LA INFORMÁTICA FORENSE HERRAMIENTA CLAVE PARA LA INVESTIGACIÓN DE DELITOS QUE GENERAN AFECTACION AL PATRIMONIO DE LAS PERSONAS Y AL ORDEN ECONOMICO NACIONAL

(Dra. Olga Jazmín Carrillo Rey)

Auditora Forense.

La informática forense es una disciplina esencial para investigar y resolver el fraude corporativo mediante el análisis de datos digitales. Estos datos se encuentran en diversos dispositivos electrónicos utilizados para registrar, procesar y almacenar información dentro de las organizaciones.

En situaciones donde se han perdido datos importantes, ya sea por fallos del sistema o eliminaciones accidentales, los expertos en informática forense aplican técnicas especializadas para recuperar información valiosa. Además, en casos de robo de secretos comerciales o propiedad intelectual, se requiere un análisis forense para demostrar el uso indebido de información confidencial.

En disputas legales, la evidencia digital puede ser fundamental. La informática forense se encarga de recolectar y preservar esta evidencia de forma que sea admisible en un tribunal.

Así mismo, los casos de acoso en línea o extorsión a menudo implican pruebas digitales que necesitan ser analizadas para identificar al perpetrador.

Cuando una organización sufre una violación de seguridad, la informática forense ayuda a determinar el alcance del daño, qué datos fueron comprometidos y cómo ocurrió la brecha. Tras un ataque cibernético, se lleva a cabo un análisis forense para entender las vulnerabilidades explotadas y prevenir futuros incidentes.

La informática forense también es crucial en la resolución de delitos cibernéticos, tales como:

1. **Hacking:** Este término se refiere al uso de habilidades técnicas para acceder a sistemas informáticos, redes o dispositivos electrónicos con el objetivo de entender su funcionamiento, modificar su comportamiento o explotar vulnerabilidades. La informática forense se utiliza para identificar al atacante, comprender cómo se llevó a cabo el ataque y recuperar datos comprometidos.

2. **Fraude en línea:** En los casos de estafas o fraudes a través de internet, los expertos en informática forense analizan correos electrónicos, transacciones y registros digitales para rastrear a los responsables.

3. **Crímenes tradicionales con elementos digitales:** En delitos como el crimen financiero que afecta el patrimonio de una organización, los dispositivos electrónicos (como computadoras y teléfonos móviles) pueden contener evidencia crucial. La informática forense permite recuperar mensajes, fotos y otros datos relevantes para resolver el caso.

La recolección de evidencia en una auditoría de informática forense es un proceso meticuloso y crítico, ya que cualquier error puede comprometer la integridad de la información.

Antes de comenzar la recolección, es fundamental diseñar un plan detallado que incluya definir los objetivos de la auditoría, identificar las fuentes de evidencia y establecer un cronograma.

Es esencial contar con las autorizaciones necesarias para realizar la auditoría, lo que puede incluir permisos legales y la aprobación de la alta dirección.

Además, es crucial evitar cualquier alteración de los datos utilizando herramientas forenses para crear copias bit a bit (imágenes forenses) de los dispositivos involucrados (discos duros, servidores, etc.) y documentar cada paso del proceso.

Mantener un registro meticuloso de todas las acciones realizadas durante la recolección. Esto incluye quién estuvo presente, qué se recolectó, cómo se manejó y cómo se almacenó la evidencia. Una vez que se ha recolectado la evidencia, comienza el análisis utilizando software forense especializado. Busca patrones inusuales o transacciones sospechosas que puedan indicar fraude.

Asegúrate de que los hallazgos sean verificables y que la evidencia sea válida; esto puede incluir comparar datos con registros contables y otros documentos relevantes.

Finalmente, elabora un informe claro y conciso que detalle los hallazgos, las metodologías utilizadas y cualquier recomendación para prevenir futuros fraudes.

En algunos casos, puede ser necesario presentar tus hallazgos ante un tribunal o en una reunión con la alta dirección. Prepárate para explicar tu metodología y responder preguntas sobre tu análisis.

La informática forense es una herramienta poderosa en la resolución de delitos y en la protección de datos. La capacidad de analizar y presentar evidencia digital es esencial en un

mundo donde gran parte de nuestras interacciones y transacciones se realizan de manera digital. Así, el Anti Fraud Institute “AFI” contribuye en la capacitación continua en técnicas forenses para mantenerse actualizado frente a las nuevas amenazas cibernéticas.

En la segunda parte de este articulo profundizaremos sobre la correcta custodia de las pruebas digitales, en la práctica de la informática forense.