International Telecommunication Union

Curso en línea

CIBERCRIMEN Y EVIDENCIA DIGITAL

Del 30 agosto al 19 setiembre

INFORMACIÓN GENERAL DEL CURSO

DESCRIPCIÓN DEL CURSO

Título	**CIBERCRIMEN Y EVIDENCIA DIGITAL**
Objetivo	El objetivo general de este curso es dar a conocer el concepto, tipos y actividades del cibercrimen, brindando una introducción al proceso de investigación forense de evidencias digitales como respuesta contra el cibercrimen.
Duración	30 horas
Costo de formación	**Ninguno**
Código del curso	21OI27698AMS-S

DESCRIPCIÓN DEL CURSO

Cuando se nos describe una escena del crimen, estamos acostumbrados a pensar en programas policiales o noticias donde contamos con la policía, investigadores y una escena del crimen con evidencia alrededor. Con el avance de la tecnología, la escena del crimen cambia, siendo lugares tangibles reemplazados por computadores, memorias, cámaras de seguridad, entre otros. Actualmente, ataques y robos informáticos, información personal o confidencial filtrada al público, o grabaciones desde dispositivos se vuelven material de interés para investigadores a la hora de descubrir qué y cómo sucedieron los hechos.

La investigación forense digital sigue los procedimientos de investigación vistos en otras disciplinas, pero usa los conocimientos de las ciencias de la computación para realizar las acciones de análisis sobre los equipos. De este modo, información que parecería abstracta y oculta en bits de 1's y 0's adquiere sentido para el investigador descubriendo así archivos, correos, imágenes, videos, registros y otros elementos que terminan siendo decisivos en procesos judiciales. Los investigadores especialistas en diferentes campos (sistemas operativos, equipos móviles, conexiones de red, y otros), trabajando en equipo, podrán llegar a la verdad.

En este curso, se brindará un panorama general del cibercrimen y la evidencia digital, enfocándose en el procedimiento de investigación y viendo más a detalle un caso práctico.

RESULTADOS DEL APRENDIZAJE

Al finalizar el curso el estudiante tendrá toda la información pertinente a los aspectos teóricos que enmarcan el mundo del cibercrimen y el análisis forense digital, además adquirirá habilidades técnicas a través de la interacción con los demás participantes y con los laboratorios que se realizarán a lo largo del curso.

A QUIÉN VA DIRIGIDO

Profesionales en tecnologías de la información, administradores de seguridad de la información, abogados, auditores, ingenieros, personal policial, ministerio público y cualquier interesado en el cibercrimen y la investigaciones forense digital.

REQUISITOS DE ADMISIÓN

Se recomienda poseer conocimiento de informática básica.

TUTORES / INSTRUCTORES

Nombre del Tutor / Instructor	Información de Contacto
Eduardo M. Rodriguez Ávila	**eduardo.rodriguez@ieee.org**
Especialista en telecomunicaciones y tecnologías de la información - ISO/IEC 27032 Senior Lead Cybersecurity Manager. - ISO/IEC 27001 Lead Implementer - Information Security Management System - ISO/IEC 27001 Lead Auditor - Information Security Management System - ISO/IEC 20000 Lead Auditor - Service Management System - Information Security Course certificado por el Ministery of Science, ICT and Future Planning, República de Corea del Sur. - Diploma en IT Management certificado por el centre for development of advanced computing C-DAC, India - Diplomado en auditoría y seguridad de tecnologías de la información, UNMSM, Perú.	

CONTENIDO DEL CURSO

Semana I

Módulo 1: Cibercrimen

… Subtema 1: Introducción
… Subtema 2: Ciberseguridad
… Subtema 3: Ciberdelincuencia
… Subtema 4: Ciberterrorismo

Módulo 2: Combatiendo el cibercrimen

… Subtema 1: Marco legal y respuesta internacional
… Subtema 2: Convenio sobre la Ciberdelincuencia de Budapest
… Subtema 3: Actividades de la Unión Internacional de Telecomunicaciones
… Subtema 4: Situación actual del cibercrimen

Semana II

Módulo 3: Investigación forense

… Subtema 1: Nociones generales de investigación forense en medios digitales.
… Subtema 2: Roles y personas involucradas en la investigación.
… Subtema 3: Tipos de investigación (civil, criminal y corporativa).
… Subtema 4: Definición del proceso y etapas en la investigación.

Módulo 4: Evidencia digital

… Subtema 1: Definición de evidencia en medios digitales.
… Subtema 2: Principios a seguir sobre el manejo de evidencia.
… Subtema 3: Propiedad y embargo de medios informáticos a investigar.
… Subtema 4: Tipos de evidencia.

Semana III

Módulo 5: Descubrimiento y análisis de evidencia.

… Subtema 1: Planificación de la búsqueda.
… Subtema 2: Cadena de custodia.
… Subtema 3: Manejo de escena del crimen.
… Subtema 4: Red de comunicación y otros elementos a considerar en escenarios digitales.
… Subtema 5: Lineamientos para la adquisición de evidencia.

Módulo 6: Información y evidencia en entornos digitales

… Subtema 1: Sistema de archivo en discos duros.
… Subtema 2: Bits y valores a considerar en análisis de archivos.
… Subtema 3: Manejo de archivos eliminados en discos duros.
… Subtema 4: Metadata en archivos.
… Subtema 5: Registro del sistema.
… Subtema 6: Métodos de reportar los hallazgos.

CRONOGRAMA DEL CURSO

Semana / Sesión	Tema	Ejercicios e interacciones
Semana 1	Cibercrimen	Desarrollar Retos: • Describir ejemplos de cibercrimen suscitados en su país • Investigar el marco legal nacional • Proponer estrategias para combatir la cibercriminalidad en su país
Semana 2	Investigación forense y evidencia digital	Desarrollar Retos: • Brindar un ejemplo en el que la investigación no puede realizarse con una copia forense necesariamente. • Explicar qué significa HASH y cómo ayuda a distinguir que dos elementos digitales son iguales • Plantear posibles ejemplos de evidencia(s) circunstancial(es) en medios digitales.

Semana 3	Descubrimiento y análisis de evidencia. Información y evidencia en entornos digitales	Desarrollar Retos: • Investigar un ejemplo de Memory Capture Tool (usado para capturar lo que se encuentra en la memoria RAM) y cómo es usado sin modificar el equipo. • Determinar si es posible analizar conexiones bluetooth y cómo. • Descargar una imagen y analizarla con un visualizador de data. Reportar que información sobre la imagen brinda el visualizador. • Analizar dos reportes digitales forenses.

METODOLOGIA

El presente curso es en línea/asincrónico. La metodología que orienta este curso será eminentemente participativa. La estrategia metodológica utilizada para el desarrollo de curso propone al participante una diversidad de actividades.

Se espera que cada estudiante participe mediante la lectura del material que estará disponible desde el inicio del curso, aportes escritos a los debates, foros, actividades, ejercicios de refuerzo y exámenes que serán definidos y los cuales serán realizadas en forma asincrónica. Esta técnica asegurará la flexibilidad de tiempo necesaria para que cada participante pueda organizarse de la manera que mejor le convenga.

Los participantes aprobados en el curso según los criterios de evaluación que sean indicados por los tutores y todos aquellos que sean aprobados recibirán un Certificado que será emitido por vía electrónica

EVALUACIÓN Y CALIFICACIÓN

El curso propone un sistema de evaluación combinado el cual se compone de: foros de debate, actividades y evaluaciones. Las fechas de cada uno de estos ítems están definidas en el cronograma. El sistema de calificación de este curso se explica a continuación junto con los porcentajes de peso de cada una de las actividades a evaluar.

Pesos de evaluación

- Foro de debate (20%): Tendrán un peso del 20% sobre la calificación final. Se realizará 1u 2 foros de debate en el curso. Cada estudiante deberá participar un mínimo de dos veces en el foro con aportes de valor para obtener el 100% del porcentaje semanalmente. En caso de participar una vez obtendrá en 50% y en caso de no participar será un 0%.
- Actividades (60%): también denominados retos, actividades, laboratorios u trabajos individuales tendrán un peso total del 60% y estarán compuestas de algunas de estas opciones: desarrollo de trabajos individuales, retos trabajos grupales, actividades con entrega en la plataforma.
- Evaluaciones (20%): Las evaluaciones del presente curso tendrán un peso total del 20% y podrán efectuarse mediante dos exámenes en línea, El esquema para este curso está indicado en el cronograma de actividades.
- Aprobación: Para aprobar este curso se debe completar un acumulado de mínimo 60%.

COORDINACION DEL CURSO

Coordinación Académica	Coordinador UIT
Eduardo M. Rodriguez Ávila	Rodrigo Robles Oficina Regional de la UIT para las Américas rodrigo.robles@itu.int

REGISTRO

Creación de la cuenta en ITU Academy

El proceso de inscripción debe ser realizado en línea a través del Portal ITU Academy. Para registrarse en el curso es **NECESARIO**, primero, crear una cuenta en la plataforma en el siguiente enlace.

Inscripción en el curso

Una vez creada la cuenta nueva, ya se puede realizar la inscripción para el curso en línea en el siguiente enlace https://academy.itu.int/training-courses/full-catalogue/cibercrimen-y-evidencia-digital

También es posible registrarse en el curso deseado por medio de nuestro catálogo de cursos.