DIPLOMA DE ESPECIALIZACIÓN EN CIBERDEFENSA Y PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Conocimientos de acceso:

LAS MISMAS QUE EL MASTER PRIMERA EDICION

Conocimientos previos necesarios:

ninguno
Se requiere titulación universitaria. Excepcionalmente se puede considerar por la Dirección el acceso a profesionales sin titulación universitaria que tengan una experiencia demostrada de más de tres años en un ámbito relacionado con el programa y acrediten requisitos legales para cursar estudios universitarios. Los alumnos matriculados en estas condiciones sólo podrán obtener un certificado de Aprovechamiento por los estudios superados pero no podrán optar a la obtención del Título Propio de postgrado.

Acción formativa dirigida a:

Profesionales del mundo de las telecomunicaciones, informáticas o carreras afines.

Temas a desarrollar:

Módulo 1. Detección y defensa frente a ciberamenazas (50 horas)
Estados y servicios. Actores APT. Atribución de amenazas. Arquitectura de la amenaza. Ciclo de vida de la amenaza. Detección del compromiso. Adquisición de datos. Detección de usos indebidos. Detección de anomalías. Monitorización de seguridad. Análisis de riesgos.
Módulo 2. Gestión de ciberincidentes (50 horas)
Ciclo de vida de la gestión de incidentes. Capacidad de gestión de incidentes. Detección de intrusiones. Respuesta. Lecciones aprendidas.
Módulo 3. Análisis de inteligencia (50 horas)
Inteligencia Técnica (TECHINT): Análisis forense, análisis de malware, ingeniería inversa. Inteligencia de fuentes abiertas (OSINT): fuentes abiertas en internet, vigilancia digital, medición de riesgo. Inteligencia de fuentes humanas (HUMINT): information sharing, grupos de interés. Técnicas de análisis de inteligencia: Big Data, correlación, herramientas.
Módulo 4. Ciberdefensa (50 horas)
Operaciones en el ciberespacio. Sistemas de información para mando y control. Cyber Situational Awreness (CySA). Hybrid Situational Awrareness (HySA). Visualización. Aspectos legales de la ciberdefensa.Experimentación y entrenamiento: Cyber Ranges.
Módulo 5. Protección de infraestructuras críticas (50 horas)
Tipos de ataque a infraestructuras críticas. Medios de defensa. Medios de detección. Medios de respuesta. Estudio de casos.

Otra Información de interés:

La Universidad Politécnica de Valencia, a través de este Master, está autorizada como centro certificador para la realización de los exámenes correspondientes a las certificaciones oficiales de Cisco así como de Palo Alto.
La Universidad Politécnica de Valencia ha recibido el Premio Cisco al Mejor Centro de Formación.
Prácticamente todos los años, existe una importante demanda de empleo de especialistas de este Máster en Empresas Privadas, tanto de los principales proveedores de servicios de telecomunicaciones e informática, como de sus empresas subcontratadas.(entorno de Telefónica). También contactan con este máster empresas subcontratadas con el Centro de seguimiento de Satélites

Condiciones generales

La acción formativa cumple las siguientes condiciones generales: http://www.cfp.upv.es/cond_gen?5

Condiciones específicas	
LAS MISMAS QUE EL MASTER PRIMERA EDICION	
Organizadores:	
Responsable de actividad	MANUEL ESTEVE DOMINGO
Coordinador	BELÉN REQUENA SÁNCHEZ
Datos básicos:	
Dirección web	www.cfp.upv.es
Correo electrónico	brequena@upvnet.upv.es
Tipo de curso	DIPLOMA DE ESPECIALIZACION
Estado	ANULADO
Duración en horas	300 horas presenciales
Créditos ECTS	30
Información técnica docente	Belén Requena Sánchez Tecnico Medio UNIVERSIDAD POLITÉCNICA DE VALENCIA ETSI TELECOMUNICACIONES Departamento de Comunicaciones Camino de Vera s/nº VALENCIA
Dónde y Cuándo:	
Dónde	VALÈNCIA
Horario	TARDE
Observaciones al horario	Lunes, martes, miércoles y jueves: Tarde
Lugar de impartición	UNIVERSIDAD POLITECNICA DE VALENCIA EDIFICIO NEXUS 6-G AULA 2-6 CFP "Centro de Formación Permanente"
Fecha Inicio	15/01/18
Fecha Fin	31/07/18 La fecha límite para entrega de trabajos, realización de prácticas y otras actividades no lectivas será el 31/07/19
Datos de matriculación:	
Matrícula desde	26/09/17
Inicio de preinscripcion	29/06/17
Mínimo de alumnos	12
Máximo de alumnos	22
Precio	2.900,00 euros
Observaciones al precio	2.900€ (en 2 plazos) Público en general 2.400€ (en 2 plazos) Alumno UPV 2.400€ (en 2 plazos) Alumni UPV PLUS 2.400€ (en 2 plazos) Personal UPV

Profesorado:

CLIMENTE ALARCON, ALFONSO
ESTEVE DOMINGO, MANUEL
MOLINA MORENO, BENJAMÍN
PALAU SALVADOR, CARLOS ENRIQUE
PÉREZ LLOPIS, ISRAEL

Asignaturas del Curso:

Asignatura	Tipo oferta	Nombre del Grupo	Previsto Inicio	Previsto Fin
DETECCIÓN Y DEFENSA FRENTE A CIBERAMENAZAS	T	17/18	15/01/18	14/02/18
GESTIÓN EN CIBERINCIDENTES	T	17/18	31/01/18	14/02/18
ANÁLISIS DE INTELIGENCIA	T	17/18	12/02/18	26/02/18
CIBERDEFENSA	T	17/18	28/02/18	14/03/18
PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS	T	17/18	21/03/18	9/04/18
TRABAJO FINAL DE DIPLOMA.CPIC	T	17/18	11/04/18	11/04/19
PRÁCTICAS FINAL DIPLOMA.CPIC	O	17/18	18/01/17	31/07/18

[O] Optativa [T] Troncal