



EUROINNOVA
INTERNATIONAL ONLINE EDUCATION

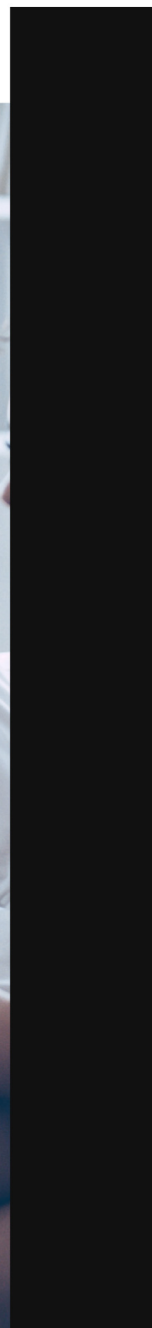


Structuralia
Engineering eLearning



UCAM
UNIVERSIDAD
CATOLICA DE MURCIA

Master's Degree in Cybersecurity + 60 ECTS Credits





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.



[Ver en la web](#)



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.



Master's Degree in Cybersecurity + 60 ECTS Credits



DURACIÓN
1500 horas



MODALIDAD
ONLINE



ACOMPANIAMIENTO
PERSONALIZADO



CREDITOS
60 ECTS

Titulación

Master's Degree in Continuing Education in Cybersecurity with 60 ECTS Credits awarded by the Catholic University of Murcia in collaboration with Structuralia

Structuralia

como Escuela de Negocios de Formación de Postgrado

EXPIDE EL PRESENTE TÍTULO PROPIO

Nombre del Alumno

con D.N.I. XXXXXXXXB ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de 425 horas, perteneciente al Plan de formación de STRUCTURALIA en la convocatoria de 2023

Y para que surta los efectos pertinentes queda registrado con Número de Expediente EDUN/2019-7349-809852

Con una calificación de **NOTABLE**

Y para que conste expido la presente TITULACIÓN en

Granada, a 11 de Noviembre de 2023

Firma del Alumno/a

NOMBRE ALUMNO/A

La Dirección Académica

NOMBRE DE AREA MANAGER

ISO 9001:2015

ISO 27001:2017

IQNET LTD

Con Carácter Consultivo, Categoría Especial del Consejo Económico y Social de la UNED (C3E) (Plan: Resolución 8048)

Ver en la web



Structuralia
Engineering eLearning

Descripción

The Cybersecurity Master's degree program is designed to provide students with deep and comprehensive knowledge of the digital world, and addresses the basic principles of network protection, evaluation, and interpretation.

Objetivos

The main objective is to develop the necessary skills to provide organizations with the security they need in today's information society. Students learn how to design and implement an organization's cybersecurity program, as well as how to secure cloud, Internet and industrial environments. Thus, one of the most important points covered in this program is how to implement and audit new regulations such as the GDPR. Furthermore, the students will be able to deal with cybersecurity challenges derived from the blockchain, a relatively recent technology that allows more secure transmissions. They will also develop the necessary skills to work as an ethical hacker.

Para qué te prepara

Therefore, this Master's degree in Cybersecurity has been designed to provide students with deep and comprehensive knowledge of the digital world, and address the basic principles of network protection, evaluation, and interpretation. It addresses the following questions : - What threats are information systems exposed to in my company? - How often could these threats occur should I not take protective measures? - How do I take measures? - How can I minimize risks?

A quién va dirigido

The Cybersecurity Master's degree program is mainly aimed at 3 specific groups or professional profiles. First, professionals with undergraduate degrees currently working in the cybersecurity, and who wish to strengthen their CV and professional experience by pursuing a prestigious graduate degree in Computer Systems and Cybersecurity. Second, professionals with experience in similar sectors or areas who wish to obtain more strategic and technical training on the subject. As a matter of fact, continuous training in this sector is essential to develop a competitive advantage that will enable us to reach higher professional goals. It is important to mention that anyone in a managerial or technical position may pursue this Master's degree, especially in an ever-changing sector that demands continuous learning and professional update. Third and last, either engineers or professionals that may be interested in managing their own business and require the essential skills to supply this type of services to small and middle-size enterprises. It may also be interesting for businessmen and consultancy firms that may be interested in opening a new business line in computer system cybersecurity for their current, or potential clients.

Salidas laborales

Thanks to this ample and updated program, the student will be able to work in a wide variety of positions such as: - Cybersecurity consultant - Cybersecurity auditor. Ethical hacker - Forensic analyst - Safe software/ systems engineer - Cybersecurity architect - Malware analyst

TEMARIO

MODULE 1. BUSINESS CYBERSECURITY VULNERABILITIES

UNIT 1. INFORMATION SECURITY VULNERABILITIES. SOCIAL MEDIA RISK ANALYSIS

1. Introduction
2. State of the art
3. Analysis
4. Actions
5. Unit summary

UNIT 2. DETECTION, RISK ANALYSIS, AND GENERAL PROTECTIONS

1. Introduction
2. Detection
3. Analysis
4. General protections
5. Unit summary

UNIT 3. CYBERSECURITY PRINCIPLES AND GOOD PRACTICES. SECURITY RISK MANAGEMENT. THREATS AND VULNERABILITIES

1. Introduction
2. Good practices
3. Risk management and mitigating factors
4. Threats and vulnerabilities
5. Unit summary

UNIT 4. STANDARDS, REGULATIONS AND LEGISLATION. CYBERSECURITY MANAGEMENT SYSTEMS

1. Introduction
2. Definition and objectives
3. Regulations
4. Cybersecurity Management Systems
5. Unit summary

MODULE 2. SAFE DEVELOPMENT AND IDENTITY MANAGEMENT

UNIT 1. SECURITY PLAN AND SAFE DEVELOPMENT

1. Introduction
2. Security plan
3. Safe development
4. Cases
5. Unit summary

UNIT 2. IDENTITY MANAGEMENT AND AUTHENTICATION

1. Introduction
2. Identity management
3. Authentication
4. Authentication schemes
5. Unit summary

UNIT 3. THREAT MODELS

1. Introduction
2. Threat models
3. Assessment
4. Risks
5. Unit summary

UNIT 4. SAFE INFORMATION MANAGEMENT AND STORAGE

1. Introduction
2. Management
3. Active storage
4. Passive storage
5. Unit summary

MODULE 3. DIGITAL IDENTITY, REPUTATION, FAKE NEWS, SOCINT AND DOCKING

UNIT 1. TYPES OF SOCIAL MEDIA

1. Introduction
2. Types of social media
3. Social media concepts
4. Social media security
5. Unit summary

UNIT 2. THREATS AND MITIGATING FACTORS IN SOCIAL MEDIA

1. Introduction
2. Social media threats
3. Mitigating mechanisms
4. Security tools
5. Unit summary

UNIT 3. DOXING AND SOCINT

1. Introduction
2. DOXING techniques
3. SOCINT techniques
4. Tools
5. Unit summary

UNIT 4. INFOXICATION. FAKE NEWS. TECHNIQUES AND ANALYSIS

1. Introduction
2. Infoxication
3. Information analysis
4. Fake news detection techniques
5. Unit summary

MODULE 4. MALWARE AND MALICIOUS CODES

UNIT 1. BASIC ATTACK CONCEPTS

1. Introduction
2. Malware definition and types
3. Static and dynamic analysis
4. Terminology
5. Unit summary

UNIT 2. MALWARE TYPE (I)

1. Introduction
2. Viruses and worms
3. Trojans
4. Spyware and Phising
5. Unit summary

UNIT 3. MALWARE TYPE (II)

1. Introduction
2. Rootkits
3. Ransomware
4. Other types
5. Unit summary

UNIT 4. VULNERABILITIES, EXPLOITS, AND PAYLOADS.

1. Introduction
2. Metasploit architecture
3. Exploits
4. Payloads
5. Unit summary

MODULE 5. BUSINESS CRYPTOGRAPHY

UNIT 1. INTRODUCTION. CLASSICAL ALGORITHMS

1. Introduction
2. Principle of cryptography
3. Classic algorithms (I)
4. Classic algorithms (II)
5. Enigma

UNIT 2. SYMMETRIC KEY ALGORITHM

1. Introduction
2. Principles of symmetric encryption
3. Symmetric key algorithms
4. Other symmetric algorithms
5. Unit summary

UNIT 3. ASYMMETRIC-KEY ALGORITHMS. HASH FUNCTION

1. Introduction
2. Asymmetric key algorithm
3. Hash function and collisions
4. Digital signature
5. Unit summary

UNIT 4. DIGITAL CERTIFICATES, PKI AND CRYPTOGRAPHIC APPLICATIONS

1. Digital certificates
2. Digital signature
3. Tools and applications (I)
4. Tools and applications (II)
5. The future of cryptography

MODULE 6. INTRODUCTION TO CORPORATE NETWORK SECURITY

UNIT 1. INTRODUCTION. CLASSICAL ALGORITHMS

1. Introduction
2. Principle of cryptography
3. Classic algorithms (I)
4. Classic algorithms (II)
5. Enigma

UNIT 2. SYMMETRIC KEY ALGORITHM

1. Introduction
2. Principles of symmetric encryption
3. Symmetric key algorithms
4. Other symmetric algorithms
5. Unit summary

UNIT 3. ASYMMETRIC-KEY ALGORITHMS. HASH FUNCTION

1. Introduction
2. Asymmetric key algorithm
3. Hash function and collisions
4. Digital signature
5. Unit summary

UNIT 4. DIGITAL CERTIFICATES, PKI AND CRYPTOGRAPHIC APPLICATIONS

1. Digital certificates
2. Digital signature
3. Tools and applications (I)
4. Tools and applications (II)
5. The future of cryptography

MODULE 7. WEB SECURITY

UNIT 1. HOW THE WEB WORKS

1. Introduction
2. HTTP and HTTPS protocols
3. Domains and DNS
4. Servers
5. Ports and other protocols

UNIT 2. WEB SECURITY

1. Types of web threats
2. Targets (I)
3. Targets (II)
4. Targets (III)
5. Targets (IV)

UNIT 3. WEBSITE ATTACK TECHNIQUES

1. Introduction
2. Cross-Site Scripting (XSS)
3. SQL Injection
4. Loss of authentication
5. Other vulnerabilities

UNIT 4. MEASURES TO IMPROVE WEB SECURITY

1. Secure server
2. Apache (I) Security
3. Apache (II) Security
4. NGINX
5. Other measures

MODULE 8. OSINT SECURITY, OPEN SOURCE INVESTIGATION

UNIT 1. OSINT SOURCE INVESTIGATION

1. What is Osint?
2. Introduction to Osint
3. Goals and levels
4. Osint investigation methodology

5. Social engineering

UNIT 2. SEARCH ENGINES

1. Introduction to search engines
2. Google search
3. General search engines
4. Other search engines
5. Metasearch engines

UNIT 3. OTHER INFORMATION SOURCES

1. Specialized search engines
2. Regular expressions
3. Osint tools
4. References
5. Dark web

UNIT 4. TOOLS

1. Osint investigation
2. Osint Workflow (I)
3. Osint Workflow (II)
4. Workflow Examples
5. Automation and references

MODULE 9. IOT SECURITY

UNIT 1. WHAT IS IOT?

1. Introduction to the Internet of Things (IoT)
2. History of IoT
3. SWOT analysis on IoT
4. Areas and sectors
5. IoT security and privacy

UNIT 2. IOT CHALLENGES

1. Introduction to IoT architecture
2. Layer models
3. Specific architectures
4. OpenFog
5. IoT development

UNIT 3. SECURITY IN CLOUD VENDORS

1. IoT and Big Data
2. IoT applications
3. Analytics
4. IoT analytics applications

5. Data aggregation and integration

UNIT 4. IOT SECURITY FRAMEWORKS

1. Sensors
2. Inter-sensor communication protocols, controllers, and interfaces
3. Communication protocols
4. Attacks and preventive measures
5. Tools and case studies

MODULE 10. MFP. MASTER'S DEGREE IN CYBERSECURITY

¿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

Telefonos 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

!Encuétranos 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

¡Síguenos para estar al tanto de todas nuestras novedades!

España     

Ver en la web



Structuralia
Engineering eLearning

Latino America  
Reública Dominicana  



