Investigación Digital y CiberInteligencia

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional. Sin embargo, debe destacarse que el desarrollo de las técnicas informáticas ha generado nuevas posibilidades de uso indebido de los sistemas, impulsando lo que se conoce como cibercrimen y creando la necesidad de regulación y análisis de los riesgos técnicos.

Objetivos generales

Esta capacitación tiene como objetivo brindar a los asistentes los conocimientos mínimos para comprender que, en la actualidad, la tecnología forma parte de la vida de las personas y, por lo tanto, de muchos de los delitos que ocurren. Desde homicidios hasta robos y extorsiones, pueden incluir en el hecho algún tipo de tecnología, o bien, quedar registrados en algún dispositivo cercano.

Para ello, se buscará a lo largo de los diferentes módulos, explicar la utilidad de la utilización adecuada de la tecnología, tanto como herramienta de investigación, así como objeto de investigación, introduciendo las bases de los distintos tipos de evidencia digital y su importancia.

Requisitos previos

Conocimiento básico sobre Seguridad de la Información e Investigación Digital

Público Objetivo

El curso está orientado a administradores de IT, responsables de seguridad, área de legales y cualquier persona comprometida con el análisis interno o externo de seguridad en una organización. También está orientado a personas interesadas en la investigación del cibercrimen.

Finalizado el curso, el asistente será capaz de:

- Conocer cómo funciona el cibercrimen organizado internacional
- Conocer las herramientas de ataque más utilizados por cibercriminales
- Comprender las metodologías para realizar Investigación Digital e Inteligencia en Internet
- Conocer el aspecto procesal penal y su importancia para la investigación de los delitos informáticos

Este curso complementa los cursos **"Aspectos Legales de las Tecnologías de la Información en el marco de la Seguridad de la información"** y **"Investigación y protección contra el malware y el cibercrimen"** dictados por **Segu-Info.**

Material a entregar

Presentaciones utilizadas durante el curso y certificado de asistencia y aprobación, ambos en formato digital.

Duración y Modalidad

Este curso teórico/práctico tiene una duración de **32 horas** y la modalidad de cursada es presencial. También puede ser desarrollado ***in-company***.

Instructores

Cristian Borghello es Licenciado en Sistemas (UTN), desarrollador, Certified Information Systems Security Professional (CISSP), Certificate of Cloud Security Knowledge (CCSK), Microsoft MVP (Most Valuable Professional) Security.

Actualmente es Director de **Segu-Info**, **Segu-Kids** y Cofundador de **ODILA**. Se desempeña como consultor independiente en Seguridad de la Información.

Ha trabajado en la investigación de malware durante más de 20 años y escribe para diversos medios especializados e investiga en forma independiente sobre Seguridad Informática y de la Información.

Ha brindado cursos y dictado congresos y seminarios nacionales e internacionales sobre la temática.

Marcelo Temperini es Abogado especialista en Derecho Informático. Doctorando CONICET dedicado a la investigación de Delitos Informáticos y Cibercrimen en el Centro de Investigación de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral.

Socio Fundador de **AsegurarTe** y Cofundador de **ODILA**.

Expositor y conferencista en numerosas Jornadas, Congresos y Eventos relacionados al Derecho y la Seguridad de la Información, nacionales e internacionales.

Maximiliano Macedo es Analista en Informática Aplicada egresado de la Facultad de Ingeniería y Ciencias Hídricas de la Universidad Nacional del Litoral, especializado en Seguridad de la Información.

Docente de las cátedras de Tecnología de la Información para cursos de nivel primario y secundario.

Es Socio Fundador de **AsegurarTe**, Creador y Desarrollador del Proyecto "Botón de Pánico AsT" y Cofundador de **ODILA**.

Expositor y conferencista en Jornadas, Congresos y Eventos relacionados a la Seguridad de la Información.

Ramiro Caire es Analista en Seguridad Informática. Actualmente se desempeña en la Central de Análisis del Ministerio de Seguridad del Gobierno de la Provincia de Santa Fe.

Es Pentester e instructor en Ethical Hacking. Autor de MKBRUTUS (Herramienta de auditoría de dispositivos corriendo RouterOS) y ha realizado múltiples investigaciones sobre seguridad de la información.

Especializaciones relacionado al Hacking, Malware Research, OSINT *(Open Source Intelligence)*, Cibercrimen, Ciberdefensa y nuevas tecnologías.

Fundador y Organizador de **RiseCON** (Rosario Information Security Conference).

Temario

Módulo 1: Tecnología y Delitos

- Conceptos básicos. Internet y Redes de información
- Proveedores de Internet y Dirección IP
- Seguridad de la Información / Seguridad Informática
- Confidencialidad. Integridad. Disponibilidad
- Medidas de seguridad básicas
- Seguridad en dispositivos móviles
- Delitos Informáticos y Cibercrimen
- Estafas electrónicas. Tipos de estafas más realizados
- Hacking y Cracking. Hacking ético y su debate
- Phishing y captación ilegítima de datos confidenciales
- Ingeniería Social. El arte del engaño
- Suplantación de Identidad. Perfiles Falsos
- Cibercrimen organizado. Evolución
- CaaS (Crime as a Service) y HaaS (Hacking as a Service)
- Monedas Virtuales: Criptomonedas. Bitcoins, Litecoins
- Privacidad y anonimato. Privacidad vs. Seguridad
- Desafíos pendientes en la investigación del cibercrimen

Módulo 2: Aspectos Legales de los Delitos Informáticos

- Delitos Informáticos. Conceptos y evolución
- Bien jurídico afectado. Diferentes posturas
- Características: Alcance. Anonimato. Masividad. Fronteras
- Estadísticas. Cifra blanca y cifra negra
- Legislación vigente en Argentina. Ley Nº 26.388. Evolución
- Distribución o Comercialización de Pornografía Infantil
- Acceso indebido a las comunicaciones. Hacking como delito
- La punición del hacking y sus diferentes posturas en el mundo
- Acceso indebido a bases de Datos Personales
- Difusión de comunicaciones electrónicas
- Fraudes Electrónicos. Phishing. El problema de su tipificación
- Proyectos en Argentina. La captura ilegítima de datos confidenciales
- Cracking. Daños informático y difusión de malware
- El colectivo Anonymous y el hacktivismo
- Corrupción de menores, grooming y su tipificación penal. Ley Nº 26.904
- Delitos Informáticos en Latinoamérica. Derecho Comparado
- Mapa de los Delitos Informáticos
- ODILA: El Mapa de los Delitos Informáticos en Latinoamérica
- Convenio de Cibercriminalidad de Budapest
- Aspectos de procesal penal y su importancia para la investigación de los delitos informáticos

Módulo 3: Ciber-inteligencia

- Introducción a la Inteligencia y Ciber-Inteligencia
- Open Source Intelligence (OSINT). La utilidad para la recolección de evidencia
- Motores de búsqueda y herramientas de análisis
- Buscadores. Metabuscadores.
- Buscadores reversos de imágenes y usuarios
- Construcción de búsquedas inteligentes de información.
- Seguridad en la realización de búsquedas
- Validación y certeza. Métodos y procedimientos
- Metadatos. Análisis y procesamientos
- Herramientas para el análisis automatizado de metadatos
- Operadores para la búsqueda avanzada de información
- WHOIS e ingeniería reversa de IPs
- Inteligencia de redes sociales
- Ciber-patrullajes. Experiencias en otros países. Legislación
- Realización de informes
- Aspectos de confidencialidad. Divulgación

Módulo 4: Deep Web

- Internet profunda (Deep Web). Conceptos y Funcionamiento
- Deep Web vs Dark Web
- Dark Markets. Otras redes anónimas
- Utilización de software específico. Browser, email, conexiones y chat anónimos
- Navegación. TOR Browser. Atlas. Bridges. Orfox
- Mails en Deep Web. Mail2Tor. Tormail
- Proxy en TOR. Orbot
- Chat Seguro. Chat-Secure, Gibberbot
- Criptomonedas: Bitcoins. Utilización. Mercado. Compra y Venta
- El funcionamiento de las chains y su potencial. Trackeo
- Ransomware: Funcionamiento. Asistencia a la víctima. Negociación. Investigación
- Métodos y herramientas de búsqueda en la internet profunda

Módulo 5: Investigaciones Digitales

- Introducción a las investigaciones digitales
- Direcciones IP y Proveedores de Internet
- Datos de tráfico y datos de contenido. Regulación legal
- Investigación de casos a partir de una dirección IP
- Investigaciones digitales en Facebook
- Funcionamiento y lógica de red.
- Términos y Condiciones Legales
- La privacidad y sus consecuencias en la evidencia
- Sistema de Seguridad
- Perfiles Falsos. Identificación. Estrategia
- Identificación de perfiles. Facebook Graph

- Informes de Facebook. Detectar sesiones abiertas. Alertas de ingreso
- Recuperación de cuentas hackeadas. Aspectos de Seguridad
- Denuncias (tipos de denuncias). Formulario. Reportes automáticos
- Facebook records. Plataforma para fuerzas de la ley. Pedidos
- Experiencias en casos reales sobre Facebook
- Investigación Digital en Twitter
- Funcionamiento y lógica de red
- Términos y Condiciones Legales
- Problemas de "alias"
- Denuncias (tipos de denuncias)
- Casos de Pornografía Infantil. Cómo denunciar. Tipos de denuncia
- Experiencias en casos reales sobre Twitter
- Investigación de sitios web
- Datos de registro del dominio
- Datos de cache de Google
- Historia de la página
- Investigación de correos electrónicos
- Código fuente de un correo electrónico
- Posibilidad de identificación de origen
- Spoofing y otras técnicas
- Investigación sobre servicios de Mensajería
- Whatsapp. Telegram. Signal
- Cifrado. Acceso a comunicaciones privadas
- Inteligencia sobre redes sociales

Módulo 6: Evidencia Digital

- La evidencia en el proceso judicial
- La evidencia digital. Características
- Normal procesales penales. El principio de libertad probatoria
- Evidencia en la información, en los dispositivos y en la nube. El desafío en el acceso transfronterizo de datos
- Alterabilidad y volatilidad de la evidencia digital
- Adquisición de la prueba. Copias y autenticidad
- El Hash y su importancia en la autenticidad de la evidencia
- La información detrás de la información. Metadatos
- Identificación de la información
- Tips prácticos para el momento del allanamiento
- Recolección y resguardo de la información. Aspectos legales
- Cadena de custodia. Modalidades y requisitos
- Puntos de pericia. La importancia de su redacción
- La función del perito. El dictamen pericial y sus límites. Delito Penal
- Protocolos existentes en Argentina y buenas prácticas internacionales
- RFC 3227. Directrices para la recolección de evidencias y su almacenamiento
- Identificación y resguardo de contenidos en la nube. Volatilidad
- Posibles problemas y errores

- La defensa y las posibles impugnaciones
- Requerimientos judiciales vs. aspectos prácticos

Módulo 7: Práctica: Casos y Ejercicios

- Práctica de caso real incluyendo:
- Recepción de la denuncia
- Formulación de preguntas
- Búsqueda de información utilizando técnicas de OSINT
- Investigación digital en Facebook
- Operaciones con Google Hacking
- Análisis de Metadatos
- Generación de informe parcial
- Redacción de pedidos a ISP
- Identificación de dispositivos sospechosos
- Proceso de allanamiento
- Actas de Recolección
- Cadena de custodia
- Redacción de puntos de pericia
- Generación informe final
- Juego de Roles
- Acusación
- Presentación de evidencia
- Impugnación de la defensa

Experiencias y casos

- Injurias y calumnias
- Suplantación de identidad
- Acosos. Amenazas. Extorsiones
- Estafas electrónicas
- Hacking y espionaje
- Grooming y pornografía infantil
- Suplantación de identidad
- Pornografía Infantil
- Mails anónimos con amenazas

Secuestros y allanamientos

- Formas de secuestro de dispositivos digitales
- Distintas situaciones y equipos. Modalidades