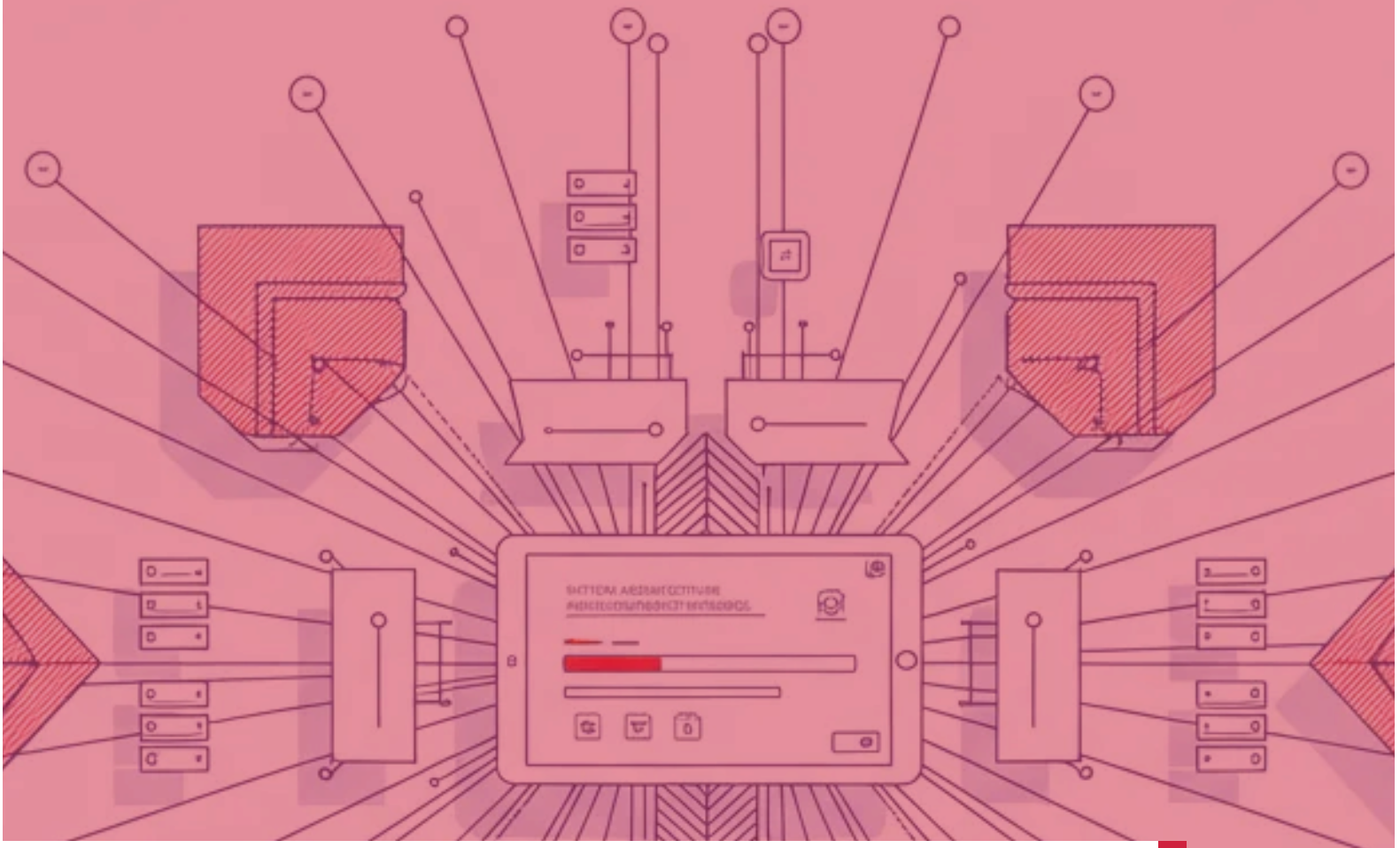


Máster online 100%

Master in Cybersecurity and Information Risk Management + 60 ECTS Credits

Structuralia

Máster online 100%

Master in Cybersecurity and Information Risk Management + 60 ECTS Credits

Modality
Online

Languages
Español

Duration
1500 hours (60 ECTS)

No Limit
AI Assistant

Does it include practices?
NO

Educational Institutions

Structuralia Engineering eLearning

UNIVERSIDAD NEBRIJA

Summary

The Master in Cybersecurity and Information Risk Management is a high-level specialization designed for professionals seeking to consolidate their experience and develop a strategic vision in the protection of digital assets and organizational resilience. This program allows you to delve deeper into the complexity of business vulnerabilities, ranging from the analysis of risks associated with social networks to the implementation of proactive detection and advanced protections. You will master the principles and good practices for the comprehensive protection of information, addressing risk management through the identification, evaluation and mitigation of sophisticated threats. You will explore the framework of standards, regulations and legislation applicable at a global level, as well as the implementation and auditing of Information Security Management Systems (ISMS), fundamental elements for effective governance. You will develop a strategic vision for the design and implementation of robust cybersecurity programs, preparing you to secure cloud, Internet and industrial environments with cutting-edge solutions. This training equips you with the skills to lead secure development initiatives and manage complex digital identities, guaranteeing the integrity and confidentiality of critical data. The program validates and updates your knowledge,

strengthening your professional career in computer security and risk management, allowing you to make strategic decisions in a digital environment that requires continuous adaptation.

Agenda

MODULE 1. VULNERABILITIES IN THE COMPANY. CYBERSECURITY

1. DIDACTIC UNIT 1. VULNERABILITIES IN INFORMATION SECURITY. ANALYSIS OF RISKS ASSOCIATED WITH SOCIAL NETWORKS

1. Introduction
2. State of the art
3. Analysis
4. Performance
5. Unit Summary

2. DIDACTIC UNIT 2. DETECTION, RISK ANALYSIS AND GENERIC PROTECTIONS

1. Introduction
2. Detection
3. Analysis
4. Generic protections
5. Unit Summary

3. DIDACTIC UNIT 3. PRINCIPLES AND GOOD PRACTICES OF INFORMATION SECURITY. SECURITY RISK MANAGEMENT. TYPES OF THREATS AND VULNERABILITIES

1. Introduction
2. Good practices
3. Risk management and mitigants
4. Threats and vulnerabilities
5. Unit Summary

4. DIDACTIC UNIT 4. REGULATIONS, REGULATIONS AND LEGISLATION. INFORMATION SECURITY MANAGEMENT SYSTEMS

1. Introduction
2. Definition and objectives
3. Regulations
4. Information security management systems
5. Unit Summary

MODULE 2. SECURE DEVELOPMENT AND IDENTITY MANAGEMENT. CYBERSECURITY

1. DIDACTIC UNIT 1. VULNERABILITIES IN INFORMATION SECURITY. ANALYSIS OF RISKS ASSOCIATED WITH SOCIAL NETWORKS

1. Introduction
2. State of the art
3. Analysis
4. Performance
5. Didactic Unit Summary

2. DIDACTIC UNIT 2. DETECTION, RISK ANALYSIS AND GENERIC PROTECTIONS

1. Introduction
2. Detection
3. Analysis
4. Generic protections
5. Didactic Unit Summary

3. DIDACTIC UNIT 3. PRINCIPLES AND GOOD PRACTICES OF INFORMATION SECURITY. SECURITY RISK MANAGEMENT. TYPES OF THREATS AND VULNERABILITIES

1. Introduction
2. Good practices
3. Risk management and mitigants
4. Threats and vulnerabilities
5. Didactic Unit Summary

4. DIDACTIC UNIT 4. REGULATIONS, REGULATIONS AND LEGISLATION. INFORMATION SECURITY MANAGEMENT SYSTEMS

1. Introduction
2. Definition and objectives
3. Regulations
4. Information security management systems
5. Didactic Unit Summary

MODULE 3. DIGITAL IDENTITY, REPUTATION. FAKE NEWS, SOCINT AND DOCXING. CYBERSECURITY

1. DIDACTIC UNIT 1. TYPE OF SOCIAL NETWORKS

1. Introduction
2. Types of Social Networks
3. Concepts in Social Networks
4. Security in Social Networks
5. Unit Summary
6. References

2. DIDACTIC UNIT 2. THREATS AND MITIGANTERS IN SOCIAL NETWORKS

1. Introduction
2. Threats on Social Networks
3. Mitigants
4. Security Tools
5. Unit Summary

3. DIDACTIC UNIT 3. DOXXING AND SOCINT

1. Introduction
2. Doxxing Techniques
3. Socmint Techniques
4. Tools

5. Unit Summary
6. References

4. DIDACTIC UNIT 4. INFORMATION INTOXICATION. FAKE NEWS. TECHNIQUES AND ANALYSIS

1. Introduction
2. Information Intoxication
3. Information Analysis
4. Fake News Detection Techniques
5. Unit Summary
6. Bibliographic References

MODULE 4. MALWARE AND MALICIOUS CODES. CYBERSECURITY

1. DIDACTIC UNIT 1. ATTACK BASICS

1. Introduction
2. Definition and Types of Malware
3. Static and Dynamic Analysis
4. Terminology
5. Unit Summary
6. References

2. DIDACTIC UNIT 2. TYPES OF MALWARE I

1. Introduction
2. Viruses and Worms
3. Trojans
4. Spyware and Phishing
5. Unit Summary
6. References

3. DIDACTIC UNIT 3. TYPES OF MALWARE II

1. Introduction
2. Rootkits
3. Ransomware
4. Other Types
5. Unit Summary
6. References

4. DIDACTIC UNIT 4. VULNERABILITIES, EXPLOITS AND PAYLOADS

1. Introduction
2. Metasploit architecture
3. Exploits
4. Payloads
5. Unit Summary
6. References

MODULE 5. CRYPTOGRAPHY FOR COMPANIES. CYBERSECURITY

1. DIDACTIC UNIT 1. ATTACK BASICS

1. Introduction
2. Types and definitions
3. Static analysis
4. Dynamic analysis
5. Didactic Unit Summary

2. DIDACTIC UNIT 2. TYPES OF MALWARE (I)

1. Introduction
2. Viruses and worms
3. Trojans
4. Spyware, Phishing
5. Didactic Unit Summary

3. DIDACTIC UNIT 3. TYPES OF MALWARE (II)

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

4. DIDACTIC UNIT 4. VULNERABILITIES, EXPLOITS AND PAYLOADS

1. Introduction
2. Vulnerabilities
3. Exploits
4. Payloads
5. Didactic Unit Summary

MODULE 6. SECURITY IN CORPORATE NETWORKS INTRODUCTION. CYBERSECURITY

1. DIDACTIC UNIT 1. SECURITY IN LOCAL NETWORKS

1. Introduction
2. Protocols in Local Networks
3. Analysis in local networks
4. Identification of Threats and Vulnerabilities
5. Unit Summary
6. Bibliography

2. DIDACTIC UNIT 2. COMMUNICATION AND DISTRIBUTED LOCAL NETWORKS. EXTRANET

1. Introduction
2. External Access to Local Networks. vpn
3. Communications Between Local Networks
4. Vulnerabilities in Extranets
5. How to See What's Happening on Our Network
6. References

3. DIDACTIC UNIT 3. SECURITY IN LINUX-BASED ARCHITECTURES

1. Introduction
2. Access Policy Definitions
3. Access to Local Servers. Acl
4. Firewalls, Proxies and Other Mechanisms
5. Linux-Based Architectures
6. References

4. DIDACTIC UNIT 4. SECURITY IN CLOUD-BASED ARCHITECTURES

1. Introduction to Security in Cloud Architectures
2. Typical Architectures
3. Options, Suppliers and Objectives
4. Access and Identity Management
5. Network Security Policies
6. References

MODULE 7. WEB SECURITY. CYBERSECURITY

1. DIDACTIC UNIT 1. HOW DOES THE WEBSITE WORK?

1. How does the website work?
2. Http and Https Protocols
3. Domains And DNS
4. Servers
5. Ports and Other Protocols
6. References

2. DIDACTIC UNIT 2. WEB SECURITY

1. Types of Web Threats
2. Objectives
3. Objectives (II)
4. Objectives (III)
5. Objectives (IV)
6. References

3. DIDACTIC UNIT 3. TECHNIQUES FOR ATTACKING WEBSITES

1. Introduction
2. Cross Site Scripting Xss
3. SQL Injection
4. Authentication Loss
5. Other Vulnerabilities
6. References

4. DIDACTIC UNIT 4. ACTIONS TO IMPROVE WEB SECURITY

1. Secure Server
2. Web Servers. Apache Securization (I)
3. Apache Securization (II)
4. Nginx
5. Other Measures

6. References

MODULE 8. OSINT SECURITY, RESEARCH IN OPEN SOURCES. CYBERSECURITY

1. DIDACTIC UNIT 1. HOW DOES THE WEBSITE WORK?

1. How does the website work?
2. HTTP and HTTPS protocols
3. Domains and DNS
4. Servers
5. Ports and other protocols

2. DIDACTIC UNIT 2. WEB SECURITY

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

3. DIDACTIC UNIT 3. TECHNIQUES FOR ATTACKING WEBSITES

1. Introduction
2. Cross-site scripting (XSS)
3. SQL injection
4. Authentication Loss
5. Other vulnerabilities

4. DIDACTIC UNIT 4. ACTIONS TO IMPROVE WEB SECURITY

1. Secure server
2. Apache Securization (I)
3. Apache Securization (II)
4. INGINX
5. Other measures

MODULE 9. INTERNET SECURITY OF THINGS. CYBERSECURITY

1. DIDACTIC UNIT 1. WHAT IS IOT?

1. Introduction to the Internet of Things (IoT)
2. History of IoT
3. IoT SWOT
4. Areas and sectors
5. IoT Security and Privacy

2. DIDACTIC UNIT 2. IOT CHALLENGES

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

3. DIDACTIC UNIT 3. IOT SECURITY IN CLOUD PROVIDERS

1. IoT and Big data
2. IoT applications
3. Analytics
4. IoT analytics applications
5. Data aggregation and integration

4. DIDACTIC UNIT 4. FRAMEWORKS IN IOT SECURITY

1. Sensors
2. Communication protocols for sensors, controllers and interfaces
3. Communication protocols
4. Attacks and preventive measures
5. Tools and case studies

MODULE 10. TFM. MASTER IN CYBERSECURITY AND INFORMATION RISK MANAGEMENT

Qualification

University Degree in Master of Lifelong Training in Cybersecurity and Information Risk Management issued by the Antonio de Nebrija University with 60 ECTS University Credits. Teachings not leading to obtaining an official qualification

Objectives

- • You will lead the implementation of comprehensive digital defense programs, adapted to the strategic needs of any organization. • You will design robust protection architectures for cloud, Internet and industrial environments, mitigating advanced vulnerabilities. • You will effectively manage information risks, applying analysis and evaluation methodologies to protect critical assets. • You will integrate Information Security Management Systems (ISMS) with international standards and regulations, ensuring legal compliance. • You will evaluate the impact of emerging threats and vulnerabilities, developing proactive detection and response strategies. • You will make strategic decisions in the protection of data and systems, based on a deep knowledge of good practices and principles of digital protection. • You will implement secure development and identity management solutions, strengthening the protection posture from the design phase. • You will lead multidisciplinary teams in responding to digital security incidents, minimizing damage and ensuring operational continuity.

What does it prepare you for?

This program equips you with the necessary skills to lead the digital defense strategy in any organization. You will acquire the ability to design and implement robust computer security programs, ranging from proactive identification of vulnerabilities to comprehensive risk management. You will develop skills to establish effective policies and strategies that reduce exposure to threats and safeguard critical information. The Master in Cybersecurity and Information Risk Management specializes in evaluating the impact of threats, allowing you to ensure the compliance and resilience of systems. You will be prepared to make informed decisions about regulations, regulations and applicable legislation, transforming the way your organization approaches information security and strengthening its posture in the face of current challenges.

Who is it addressed to?

This program is aimed at professionals in the computer and systems security sector who already practice in the field of data protection and information security management. If you are looking to validate and update your knowledge to strengthen your professional career with a high-level specialization, this master's degree offers you the tools to do so. It is ideal for those who want to delve deeper into vulnerability detection, advanced risk analysis and incident response, consolidating their technical and strategic expertise. It is also designed for profiles oriented to the strategic direction of digital security, with a marked interest in the implementation of security management systems and regulatory compliance on a global scale.

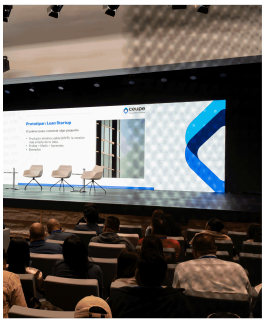
Official Character

This training is not included within the scope of official regulated training (Early Childhood Education, Primary Education, Secondary Education, Official Vocational Training FP, Baccalaureate, University Degree, Master University Officer and Doctorate). It is therefore a complementary and/or specialization training, aimed at the acquisition of certain competencies, skills or aptitudes of a professional nature, which can be assessed as merit in job boards and/or competitive examinations, always within the section of Complementary Training and/or Continuous Training. It is always essential to review the specific grading requirements of the specific public job boards to which we wish to apply.

Professional Outings

- Specialization in systems protection and risk management will strategically position you in the market, allowing you to assume roles of high responsibility and leadership. You will be able to work as a Digital Security Consultant, providing advanced solutions in the defense of critical infrastructures and the evaluation of business risks. You will stand out as an Information Security Auditor, evaluating the robustness of the systems and guaranteeing regulatory compliance with the ISMS. You will contribute as a Systems Security Engineer, integrating security from the initial phases of development and technological architecture. This training promotes your progression towards technical and strategic management in the field of digital security, including functions such as Forensic Analyst or Ethical Hacker, strengthening the security posture of any organization.







Live Madrid

Live the International Week

As an additional complement to your training, you can be part of the SIM: Week International in Madrid. A unique meeting that brings together students from all over the world. For seven days you can live an academic and cultural experience in the heart of Europe, culminating with the graduation ceremony in Madrid.

- Conferences and workshops with international experts
- Visits to companies and reference organizations
- Networking with students from different countries
- Cultural activities and discovery of Madrid
- graduation ceremony

Structural

Structuralia is a leading educational institution in postgraduate and highly specialized online training, focused on the fields of engineering, architecture, construction, energy, technology and digital transformation.

Founded in 2001 with a strong industrial DNA, the result of collaboration between large companies in the sector and the Universitat Politècnica de Catalunya (UPC), for more than 25 years we have accompanied technical professionals in their academic and professional development through practical, flexible training aligned with the reality of the labor market.

Our training proposal connects advanced technical knowledge, real employability and international projection, acting as key support in the professional evolution of those seeking to specialize, grow professionally and generate impact in their sector, with a firm commitment to the democratization of access to technical excellence.



+350.000

Students have gone through our virtual classrooms



+20 years

Experience in the training sector



5 stars

QS ranking in online education

EDUCA EDTECH
Group

Educa Edtech GROUP

When you enroll in a course or master's degree, you will get a free subscription to MyLXP while your training lasts. You will have access to more than 400 key courses (soft skills, languages, digital skills, etc.) and other surprises. Sign up and see how MyLXP improves your learning.

EDUCA LXP Methodology

The comprehensive tailored online education experience

EDUCA LXP is more than a methodology, it is a completely educational experience personalized thanks to all the possibilities offered by artificial intelligence. Now the content adapts to you, your needs and preferences, while offering you access to updated and practical content that really makes a difference in the labor market.

Flexibility

100% online learning adapted to your schedule: study from any device wherever, whenever and however you want.

Personalization

Contents and training itineraries adapted to your needs, thanks to AI.

Innovation

Constantly evolving technological developments driven by AI through the Learning Experience Platform.

Artificial intelligence

Discover PHIA, your learning assistant that will help you every step of the way.

Teaching support

Human empathy and academic guidance from a specialized teaching team.

Educational Experience

Didactic approach oriented to work by competencies, which favors practical and meaningful learning.

MY LXP

When you enroll in a course or master's degree, you will get a free subscription to MyLXP while your training lasts

You will have access to more than 400 key courses (soft skills, languages, competencies digital, etc.) and other surprises. Sign up and see how MyLXP improves your learning.

Meet PHIA, your personalized learning assistant

Use all the possibilities of artificial intelligence to get the most out of it match to your training

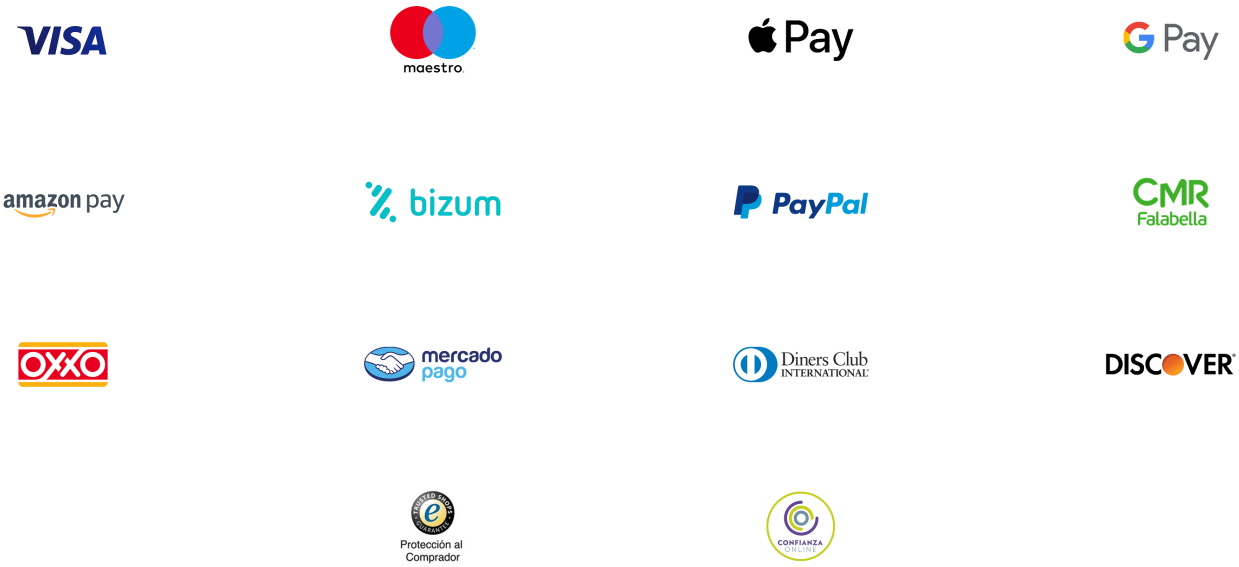
EDUCA EDTECH Group leads the digital revolution in education, promoting the continuous learning and technological transformation. The group is made up of recognized training institutions and its mission is to democratize access to education, promote the transfer of knowledge, technological development and research.

With the experience accumulated over more than 20 years, we have perfected our learning platform EDUCA LXP (Learning Experience Platform), the basis of our educational methodology, which provides students with online training practical and meaningful.



Discover all the payment facilities

We adapt to all international payment methods.



Funding and scholarships

Finance your course or master's degree and enjoy the available scholarships. Contact our expert team to know which one best suits your profile.

25%
Alumni Scholarship

15%
Scholarship recommended

20%
Functional Diversity Scholarship

20%
Unemployment scholarship

15%
GROUP Scholarship

20%
Scholarship for Professionals, Healthcare, members

15%
Entrepreneurship Scholarship

20%
Large Family Scholarship