MÁSTER EN INTELIGENCIA DE SEGURIDAD, CIBERDEFENSA Y PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Conocimientos de acceso:

titulados superiores en Telecomunicaciones o Informática. 10% de Profesionales de las materias con más de tres años de experiencia profesional

Conocimientos previos necesarios:

ningunos
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:

titulados Universitarios en las ramas de Telecomunicaciones y Informática. Titulados en FP SUPERIOR en ramas de Telecomunicaciones y Informática con 3 años de experiencia profesional en la rama.
Futuros titulados universitarios en las ramas de Telecomunicaciones y Informática a falta de una asignatura y del TFC
Profesionales del mundo de las telecomunicaciones, informática y carreras afines

Temas a desarrollar:

Módulo 1. Ciberinteligencia (50 horas)
Riesgos y amenazas. Information Operations (IO). Modelos de análisis de seguridad. Técnicas de ataque. Sistemas de detección de intrusos. Vigilancia de fuentes abiertas. Ciberinteligencia (CYBINT). Ciclo de vida de inteligencia. Operaciones en el ámbito cyber. Tácticas, técnicas y procedimientos
Módulo 2. Cyber Security Specialist (Certificación Cisco Cybersecurity Essentials +CCNA Security) (100 horas)
Seguridad en dispositivos de red. Control de usuarios. AAA. Radius. Cortafuegos. Servicios de detección y prevención de intrusos. Seguridad en LAN. Criptografía. VPN. IPSec.
Módulo 3. Accredited Configuration Engineer (Certificación Palo Alto Networks) (100 horas)
Tipos y técnicas de ciberataques. Principios y buenas prácticas de seguridad.
Modelos de seguridad de red: basada en perímetros, Zero Trust. Cloud Computing Security. Endpoint Security. Configuración avanzadas de firewalls. Configuración avanzada de IDS/IPS. Next Generation Firewalls. Prevención de amenazas: Wildfire. Mobile Security and VPN management. SaaS Security.
Diploma de Especialización en Ciberdefensa y Protección de Infraestructuras Críticas (25 ECTS + 5 ECTS DE TESINA-300 HORAS)
Matrícula general: 2.900 EUROS
Comunicad UPV y otros: 2.400 EUROS
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

Metodología didáctica:

Clases presenciales, practicas en laboratorio y semipresencial via on-line conectado a los profesores.

Documentación a entregar a los alumnos:

El material de estudio desarrollado por los profesores de la UPV es totalmente original y elaborado ex profeso para el Master, con un elevado contenido práctico y aplicado.

Todos los módulos del master se desarrollarán en aula informática con un puesto de trabajo (PC conectado a internet para cada alumno)

Condiciones generales

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

Condiciones específicas

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 ONU. Parte de su plantilla actualmente son alumnos de este máster.

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	MASTER
Estado	ANULADO
Duración en horas	600 horas presenciales
Créditos ECTS	60
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	15/1/18
Fecha Fin	31/7/18 La fecha límite para entrega de trabajos, realización de prácticas y otras actividades no lectivas será el 31/7/19
Datos de matriculación:	
Matrícula desde	8/9/17
Inicio de preinscripcion	29/6/17
Mínimo de alumnos	12
Máximo de alumnos	22
Precio	5.700,00 euros
Observaciones al precio	5.700€ (en 3 plazos) Público en general 4.700€ (en 3 plazos) Personal UPV 4.700€ (en 3 plazos) Alumno UPV 4.700€ (en 3 plazos) Alumni UPV PLUS 4.700€ (en 3 plazos) Antiguo Alumno del Máster de Redes
Profesorado:	
CLIMENTE ALARCON, ALFONSO ESTEVE DOMINGO, MANUEL LOPEZ PATIÑO, JOSE ENRIQUE MOLINA MORENO, BENJAMÍN PALAU SALVADOR, CARLOS ENRIQUE PÉREZ LLOPIS, ISRAEL REQUENA SÁNCHEZ, BELÉN ROMERO MARTINEZ, JOSE OSCAR	

Asignaturas del Curso:				
Asignatura	Tipo oferta	Nombre del Grupo	Previsto Inicio	Previsto Fin
ACCREDITED CONFIGURATION ENGINEER (PALO ALTO NETWORKS)	T	17/18	29/6/18	28/7/18
DETECCIÓN Y DEFENSA FRENTE A CIBERAMENAZAS	T	17/18	15/1/18	14/2/18
GESTIÓN EN CIBERINCIDENTES	T	17/18	31/1/18	14/2/18
ANÁLISIS DE INTELIGENCIA	T	17/18	12/2/18	26/2/18
CIBERDEFENSA	T	17/18	28/2/18	14/3/18
PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS	T	17/18	21/3/18	9/4/18
TESINA.ISCP	T	17/18	11/4/18	11/4/19
CIBERINTELIGENCIA. CIBERSEGURIDAD	T	17/18	16/1/18	8/2/18
CCNA SECURITY. CIBERSEGURIDAD	T	17/18	13/2/18	22/3/18
TALLERES CYBER SECURITY SPECIALIST. CIBERSEGURIDAD	T	17/18	13/2/18	23/3/18
PRÁCTICA.ISCP	O	17/18	15/1/18	31/7/18
[O] Optativa [T] Troncal				