Computación Forense

Historia y Objetivos de la Ciencia Forense

S1V2

Profesor: Ing. Alex Araya Rojas, MT

CISSP, CISM

Historia y Objetivos de la Ciencia Forense

Conjunto de procedimientos y técnicas metodológicas que ayudan a identificar, preservar, extraer, interpretar, documentar y presentar evidencia de equipos informáticos.

Certificación Oficial CHFI

Historia y Objetivos de la Ciencia Forense

Objetivos

- Obtener evidencia probatoria sobre actos ilegales o que atenten contra las normas establecidas y que permita llevar exponer a los autores de los mismos.

- Estimar el impacto potencial de una actividad maliciosa y minimizar las pérdidas asociadas así como eliminar causas raíz para evitar que los eventos sigan presentándose.

- Preparar a la organización en procesos de respuesta a incidentes.

Historia y Objetivos de la Ciencia Forense

Cibercrímenes

- Internos
- Externos

- Civiles
- Penales
- Administrativos/Laborales

Historia y Objetivos de la Ciencia Forense

Retos para un investigador forense

- Innovación tecnológica
- Herramientas de anonimato
- Volatilidad de las evidencias
- Tamaño de la evidencia y complejidad
- Técnicas Anti-Digital Forensic (ADF)
- Globalidad y legislación específica de cada país o región.

Historia y Objetivos de la Ciencia Forense

Evidencia Digital

Se entiende como cualquier evidencia con valor probatorio que está almacenado o ha sido transmitido en una forma digital.

Certificación Oficial CHFI

Tipos de Evidencia Digital

Evidencia de Tipo Volátil

Datos que se pierden cuando el equipo es apagado.

- Información en la memoria RAM
- Información de la red

Evidencia de Tipo No Volátil

Datos persistentes que son almacenados en discos duros, tarjetas de memoria, entre otros.

Características Deseables

Legal, Real, Completa y Confiable

Preparación

¿Paso a paso que deberíamos hacer?

1. Antes de que se presenten los incidentes, deberíamos mapear las capacidades de nuestra organización para hacerle frente a los mismos.

2. Es importante tener plena identificación de las fuentes de evidencia y los mecanismos para extraerla.

3. Debemos capacitar a nuestro personal en los temas relacionados para que llegado el momento sepan lo que tienen que hacer.

4. Entrenar a la organización en el manejo de la evidencia y documentar el procedimiento utilizado así como la cadena de custodia.

5. Aplicar lecciones aprendidas y validar las iniciativas de terceros que puedan aplicarse a nuestra organización.

Privacidad y Legalidad

Premisas a tener en consideración

1. Deben mantenerse el anonimato de las partes hasta que se determine su culpabilidad y más allá inclusive si es necesario.

2. Sin el permiso administrativo/legal, no se puede actuar, salvo casos críticos debidamente justificados.

Reglas básicas para manejar evidencia

1. La evidencia es de acceso restringido, se trabaja con copias SIEMPRE!!!
2. Crear el documento de cadena de custodia es muy importante.
3. La evidencia debe estar relacionada con el incidente, debemos respetar otra información si no tiene relación con el caso, salvo si representa un delito.
4. Es necesario contar con sitios seguros para el manejo de la evidencia.

Proceso General Equipo Forense

Gracias