Structuralia
Engineering eLearning

UNIVERSIDAD
NEBRIJA

Master´s Degree in Cybersecurity + 60 ECTS Credits





Choose to learn at school
leader in online training

INDICE

1 | About **Structuralia**

2 | **Alliance**

3 | **Rankings**

4 | By **EDUCA EDTECH Group**

5 | LXP **Methodology**

6 | **Why choosing** Structuralia?

7 | Trainning **program**

8 | **List of Subjects**

9 | **Contact**

ABOUT STRUCTURALIA

Structuralia is an online educational institution offering highly specialized postgraduate programs in engineering, infrastructure, construction, energy, building, digital transformation, and new technologies. Since our founding in 2001, we have been committed to providing quality training for the professional development of **engineers, architects, and STEM professionals.**

We provide a platform where you can acquire new skills and enhance your knowledge without being limited by time or location. Our methodology ensures an engaging, interactive, and **supportive educational experience,** equipping our students to meet future challenges in their respective fields of work.

More than **20** years of experience

Over **200k** student have learnt with us

More than **90** nationalities among our students



Specialize to
advance your career

STRUCTURALIA ALLIANCE AND NEBRIJA UNIVERSITY

Structuralia and the University of Nebrija successfully consolidate a strategic partnership. Thus, the collaboration between Structuralia and the University of Nebrija promotes a collaborative, innovative and accessible approach towards learning that is adapted to the individual needs of students.

The two institutions prioritize practical and flexible learning, adapted to the demands of today's working world, and which promotes the personal and professional development of each student. The purpose is to acquire new knowledge in a dynamic and didactic way, which facilitates its retention and contributes to developing the necessary skills to be ready to take part in a society in constant and rapid transformation.

Structuralia and the University of Nebrija have set as their main objective the democratization of education to bring it to even the most remote areas and taking advantage of the latest technological innovations. In addition, they have a team of highly specialized teachers and learning platforms that incorporate cutting-edge educational technology to provide academic support throughout the entire educational process.



STRUCTURALIA RANKINGS

Structuralia has achieved the recognition of different national and international rankings, thanks to its commitment to **democratize education** and bet on educational innovation to **achieve excellence.**

For the elaboration of these rankings, **indicators** such as online and offline reputation, the quality of the institution, social responsibility, educational innovation or the profile of professionals are used.















QS, seal of academic excellence

Structuralia: 5 stars in online education

BY EDUCA EDTECH

Structuralia is a brand endorsed by **EDUCA EDTECH Group,** which is composed of a group of experienced and recognized **educational institutions of online training.** All the entities that make it up share the mission of **democratizing access to education** and are committed to knowledge transfer, technological development and research.

EDUCA EDTECH Group

ONLINE EDUCATION

EUROINNOVA INTERNATIONAL ONLINE EDUCATION

inesem business school

INEAF BUSINESS SCHOOL

red educa.net

inesalud

EDU SPORT

EDUCA business school

ESIBE ESCUELA IBEROAMERICANA DE POSTGRADO

Educa.Pro

ceupe European Business School

UDAVINCI

CAPMAN testing solutions

Structuralia Engineering eLearning

UNIMIAMI International University of Miami

Educa PHAROS

LXP METHODOLOGY

The **EDUCA LXP** methodology enhances the learning experience by incorporating AI into e-learning processes. It utilizes highly customized predictive models based on the analysis of student interactions with their virtual environments.

EDUCA LXP is the outcome of **Research Results Transfer** from multiple interdisciplinary R&D+i projects, involving international universities dedicated to knowledge transfer, technological development and research.



1. Flexibility

100% online and flexible learning, allowing students to study where, when and how they want.



2. Accessibility

We believe in making education accessible to all, working to ensure that everyone has the opportunity to continue their learning journey.



3. Personalization

We offer customized learning paths tailored to each student's unique needs and preferences.



4. Accompaniment / Academic mentoring

Guidance and support. Our team of expert teachers provides academic guidance, advocating for educational quality and adapting to the needs of the ever-changing labor market.



5. Innovation

We are at the forefront of technological development, constantly evolving with AI-driven Learning Experience Platforms.



6. Educational excellence

Our didactic approach focuses on competence based learning, promoting practical and meaningful learning experiences to ensure professional development.



Programs

Our own university and official programs

WHY CHOOSIG STRUCTURALIA

1. Our Experience

- ✓ More than **20 years of experience**.
- ✓ More than **200.000 students** have already learnt in our virtual classrooms.
- ✓ More than **90 nationalities** among our student body.

2. Our Team

Currently, Structuralia has a team of **more than 550 professionals working in the STEM (Science, Technology, Engineering and Mathematics)**. Our staff is solidly framed in a structure that facilitates the highest quality in the attention to students.

3. Our Methodology



100% ONLINE

Study at your convenience, wherever you are. Access our virtual campus from any device.



LEARNING

We strive for a deep integration of new knowledge into your cognitive framework.



TEAM TEACHERS

Structuralia has a team of professionals to elevate your study experience with topquality education.



NOT BE ALONE

Receive continuous guidance from our tutoring team throughout your student journey.

4. AENOR Quality

- ✓ We are Collaboration Agency Nº99000000169 authorized by the Ministry of Employment and Social Security.
- ✓ Annual external audits are carried out to ensure the highest quality by AENOR.
- ✓ Our teaching processes are certified by AENOR under ISO 9001.

Master´s Degree in Cybersecurity + 60 ECTS Credits

LENGHT
1500 horas

MODE
ONLINE

ASSISTANCE
PERSONALIZED

CREDIT
60 ECTS

Certificacion

Master´s Degree in Cybersecurity with 60 ECTS Credits awarded by the Antonio de Nebrija University. Teaching not leading to an officially accredited qualification



Description

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.

Goals

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.

What does it prepare you for?

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?

Who is the target audience?

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.

Job opportunities

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

List of subjects

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 investgation
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

Did you find this information interesting?

If you still have questions, our academic advising team will be happy to answer them.

Ask us about our training method, our teachers, scholarships or even just get to know us.

Request information without commitment.

Find us here!

info@structuralia.com

www.structuralia.com

Follow us to stay updated!

España

inglaterra



Structuralia
Engineering eLearning



By
EDUCA EDTECH
Group