UTADEO
UNIVERSIDAD DE BOGOTÁ JORGE TADEO LOZANO
EDUCACIÓN CONTINUADA

DIPLOMADO

INFORMÁTICA FORENSE

Objetivos del programa

- Identificar y comprender la naturaleza del delito informático y sus diferentes formas.
- Obtener una visión clara de la actualidad de los delitos informáticos a través de estadísticas mundiales y regionales.
- Reconocer la importancia de contar con un programa para atención de incidentes de seguridad de la información.
- Entender la metodología de atención de incidentes de seguridad de la información a través de la comprensión de cada una de las diferentes fases del proceso.
- Adquirir experiencia teórico-práctica en la adquisición, recolección, preservación y presentación de evidencia digital.
- Conocer las consideraciones legales asociadas al delito informático desde el punto de vista de la legislación colombiana.

Dirigido a

Profesionales en Ingeniería de Sistemas, Ingeniería Eléctrica o Electrónica, profesionales que estén iniciando su labor en seguridad informática, Auditores de Sistemas de Información, Jefes, Directores o Gerentes de áreas de TI y en general a todos aquellos profesionales del área de tecnología informática interesados en profundizar sus conocimientos en este tema.

Intensidad: 120 horas

Educación Continuada
Cra. 4 No 23 - 76
Módulo 29 of. 201
PBX: (+571) 242 7030
Exts.: 3956/57/58
Teléfono: 321 3571

www.utadeo.edu.co

UTADEO
UNIVERSIDAD DE BOGOTÁ JORGE TADEO LOZANO
EDUCACIÓN CONTINUADA

DIPLOMADO

INFORMÁTICA FORENSE

Módulo I. Introducción al delito informático

- El comportamiento humano en la red.
- La naturaleza del delito informático y su definición.
- Las diferentes formas del delito informático.
- Diferencias entre el delito informático y el delito tradicional.
- Clases de atacantes y su perfil psicológico
- El modelo conceptual de hacking.
- Laboratorio: Introducción al Hacking.

Módulo II. Introducción a la respuesta a incidentes de S.I.

- El modelo de referencia para la respuesta a incidentes de S.I.
- Objetivo de la repuesta a incidentes de SI.
- Preparación de la organización (Políticas, etc).
- Detección del incidente.
- Respuesta inicial.
- Formulación de la estrategia de respuesta.
- Investigación del incidente.
- Solución y reporte del incidente.

Módulo III. Introducción a la computación forense

- Premisas de las ciencias forenses.
- Principio de Intercambio de Locard.
- Dinámica de la evidencia.
- Reconstrucción del crimen.
- El método científico aplicado a las ciencias forenses.
- El modelo de referencia.
- Medios de almacenamiento.

Módulo IV. Windows Forensics

- Preparando el Sistema (Conf. Auditorias, Logs).
- Recolección de información volátil.
- Análisis de Malware.
- Recuperación y análisis de evidencia digital.
- Los sistemas de archivos FAT y NTFS.
- Windows Registry.
- Historial de Navegación.
- Metadata Análisis.
- Recuperación de archivos.
- Password Cracking.
- Interpretación de Logs.

Módulo V. Unix Forensics

- Preparando el Sistema (Conf. Auditorias, Logs).
- Recolección de información volátil.
- Recuperación y análisis de evidencia digital.
- Los sistemas de archivos EXT2 y EXT3.
- Recuperación de archivos.
- Password Cracking.
- Interpretación de Logs.

Módulo VI. Network Forensics

- Preparando el Sistema (Conf. Auditorias, Logs).
- Sistemas de Detección-Prevención de Intrusiones.
- Network AnomalyDetection.
- Recolección de información volátil.
- Recuperación y análisis de evidencia digital.
- Disección de protocolos y análisis de tráfico (Ethereal, Wireshark).
- IP tracking (Whois, DSNS Lookups, Geolocalización de IPs).

Módulo VII. Técnicas anti-forenses

- Criptografía.
- Esteganografía.
- MetaData y MAC Times spoofing.
- Borrado Seguro.
- Navegación anónima.
- Eliminando los rastros.

Módulo VIII. Consideraciones legales en Colombia

- El derecho a la intimidad, privacidad y el buen nombre Vs. el derecho a la información y a la libre expresión.
- El mensaje de datos.
- La firma electrónica y la firma digital.
- El comercio electrónico.
- El derecho a la autodeterminación informativa (Habeas Data).
- El derecho a la protección de los datos y la información.
- El derecho de autor en el mundo digital.