Datos básicos

Número de créditos: 66,00 ECTS
Preinscripción: A partir del 30/06/2020
Matrícula: A partir del 01/09/2020
Impartición: Del 16/10/2020 al 25/09/2021 (clases hasta el 26/06/2021)
Precio (euros): 3.789,00 (tasas incluidas)
Pago fraccionado: Sí
Modalidad: Semipresencial
Plataforma Virtual: Plataforma Virtual US
Prácticas en empresa/institución: Sí (extracurriculares)
Procedimientos de Evaluación: Asistencia, Pruebas, Trabajos

Dirección

Unidad Organizadora:
Departamento de Ingeniería Telemática

Director de los estudios:
D. Rafael Estepa Alonso

Requisitos

- Estar en posesión de algún Título de Ingeniería Técnica, Ingeniería o Grado en Ingeniería.
- También es posible estar en posesión del Título de Licenciado (o Graduado) en Ciencias Matemáticas o Física con experiencia en el sector TIC.

Objetivos

- Se formará a un Máster Ingeniero en ciberseguridad con capacidad para resolver los problemas técnicos de nivel avanzado asociados a la seguridad en redes, servicios y sistemas de información corporativos. La formación incidirá en los aspectos tecnológicos y procedimentales.
- El Máster busca abordar con la suficiente profundidad técnica TODOS los aspectos relacionados con la ciberseguridad, capacitando para el desarrollo de software seguro en plataformas Windows/Línux y plataformas móviles (apps), el bastionado de la red y sistemas TICs, la implantación de un sistema de gestión de seguridad en una empresa, la realización auditorías de seguridad incluyendo técnicas avanzadas de Hacking Ético y la elaboración de informes periciales de informática forense en el ámbito de las TICs.
- El curso, impartido en su mayor parte por expertos de empresas del sector, pretende cubrir las necesidades formativas de nivel avanzado de los futuros profesionales en el incipiente mercado de la ciberseguridad. Las clases presenciales, viernes de 16:30 a 20:30 y sábado de 9:30 a 13:30, permiten la compatibilidad con el horario laboral.

Competencias Generales

Algunas competencias específicas que busca la propuesta son:

- Capacidad de análisis y detección de problemas potenciales desde el punto de vista de la ciberseguridad en las TICs.
- Ser capaz de proteger y bastionar ante posibles ataques tanto las redes como los principales sistemas y servicios TICs (incluyendo entornos cloud).
- Ser capaz de implantar un sistema de gestión de seguridad, plan de continuidad y análisis de riesgos tecnológicos en un entorno corporativo.
- Ser capaz de elaborar informes periciales completos de informática forense.
- Ser capaz desarrollar software de forma segura.
- Capacidad de realizar y redactar de auditorias e informes técnicos de ciberseguridad (aplicar técnicas avanzadas de hacking si fuera necesario).
- Capacidad de comunicación aplicada a la implantación de políticas de seguridad, así como capacidad de búsqueda autónoma de información de interés en la red.

Información

Teléfono: **954 48 73 84**
Web: **http://trajano.us.es/seguridadtic**
Email: **seguridadtic@trajano.us.es**

https://cfp.us.es

Centro de Formación Permanente
Vicerrectorado de Ordenación Académica

Máster Propio
2020-2021

Seguridad en la Información y las Comunicaciones
(VIII edición)

UNIVERSIDAD D SEVILLA

Comisión Académica

D. Antonio Estepa Alonso. Universidad de Sevilla - Ingeniería Telemática
D. Germán Madinabeitia Luque. Universidad de Sevilla - Ingeniería Telemática
D. Rafael Estepa Alonso. Universidad de Sevilla - Ingeniería Telemática

Profesorado

D. José Carlos Álvarez Parralo. - PwC
D. Miguel Ángel Arroyo Moreno. - SEMIC
D. Josep Bardallo Gay. - A2Secure
D. Ignacio Campos Rivera. Universidad de Sevilla - Ingeniería Telemática
D. Fernando Cárdenas Fernández. Universidad de Sevilla - Ingeniería Telemática
D. Rafael Ceballos Guerrero. Universidad de Sevilla - Lenguajes y Sistemas Informáticos
D. Alfonso Chaves Coronilla. - ORACLE
D. Sergio De Los Santos Vílchez. - ElenenPaths
D. Antonio Luis Delgado González. Universidad de Sevilla - Ingeniería Telemática
D. Jesús Díaz Verdejo. Universidad de Granada- Teoría de la Señal, Telemática y Comunicaciones
D. Rafael Estepa Alonso. Universidad de Sevilla - Ingeniería Telemática
D. Antonio Estepa Alonso. Universidad de Sevilla - Ingeniería Telemática
D. Alberto Fernández Fernández. - Informática Forense
D. Francisco José Fernández Jiménez. Universidad de Sevilla - Ingeniería de Sistemas y Automática
D. Godofredo Fernández Requena. Universidad de Sevilla - Ingeniería Telemática
D. José Manuel Fornés Rumbao. Universidad de Sevilla - Ingeniería de Sistemas y Automática
D. Roberto García Fernández. Universidad de Oviedo - Informática
D. Xicu Xabiel García Pañeda. Universidad de Oviedo - Informática
D. José Girón Gómez. - MInisterio del Interior
D. Julián González Caracuel. - DevSecOps
D. Oliver Daniel López Yela. - EUIGS Admiral Group
D. Germán Madinabeitia Luque. Universidad de Sevilla - Ingeniería Telemática
D. Andrés Marchante Tirado. - DELL
D. Rafael Martínez Gasca. Universidad de Sevilla - Lenguajes y Sistemas Informáticos
D. Francisco Javier Muñoz Calle. Universidad de Sevilla - Ingeniería de Sistemas y Automática
D. José Manuel Pavón Álvarez. - Metsi Technologies
D. Francisco Pérez Fernández. - Miratech
Dª. Isabel Román Martínez. Universidad de Sevilla - Ingeniería Telemática
D. Juan Antonio Ternero Muñiz. Universidad de Sevilla - Ingeniería Telemática
D. Angel Jesús Varela Vaca. Universidad de Sevilla - Lenguajes y Sistemas Informáticos
D. Ezequiel Vázquez De la Calle. - Lullabot
D. Enrique Villa Crespo. - Wellness Telecom
D. Juan Manuel Vozmediano Torres. Universidad de Sevilla - Ingeniería Telemática

Asignaturas del Curso

Módulo/Asignatura 1. Introducción a la Seguridad e Identificación Digital

Número de créditos: 5,00 ECTS
Contenido:
- Introducción a la seguridad: conceptos básicos de seguridad, riesgos y amenazas, principales actores, tendencias tecnológicas y de mercado.
- Conceptos básicos de criptografía práctica.
- Introducción a la identificación digital e infraestructuras de clave pública (PKI), firma electrónica y comercio electrónico.

Fechas de inicio-fin: 16/10/2020 - 06/11/2020

Módulo/Asignatura 2. Seguridad en Redes de Datos (I)

Número de créditos: 8,00 ECTS
Contenido:
- Introducción a las redes y protocolos de seguridad (TLS, SSL).
- Seguridad básica en LAN (VLAN, DHCP, 802.1x, 802.11).
- Seguridad en routers y firewall (configuraciones, DMZ).

Fechas de inicio-fin: 07/11/2020 - 11/12/2020

Módulo/Asignatura 3. Seguridad en Servicios y Sistemas de Información

Número de créditos: 8,00 ECTS
Contenido:
- Seguridad en Windows (DEP, ASLR, MIC, UAC, EMET, opciones y privilegios).
- Malware (estado actual, análisis de las diversas escuelas internacionales y análisis básico).
- Seguridad en Linux (administración básica de seguridad) y sus servicios básicos.
- Sistemas de gestión de identidad y autorización (LDAP, Kerberos,...).

Fechas de inicio-fin: 12/12/2020 - 28/01/2021

Módulo/Asignatura 4. Hacking Ético y Auditorías de Seguridad

Número de créditos: 7,00 ECTS
Contenido:
- Metodologías y técnicas de hacking para análisis de vulnerabilidades.
- Test de penetración y hacking ético: analisis de vulnerabilidades en red, herramientas de hacking (NMAP, NESSUS, Metasploit, etc.), técnicas de hacking (pivoting, etc.).
- Hacking a portales web (sistemas gestores de contenidos).

Fechas de inicio-fin: 29/01/2021 - 04/03/2021

Módulo/Asignatura 5. Gestión de la Seguridad en Organizaciones

Número de créditos: 8,00 ECTS
Contenido:
- Estándares y buenas prácticas de seguridad (serie ISO 27000,...), normativa de seguridad y legislación (LOPD, ENS, ...).
- Análisis y gestión de riesgos (MAGERIT) y plan de continuidad del negocio (BS25999).
- Implantación de un sistema de gestión de seguridad (herramientas, plan director, cuadro de mando, ...).

Fechas de inicio-fin: 05/03/2021 - 25/03/2021

Módulo/Asignatura 6. Accesos VPN, IDS/IPS, SIEM-Operaciones en Ciberseguridad y Ciberseguridad Industrial, y en IoT

Número de créditos: 6,00 ECTS
Contenido:
- Seguridad en acceso remoto (VPN) y control de acceso en red. (VPN Host-to-Host, VPN Web SSL, Open VPN, VPN en dispositivos móviles).
- Configuración avanzada de sistemas IDS/IPS: casos prácticos y equipos de mercado.
- Sistemas de monitorización NMS y operaciones en seguridad (SOC).
- Seguridad en redes locales industriales.
- Seguridad en IPv6.

Fechas de inicio-fin: 26/03/2021 - 06/04/2021

Módulo/Asignatura 7. Seguridad en el Desarrollo de Software y Aplicaciones Móviles

Número de créditos: 6,00 ECTS
Contenido:
- Seguridad en el ciclo de vida de las aplicaciones (gestión de riesgos, vulnerabilidades en el software).
- Seguridad en la desarrollo de aplicaciones web (guías para desarrollo seguro, herramientas para auditorias de software).
- Seguridad en el desarrollo de aplicaciones móviles (iOS y android).

Fechas de inicio-fin: 07/05/2021 - 27/06/2021

Módulo/Asignatura 8. Seguridad en Cloud Computing

Número de créditos: 4,00 ECTS
Contenido:
- Introducción a los sistemas de cloud computing (modalidades de servicio y entornos).
- Securización de sistemas de cloud computing: gestión AAA en entornos cloud, modelo integral de seguridad en cloud (ITIL, 27000,27002), auditorías y conformidad con la regulación.

Fechas de inicio-fin: 28/05/2021 - 10/06/2021

Módulo/Asignatura 9. Informática Forense

Número de créditos: 8,00 ECTS
Contenido:
- Peritaciones en procedimientos penales: legislación penal, introducción a las herramientas y metodología para captura de evidencias.
- Peritaje en procedimientos civiles y casos prácticos.
- Labores en electrónica forense y análisis forense en telefonía móvil.
- Herramientas avanzadas para pericias de informática forense: Encase y WinHex.
- Forense para respuesta ante incidentes.

Fechas de inicio-fin: 11/06/2021 - 26/06/2021

Módulo/Asignatura 10. Trabajo Fin de Máster

Número de créditos: 6,00 ECTS
Contenido:
- Puesta en práctica de los contenidos tratados en el Máster con un trabajo profesional que los desarrolle.

Fechas de inicio-fin: 26/06/2021 - 28/08/2021