[Curso de Informática Forense](https://platzi.com/clases/forense/)

**ArtículoElaboración de informe preliminar**

[**Juan Pablo Caro**](https://platzi.com/%40juanpcaro)

23 de Mayo de 2019

Cuando ocurre un incidente informático, las personas afectadas siempre necesitan tener respuesta rápidamente. Esta es una constante con la que te vas a encontrar en tus investigaciones, y tu capacidad, no solo para responder rápidamente al incidente, sino para manejar las expectativas de quienes esperan tu análisis, va a ser muy importante en tu carrera como investigador.

Precisamente por esta expectativa y necesidad de respuesta que siempre se encuentran en las investigaciones, en muchas ocasiones es útil realizar un análisis preliminar e incluso presentar un informe con los resultados que obtengas, con el fin de dar un primer avance en el desarrollo de la investigación. Regularmente, un informe de análisis preliminar incluye:

1. **Introducción al caso:** Una presentación general del incidente y el contexto de la investigación. Debe mostrarle al lector claramente por qué se inició una investigación, y quién está a cargo de la misma.
2. **Resumen general:** Una descripción breve del proceso de investigación que se está ejecutando, y las actividades que se han desarrollado hasta este punto. Si hay resultados importantes que se hayan obtenido, es muy importante incluirlos acá para mostrar avances en la investigación.
3. **Inventario de evidencia identificada:** Una relación general de la evidencia que se ha preservado y sobre la que se está realizando el análisis. Es importante mencionar los criterios usados durante la etapa de identificación para escoger los dispositivos en particular, así como explicar las decisiones que se han tomado durante el proceso de investigación (¿Por qué se decidió analizar un dispositivo en particular?, ¿Por qué se utilizó cierta estrategia o herramienta?).
4. **Reportes de adquisición de evidencia:** Los informes técnicos de adquisición. Es importante asegurar desde las primeras etapas que la información con la que estamos trabajando es íntegra, sobre todo en contextos o escenarios donde pueda haber dudas sobre la calidad de la información obtenida. Recuerda documentar todos los pasos y decisiones que hayas tomado durante la preservación de cada elemento.
5. **Información general de los sistemas preservados:** La primera etapa del análisis consiste en identificar qué información hay disponible y cómo está almacenada. Regularmente esto implica analizar los sistemas operativos e identificar datos sobre ellos como la zona horaria, la fecha de instalación, los usuarios configurados, entre otros.
6. **Información encontrada en las imágenes forenses:** Para tomar decisiones sobre cómo avanzar en la investigación, es necesario tener claro qué información se encontró. Datos como cuentas de correo electrónico, carpetas de usuario, documentos y similares, son importantes en esta etapa y es necesario documentarlos.
7. **Hallazgos preliminares, si existen:** Es importante describir detalladamente cualquier hallazgo o resultado importante que se haya encontrado. En muchas ocasiones los resultados más importantes se identifican en la primera etapa de la investigación, y es importante documentarlos rápidamente para mostrar avances.
8. **Siguientes pasos:** Finalmente, un buen indicador de una investigación estructurada y que está avanzando es un plan de trabajo sobre los resultados identificados. En un informe preliminar idealmente debería explicarse el plan de trabajo que se está siguiendo, el avance actual sobre este y los pasos a seguir para concluir satisfactoriamente la investigación.

Como siempre, ten en cuenta que esto no es un absoluto, y siempre encontrarás escenarios, investigaciones o casos que tengan requerimientos diferentes o muy específicos. Una de las características más valiosas en un investigador es su capacidad de adaptarse a situaciones diversas. No pierdas de vista el objetivo principal de la investigación y recuerda, para tu plan de acción, las 6 preguntas básicas del método de investigación.

Reportar un problema

**Crear una imagen de contenido personalizado para análisis**