ESPE Innovativa

DESARROLLA
ESPECIALIZA
TRANSFIERE

Presentación del Curso

Seguridad Forense

Unidad de
Capacitación y Certificación

Tabla de contenido

SEGURIDAD FORENSE

Descripción general

El presente curso se desarrollará en la modalidad presencial, el cual permitirá fortalecer conocimientos y técnicas específicas para presentar, obtener y preservar datos que han sido procesados electrónicamente y guardados en soportes informáticos.

En esta capacitación se estudiará las herramientas que se utilizarán para recolectar información de los dispositivos que van desde ordenadores, teléfonos móviles y servidores de correo electrónico.

Este curso se encuentra organizado en cinco unidades:

En la primera unidad se analiza el cibercrimen y cómo combatirlo, el mismo que es una amenaza creciente en el internet.

En la segunda unidad se analiza el proceso de recuperar la información a través del descifrado de contraseñas almacenadas en el browser.

En la tercera unidad se analiza la cadena de custodia que maneja el experto forense.

En la cuarta unidad se analiza los dispositivos como: ordenadores, teléfonos móviles y servidores de correo electrónico para recopilar información y respaldar las evidencias de acuerdo al informe forense.

En la quinta unidad se analiza el rol del perito en el proceso pericial.

Con esta capacitación logrará mejorar el desempeño profesional y competente de las personas que trabajan en los diferentes departamentos de la empresa, considerando medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, la integridad y la disponibilidad de los recursos informáticos.

Público objetivo

El curso está dirigido a jóvenes universitarios, egresados, técnicos, profesionales, administradores de red y público en general que deseen conocer sobre la seguridad informática y los tipos de amenazas a las que nos podemos enfrentar, para poder defendernos de ellas.

Objetivos de aprendizaje

Objetivo general

- Promover el desarrollo de conocimientos a los participantes para la utilización de herramientas específicas para adquirir, preservar y presentar datos o evidencias de

acuerdo a la cadena de custodia que asegura que la información no sea alterada o manipulada durante la investigación.

Objetivos específicos

- Aplicar distintas técnicas de análisis forense dependiendo de la naturaleza del caso para recuperar la información.
- Estar en la capacidad de identificar la información accedida y extraída de los dispositivos para reconstruir los hechos.
- Estar en la capacidad de elaborar un informe en el que se explica la información encontrada de una forma objetiva y clara para así ayudar a entender qué ha pasado al personal no técnico, como jueces y abogados.

Duración

El curso tiene una duración de 40 horas.

Contenidos

BLOQUE 1: Cybercrimen y definiciones

1.1 Conceptos Ethical Hacking
1.2 Informática
1.3 El Cybercrimen

BLOQUE 2: Identificación de la evidencia

2.1 Identificación de Evidencia
2.2 Manejo de Evidencia
2.3 Recuperación de Información
2.4 Ruptura de contraseñas en S.O. I y II
2.5 Ruptura de contraseñas USB de BitLocker
2.6 Descifrado de contraseñas almacenadas en el Browser

BLOQUE 3: Preservación de evidencia

3.1 Cadena de Custodia
3.2 Manual de Custodia
3.3 Metadatos
3.4 Preservación de Evidencia

BLOQUE 4: Análisis de evidencia

4.1 Análisis Forense de Equipos de Computo
4.2 Análisis Forense de Dispositivos

4.3 Estudio Forense Equipos Celulares
4.4 Discos Duros
4.5 Análisis Forense de Windows
4.6 Estegranografía y Criptografía
4.7 Seguridad en 802.11

5.1 Presentación de Evidencia
5.2 El Rol del Perito en el proceso Pericial
5.3 El Perfil del Perito
5.4 Formato Informe Pericial
5.5 Ejemplo Informe
5.6 Reglamento Sistema Pericial
5.7 Defensa del Informe Pericial

Competencias previas

Conocimientos: Los participantes deben tener conocimientos básicos de Linux, Windows y de Redes IP/TCP, Tener aprobado el curso de seguridad informática y hacking ético I y II.

Habilidades o destrezas: Los participantes deben manejar herramientas ofimáticas, principalmente el internet.

Valores: Los participantes deben tener criterios éticos para aplicar estrategias necesarias para la protección de los sistemas que se encuentren amenazados.

Recursos

Los recursos que se requieren para la ejecución del curso presencial son los siguientes:

- Acceso a un equipo de computación con conexión a internet.
- Acceso al paquete Microsoft Office en sus componentes Word, Excel y power point.
- Disponer de un software para lectura de archivos PDF.
- Casos prácticos
- Block, esfero

Aspectos metodológicos

El curso presencial se desarrolla totalmente en las aulas de clase, la metodología a seguirse en este curso será sobre la base de charlas magistrales, de aprendizaje participativo que promueva el análisis de los casos relacionados con la experiencia de los participantes, en cuyo caso el profesor tendrá un rol de Facilitador.

Se analizara toda la información obtenida que será utilizada por el experto forense que gestione el caso para reconstruir los hechos en base a las pruebas recogidas y la correlación de los eventos en orden cronológico.

Se desarrollarán casos prácticos que permitan a los estudiantes poner en práctica el conocimiento teórico impartido.

El contenido del curso se pondrá a disposición de todos los participantes, para el desarrollo del proceso de capacitación.

Criterios de aprobación

- Cumplimiento de las actividades propuestas en el plazo establecido
- Participación activa en las clases
- Asistencia del 80%
- Obtención de un rendimiento mínimo de 7/10 puntos en el curso

Certificado

El participante que cumpla con los criterios de aprobación, recibirá un certificado con el aval de la Universidad de las Fuerzas Armadas – ESPE, ESPE INNOVATIVA EP y SETEC.

Perfil del Facilitador

Formación académica

Pregrado:
Ingeniería en Sistemas, Ingeniero en informática y ciencias de la computación o áreas afines

Posgrado
Magíster en tecnologías de la información.

Otros
Capacitación en áreas a fines

Experiencia relacionada
Experiencia profesional en el sector público-privado y docencia en el área de seguridad informática y forense.