UCACEP

PROFRA: MARIA DE LOS ANGELES VILLAVICENCIO PICHARDO

CRIMINALISTICA II

TEMA 7.- INFORMATICA FORENSE

INFORMATICA FORENSE

- El **objetivo principal de la INFORMATICA FORENSE es la obtención de evidencias relativas a un crimen digital.**

La **informática forense** se refiere a un conjunto de procedimientos y técnicas metodológicas para identificar, recolectar, preservar, extraer, interpretar, documentar y presentar las evidencias del equipamiento de computación de manera que estas evidencias sean aceptables durante un procedimiento legal o administrativo en un juzgado.

USO DE LA INFORMATICA FORENSE

- La informática forense es escencial para:
- Asegurar la integridad y disponibilidad de la infraestructura de red cuando sucede un incidente de ciberseguridad o ataque informático.
- Identificar y obtener evidencias de los cibercrímenes de manera apropiada.
- Asegurar la **protección adecuada de los datos** y el cumplimiento regulatorio.
- Proteger a las organizaciones para que no vuelvan a suceder en el futuro los incidentes ocurridos.
- Ayudar en la protección de **crímenes online**, como abusos, *bullying*…
- Minimizar las pérdidas tangibles o intangibles de las organizaciones o individuos relativas a incidentes de seguridad.
- Soportar el proceso judicial de enjuiciamiento de los criminales.

LA INFORMÁTICA FORENSE Y EL DELITO

- La informática forense es de ayuda cuando se producen delitos o incidentes de seguridad de la información que involucran sistemas o tecnologías de la información y las comunicaciones. La mayoría de las organizaciones buscan en la informática forense:
- Prepararse contra los incidentes de ciberseguridad mediante la **securización de sus mecanismos de defensa** y subsanar las vulnerabilidades encontradas en ellos.
- Para asegurar el **cumplimiento de las regulaciones y leyes** al respecto que le son de aplicación.
- Reportar los **incidentes de seguridad** de la información de manera adecuada y detallada.
- Identificar las acciones necesarias de respuesta ante incidentes.
- Actuar contra el **robo o la utilización ilegal** de la propiedad intelectual.
- Resolver disputas entre los empleados o con ellos.
- Estimar o minimizar los **daños sufridos** en un incidente de seguridad.
- Crear las normas y/o procedimientos de investigación forense.

EL PERFIL DE ESPECIALISTA EN INFORMÁTICA FORENSE

- Las **funciones** de un especialista en informática forense son:
- Identificar, obtener y preservar las evidencias o pruebas de un cibercrimen.
- Rastrear e identificar a los culpables.
- Interpretar, documentar y presentar las evidencias para que sean admisibles judicialmente.
- Estimar el impacto potencial de la actividad maliciosa para la víctima o los activos.
- Encontrar vulnerabilidades o brechas de seguridad que ayudan a los atacantes.
- Entender las técnicas y métodos utilizados por los atacantes para evitar ser cazados.
- Recuperar archivos borrados, ocultos y datos temporales que pueden utilizarse como evidencias.
- Realizar la respuesta ante incidentes de seguridad de la información para prevenir la pérdida de información, económica y de reputación.
- Disponer de conocimiento sobre las leyes de aplicación en diferentes áreas y regiones relativas al crimen digital.
- Conocer el proceso de manipulación para la investigación forense de múltiples plataformas, tipos de datos y sistemas operativos.
- Manejar herramientas específicas de investigación forense.

¿CUÁL ES EL PROCESO DE INVESTIGACIÓN EN EL ÁMBITO INFORMÁTICO?

- Las fases de la investigación forense en informática son:
- **Preinvestigación**
- Todas las tareas realizadas de manera previa al inicio de la investigación. Comprende, entre otras, la instalación o preparación del laboratorio forense, la configuración del ordenador de trabajo para la investigación y las herramientas necesarias, la designación del equipo de investigación, la autorización para la investigación, la planificación del proceso a realizar, objetivos, securizar el perímetro del caso y los dispositivos involucrados…

INVESTIGACIÓN

- Adquisición, preservación y análisis de las evidencias para identificar el origen del crimen o incidente y los culpables. En esta fase hay que poner en juego los conocimientos técnicos necesarios para encontrar las evidencias, examinarlas, documentarlas y preservar los hallazgos. Es crucial asegurar la calidad (inequívocos, claros y exactos) e integridad (no han sido manipulados, se ha asegurado la cadena de custodia) de los hallazgos para que no sean desestimados en el juzgado.

POSTINVESTIGACIÓN

- Reporte y documentación de todas las acciones llevadas a cabo para la obtención de los hallazgos. El informe debe ser claro, conciso, exacto y, por lo tanto, fácilmente entendible por la audiencia y proveer las evidencias adecuadas.
- La informática forense es un proceso clave para **rastrear e identificar a los culpables** de haber cometido un crimen en el que se vean involucrados dispositivos de computación y también para los incidentes de seguridad de la información. Además, desde un punto de vista de ciberseguridad la informática forense ayuda también en la prevención y respuesta ante ciberincidentes.

GRACIAS

REALIZA UNA RETROALIMENTACIÓN Y SUBE A PLATAFORMA