informe forense real, para entender cómo se refleja nuestro trabajo y conclusiones. Veremos qué puntos deberemos incluir y cuáles podrían haber mejorado nuestro informe.
El informe en: https://drive.google.com/file/d/1xB1QosHqXz5NO3TlPAoSL5UY_X1Q3KaX/view?pli=1

PREGUNTA 1: ¿Qué puntos echas de menos dentro del informe?
El informe está bastante técnico y detallado, pero hay algunos aspectos clave que faltan:

- Falta dar un contexto más claro, no se explica en profundidad para qué se analiza el video, ni por qué es importante. Se podría especificar si es una prueba para un juicio o si están poniendo en duda su validez, estos detalles ayudarían a entender mejor la relevancia del análisis.
- Herramienta utilizada, se menciona el análisis del video pero no se especifica que software o técnica se empleó para la verificación. Saber la herramienta que se utilizaron ayudaría a validar el análisis. Por ejemplo si se usaron programas forenses como Amped Authenticate o herramientas para el análisis de metadatos, esto daría más credibilidad al informe.
- Explicaciones visuales, aunque el documento incluya imágenes y capturas, sería útil tener explicaciones más detalladas de cada una y cómo se relacionan con el análisis realizado. Para tener una mejor comprensión del informe, sobre todo para quienes no tengan conocimientos técnicos, se podrían añadir gráficos o diagramas que ilustren los resultados.
- Limitaciones del análisis, se mencionan que hay restricciones, pero no se entra en detalle de cuales son (si es la calidad del video, la falta de datos, ediciones previas...) detallar estas limitaciones ayudaría a entender mejor los posibles errores o incertidumbre del resultado..

PREGUNTA 2: ¿Qué puedes decir del marcado de TLP del informe? ¿Qué grado le darías?
El TLP (Traffic Light Protocol) es un sistema que indica el nivel de confidencialidad de un documento. En este caso, el informe no parece tener marcado explícitamente el TLP, lo cual ya indica un problema, porque este sistema indica la sensibilidad de la información.
Si tuviese que asignar un grado, le daría TLP:AMBER porque parece ser un documento con información sensible relevante en un caso legal, no debería circular libremente, solo debe compartirse con aquellas personas relacionadas con el caso. Esto significa que la información es sensible y debe ser manejada con cuidado, compartida solo con aquellos que necesiten saber para cumplir con sus responsabilidades.
En caso de que el informe debiera ser completamente privado y solo pudiese acceder a él un número muy reducido de personas, podría ser TLP:RED, esto indicaría que la información es extremadamente sensible y su distribución debe limitarse al máximo. Pero si estuviese destinado a un ser público, debería tener una versión con TLP:WHITE, lo que significa que la información puede ser compartida libremente.

PREGUNTA 3: ¿Cuáles son las conclusiones del resumen ejecutivo? ¿En qué añadirías y en qué lo basarías?

Las conclusiones sacadas del informe ejecutivo:

- El video no presenta signos de haber sido manipulado.
- La transcripción del audio es precisa y fiable.
- Se garantiza la autenticidad del contenido del video

Se podría añadir:

- Se podría añadir una parte con una explicación del análisis incluyendo términos simples en la que se detalle lo realizado y las conclusiones, sin necesidad de ser experto en informática. Esto ayudaría a que cualquier persona independientemente de su nivel de conocimiento técnico pueda entender el análisis.
- Pruebas visuales que muestren cómo se analizaron las imágenes o el audio. Esto proporciona una representación visual de los hallazgos, haciendo que el informe sea más fiable y entendible.
- Indicar consecuencias según el resultado del análisis, en caso de que el video fuese falso indicar las consecuencias que hubiese podido haber y en caso de ser verdadero cómo afecta al proceso legal. Además de indicar el margen de error existente y que pruebas respaldan esa resolución. Esto ayudaría a entender las implicaciones legales de los resultados obtenidos.

PREGUNTA 4: ¿Qué opinas de la identificación de evidencias?

La identificación de evidencias está bien estructurada y es bastante precisa, pero algunos aspectos podrían mejorarse. La parte positiva sería que se documentan momentos clave del video con las marcas de tiempo y se menciona el uso de técnicas forenses para garantizar que el video no ha sido editado. Como partes a mejorar se podrían destacar:

- Informar acerca de la cadena de custodia, no se explica cómo se obtuvo el video, quién lo entregó y cómo se asegura que no fue alterado antes del análisis. Detallar la cadena de custodia ayudaría a demostrar la integridad de esa información.
- No se menciona si analizaron los metadatos, como la fecha de creación, posibles modificaciones, dispositivos usados… Revisar los metadatos proporciona información adicional sobre su autenticidad.
- Realizar una doble verificación, no se detalla qué técnicas usaron para descartar manipulaciones, ni indican una contrastación con varias herramientas.Utilizar múltiples herramientas y técnicas para realizar las verificaciones, demuestra la autenticidad del video y por tanto la fiabilidad del análisis.

PREGUNTA 5: ¿Qué opinas del lenguaje usado?

El lenguaje usado en el informe es técnico y formal, lo cual es adecuado para un documento pericial. Mantiene una estructura ordenada y clara para expertos en la materia. Sin embargo, para alguien sin mucho conocimiento en informática forense podría resultar complicado, por tanto sería útil incluir explicaciones más sencillas y ejemplos para hacer el contenido más entendible a personas con menos nivel en la materia.

- Se deduce que es un informe técnico por no aclarar términos que podrían ser desconocidos para una persona sin formación técnica, falta claridad en las explicaciones y faltarían ejemplos para apoyar los hallazgos.
- Está bien para un informe legal, pero se agradecería un poco más de claridad en las explicaciones. Utilizar un lenguaje más accesible y menos técnico ayudaría a que el informe sea comprensible para un mayor público.

PREGUNTA 6: ¿Qué más te llama la atención?

- El análisis del comportamiento de las personas dentro del video proporciona información adicional relevante para el caso, no se limita solo a verificar la autenticidad de la grabación, esto sugiere que puede ser parte de una investigación judicial.
- Se hace un estudio exhaustivo de la transcripción del video, no solo se analiza la imagen, lo que refuerza su autenticidad. La transcripción es crucial para garantizar que el contenido es auténtico y no ha sido manipulado.
- No queda clara la conclusión definitiva sobre su autenticidad, se hacen observaciones sobre el video pero no se afirma su veracidad. Sería útil tener una conclusión clara y definitiva.
- La estructura del informe está bien estructurada pero se repiten aspectos sin aportar nueva información. Se debería mejorar la estructura del informe para evitar repeticiones y dar la máxima información relevante a la vez.

En conclusión el informe es sólido y bien estructurado, pero podría mejorar en claridad y profundidad, desarrollando y explicando con lenguaje menos técnico algunos conceptos. Faltan detalles técnicos sobre el software y los métodos utilizados, una mejor identificación de la evidencia, como su origen o finalidad y una explicación más accesible del análisis. Además, no tiene un marcado TLP, lo que podría generar dudas sobre la confidencialidad del documento.