

Panorama General

La metodología de análisis forense desarrollada por los consultores de HIXSA está basada en las buenas prácticas y metodologías recomendadas por organizaciones especializadas en la seguridad informática como NIST SP800-86, SANS FOR500, SANS FOR 508 y SANS FOR 526, así como en la amplia experiencia de nuestros consultores forenses.

La metodología es independiente del sistema operativo o versión que se esté analizando y los pasos listados serán ejecutados en cada análisis realizado, sin embargo, en la ejecución del análisis existen diferencias específicas que dependen de cada sistema operativo, versión particular o herramientas que se deberán usar en cada fase.

1 Adquisición de evidencia

- Entrevistas
- Verificación
- Descripción del sistema
- Adquisición
- Preservación de evidencia

2 Investigación y análisis

- Búsqueda y análisis de archivos relacionados
- Búsqueda de cadenas o bytes
- Recuperación de información
- Análisis de la línea de tiempo
- Búsqueda de información relevante en componentes ajenos involucrados

3 Entrega de resultados

- Generación de reporte
- Emisión de recomendaciones
- Descripción del sistema
- Lecciones aprendidas

A continuación, se muestran algunas capacidades del servicio:

- Aplicación de entrevistas
- Generación de cadena de custodia
- Adquisición de imágenes
- Adquisición de memoria volátil
- Preservación de evidencia
- Investigación en servicios de red
- Investigación dispositivos móviles desbloqueados (iOS, LG, Motorola, Samsung)
- Preservación de la integridad de la información recibida durante la ejecución del proceso de análisis forense.
- Recuperación de información modificada o borrada
- Obtención de información en fuentes públicas en la red en caso de que estas pudieran llegar a ser relevantes para la investigación realizada.

Detalles del servicio

El servicio consta de una serie de actividades considerando:

- Integración de todas las tareas necesarias para la ejecución de los Análisis Forenses
- Apoyo en la definición del objetivo parámetros y cuestionario que resulten de interés para la investigación solicitada.
- Dar continuidad y seguimiento a los casos solicitados, así como, el registro de los indicadores correspondientes.
- Preservación de la integridad de la información recibida durante la ejecución del proceso de análisis forense (cadena de custodia).
- Participación en entrevistas con los principales involucrados con la finalidad de obtener el contexto necesario en las investigaciones digitales que deban realizarse.
- Obtención de información de fuentes públicas en la red en caso de que estas pudieran llegar a ser relevantes para la investigación realizada.
- Evaluación de información en los equipos de cómputo, servidores físicos, servidores virtuales, dispositivos móviles, equipo de comunicaciones, entre otros, para la identificación de indicios de compromiso y su evidencia correspondiente.
- Ejecución de un proceso de recuperación de información que haya sido borrada previamente.
- Elaboración de un dictamen técnico, por cada requerimiento atendido, con la información identificada en el o los procesos de análisis forense, considerando la generación y firma de los documentos que expresen los resultados de la investigación en forma clara y concisa, de manera que puedan ser comprendidos por aquellos que no conocen o dominan el lenguaje técnico.

Volumetría

1 análisis forense
CDMX y AM

Tiempo

15 días hábiles