MÁSTER EN CIBERSEGURIDAD Y GESTIÓN DE RIESGOS EN LA INFORMACIÓN

Online

12 meses

60 ECTS

UCAM
UNIVERSIDAD
CATÓLICA DE MURCIA

Structuralia

ÍNDICE

STRUCTURALIA

Structuralia es una escuela online de posgrados y formación continua especializada en ingeniería, infraestructuras, construcción, energía, edificación, transformación digital y nuevas tecnologías. Estamos comprometidos con la formación de calidad para el desarrollo profesional de ingenieros, arquitectos y profesionales del sector STEM (ciencia, tecnología, ingeniería y matemáticas).

Desde nuestra fundación en 2001, han pasado por nuestras aulas virtuales más de 200.000 alumnos provenientes de más de 90 países. Trabajamos constantemente por difundir el conocimiento e impulsar el éxito profesional.

Para ello, contamos con la colaboración de grandes expertos internacionales en cada una de sus áreas, lo que permite a nuestro alumnado desarrollar su especialización de la mano de los mejores profesionales en activo.

El contacto permanente con grandes empresas de cada sector, como su proveedor de formación especializada, nos permite crear material didáctico de alto valor orientado a cubrir los requisitos laborales actuales de nuestro alumnado.

Nuestros programas de máster están certificados por universidades del mayor prestigio y referencia internacional como: Universidad Católica San Antonio de Murcia, UDAVINCI o Universidad Isabel I.

Nos esforzamos cada día para ofrecer la mejor formación a los colectivos de ingenieros, arquitectos y profesionales STEM con un fin claro: tu preparación para el éxito profesional.

PRESENTACIÓN

El Máster de Ciberseguridad está diseñado para proporcionar a los estudiantes los conocimientos más completos en el área digital. Abarca desde los principios básicos de protección en red hasta su evaluación y la posterior interpretación de los mismos.

¿A qué amenazas está expuesta la información en los sistemas informáticos de mi empresa?

¿Con qué probabilidad pueden ocurrir estas amenazas si no tomo medidas de protección?

¿Cómo tomo medidas?

¿Cómo puedo minimizar el riesgo?

La seguridad de la información se ocupa de gestionar este riesgo en base a unas normas.

SALIDAS PROFESIONALES

Los estudios en el Máster en Ciberseguridad están fundamentalmente dirigido a tres grupos o perfiles de interés profesional. En primer lugar, interesa a titulados en estudios universitarios profesionales que, estando ya en el ejercicio de la profesión en seguridad informática, deseen respaldar su CV y su experiencia profesional con un postgrado de prestigio en el área de sistemas y seguridad de la información.

También pueden acceder al máster profesionales que, trabajando en el medio o similares, deseen una formación estratégica y técnica. Continuar formándose en el sector no deja de otorgar a la persona una ventaja competitiva importante, con la que es posible alcanzar cotas profesionales más altas.

Cabe mencionar que los mandos profesionales, técnicos intermedios o directivos del sector también pueden realizar el máster. Especialmente, porque una formación continua es básica. Mantenerse actualizado es un factor que hace de la persona un gran profesional.

Finalmente, tanto ingenieros como profesionales que quieran trabajar de manera autónoma y dar cobertura a pymes y pequeñas empresas pueden adquirir importantes habilidades con el máster. También resulta de interés a empresarios y directivos de consultoras, asesorías o despachos que quieran abrir una nueva línea de negocio en procesos de seguridad de la información para sus actuales o potenciales clientes.

OBJETIVOS

El principal objetivo es desarrollar en los futuros profesionales las competencias necesarias para proporcionar a las organizaciones la seguridad que necesitan en la actual sociedad de la información. Los alumnos aprenden cómo diseñar e implantar el programa de ciberseguridad de una organización, así como a securizar entornos cloud, de Internet e industriales.

Así, uno de los puntos más importantes que se tratan en el máster es cómo implantar y auditar nueva normativa como GDPR. Pero, del mismo modo, podrán aprender a lidiar con los retos de ciberseguridad derivados del blockchain, una tecnología relativamente reciente que permite transmisiones más seguras. También desarrollarán las habilidades necesarias para trabajar como hacker ético.

Gracias a un programa amplio y actualizado, el alumno estará capacitado para trabajar en una amplia variedad de puestos entre los que cabe destacar los siguientes:

- Consultor de ciberseguridad.

- Auditor de ciberseguridad. Hacker ético.

- Analista forense.

- Ingeniero de software seguro o de sistemas seguros.

- Arquitecto de ciberseguridad.

- Analista de malware.

METODOLOGÍA

En Structuralia trabajamos con una metodología actual adecuada al proceso de cambio que vivimos hoy en día. Nuestro entorno educativo se basa en un sistema de aprendizaje online: aprender observando, reflexionando y practicando con un ritmo de estudio ordenado y programado. Siempre acompañado de nuestro equipo. Aprendizaje acorde con nuestro ritmo de vida, mantenemos siempre una misma estructura uniforme, mejorando y potenciando el aprendizaje, e intercalando continuas evaluaciones y prácticas para fijar conocimientos.

Nuestro calendario del máster se compone de 9 módulos mensuales, los cuáles se dividen a su vez en 4 unidades didácticas semanales. Además, se cuenta con 3 meses para el Trabajo fin de máster (TFM). Esta estructura puede verse alterada en algunos másteres por la propia complejidad de los contenidos.

En cada una de estas unidades hay videos introductorios sobre conceptos, temario elaborado por nuestros expertos (que se podrá visualizar online o descargar en PDF) y autoevaluaciones para que uno mismo, de forma automática e inmediata, sepa si ha asimilado lo expuesto en las unidades. En algunas unidades podrá haber ejercicios o ejemplos prácticos, si el experto así lo requiere. Al final de cada módulo hay un examen que es obligatorio para dar el módulo por superado.

El Director planteará a todos los alumnos la realización de un Trabajo de fin de máster, en el que se trabajará de forma práctica todo lo aprendido en los módulos previos. Se contará con un plazo de 3 meses para presentarlo. El alumno estará siempre asesorado por el equipo.

Por parte de nuestro equipo recibirás apoyo e informes de estado mediante seguimiento periódicos a lo largo de todo tu proceso.

PROGRAMA

1. VULNERABILIDADES EN LA EMPRESA

UNIDAD 1. Vulnerabilidades en la seguridad de la información. Análisis de riesgos asociados a las redes sociales

SESIÓN 1: Introducción
SESIÓN 2: Estado del arte
SESIÓN 3: Análisis
SESIÓN 4: Actuación
SESIÓN 5: Resumen de la unidad

UNIDAD 2. Detección, análisis de riesgos y protecciones genéricas

SESIÓN 1: Introducción
SESIÓN 2: Detección
SESIÓN 3: Análisis
SESIÓN 4: Protecciones genéricas
SESIÓN 5: Resumen de la unidad

UNIDAD 3. Principios y buenas prácticas de la Seguridad de la Información. Gestión de riesgos de seguridad. Tipos de amenazas y vulnerabilidades

SESIÓN 1: Introducción
SESIÓN 2: Buenas prácticas
SESIÓN 3: Gestión de riesgos y mitigantes
SESIÓN 4: Amenazas y vulnerabilidades
SESIÓN 5: Resumen de la unidad 2

UNIDAD 4. Normativas, regulaciones y legislación. Sistemas de Gestión de la Seguridad de la Información

SESIÓN 1: Introducción
SESIÓN 2: Definición y objetivos
SESIÓN 3: Regulaciones
SESIÓN 4: Sistemas de gestión de seguridad de la información
SESIÓN 5: Resumen de la unidad

2. DESARROLLO SEGURO Y GESTIÓN DE IDENTIDAD

UNIDAD 1. Plan de seguridad y desarrollo seguro

SESIÓN 1: Introducción
SESIÓN 2: Plan de seguridad
SESIÓN 3: Desarrollo seguro
SESIÓN 4: Casos de uso
SESIÓN 5: Resumen de la unidad

UNIDAD 2. Gestión de identidad y autenticación

SESIÓN 1: Introducción
SESIÓN 2: Gestión de identidad
SESIÓN 3: Autenticación
SESIÓN 4: Esquemas de autenticación
SESIÓN 5: Resumen de la unidad

UNIDAD 3. Modelos De Amenazas

SESIÓN 1: Introducción
SESIÓN 2: Modelos de amenazas
SESIÓN 3: Evaluación
SESIÓN 4: Riesgos
SESIÓN 5: Resumen de la unidad

UNIDAD 4. Gestión y almacenamiento seguro de la información

SESIÓN 1: Introducción
SESIÓN 2: Gestión
SESIÓN 3: Almacenamiento activo
SESIÓN 4: Almacenamiento pasivo
SESIÓN 5: Resumen de la unidad

3. IDENTIDAD DIGITAL, REPUTACIÓN. FAKE NEWS, SOCINT Y DOCXING

UNIDAD 1. Tipología de redes sociales

SESIÓN 1: Introducción
SESIÓN 2: Tipos de redes sociales
SESIÓN 3: Conceptos en redes sociales
SESIÓN 4: Seguridad en redes sociales
SESIÓN 5: Resumen de la unidad

UNIDAD 2. Amenazas y mitigantes en redes sociales

SESIÓN 1: Introducción
SESIÓN 2: Amenazas en redes sociales
SESIÓN 3: Mitigantes
SESIÓN 4: Herramientas de seguridad
SESIÓN 5: Resumen de la unidad

UNIDAD 3. DOXING y SOCINT

SESIÓN 1: Introducción
SESIÓN 2: Técnicas de DOXING
SESIÓN 3: Técnicas SOCINT
SESIÓN 4: Herramientas
SESIÓN 5: Resumen de la unidad

UNIDAD 4. Intoxicación de la información. Fake news. Técnicas y análisis.

SESIÓN 1: Introducción
SESIÓN 2: Intoxicación de la información
SESIÓN 3: Análisis de la información
SESIÓN 4: Técnicas de detección de Fake news
SESIÓN 5: Resumen de la unidad

4. MALWARE Y CÓDIGOS MALICIOSOS

UNIDAD 1. Tipología de redes sociales

SESIÓN 1: Introducción
SESIÓN 2: Tipos y definiciones
SESIÓN 3: Análisis estático
SESIÓN 4: Análisis dinámico
SESIÓN 5: Resumen de la unidad

UNIDAD 2. Tipos de Malware I

SESIÓN 1: Introducción
SESIÓN 2: Virus y gusanos
SESIÓN 3: Troyanos
SESIÓN 4: Spyware, Phising
SESIÓN 5: Resumen de la unidad

UNIDAD 3. Tipos de Malware II

SESIÓN 1: Introducción
SESIÓN 2: Rootkits
SESIÓN 3: Ransomware
SESIÓN 4: Otros tipos
SESIÓN 5: Resumen de la unidad

UNIDAD 4. Vulnerabilidades, exploits y payloads.

SESIÓN 1: Introducción
SESIÓN 2: Vulnerabilidades
SESIÓN 3: Exploits
SESIÓN 4: Payloads
SESIÓN 5: Resumen de la unidad

5. CRIPTOGRAFÍA PARA EMPRESAS

UNIDAD 1. Introducción. Algoritmos clásicos

SESIÓN 1: Introducción
SESIÓN 2: Principios de la criptografía
SESIÓN 3: Algoritmos clásicos
SESIÓN 4: Algoritmos clásicos II (ENIGMA)
SESIÓN 5: Resumen de la unidad

UNIDAD 2. Algoritmos de clave simétricas

SESIÓN 1: Introducción
SESIÓN 2: Principios del cifrado simétrico
SESIÓN 3: Algoritmos de claves simétricas
SESIÓN 4: Vulnerabilidades
SESIÓN 5: Resumen de la unidad

UNIDAD 3. Algoritmos de clave asimétrica funciones hash

SESIÓN 1: Introducción
SESIÓN 2: Algoritmos de clave asimétrica
SESIÓN 3: Funciones hash y colisiones
SESIÓN 4: Firma digital

SESIÓN 5: Resumen de la unidad

UNIDAD 4. Certificados digitales, PKI y aplicaciones criptográficas.

SESIÓN 1: Introducción
SESIÓN 2: Certificados digitales
SESIÓN 3: Firma digital
SESIÓN 4: Herramientas y aplicaciones
SESIÓN 5: Resumen de la unidad

6. SEGURIDAD EN REDES CORPORATIVAS INTRODUCCIÓN

UNIDAD 1. Seguridad en redes locales

SESIÓN 1: Introducción
SESIÓN 2: Protocolos en redes locales
SESIÓN 3: Análisis en redes locales
SESIÓN 4: Identificación de amenazas y vulnerabilidades
SESIÓN 5: Resumen de la unidad

UNIDAD 2. Comunicación y redes locales distribuidas. Extranet

SESIÓN 1: Introducción
SESIÓN 2: Accesos externos a redes locales. VPN
SESIÓN 3: Comunicaciones entre redes locales
SESIÓN 4: Vulnerabilidades en extranets
SESIÓN 5: Resumen de la unidad

UNIDAD 3. Seguridad en arquitecturas basadas en Linux

SESIÓN 1: Introducción
SESIÓN 2: Definiciones de políticas de accesos
SESIÓN 3: Accesos a servidores locales. Protocolos
SESIÓN 4: Firewalls, proxies y otros mecanismos
SESIÓN 5: Resumen de la unidad

UNIDAD 4. Seguridad en arquitecturas basadas en Cloud 8

SESIÓN 1: Introducción
SESIÓN 2: Opciones, proveedores y objetivos
SESIÓN 3: Definiciones de roles
SESIÓN 4: Arquitecturas típicas
SESIÓN 5: Resumen de la unidad

7. SEGURIDAD WEB

Unidad 1: ¿Cómo funciona la web?

SESIÓN 1: ¿Cómo funciona la web?
SESIÓN 2: Protocolos HTTP y HTTPS
SESIÓN 3: Dominios y DNS
SESIÓN 4: Servidores
SESIÓN 5: Puertos y otros protocolos

Unidad 2: Seguridad web

SESIÓN 6: Tipos de amenazas web
SESIÓN 7: Objetivos
SESIÓN 8: Objetivos II
SESIÓN 9: Objetivos III
SESIÓN 10: Objetivos IV

Unidad 3: Técnicas de ataque a sitios web

SESIÓN 11: Introducción
SESIÓN 12: Cross-site scripting (XSS)
SESIÓN 13: SQL injection
SESIÓN 14: Pérdida de autenticación
SESIÓN 15: Otras vulnerabilidades

Unidad 4: Acciones para mejorar la seguridad web

SESIÓN 16: Servidor seguro
SESIÓN 17: Securización de apache I
SESIÓN 18: Securización de apache II
SESIÓN 19: INGINX
SESIÓN 20: Otras medidas

8. SEGURIDAD OSINT, INVESTIGACIÓN EN FUENTES ABIERTA

Unidad 1. Osint

- ¿Qué es OSINT?
- Introducción a OSINT
- Objetivos y niveles OSINT
- Metodología de una investigación OSINT
- Ingeniería social

Unidad 2. Buscadores

- Introducción a los buscadores
- Buscador Google
- Buscadores general
- Otros buscadores
- Metabuscadores

Unidad 3. Otras fuentes de información

- Buscadores especializados
- Expresiones regulares
- Herramientas OSINT
- Referencias
- Dark web

Unidad 4. Herramientas

- La investigación OSINT
- OSINT Workflow I
- OSINT Workflow II
- Ejemplos de workflow
- Automatización y referencias

9. SEGURIDAD. INTERNET DE LAS COSAS. CIBERSEGURIDAD

- Sesión 1: Introducción al internet de las cosas (IOT)
- Sesión 2: Historia de IOT
- Sesión 3: DAFO de IOT
- Sesión 4: Áreas y sectores
- Sesión 5: Seguridad y privacidad de IOT

UNIDAD 2. Retos de IoT

- Sesión 1: Introducción a la arquitectura de IOT
- Sesión 2: Modelos de capas
- Sesión 3: Arquitecturas específicas
- Sesión 4: Openfog
- Sesión 5: Desarrollo IOT

UNIDAD 3. Seguridad IoT en proveedores Cloud

- Sesión 1: IOT y Big data
- Sesión 2: Aplicaciones IOT
- Sesión 3: Analítica
- Sesión 4: Aplicaciones de la analítica IOT
- Sesión 5: Agregación e integración de datos

UNIDAD 4. Frameworks en seguridad IoT

- Sesión 1: Sensores
- Sesión 2: Protocolos de comunicación de sensores, controladores e interfaces
- Sesión 3: Protocolos de comunicación
- Sesión 4: Ataques y medidas preventivas
- Sesión 5: Herramientas y casos prácticos

TRABAJO FIN DE MÁSTER

El programa está sujeto a posibles variaciones / actualizaciones de los contenidos para incrementar la calidad de estos.

EVALUACIÓN

La evaluación será continua a lo largo de todo el programa formativo y tendrá en cuenta no sólo la adquisición de conocimientos, sino también el desarrollo de habilidades y actitudes.

Al término de cada tema evaluable, el alumno debe contestar a un examen tipo test en la plataforma de formación on-line, además de plantear diversos casos prácticos a lo largo de los temas de forma que se logre la máxima consolidación de conceptos técnicos.

Para la obtención del título será necesario aprobar los módulos evaluables del programa.

TITULACIÓN

El alumno que haya visualizado todas las lecciones, superado con éxito las autoevaluaciones, exámenes y el proyecto final de Máster, recibirá en formato digital la titulación de Structuralia y el título propio de Máster en Formación Permanente de la Universidad Católica San Antonio de Murcia (UCAM).

Del mismo modo, el alumno puede solicitar certificado de estar cursando el máster o certificado de finalización por parte de Structuralia con el objetivo de que en todo momento pueda acreditar su preparación.

Si lo desea, el alumno podrá solicitar también de manera opcional a la universidad certificado de estar cursando el máster, certificado de finalización o apostillar su título, siempre por un importe adicional.

PROFESORADO

DIRECTOR DEL MÁSTER:

Oscar García-Rama

Oscar es socio fundador de SupportFactory.net, empresa con más de 15 años en el sector del desarrollo tecnológico y especializado en seguridad en entornos EdTech. Actualmente es CEO de un spin-off de esta empresa; Content Away; enfocada en EdTech para educación superior.
Ha participado en diferentes proyectos y eventos con multinacionales y organismos públicos. Ponente invitado en conferencias con el Ministerio de Defensa y Ministerio de Educación entre otros para tratar temas relativos a motivación en entornos educativos y seguridad.

En Telefónica participó en proyectos de I+D, analizando mecanismos de seguridad en el envío de información a través de redes inalámbricas. En IBM pertenecía al IBM Learning Services, realizando y programando diversos programas para formación tanto en sistemas como en seguridad de la información.

Rocío Carracedo

Rocío es Socia Fundadora de SupportFactory.net, empresa con más de 15 años en el sector deldesarrollo tecnológico y está especializada en entornos EdTech especialmente en la parte de seguridad.
Ha realizado y coordinado proyectos con multinacionales como Intel y Macmillan; coordinado el trabajo de varios equipos multidisciplinares en diferentes sedes. Especializada en metodologías ágiles y optimización de procesos.

Rocío ha participado en diferentes start-up liderando los procesos de creación y consolidación de empresas en diferentes campos (salud, educación, seguridad, finanzas, etc).
En Telefónica participó como especialista en Big Data, realizando análisis de datos en las campañas que telefónica organizaba, tanto en fidelización de clientes como en la captación de nuevos.

Juan Navarro

Consultor y jefe de proyectos en ciberseguridad en IAG, más de 15 años en el mundo de las nuevas tecnologías y la innovación han transformado a este ingeniero informático que empezó su andadura en el Laboratoria Europeo de Partículas (CERN) y que ha transitado por todas las herramientas de gestión en empresa, en un profesional completo en ciberseguridad. El ataque Wannacry y grandes proyectos en la seguridad de la información han forjado un comunicador que tiende puentes entre la tecnología más puntera con las necesidades de las personas.

MÁSTER EN CIBERSEGURIDAD Y GESTIÓN DE RIESGOS EN LA INFORMACIÓN

UCAM
UNIVERSIDAD
CATÓLICA DE MURCIA

Structuralia