



EUROINNOVA
INTERNATIONAL ONLINE EDUCATION



Structuralia
Engineering eLearning



UCAM
UNIVERSIDAD
CATOLICA DE MURCIA

Máster en Ciberseguridad y Gestión de Riesgos en la Información + 60 Créditos ECTS





Elige aprender en la escuela
líder en formación online

ÍNDICE

1 | Somos
Structuralia

2 | Universidad

3 | Rankings

4 | By EDUCA
EDTECH Group

5 | Metodología
LXP

6 | Razones por las
que elegir
Structuralia

7 | Programa
Formativo

8 | Temario

9 | Contacto

SOMOS STRUCTURALIA

Structuralia es una **institución educativa online de posgrados de alta especialización** en ingeniería, infraestructuras, construcción, energía, edificación, transformación digital y nuevas tecnologías. Desde nuestra fundación en 2001, estamos comprometidos con la formación de calidad para el desarrollo profesional de **ingenieros, arquitectos y profesionales del sector STEM**.

Ofrecemos una plataforma donde poder adquirir nuevas habilidades y actualizarse sin límites de tiempo o espacio. Gracias a nuestra metodología proporcionamos a nuestros estudiantes una **experiencia educativa comprometida** interactiva y de apoyo para que puedan enfrentarse a los desafíos del futuro en sus respectivos campos de trabajo.

Más de
20
años de
experiencia

Más de
200k
estudiantes
formados

Más de
90
nacionalidades entre
nuestro alumnado

[Ver en la web](#)



Structuralia
Engineering eLearning



Especialízate para
avanzar en tu **carrera profesional**

ALIANZAS STRUCTURALIA Y UNIVERSIDAD UCAM

Structuralia y la Universidad Católica de Murcia cierran una colaboración de forma exitosa. De esta forma, Structuralia y la Universidad Católica de Murcia apuestan por un aprendizaje colaborativo, innovador y diferente, al alcance de todos y adaptado al alumnado.

Además, ambas instituciones educativas apuestan por una educación práctica, que promueva el crecimiento personal y profesional del alumno/a. Todo con el fin de interiorizar nuevos conocimientos de forma dinámica y didáctica, favoreciendo su retención y adquiriendo las capacidades para adaptarse a una sociedad global en permanente cambio.

La democratización de la educación es uno de los objetivos de Structuralia y la Universidad Católica de Murcia, ya que ambas instituciones apuestan por llevar la educación a los rincones más remotos del mundo, aprovechando las innovaciones a nivel tecnológico. Además, gracias al equipo de docentes especializados, se ofrece un acompañamiento tutorizado a lo largo de la formación.



UCAM
UNIVERSIDAD
CATÓLICA DE MURCIA



Structuralia
Engineering eLearning



[Ver en la web](#)



Structuralia
Engineering eLearning

RANKINGS DE STRUCTURALIA

Structuralia ha conseguido el reconocimiento de diferentes rankings a nivel nacional e internacional, gracias por su apuesta de **democratizar la educación** y apostar por la innovación educativa para **lograr la excelencia**.

Para la elaboración de estos rankings, se emplean **indicadores** como la reputación online y offline, la calidad de la institución, la responsabilidad social, la innovación educativa o el perfil de los profesionales.



[Ver en la web](#)

BY EDUCA EDTECH

Structuralia es una marca avalada por **EDUCA EDTECH Group**, que está compuesto por un conjunto de experimentadas y reconocidas **instituciones educativas de formación online**. Todas las entidades que lo forman comparten la misión de **democratizar el acceso a la educación** y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación.



ONLINE EDUCATION



Ver en la web



METODOLOGÍA LXP

La metodología **EDUCA LXP** permite una experiencia mejorada de aprendizaje integrando la AI en los procesos de e-learning, a través de modelos predictivos altamente personalizados, derivados del estudio de necesidades detectadas en la interacción del alumnado con sus entornos virtuales.

EDUCA LXP es fruto de la **Transferencia de Resultados de Investigación** de varios proyectos multidisciplinares de I+D+i, con participación de distintas Universidades Internacionales que apuestan por la transferencia de conocimientos, desarrollo tecnológico e investigación.



1. Flexibilidad

Aprendizaje 100% online y flexible, que permite al alumnado estudiar donde, cuando y como quiera.



2. Accesibilidad

Cercanía y comprensión. Democratizando el acceso a la educación trabajando para que todas las personas tengan la oportunidad de seguir formándose.



3. Personalización

Itinerarios formativos individualizados y adaptados a las necesidades de cada estudiante.



4. Acompañamiento / Seguimiento docente

Orientación académica por parte de un equipo docente especialista en su área de conocimiento, que aboga por la calidad educativa adaptando los procesos a las necesidades del mercado laboral.



5. Innovación

Desarrollos tecnológicos en permanente evolución impulsados por la AI mediante Learning Experience Platform.



6. Excelencia educativa

Enfoque didáctico orientado al trabajo por competencias, que favorece un aprendizaje práctico y significativo, garantizando el desarrollo profesional.



Programas

**PROPIOS
UNIVERSITARIOS**

RAZONES POR LAS QUE ELEGIR STRUCTURALIA

1. Nuestra Experiencia

- ✓ Más de **20 años de experiencia**.
- ✓ Más de **200.000 alumnos** ya se han formado en nuestras aulas virtuales.
- ✓ Más de **90 nacionalidades** entre nuestro alumnado.

2. Nuestro Equipo

En la actualidad, Structuralia cuenta con un equipo humano formado por más **550 profesionales que trabajan en el sector STEM (Science, Technology, Engineering and Mathematics)**. Nuestro personal se encuentra sólidamente enmarcado en una estructura que facilita la mayor calidad en la atención al alumnado.

3. Nuestra Metodología



100% ONLINE

Estudia cuando y desde donde quieras. Accede al campus virtual desde cualquier dispositivo.



APRENDIZAJE

Pretendemos que los nuevos conocimientos se incorporen de forma sustantiva en la estructura cognitiva



EQUIPO DOCENTE

Structuralia cuenta con un equipo de profesionales que harán de tu estudio una experiencia de alta calidad educativa.



NO ESTARÁS SOLO

Acompañamiento por parte del equipo de tutorización durante toda tu experiencia como estudiante



4. Calidad AENOR

- ✓ Somos Agencia de Colaboración N°99000000169 autorizada por el Ministerio de Empleo y Seguridad Social de España.
- ✓ Se llevan a cabo auditorías externas anuales que garantizan la máxima calidad AENOR.
- ✓ Nuestros procesos de enseñanza están certificados por **AENOR** por la ISO 9001.



Máster en Ciberseguridad y Gestión de Riesgos en la Información + 60 Créditos ECTS



DURACIÓN
1500 horas



**MODALIDAD
ONLINE**



**ACOMPANIAMIENTO
PERSONALIZADO**



CREDITOS
60 ECTS

Titulación

Titulación Universitaria de Máster de Formación Permanente en Ciberseguridad y Gestión de Riesgos en la Información con 1500 horas y 60 créditos ECTS por la Universidad Católica de Murcia

[Ver en la web](#)



Structuralia
Engineering eLearning



Descripción

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

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.

Para qué te prepara

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 profesional 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.

A quién va dirigido

El siguiente máster te dará la preparación necesaria para realizar la protección efectiva de sistemas y datos en las diferentes organizaciones en las que dediques tu actividad profesional. Logra establecer unas estrategias y políticas de seguridad para reducir el riesgo y cuidar de la información.

Salidas laborales

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.

TEMARIO

MÓDULO 1: VULNERABILIDADES EN LA EMPRESA. CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN. ANÁLISIS DE RIESGOS ASOCIADOS A LAS REDES SOCIALES

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

UNIDAD DIDÁCTICA 2. DETECCIÓN, ANÁLISIS DE RIESGOS Y PROTECCIONES GENÉRICAS

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

UNIDAD DIDÁCTICA 3. PRINCIPIOS Y BUENAS PRÁCTICAS DE LA SEGURIDAD DE LA INFORMACIÓN. GESTIÓN DE RIESGOS DE SEGURIDAD. TIPOS DE AMENAZAS Y VULNERABILIDADES

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

UNIDAD DIDÁCTICA 4. NORMATIVAS, REGULACIONES Y LEGISLACIÓN. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

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

MÓDULO 2: DESARROLLO SEGURO Y GESTIÓN DE IDENTIDAD. CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN. ANÁLISIS DE RIESGOS ASOCIADOS A LAS REDES SOCIALES

1. Introducción
2. Estado del arte
3. Análisis

4. Actuación
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 2. DETECCIÓN, ANÁLISIS DE RIESGOS Y PROTECCIONES GENÉRICAS

1. Introducción
2. Detección
3. Análisis
4. Protecciones genéricas
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 3. PRINCIPIOS Y BUENAS PRÁCTICAS DE LA SEGURIDAD DE LA INFORMACIÓN. GESTIÓN DE RIESGOS DE SEGURIDAD. TIPOS DE AMENAZAS Y VULNERABILIDADES

1. Introducción
2. Buenas prácticas
3. Gestión de riesgos y mitigantes
4. Amenazas y vulnerabilidades
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 4. NORMATIVAS, REGULACIONES Y LEGISLACIÓN. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. Introducción
2. Definición y objetivos
3. Regulaciones
4. Sistemas de gestión de seguridad de la información
5. Resumen de la Unidad Didáctica

MÓDULO 3: IDENTIDAD DIGITAL, REPUTACIÓN. FAKE NEWS, SOCINT Y DOCXING. CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. PLAN DE SEGURIDAD Y DESARROLLO SEGURO

1. Introducción
2. Plan de seguridad
3. Desarrollo seguro
4. Casos de uso
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 2. GESTIÓN DE IDENTIDAD Y AUTENTICACIÓN

1. Introducción
2. Gestión de identidad
3. Autenticación
4. Esquemas de autenticación
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 3. MODELOS DE AMENAZAS

1. Introducción

2. Modelos de amenazas
3. Evaluación
4. Riesgos
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 4. GESTIÓN Y ALMACENAMIENTO SEGURO DE LA INFORMACIÓN

1. Introducción
2. Gestión
3. Almacenamiento activo
4. Almacenamiento pasivo
5. Resumen de la Unidad Didáctica

MÓDULO 4: MALWARE Y CÓDIGOS MALICIOSOS. CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. TIPOLOGÍA DE REDES SOCIALES

1. Introducción
2. Tipos de redes sociales
3. Conceptos en redes sociales
4. Seguridad en redes sociales
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 2. AMENAZAS Y MITIGANTES EN REDES SOCIALES

1. Introducción
2. Amenazas en redes sociales
3. Mitigantes
4. Herramientas de seguridad
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 3. DOXING Y SOCINT

1. Introducción
2. Técnicas de DOXING
3. Técnicas SOCINT
4. Herramientas
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 4. INTOXICACIÓN DE LA INFORMACIÓN. FAKE NEWS. TÉCNICAS Y ANÁLISIS.

1. Introducción
2. Intoxicación de la información
3. Análisis de la información
4. Técnicas de detección de Fake news
5. Resumen de la Unidad Didáctica

MÓDULO 5: CRIPTOGRAFÍA PARA EMPRESAS. CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. CONCEPTOS BÁSICOS DE ATAQUES

1. Introducción
2. Tipos y definiciones
3. Análisis estático
4. Análisis dinámico
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 2. TIPOS DE MALWARE (I)

1. Introducción
2. Virus y gusanos
3. Troyanos
4. Spyware, Phising
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 3. TIPOS DE MALWARE (II)

1. Introducción
2. Rootkits
3. Ransomware
4. Otros tipos
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 4. VULNERABILIDADES, EXPLOITS Y PAYLOADS

1. Introducción
2. Vulnerabilidades
3. Exploits
4. Payloads
5. Resumen de la Unidad Didáctica

MÓDULO 6: SEGURIDAD EN REDES CORPORATIVAS INTRODUCCIÓN. CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN. ALGORITMOS CLÁSICOS

1. Introducción
2. Principios de la criptografía
3. Algoritmos clásicos (I)
4. Algoritmos clásicos (II) (ENIGMA)
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 2. ALGORITMOS DE CLAVE SIMÉTRICAS

1. Introducción
2. Principios del cifrado simétrico
3. Algoritmos de claves simétricas
4. Vulnerabilidades
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 3. ALGORITMOS DE CLAVE ASIMÉTRICA FUNCIONES HASH

1. Introducción
2. Algoritmos de clave asimétrica
3. Funciones hash y colisiones
4. Firma digital
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 4. CERTIFICADOS DIGITALES, PKI Y APLICACIONES CRIPTOGRÁFICAS.

1. Introducción
2. Certificados digitales
3. Firma digital
4. Herramientas y aplicaciones
5. Resumen de la Unidad Didáctica

MÓDULO 7: SEGURIDAD WEB. CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. SEGURIDAD EN REDES LOCALES

1. Introducción
2. Protocolos en redes locales
3. Análisis en redes locales
4. Identificación de amenazas y vulnerabilidades
5. Resumen de la Unidad Didáctica

UNIDAD DIDÁCTICA 2. COMUNICACIÓN Y REDES LOCALES DISTRIBUIDAS. EXTRANET

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

UNIDAD DIDÁCTICA 3. SEGURIDAD EN ARQUITECTURAS BASADAS EN LINUX

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

UNIDAD DIDÁCTICA 4. SEGURIDAD EN ARQUITECTURAS BASADAS EN CLOUD 8

1. Introducción
2. Opciones, proveedores y objetivos
3. Definiciones de roles
4. Arquitecturas típicas
5. Resumen de la Unidad Didáctica

MÓDULO 8: SEGURIDAD OSINT, INVESTIGACIÓN EN FUENTES ABIERTAS.CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. ¿CÓMO FUNCIONA LA WEB?

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

UNIDAD DIDÁCTICA 2. SEGURIDAD WEB

1. Tipos de amenazas web
2. Objetivos (I)
3. Objetivos (II)
4. Objetivos (III)
5. Objetivos (IV)

UNIDAD DIDÁCTICA 3. TÉCNICAS DE ATAQUE A SITIOS WEB

1. Introducción
2. Cross-site scripting (XSS)
3. SQL injection
4. Pérdida de autenticación
5. Otras vulnerabilidades

UNIDAD DIDÁCTICA 4. ACCIONES PARA MEJORAR LA SEGURIDAD WEB

1. Servidor seguro
2. Securización de apache (I)
3. Securización de apache (II)
4. INGINX
5. Otras medidas

MÓDULO 9: SEGURIDAD INTERNET DE LAS COSAS. CIBERSEGURIDAD

UNIDAD DIDÁCTICA 1. ¿QUÉ ES IOT?

1. Introducción al internet de las cosas (IoT)
2. Historia de IoT
3. DAFO de IoT
4. Áreas y sectores
5. Seguridad y privacidad de IoT

UNIDAD DIDÁCTICA 2. RETOS DE IOT

1. Introducción a la arquitectura de IoT
2. Modelos de capas
3. Arquitecturas específicas
4. Openfog
5. Desarrollo IoT

UNIDAD DIDÁCTICA 3. SEGURIDAD IOT EN PROVEEDORES CLOUD

1. IoT y Big data
2. Aplicaciones IoT
3. Analítica
4. Aplicaciones de la analítica IoT
5. Agregación e integración de datos

UNIDAD DIDÁCTICA 4. FRAMEWORKS EN SEGURIDAD IOT

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

MÓDULO 10: TFM. MÁSTER EN CIBERSEGURIDAD Y GESTIÓN DE RIESGOS EN LA INFORMACIÓN

¿Te ha parecido interesante esta información?

Si aún tienes dudas, nuestro equipo de asesoramiento académico estará encantado de resolverlas.

Pregúntanos sobre nuestro método de formación, nuestros profesores, las becas o incluso simplemente conócenos.

Solicita información sin compromiso

Teléfonos de contacto

España		+34 900 831 200	Argentina		54-(11)52391339
Bolivia		+591 50154035	Estados Unidos		1-(2)022220068
Chile		56-(2)25652888	Guatemala		+502 22681261
Colombia		+57 601 50885563	Mexico		+52-(55)11689600
Costa Rica		+506 40014497	Panamá		+507 8355891
Ecuador		+593 24016142	Perú		+51 1 17075761
El Salvador		+503 21130481	República Dominicana		+1 8299463963

!Encuéntranos aquí!

Edificio Educa Edtech

Camino de la Torrecilla N.º 30 EDIFICIO EDUCA EDTECH,
C.P. 18.200, Maracena (Granada)

 formacion@euroinnova.com

 www.euroinnova.com

Lunes a viernes: 9:00 a 20:00h Horario España

Ver en la web



Structuralia
Engineering eLearning

¡Síguenos para estar al tanto de todas nuestras novedades!



