Control de delitos informáticos

Presentación

El proyecto de Educación Continua en Delitos Informáticos está dirigido a profesionales no técnicos principalmente de carreras del Área de Ciencias Jurídicas, y responde a la creciente necesidad de entender como los principales ataques a personas e infraestructuras, se enlazan con los artículos del COIP-2014 de la República del Ecuador.

Delitos Informáticos será abordado desde la perspectiva de un especialista en Seguridad de la Información, con el mismo se presentarán conceptos y casos de ejemplos prácticos y eventos que han sido noticia en nuestro país, enfocados a los delitos en los cuales se usa como herramienta o es medio de cometimiento un equipo informático.

Finalmente se hablará del Análisis Forense Digital, como se mantiene y las mejores prácticas internacionales para la recolección y manejo de evidencia.

Objetivos

- Realizar una actualización y generar nuevos entornos de aprendizaje entorno a los delitos informáticos.
- Apoyar a los asistentes en el entendimiento de los delitos informáticos.

Dirigido a

El proyecto está enfocado principalmente a Abogados, pero al no tratar temas desde un enfoque técnico, y al explicar la terminología, se puede realizar la apertura a personas interesadas en conocer sobre el tema.

UTPL Centro de Educación Continua

UTPL Centro de Educación Continua

Requisitos de ingreso

Nociones básicas de informática, y equipamiento informático.

Perfil de salida

La persona que apruebe el curso tendrá las aptitudes para aplicar y promover la aplicación adecuada de la norma Ecuatoriana respecto a delitos informáticos o en incidentes, generá un mayor entendimiento de las noticias en los medios de comunicación nacionales e internacionales brindándole la capacidad de discernir entre los términos asociados a los eventos, basado en estándares nacionales e internacionales y aspectos éticos-legales que rigen a los Delitos Informáticos.

Modalidad de estudio

El curso se desarrollará bajo la modalidad de estudios:

x	Semipresencial
	Presencial
	Online

Estructura de contenidos

La estructura a desarrollar es la que se presenta a continuación:

1. Definiciones.

- ¿Qué es delito?
- ¿Qué es Información?
- ¿Qué es delito informático?
- ¿Qué es Información Confidencial?
- ¿Qué es Información Electrónica?
- ¿Qué es información privilegiada?
- ¿Qué es Sistema de Información?
- ¿Qué es medio Telemático?
- ¿Qué es Criptografía?

2. Características de los delitos informáticos.

- Son difíciles de demostrar.
- No se requiere de presencia física.
- Se pueden ocultar por largos períodos de tiempo.
- Evolucionan con rapidez
- Solo personas con conocimientos técnicos los pueden ejecutar.
- Es necesario eliminar el mayor número posible de incertidumbres para obtener el mayor grado de certeza.

3. Delitos informáticos más comunes.

- Accesos no autorizados.
  - Fallos y vulnerabilidades.
  - Art. 178.- Violación a la intimidad.
  - Art. 190.- Apropiación fraudulenta por medios electrónicos.
  - Art. 211.-Supresión, alteración o suposición de la identidad y estado civil.
  - Art. 212.- Suplantación de identidad.
  - Art. 231.- Transferencia electrónica de activo patrimonial.
  - Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.
- Pornografía.
- Pornografía Infantil.
  - Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.
- Estafas.
  - Correos Nigerianos, Loterías, Actualización de información Bancaria, Phishing
  - Art. 190.- Apropiación fraudulenta por medios electrónicos.
  - Art. 211.-Supresión, alteración o suposición de la identidad y estado civil
  - Art. 212.- Suplantación de identidad
- Secuestro.
  - Ransomware
  - Art. 212.- Suplantación de identidad
- Robo de Identidad.
  - Escucha de redes, Phishing.
  - Art. 178.- Violación a la intimidad
  - Art. 211.-Supresión, alteración o suposición de la identidad y estado civil
- Robo de Información.
  - Art. 190.- Apropiación fraudulenta por medios electrónicos.
  - Art. 229.- Revelación ilegal de base de datos.-
  - Art. 230.- Interceptación ilegal de datos.-
- Código malicioso.
  - Virus, malware, vulneravilidades.
  - Art. 231.- Transferencia electrónica de activo patrimonial
  - Art. 232.- Ataque a la integridad de sistemas informáticos
- Interrupción del Servicio.
  - DDO, DDOs
  - Art. 232.- Ataque a la integridad de sistemas informáticos
  - Art. 233.- Delitos contra la información pública reservada legalmente
- Utilización no autorizada de servicios.
  - Actividades propias, hacktivismo, botnets.
  - Art. 233.- Delitos contra la información pública reservada legalmente

4. Casos más relevantes en el Ecuador.

- 3.106 cupos sin sorteo dio el Ministerio, revela auditoría.
- Robo electrónico.
- Cibercrimen usa imagen de un banco ecuatoriano para perpetrar robos.
- Cuenta de Twitter del SRI fue hackeada.
- El 63% de delitos cometidos en la Internet tiene una sanción penal.
- El hackeo de autos y los peligros de la “Internet de las cosas”.
- Firma Hacking Team fue contactada por Estado ecuatoriano.
- Gabriela Rivadeneira, molesta por hackeo de su cuenta.
- Hasta 7 años de cárcel para quienes inscribieron títulos falsos.
- La Fiscalía investiga cómo fueron inscritos 366 títulos superiores.
- Los servicios de ‘hacker’ y espionaje se ofertan sin restricción en la web.

5. Principales conceptos del análisis forense informático.

- El principio de Locard.
- Evidencia Digital.
- Recolección y manejo de evidencia.
  - Orden de recolección.
  - Datos físicos de los ordenadores.
  - Actualizaciones de Seguridad.
  - Procesos, puertos y servicios.
  - DLLs y verificación de firmas.
  - Tipos de copias.
  - Validador de la integridad.
  - La cadena de custodia.

Evaluación

Las herramientas de evaluación consideradas son:

Trabajo a distancia	30%
Examen presencial	70%

En caso de que los participantes no alcancen la nota mínima (70%), podrán rendir una evaluación de recuperación, al final del curso.

Certificación y aprobación

Este curso tiene una duración de 40 horas académicas, distribuidas en 20 horas presenciales, 12 horas virtuales y 8 horas de trabajo autónomo del participante.

La aprobación se realiza con el 70% como mínimo de la nota total. Al finalizar el curso se entregará un Certificado aprobatorio en **Control de delitos Informáticos**, avalado por la Universidad Técnica Particular de Loja (UTPL).

Cuerpo de instructores

El centro de Educación Continua de la UTPL, cuenta con instructores de gran experiencia en su área del conocimiento, tanto a nivel profesional como de enseñanza a nivel superior.

La asignación de docentes a cada ciudad es potestad exclusiva de la UTPL

Jorge Guerrón

- Máster Universitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones.
- Ingeniero en sistemas. Especialista en Seguridad de Bases de Datos y Aplicaciones Web.
- Diplomado en Gobierno de TI, Auditoría y Seguridad de los Sistemas de Información, Centro de Innovación Tecnológica Fundación Libertad.
- Auditor Interno en Sistemas de Gestión de la Seguridad de la Información UNE-ISO/IEC 27001:2005.

Diseño: Ediloja Cía. Ltda. - Loja-Ecuador
Imagen de portada: Shutterstock