udima
UNIVERSIDAD A DISTANCIA DE MADRID

Telf. 91 856 16 99

Curso de verano: Cibercriminología y Ciberseguridad: la última frontera II

Presentación

Los cursos de verano de la Universidad de Verano-UDIMA se configuran como una oferta académica diferente y atractiva para el periodo estival. Versan sobre diferentes temas de actualidad en el campo de las ciencias sociales, las ciencias jurídicas, la educación, la economía, el marketing o el turismo. Estos cursos tienen el formato on-line

Presentación del curso

Este curso pretende conocer desde un prisma multidisciplinar el cibercrimen y su respuesta desde la ciberseguridad. De esta manera se parte de la premisa básica de que no es posible una intervención adecuada sin unos conocimientos técnicos, criminológicos y legales adecuados. Por ese motivo, en esta formación se ahondará en el conocimiento de las tipologías ciberdelictivas, el comportamiento de los cibercriminales, las explicaciones para su prevención, la regulación legal y el ámbito más técnico forense y de investigación tecnológica, ciberinteligencia, así como de ciberprotección empresarial. Este curso pretende profundizar en estos aspectos a partir de la edición del año pasado, aunque quien no lo haya cursado también puede "engancharse" a esta nueva edición.

Dirigido a

Profesionales del mundo de la seguridad privada (directores de seguridad, jefes de seguridad y responsables), profesionales de las Fuerzas y Cuerpos de Seguridad, profesionales del ámbito de la criminología y de la ciberseguridad, así como, estudiantes de Ingenierías, Criminología, Derecho, Psicología, Sociología, o cualquier rama de las ciencias del comportamiento y técnicas que estén interesados en el ámbito de la ciberseguridad. Y a todos aquellos que quieran acercarse al mundo de la cibercriminología y la ciberseguridad.

Objetivos

Dotar de los conocimientos básicos en cibercriminología (oportunidad criminal, tipologías ciberdelictivas, perfil de ciberdelincuentes y cibervíctimas) y explorar la relación entre la teoría criminológica y su aplicación al ámbito de la ciberseguridad (prevención situacional en el ciberespacio).

Conocer los riesgos del uso de datos y comprender la normativa y obligaciones que conllevan.

Explorar la regulación de los ciberdelitos y las especialidades de la prueba tecnológica.

Obtener y explorar inteligencia por medio del análisis de datos disponibles en el Espacio Red.

Acercar a una perspectiva real de las técnicas evolutivas del cibercrimen, y, en concreto, establecer metodologías preventivas de la lucha contra el cibercrimen.

Informar de la realidad de la ciberdelincuencia en las instalaciones civiles y realizar prospectiva de vulnerabilidades de las mismas.

Programa

Unidad 1. Cibercriminología

Teoría criminológica aplicada a la ciberseguridad
El factor humano aplicado a la ciberseguridad
Cibercriminales técnicos
Cibercrimen económico
Capacidades de defensa, especial atención al ciberterrorismo
Prevención primaria, secundaria y terciaria

Unidad 2. Ciberderecho (Legalidad en el entorno de las ciberinvestigaciones)

Licitud de la obtención de las evidencias digitales.
Prueba indiciaria tecnológica y características cuando es aportada por particular.
Autenticidad, integridad y cadena de custodia de las pruebas electrónicas.
El papel del perito informático en el proceso judicial.

Unidad 3. Ciberinteligencia

Inteligencia en fuentes abiertas
Metodología de trabajo
Casos prácticos y elaboración de informes

Unidad 4. Ransomware: "nunca secuestrar fue tan fácil"

¿Qué es Ransomware
Seguimos explicando: Tipos de Ransomware
¿Puedo hacerme mi propio Ransomware?
¿No sé programar? ¿Cómo puedo conseguirlo?
Campañas de Ransomware, dónde, cómo y a quién.
¿Podemos luchar contra esto?
Conclusiones

Unidad 5. La ciberseguridad empresarial como agente de protección de la información

La realidad de la ciberseguridad en instalaciones civiles hoy día
La protección de la información como objetivo de la ciberseguridad
La colaboración entre la dirección de seguridad y las TIC como elemento de rotección
Herramientas para la prospección de vulnerabilidades

Director-es

Dr. Abel González García. Universidad a Distancia de Madrid (UDIMA).

Equipo docente

D. Abel González García. Universidad a Distancia de Madrid (UDIMA). Director del Departamento de Criminología de UDIMA, Doctor en Criminología, última publicación más relevante en este ámbito: "Blanqueo de capitales y su relación con la cibercriminalidad" (coordinador) (2019), líneas de investigación: cibercriminología, prevención y tratamiento de la delincuencia, policing en el ciberespacio.

D. Juan Luis Rubio Sánchez. Universidad a Distancia de Madrid (UDIMA). Vicerrector de relaciones Universidad-Empresa. Doctor en Ingeniería Industrial. Líneas de investigación: sistemas empresariales y ciberseguridad, automatización de proyectos y gestión industrial.

D. Pablo Luis Gómez Sierra. Graduado en Criminología (UDIMA). Máster Universitario en Dirección de Proyectos Informáticos (UAH) y Especialista Universitario en Tecnologías de la Seguridad de la Información e Investigación Digital (UAH).

D. Ramón Fuentes Requena. Graduado en Criminologia por UDIMA y Profesional de las FCSE con más de 20 años de experiencia en Nuevas Tecnologías. A lo largo de su carrera profesional ha desempeñado trabajo operativo en áreas de Ciberinteligencia y Ciberseguridad en el ámbito público, así como investigación de delitos tecnológicos. Ponente habitual sobre Ciberseguridad y Nuevas Tecnologías para FCSE y ONUDC. Profesor en materia de "Hacking y Malware" a nivel Máster.

D. Juan Carlos Fernández. Abogado CEO & Founder de TECNOGADOS. Despacho especialista en asuntos digitales. Compatibiliza el ejercicio de la abogacía como profesor del Máster de Ciberseguridad de la Universidad de CLM, curso de peritos informáticos en el Colegio de Ingenieros de Madrid y en las Escuelas de Organización Industrial y de Seguridad de CLM. Ponente en los principales Congresos de Seguridad Informática, así como en universidades y Colegio de Abogados de Madrid.

Sistema de enseñanza y metodología de estudio

Al matricularse en el curso el estudiante tendrá acceso a un aula virtual a lo largo de 2 semanas. Durante la primera de ellas, en la que se celebrarán las conferencias y/o clases magistrales, se dispondrá de todo el material didáctico (incluidas las grabaciones de las conferencias/clases), así como de las orientaciones necesarias para la realización del curso. El estudiante tendrá 2 semanas para realizar las actividades académicas, tras lo cual, el curso se cerrará. Aquellos estudiantes, matriculados y que hayan realizado las actividades previstas, con la valoración de Apto, recibirán un diploma acreditativo del curso, así como 2 créditos ECTS**(*)**.

(*) Los estudiantes de la UDIMA pueden acumular hasta 6 créditos y solicitar el reconocimiento de los mismos siempre y cuando estén asociados a la tipología optativa de su plan de estudios de Grado (no aplicable a la optatividad de mención).

Material didáctico

El curso se desarrollará con el material disponible on-line en el aula virtual (grabaciones de conferencias, documentos gráficos, textos...).

udima
UNIVERSIDAD A DISTANCIA
DE MADRID

Telf. 91 856 16 99