Professional Master's Degree

Cybersecurity Management (CISO, Chief Information Security Officer)

tech global university

tech global university

Professional Master's Degree

Cybersecurity Management (CISO, Chief Information Security Officer)

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Global University**
- Credits: **60 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/us/information-technology/professional-master-degree/master-direccion-ciberseguridad-ciso-chief-information-security-officer

Index

01

Introduction

In a hyper-connected world, where access to any information is just a click away, protecting the security of people, companies and organizations on the network has become essential. Thereby, as technology advances, so do threats and attack techniques. The more new functionalities there are and the more we communicate, the more our attack surface increases. In other words, the possibilities and ways for cybercriminals to achieve their goals are growing. It is in this context where TECH presents this program with which professionals will learn in a comprehensive way to protect and secure various digital environments. All this, from an eminently practical perspective and adapted to current times.

As technology and connectivity advance, so do the number and form of potential threats. It is therefore crucial that future Chief Information Security Officers update their knowledge to offer solutions that are more adapted to the company's idiosyncrasies"

Nowadays, the information and communication era is in full swing, as everyone is connected both at home and in corporate environments. Thereby, it is that you have access to a multitude of information with a single click, with a single search in any of the engines at our disposal, either from a smartphone, personal or work computer. In this context, "Time is money", but so is information.

As technology advances for the average citizen and employee, so do threats and attack techniques. The more new functionalities there are, the more the world communicates and the more the attack surface increases. In other words, the possibilities and ways for cybercriminals to achieve their goals are growing.

Given this worrying context, TECH launches this Professional Master's Degree in Cybersecurity Management (Chief Information Security Officer) which has been developed by a team with different professional profiles specialized in different sectors that combine international professional experience in the private sector in R+D+i and extensive teaching experience. Therefore, they are not only up to date in each of the technologies, but they also have a perspective towards the future needs of the sector and expose them in a didactic way.

The Program encompasses the different core subjects in the area of Cybersecurity Management (Chief Information Security Officer), carefully selected to rigorously cover a broad spectrum of technologies applicable in different work areas. But it will also deal with another branch of subjects that are usually scarce in the academic catalog of other institutions and that will deeply nourish the professional's curriculum.

This **Professional Master's Degree in Cybersecurity Management (Chief Information Security Officer)** contains the most complete and up-to-date program on the market. The most important features include:

- The development of case studies presented by cybersecurity experts
- The graphic, schematic, and practical contents with which they are created, provide scientific and practical information on the disciplines that are essential for professional practice
- Practical exercises where self-assessment can be used to improve learning
- Its special emphasis on innovative methodologies in Advanced Practice Nursing
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- Content that is accessible from any fixed or portable device with an Internet connection

Prepare yourself to work as Chief Information Security Officer, a key profile in the company for its role as protector and guarantor of information security"

Stand out in a booming sector and become an expert in cybersecurity with this Professional Master's Degree from TECH. It's the most complete on the market"

The ways in which people exchange information are evolving rapidly. This demands new forms of cyber protection from professionals.

A 100% online program with an eminently practical approach that will lay the foundations for your professional growth.

The program's teaching staff includes professionals from the sector who contribute their work experience to this training program, as well as renowned specialists from leading societies and prestigious universities.

The multimedia content, developed with the latest educational technology, will provide the professional with situated and contextual learning, i.e., a simulated environment that will provide immersive specialization programmed to learn in real situations.

This program is designed around Problem-Based Learning, whereby the professional must try to solve the different professional practice situations that arise throughout the program. This will be done with the help of an innovative system of interactive videos made by renowned experts.

02

Objectives

Being fully aware of the relevance of Cybersecurity Management (Chief Information Security Officer) for companies, TECH has developed this Professional Master's Degree that aims to nurture and update the knowledge of professionals in the detection, protection and prevention of cybercrime. In this way, the future graduate will become a key player in the care of data and information, minimizing the possibility of criminals taking advantage of possible existing security breaches. A professional competence that in TECH, in only 12 months, the professional will be able to acquire.

This is a unique opportunity to make your dreams and goals come true and become an expert in Cybersecurity Management (Chief Information Security Officer)"

General Objectives

- Analyze the role of the cybersecurity analyst.
- Study in depth on social engineering and its methods
- Examine OSINT, HUMINT, OWASP, PTEC methodologies. OSSTM, OWISAM
- Conduct a risk analysis and understand risk metrics
- Determine the appropriate use of anonymity and use of networks such as TOR, I2P and Freenet
- Generate specialized knowledge to perform a security audit
- Develop appropriate usage policies
- Examine the most important threat detection and prevention systems
- Evaluate new threat detection systems, as well as their evolution with respect to more traditional solutions
- Analyze the main current mobile platforms, their characteristics and use
- Identify, analyze and assess security risks of the IoT project parts
- Evaluate the information obtained and develop prevention and Hacking mechanisms
- Apply reverse engineering to the cybersecurity environment
- Specify the tests to be performed on the developed software
- Collect all existing evidence and data to conduct a forensic report
- Duly submit the forensic report
- Analyze the current and future state of computer security
- Examining the risks of new emerging technologies
- Compile the different technologies in relation to computer security

Specific Objectives

Module 1. Cyberintelligence and Cybersecurity

- Develop methodologies used in cybersecurity
- Examine the intelligence cycle and establish its application in cyberintelligence
- Determine the role of the intelligence analyst and the obstacles to evacuation activity
- Analyze OSINT, OWISAM, OSSTM, PTES, OWASP Methodologies
- Establishing the most common tools for intelligence production
- Conduct a risk analysis and understand the metrics used
- Concretize the options for anonymity and the use of networks such as TOR, I2P, FreeNet
- Detail the current cybersecurity regulations

Module 2. Host Security

- Specify the *Backup* policies for personal and professional data
- Assess the different tools to provide solutions to specific security problems.
- Establish mechanisms to have an up-to-date system
- Scan equipment for Intruders
- Determine system access rules
- Screen and classify mails to avoid frauds
- Generate lists of allowed software

Module 3. Network Security (Perimeter)

- Analyze current network architectures to identify the perimeter to protect
- Develop specific firewall and Linux configurations to mitigate the most common attacks
- Compile the most commonly used solutions such as Snort and Suricata, as well as their configuration
- Examine the different additional layers provided by next-generation firewalls and networking capabilities in Cloud environments
- Determine the tools for network protection and demonstrate why they are fundamental to a multilayer defence

Module 4. Smartphone Security

- Examine the various attack vectors to avoid becoming an easy target
- Determine the main attacks and types of *Malware* to which mobile device users are exposed.
- Analyze the most current devices to establish greater security in the configuration.
- Specify the main steps to perform a penetration test on both iOS and Android platforms.
- Develop specialized knowledge about the different protection and security tools
- Establish best practices in programming for mobile devices

Module 5. IoT Security

- Analyze the main IoT architectures
- Examine connectivity technologies
- Develop the main application protocols
- Specify the different types of existing devices
- Assessing risk levels and known vulnerabilities
- Develop safe use policies
- Establishing appropriate conditions of use for these devices

Module 6. Ethical Hacking

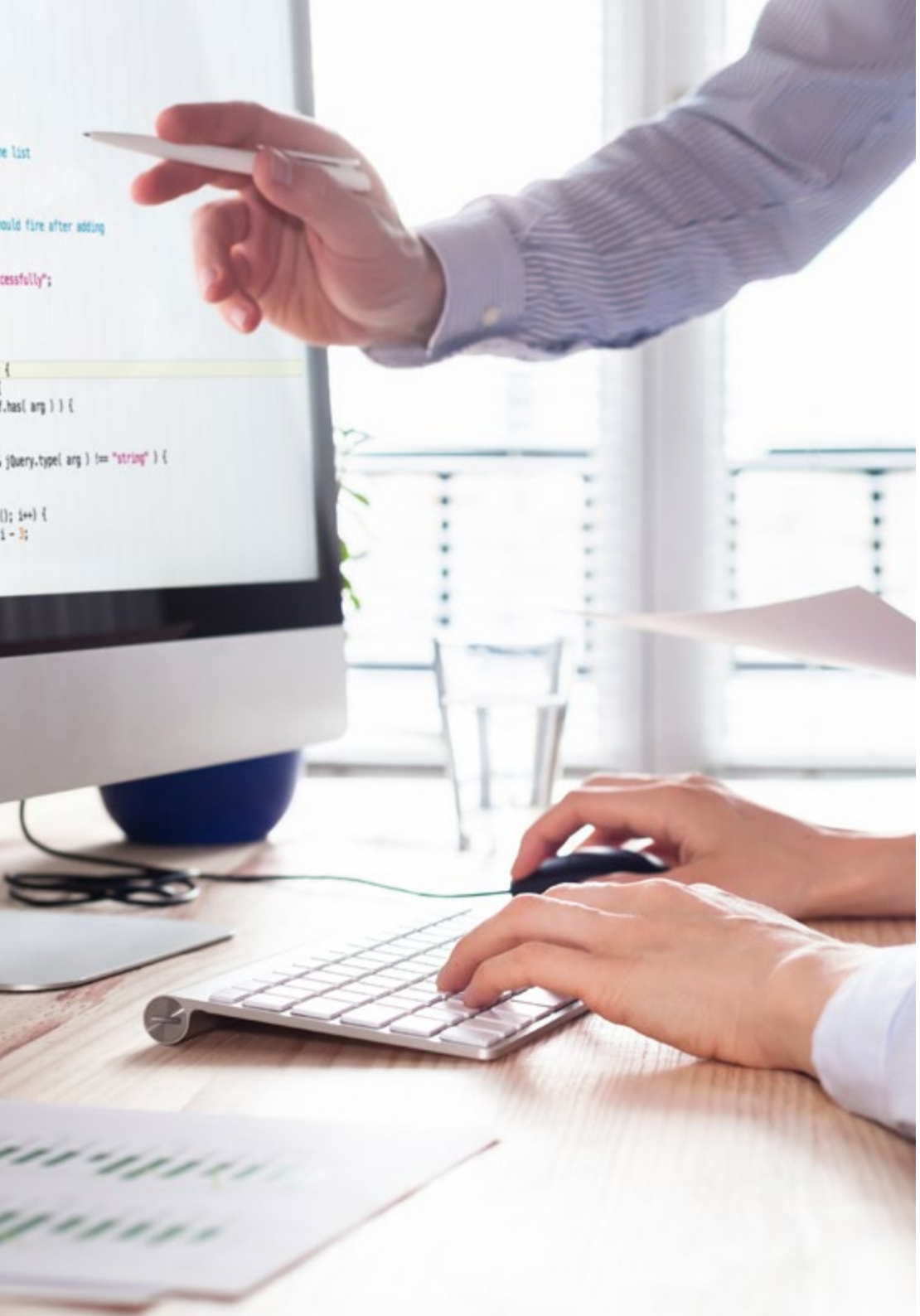
- Examine OSINT methods
- Compile the information available in public media
- Scan networks for active mode information
- Develop testing laboratories
- Analyze the tools for Pentesting performance
- Catalog and assess the different vulnerabilities of the systems.
- Specify the different Hacking methodologies

Module 7. Inverse Engineering

- Analyze the phases of a compiler
- Examining x86 processor architecture and ARM processor architecture
- Determine the different types of analysis
- Apply Sandboxing in different environments
- Develop different Malware analysis techniques
- Establish tools oriented to Malware analysis

Module 8. Secure Development

- Establish the necessary requirements for the correct operation of an application in a secure manner
- ExamineLog files to understand error messages
- Analyze the different events and decide what to show to the user and what to save in the Logs
- Generate a sanitized, easily verifiable, and quality code
- Evaluate appropriate documentation for each phase of development
- Specify the behavior of the server to optimize the system
- Develop modular, reusable and maintainable code



Module 9: Forensic Analysis

- Identify the different elements that evidence a crime
- Generate specialized knowledge to obtain data from different media before they are lost
- Recovery of intentionally deleted data
- Analyze system *Logs* and records
- Determine how data is duplicated so as not to alter the originals
- Substantiate the evidence for consistency
- Generate a solid and seamless report
- Present conclusions in a coherent manner
- Establish how to defend the report before the competent authority
- Specify strategies for safe teleworking

Module 10. Current and Future Challenges in Information Security

- Know the syntactic principles of graphic language and apply its rules to clearly and accurately describe objects and ideas
- Know the origin of letters and their historical importance
- Recognize, study and consistently apply typography to graphic processes.
- Know and apply the aesthetic fundamentals of typography
- Know how to analyze the layout of texts in the design object
- Be able to carry out professional work starting from typesetting

03

Skills

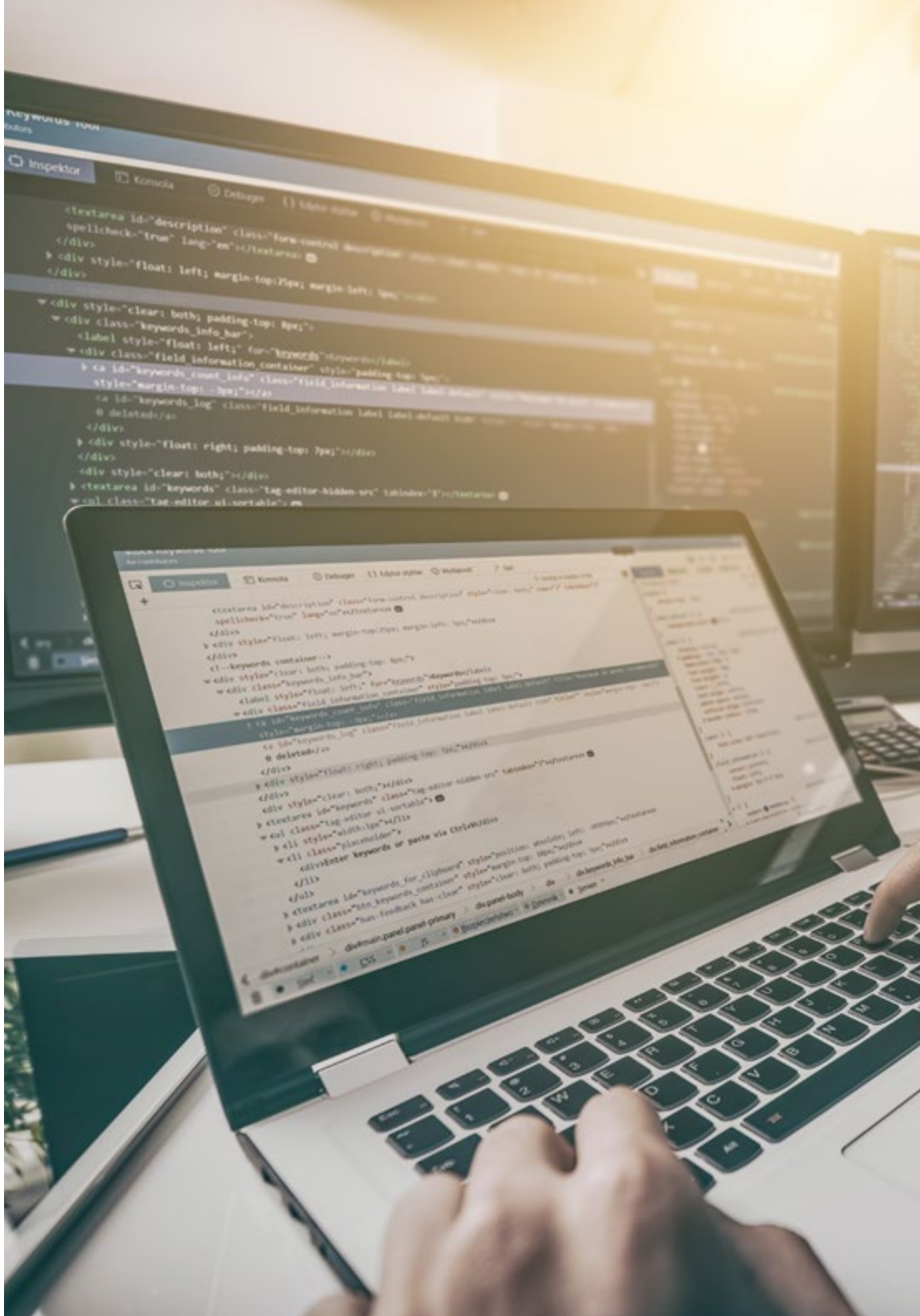
After completing the evaluation process of this Professional Master's Degree, the professional will have acquired a series of knowledge, tools and competencies that will allow him/her to work in this sector with greater guarantees of success. In this way, the student will not only become an expert in Cybersecurity, but will also contribute positively to the reduction of cybercrime through the forging of a safer and stronger network for all.

The cybersecurity industry requires constant updating of knowledge. With programs like this, the professional gets it done quickly and effectively"

General Skills

- Know the methodologies used in cybersecurity
- Know how to evaluate each type of threat in order to offer an optimal solution in each case
- Be able to generate complete intelligent solutions to automate incident behaviors
- Know how to assess the risks associated with vulnerabilities both outside and inside the company
- Understand the evolution and impact of IoT over time
- Be able to demonstrate that a system is vulnerable, attack it for preventive purposes and solve such problems
- Know how to apply *sandboxing* in different environments
- Know the guidelines that a good developer must follow in order to comply with the necessary security requirements

Improving your skills in a service for all will boost your professional and personal career"



Specific Skills

- Know how to perform defensive security operations
- Have a deep and specialized perception of IT security
- Possess specialized knowledge in the field of cybersecurity and cyberintelligence
- Have in-depth knowledge of fundamental aspects such as the intelligence cycle, intelligence sources, social engineering, OSINT methodology, HUMINT, anonymization, risk analysis, existing methodologies (OWASP, OWISAM, OSSTM, PTES)
- Understand the importance of devising a multi-layer defense, also known as "Defence in Depth", covering all aspects of a corporate network where some of the concepts and systems that will be discussed can also be used and applied in a home environment
- Know how to apply security processes for smartphones and portable devices
- Know the means to perform the so-called Ethical Hacking and protect a company from a cyber-attack
- Be able to investigate a cybersecurity incident
- Know the different attack and defence techniques available
- Analyze the role of the Cybersecurity Analyst
- Know how social engineering works and its methods

04

Course Management

The Professional Master's Degree in Cybersecurity Management (Chief Information Security Officer) has been developed by a team of people with different professional profiles specialized in different sectors that combine international professional experience in the private sector in R&D&i and extensive teaching experience. Therefore, they are not only up to date in each of the technologies, but they also have a perspective towards the future needs of the sector and expose them in a didactic way. Thereby, the professional is assured of learning from the best in the industry, with the guarantee of having the most up to date knowledge.

During the program you will be accompanied by a number of professional experts who will make your educational experience unique"

Director Invitado Internacional

Dr. Frederic Lemieux is internationally recognized as an innovative expert and inspirational leader in the fields of Intelligence, National Security, Internal security, Cybersecurity and Disruptive Technologies. His constant dedication and relevant contributions in Research and Education position him as a key figure in the promotion of security and the understanding of today's emerging technologies. During his professional career, he has conceptualized and directed cutting-edge academic programs at various renowned institutions, such as the University of Montreal, George Washington University and Georgetown University.

Throughout his extensive background, he has published multiple books of great relevance, all related to criminal intelligence, policing, cyber threats and international security. He has also contributed significantly to the field of Cybersecurity with the publication of numerous articles in academic journals, which examine crime control during major disasters, counter-terrorism, intelligence agencies and police cooperation. In addition, he has been a panelist and keynote speaker at various national and international conferences, establishing himself as a reference in the academic and professional arena.

Dr. Lemieux has held editorial and evaluative roles in different academic, private and governmental organizations, reflecting his influence and commitment to excellence in his field of expertise. As such, his prestigious academic career has led him to serve as Professor of Practice and Faculty Director of the MPS programs in Applied Intelligence, Cybersecurity Risk Management, Technology Management and Information Technology Management at Georgetown University.

Dr. Lemieux, Frederic

- Researcher in Intelligence, Cybersecurity and Disruptive Technologies, Georgetown University
- Director of the Master's Degree in Information Technology Management at Georgetown University
- Director of the Master's Degree in Technology Management at Georgetown University
- Director of the Master's Degree in Cybersecurity Risk Management at Georgetown University
- Director of the Master's Degree in Applied Intelligence at Georgetown University
- Professor of Internship at Georgetown University
- PhD in Criminology from the School of Criminology, University of Montreal
- B.A. in Sociology, Minor Degree in Psychology, University of Laval
- Member of: New Program Roundtable Committee, Georgetown University

Thanks to TECH you will be able to learn with the best professionals in the world"

Management

Ms. Fernández Sapena, Sonia

- Computer Security and Ethical Hacking Trainer. Getafe National Reference Center for Informatics and Telecommunications. Madrid
- Certified E-Council instructor. Madrid
- Trainer in the following certifications: EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Accredited expert trainer by the CAM of the following certificates of professionalism: Computer Security (IFCT0190), Voice and Data Network Management (IFCM0310), Departmental Network Administration (IFCT0410), Alarm Management in Telecommunications Networks (IFCM0410), Voice and Data Network Operator (IFCM0110), and Internet Services Administration (IFCT0509)
- Colaboradora externa CSO/SSA (Chief Security Officer/Senior Security Architect). University of the Balearic Islands
- Computer Engineer. Alcalá de Henares University. Madrid
- Master in DevOps: Docker and Kubernetes. Cas Training. Madrid
- Microsoft Azure Security Technologies. E-Council. Madrid

Professors

Mr. Catalá Barba, José Francisco

- Middle management in MINISDEF Different tasks and responsibilities within GOE III, such as administration and incident management of the internal network, development of customized programs for different areas, training courses for network users and group personnel in general
- Electronic technician in Ford Factory located in Almusafes, Valencia, robot programming, PLC's, repair and maintenance
- Electronic Technician
- Developer of applications for mobile devices

Mr. Jiménez Ramos, Álvaro

- Senior Security Analyst at The Workshop
- Cybersecurity Analyst L1 at Axians
- Cybersecurity Analyst L2 at Axians
- Cybersecurity analyst at SACYR S.A.
- Degree in Telematics Engineering from the Polytechnic University of Madrid
- Professional Master's Degree in Cybersecurity and Ethical Hacking by CICE
- Advanced Course in Cybersecurity by Deusto Training

Ms. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Application Developer at B60 UK
- Analyst Programmer for the management, coordination and documentation of virtualized environment of security alarms at client's site
- Analyst Programmer of Java applications for ATMs at client's site
- Software Development Professional for signature validation and document management application at customer's site
- Systems Technician for the migration of equipment and for the management, maintenance and training of PDA mobile devices at the customer's site
- Technical Engineering of Computer Systems Universitat Oberta de Catalunya (UOC)
- Professional Master's Degree in Computer Security and Ethical Hacking Official EC-Council and CompTIA by the Professional School of New Technologies CICE

Mr. Peralta Alonso, Jon

- Attorney / DPO Altia Consultores S.A
- Lecturer in Professional Master's Degree in Personal Data Protection, Cybersecurity and ICT Law. Public University of the Basque Country (UPV-EHU)
- Lawyer / Legal advisor. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Legal Advisor / Intern. Professional office: Oscar Padura
- Law Degree. Public University of the Basque Country
- Professional Master's Degree in Data Protection Officer. Escuela innovadora EIS
- Professional Master's Degree in Law. Public University of the Basque Country
- Professional Master's Degree in Civil Litigation Practice. International University Isabel I of Castile

Mr. Redondo, Jesús Serrano

- Junior FrontEnd Developer & Junior Cybersecurity Technician
- FrontEnd Developer at Telefónica, Madrid
- FrontEnd Developer. Best Pro Consulting SL, Madrid
- Telecommunications equipment and services installer. Zener Group, Castilla y León
- Telecommunications equipment and services installer. Lican Comunicaciones SL, Castilla y León
- Certificate in Computer Security. CFTIC Getafe, Madrid
- Senior Technician: Telecommunications and Computer Systems. IES Trinidad Arroyo, Palencia
- Senior Technician: MV and LV Electrotechnical Installations. IES Trinidad Arroyo, Palencia
- Training in reverse engineering, stenography, encryption. Incibe Hacker Academy (Incibe Talents)

05

Structure and Content

To ensure that the student acquires the most rigorous and cutting-edge knowledge in Cybersecurity Management (CISO), TECH has designed a series of materials that bring together the latest updates in the profession. These contents have been designed by a group of experts in the field, so they are adapted to the current needs of the positions offered in the sector. A unique and eminently professionalizing opportunity that will catapult students to success in their professional development.

A high-level syllabus, designed by and for high level professionals, are you going to miss this opportunity? "

Module 1. Cyberintelligence and Cybersecurity

1.1. Cyberintelligence
- 1.1.1. Cyberintelligence
  - 1.1.1.1. Intelligence
    - 1.1.1.1.1. Intelligence Cycle
  - 1.1.1.2. Cyberintelligence
  - 1.1.1.3. Cyberintelligence and Cybersecurity
- 1.1.2. The Intelligence Analyst
  - 1.1.2.1. The Role of the Intelligence Analyst
  - 1.1.2.2. The Intelligence Analyst's Biases in Evaluative Activity

1.2. Cybersecurity
- 1.2.1. Layers of Security
- 1.2.2. Identification of Cyber Threats
  - 1.2.2.1. External Threats
  - 1.2.2.2. Internal Threats
- 1.2.3. Adverse Actions
  - 1.2.3.1. Social Engineering
  - 1.2.3.2. Commonly Used Methods

1.3. Techniques and Tools of Intelligences
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. Humit
- 1.3.4. Linux Distributions and Tools
- 1.3.5. OWISAM
- 1.3.6. OWASP
- 1.3.7. PTES
- 1.3.8. OSSTMM

1.4. Evaluation Methodologies
- 1.4.1. Intelligence Analysis
- 1.4.2. Techniques for Organizing Acquired Information
- 1.4.3. Reliability and Credibility of Information Sources
- 1.4.4. Analysis Methodologies
- 1.4.5. Presentation of Intelligence Results

1.5. Audits and Documentation
- 1.5.1. Computer Security Auditing
- 1.5.2. Documentation and Permits for Auditing
- 1.5.3. Types of Audits
- 1.5.4. Deliverables
  - 1.5.4.1. Technical Report
  - 1.5.4.2. Executive Report

1.6. Anonymity in the Network
- 1.6.1. Use of Anonymity
- 1.6.2. Anonymity Techniques (Proxy, VPN)
- 1.6.3. TOR, Freenet and IP2 Networks

1.7. Threats and Types of Security
- 1.7.1. Types of Threats
- 1.7.2. Physical Security
- 1.7.3. Network Security
- 1.7.4. Logical Security
- 1.7.5. Web Application Security
- 1.7.6. Security on Mobile Devices

1.8. Regulations and Compliance
- 1.8.1. The GDPR
- 1.8.2. ISO 27000 Family
- 1.8.3. NIST Cybersecurity Framework
- 1.8.4. PIC
- 1.8.5. ISO 27032
- 1.8.6. Cloud Regulations
- 1.8.7. SOX
- 1.8.8. PCI

1.9. Risk Analysis and Metrics
- 1.9.1. Extent of Risk
- 1.9.2. The Assets
- 1.9.3. Threats
- 1.9.4. Vulnerabilities
- 1.9.5. Risk Evaluation
- 1.9.6. Risk Treatment

1.10. Important Cybersecurity Agencies
- 1.10.1. NIST
- 1.10.2. OEA
- 1.10.3. UNASUR PROSUR

Module 2. Host Security

2.1. Backup Copies
- 2.1.1. Backup Strategies
- 2.1.2. Tools for Windows
- 2.1.3. Tools for Linux
- 2.1.4. Tools for MacOS

2.2. User Antivirus
- 2.2.1. Types of Antivirus
- 2.2.2. Antivirus for Windows
- 2.2.3. Antivirus for Linux
- 2.2.4. Antivirus for MacOS
- 2.2.5. Antivirus for Smartphones

2.3. HIDS Intrusion Detectors
- 2.3.1. Intrusion Detection Methods
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. Local Firewall
- 2.4.1. Firewalls for Windows
- 2.4.2. Firewalls for Linux
- 2.4.3. Firewalls for MacOS

2.5. Password Managers
- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. Sticky password
- 2.5.5. RoboForm

2.6. Detectors for Phishing
- 2.6.1. Manual Detection of Phishing
- 2.6.2. AntiphishingTools

2.7. Spyware
- 2.7.1. Avoidance Mechanisms
- 2.7.2. Antispyware Tools

2.8. Trackers
- 2.8.1. Measures to Protect the System
- 2.8.2. Anti-tracking Tools

2.9. EDR- End point Detection and Response
- 2.9.1. EDR System Behavior
- 2.9.2. Differences between EDR and Antivirus
- 2.9.3. The Future of EDR Systems

2.10. Control Over Software Installation
- 2.10.1. Repositories and Software Stores
- 2.10.2. Lists of Permitted or Prohibited Software
- 2.10.3. Update Criteria
- 2.10.4. Software Installation Privileges

Module 3. Network Security (Perimeter)

3.1. Threat Detection and Prevention Systems
- 3.1.1. General Framework for Security Incidents
- 3.1.2. Current Defence Systems: Defence in Depth and SOC
- 3.1.3. Current Network Architectures
- 3.1.4. Types of Tools for Incident Detection and Prevention
  - 3.1.4.1. Network-based Systems
  - 3.1.4.2. Host-Based Systems
  - 3.1.4.3. Centralized Systems
- 3.1.5. Instance/Hosts, Container and Serverless Communication and Detection

3.2. Firewall
- 3.2.1. Types of Firewalls
- 3.2.2. Attacks and Mitigation
- 3.2.3. Common Firewalls in Linux Kernel
  - 3.2.3.1. UFW
  - 3.2.3.2. Nftables and Iptables
  - 3.2.3.3. Firewalls
- 3.2.4. Detection Systems Based on System Logs
  - 3.2.4.1. TCP Wrappers
  - 3.2.4.2. BlockHosts and DenyHosts
  - 3.2.4.3. Fail2Ban

3.3. Intrusion Detection and Prevention Systems (IDS/IPS)
- 3.3.1. Attacks on IDS/IPS
- 3.3.2. IDS/IPS Systems
  - 3.3.2.1. Snort
  - 3.3.2.2. Suricata

3.4. Next Generation Firewalls (NGFW)
- 3.4.1. Differences between NGFW and Traditional Firewall
- 3.4.2. Main Capabilities
- 3.4.3. Commercial Solutions
- 3.4.4. Firewalls for Cloud Services
  - 3.4.4.1. Architecture Cloud VPC
  - 3.4.4.2. Cloud ACLs
  - 3.4.4.3. Security Group

3.5. Proxy
- 3.5.1. Types of Proxy
- 3.5.2. Uses of Proxies. Advantages and Disadvantages

3.6. Antivirus Engines
- 3.6.1. General Context of Malware and IOCs
- 3.6.2. Antivirus Engine Problems

3.7. Email Protection Systems
- 3.7.1. Antispam
  - 3.7.1.1. Black and White Lists
  - 3.7.1.2. Bayesian Filters
- 3.7.2. Mail Gateway (MGW)

3.8. SIEM
- 3.8.1. Components and Architecture
- 3.8.2. Correlation Rules and Use Cases
- 3.8.3. Current Challenges of SIEM Systems

3.9. SOAR
- 3.9.1. SOAR and SIEM: Enemies or Allies
- 3.9.2. The Future of SOAR Systems

3.10. Others Network-based Systems
- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. HoneyPots and HoneyNets
- 3.10.4. CASB

Module 4. Smartphone Security

4.1. The World of Mobile Devices
- 4.1.1. Types of Mobile Platforms
- 4.1.2. IOS Devices
- 4.1.3. Android Devices

4.2. Mobile Security Management
- 4.2.1. OWASP Mobile Security Project
  - 4.2.1.1. Top 10 Vulnerabilities
- 4.2.2. Communications, Networks and Connection Modes

4.3. The Mobile Device in the Enterprise Environment
- 4.3.1. Risk
- 4.3.2. Device Monitoring
- 4.3.3. Mobile Device Management (MDM)

4.4. User Privacy and Data Security
- 4.4.1. Statements of Information
  - 4.4.2.1. Licences
  - 4.4.2.2. Encryption
- 4.4.2. Secure Data Storage
  - 4.4.2.1. Secure Storage on iOS
  - 4.4.2.2. Secure Storage on Android
- 4.4.3. Best Practices in Application Development

4.5. Vulnerabilities and Attack Vectors
- 4.5.1. Vulnerabilities
- 4.5.2. Attack Vectors
  - 4.5.2.1. Malware
  - 4.5.2.2. Data Exfiltration
  - 4.5.2.3. Data Manipulation

4.6. Main Threats
- 4.6.1. Unforced User
- 4.6.2. Malware
  - 4.6.2.1. Types of Malware
- 4.6.3. Social Engineering
- 4.6.4. Data Leakage
- 4.6.5. Information Theft
- 4.6.6. Unsecured Wi-Fi Networks
- 4.6.7. Outdated Software
- 4.6.8. Malicious Applications
- 4.6.9. Insecure Passwords
- 4.6.10. Weak or No Security Configuration
- 4.6.11. Physical Access
- 4.6.12. Loss or Theft of the Device
- 4.6.13. Identity Theft (Integrity)
- 4.6.14. Weak or Broken Cryptography
- 4.6.15. Denial of Service (DoS)

4.7. Main Attacks
- 4.7.1. Phishing Attacks
- 4.7.2. Attacks Related to Communication Modes
- 4.7.3. Smishing Attacks
- 4.7.4. Cryptojacking Attacks
- 4.7.5. Man in the middle

4.8. Hacking
- 4.8.1. Rooting and Jailbreaking
- 4.8.2. Anatomy of a Mobile Attack
  - 4.8.2.1. Threat Propagation
  - 4.8.2.2. Malware Installation on the Device
  - 4.8.2.3. Persistence
  - 4.8.2.4. Payload Execution and Information Extraction
- 4.8.3. Hacking on iOS Devices: Mechanisms and Tools
- 4.8.4. Hacking on Android Devices: Mechanisms and Tools

4.9. Penetration Testing
- 4.9.1. iOS Pentesting
- 4.9.2. Android Pentesting
- 4.9.3. Tools

4.10. Safety and Security
- 4.10.1. Security Configuration
  - 4.10.1.1. On iOS Devices
  - 4.10.1.2. On Android Devices
- 4.10.2. Safety Measures
- 4.10.3. Protection Tools

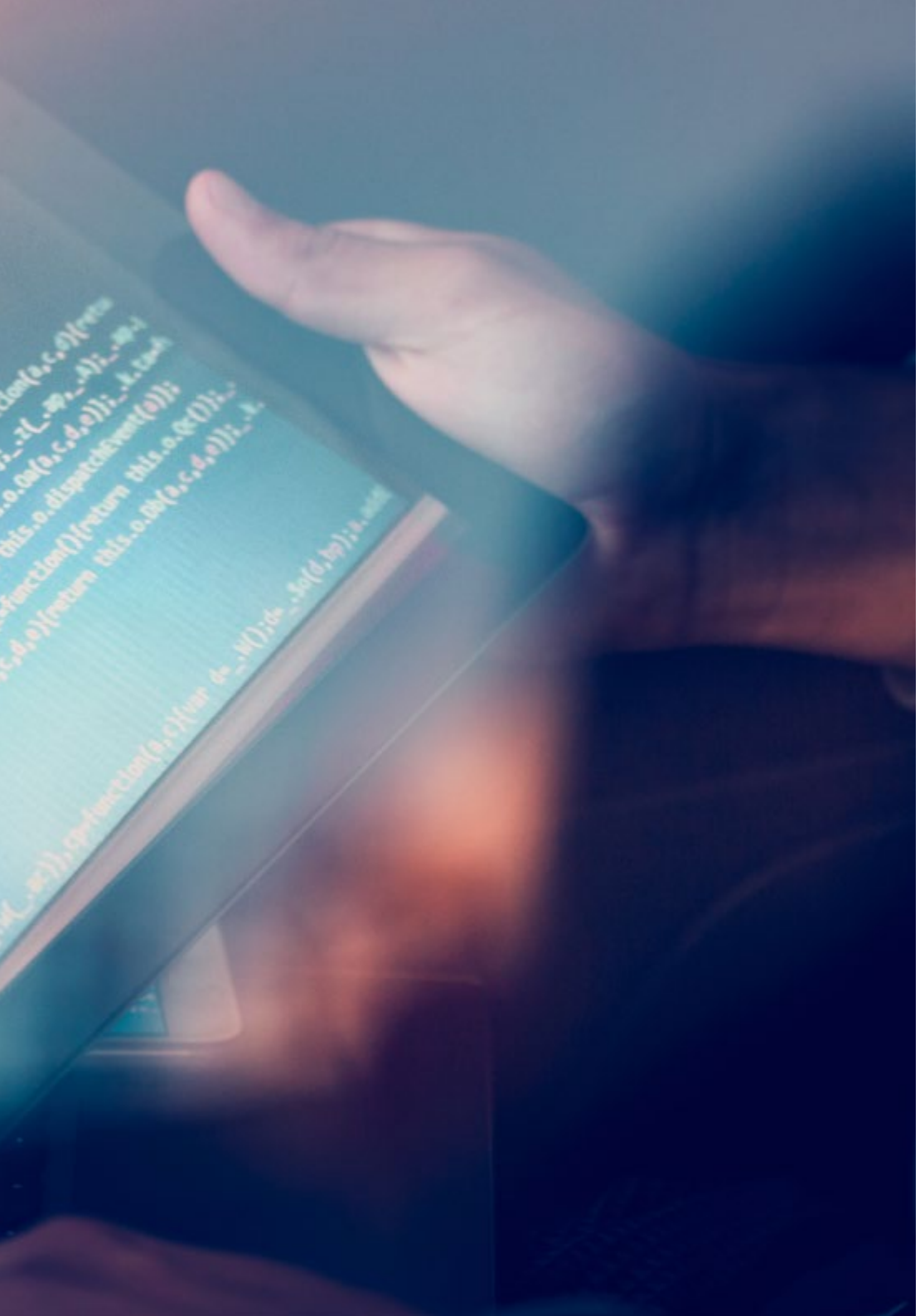
Module 5. IoT Security

5.1. Devices
- 5.1.1. Types of Devices
- 5.1.2. Standardized Architectures
  - 5.1.2.1. OneM2M
  - 5.1.2.2. IoTWF
- 5.1.3. Application Protocols
- 5.1.4. Connectivity Technologies

5.2. IoT Devices. Areas of Application
- 5.2.1. SmartHome
- 5.2.2. SmartCity
- 5.2.3. Transportation
- 5.2.4. Wearables
- 5.2.5. Health Sector
- 5.2.6. IIoT

5.3. Communication Protocols
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. SmartHome
- 5.4.1. Home Automation
- 5.4.2. Networks
- 5.4.3. Household Appliances
- 5.4.4. Surveillance and Security



5.5. SmartCity
- 5.5.1. Lighting
- 5.5.2. Meteorology
- 5.5.3. Security/Safety

5.6. Transportation
- 5.6.1. Localisation
- 5.6.2. Making Payments and Obtaining Services
- 5.6.3. Connectivity

5.7. Wearables
- 5.7.1. Smart Clothing
- 5.7.2. Smart Jewelry
- 5.7.3. Smart Watches

5.8. Health Sector
- 5.8.1. Exercise/Heart Rate Monitoring
- 5.8.2. Monitoring of Patients and Elderly People
- 5.8.3. Implantable
- 5.8.4. Surgical Robots

5.9. Connectivity
- 5.9.1. Wi-Fi
- 5.9.2. Bluetooth
- 5.9.3. Built-in Connectivity

5.10. Securitization
- 5.10.1. Dedicated Networks
- 5.10.2. Password Managers
- 5.10.3. Use of Encrypted Protocols
- 5.10.4. Tips for Use

Module 6. Ethical Hacking

6.1. Work Environment
- 6.1.1. Linux Distributions
  - 6.1.1.1. Kali Linux - Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Virtualization Systems
- 6.1.3. Sandbox
- 6.1.4. Deployment of Laboratories

6.2. Methods
- 6.2.1. OSSTMM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. Footprinting
- 6.3.1. Open-Source Intelligence (OSINT)
- 6.3.2. Search for Data Breaches and Vulnerabilities
- 6.3.3. Use of Passive Tools

6.4. Network Scanning
- 6.4.1. Scanning Tools
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Other Scanning Tools
- 6.4.2. Scanning Techniques
- 6.4.3. Firewalland IDS Evasion Techniques
- 6.4.4. Banner Grabbing
- 6.4.5. Network Diagrams

6.5. Enumeration
- 6.5.1. SMTP Enumeration
- 6.5.2. DNS Enumeration
- 6.5.3. NetBIOS and Samba Enumeration
- 6.5.4. LDAP Enumeration
- 6.5.5. SNMP Enumeration
- 6.5.6. Other Enumeration Techniques

6.6. Vulnerability Analysis
- 6.6.1. Vulnerability Scanning Solutions
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. Vulnerability Scoring Systems
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Attacks on Wireless Networks
- 6.7.1. Methodology of Hacking in Wireless Networks
  - 6.7.1.1. Wi-Fi Discovery
  - 6.7.1.2. Traffic Analysis
  - 6.7.1.3. Aircrack Attacks
    - 6.7.1.3.1. WEP Attacks
    - 6.7.1.3.2. WPA/WPA2 Attacks
  - 6.7.1.4. Evil Twin Attacks
  - 6.7.1.5. Attacks on WPS
  - 6.7.1.6. Jamming
- 6.7.2. Tools for Wireless Security

6.8. Hacking of Web Servers
- 6.8.1. Cross site Scripting
- 6.8.2. CSRF
- 6.8.3. Session Hijacking
- 6.8.4. SQL Injection

6.9. Exploiting Vulnerabilities
- 6.9.1. Use of Known Exploits
- 6.9.2. Use of Metasploit
- 6.9.3. Use of Malware
  - 6.9.3.1. Definition and Scope
  - 6.9.3.2. Malware Generation
  - 6.9.3.3. Bypass of Antivirus Solutions

6.10. Persistence
- 6.10.1. Rootkits Installation
- 6.10.2. Use of Ncat
- 6.10.3. Use of Scheduled Tasks for Backdoors
- 6.10.4. User Creation
- 6.10.5. HIDS Detection

Module 7. Inverse Engineering

7.1. Compilers
- 7.1.1. Types of Codes
- 7.1.2. Phases of a Compiler
- 7.1.3. Table of Symbols
- 7.1.4. Error Manager
- 7.1.5. GCC Compiler

7.2. Types of Analysis in Compilers
- 7.2.1. Lexical Analysis
  - 7.2.1.1. Terminology.
  - 7.2.1.2. Lexical Components
  - 7.2.1.3. LEX Lexical Analyzer
- 7.2.2. Parsing
  - 7.2.2.1. Context-free Grammars
  - 7.2.2.2. Types of Parsing
    - 7.2.2.2.1. Top-down Analysis
    - 7.2.2.2.2. Bottom-up Analysis
  - 7.2.2.3. Syntactic Trees and Derivations
  - 7.2.2.4. Types of Parsers
    - 7.2.2.4.1. LR Analyzers (Left to Right)
    - 7.2.2.4.2. LALR Analyzers
- 7.2.3. Semantic Analysis
  - 7.2.3.1. Attribute Grammars
  - 7.2.3.2. S-attributes
  - 7.2.3.3. L-attributes

7.3. Data Structures in Assembler
- 7.3.1. Variables:
- 7.3.2. Arrays
- 7.3.3. Pointers
- 7.3.4. Structures
- 7.3.5. Objects

7.4. Assembler Code Structures
- 7.4.1. Selection Structures
  - 7.4.1.1. If, else if, Else
  - 7.4.1.2. Switch
- 7.4.2. Iteration Structures
  - 7.4.2.1. For
  - 7.4.2.2. While
  - 7.4.2.3. Use of Break
- 7.4.3. Functions

7.5. X86 Architecture Hardware
- 7.5.1. x86 Processor Architecture
- 7.5.2. x86 Data Structures
- 7.5.3. x86 Code Structures
- 7.5.3. x86 Code Structures

7.6. ARM Architecture Hardware
- 7.6.1. ARM Processor Architecture
- 7.6.2. ARM Data Structures
- 7.6.3. ARM Code Structures

7.7. Static Code Analysis
- 7.7.1. Disassemblers
- 7.7.2. IDA
- 7.7.3. Code Rebuilders

7.8. Dynamic Code Analysis
- 7.8.1. Behavioral Analysis
  - 7.8.1.1. Communication
  - 7.8.1.2. Monitoring
  - 7.8.2. Linux Code Debuggers
- 7.8.3. Windows Code Debuggers

7.9. Sandbox
- 7.9.1. Sandbox Architecture
- 7.9.2. Sandbox Evasion
- 7.9.3. Detection Techniques
- 7.9.4. Avoidance Techniques
- 7.9.5. Countermeasures
- 7.9.6. Sandbox and Linux
- 7.9.7. Sandbox and Windows
- 7.9.8. Sandbox on MacOS
- 7.9.9. Sandbox on android

7.10. Malware Analysis
- 7.10.1. Malware Analysis Methods
- 7.10.2. Malware Obfuscation Techniques
  - 7.10.2.1. Executable Obfuscation
  - 7.10.2.2. Restriction of Execution Environments
- 7.10.3. Malware Analysis Tools

Module 8. Secure Development

8.1. Secure Development
- 8.1.1. Quality, Functionality and Safety
- 8.1.2. Confidentiality, Integrity and Availability
- 8.1.3. Software Development Life Cycle

8.2. Requirements Phase
- 8.2.1. Authentication Control
- 8.2.2. Role and Privilege Control
- 8.2.3. Risk-oriented Requirements
- 8.2.4. Privilege Approval

8.3. Analysis and Design Phases
- 8.3.1. Component Access and System Administration
- 8.3.2. Audit Trails
- 8.3.3. Session Management
- 8.3.4. Historical Data
- 8.3.5. Proper Error Handling
- 8.3.6. Separation of Functions

8.4. Implementation and Coding Phase
- 8.4.1. Ensuring the Development Environment
- 8.4.2. Preparation of Technical Documentation
- 8.4.3. Secure Codification
- 8.4.4. Communications Security

8.5. Good Secure Coding Practices
- 8.5.1. Input Data Validation
- 8.5.2. Coding of Output Data
- 8.5.3. Programming Style
- 8.5.4. Change Log Management
- 8.5.5. Cryptographic Practices
- 8.5.6. Error and Log Management
- 8.5.7. File Management
- 8.5.8. Memory Management
- 8.5.9. Standardization and Reuse of Security Functions

8.6. Server Preparation and Hardening
- 8.6.1. Management of Users, Groups and Roles on the Server
- 8.6.2. Software Installation
- 8.6.3. Server Hardening
- 8.6.4. Robust Configuration of the Application Environment

8.7. DB Preparation and Hardening
- 8.7.1. DB Engine Optimization
- 8.7.2. Create Your Own User for the Application
- 8.7.3. Assigning the Required Privileges to the User
- 8.7.4. Hardening of the BBDD

8.8. Testing Phase
- 8.8.1. Quality Control in Security Controls
- 8.8.2. Phased Code Inspection
- 8.8.3. Checking Configuration Management
- 8.8.4. Black Box Testing

8.9. Preparing the Transition to Production
- 8.9.1. Perform Change Control
- 8.9.2. Carry out Production Changeover Procedure
- 8.9.3. Perform Rollback Procedure
- 8.9.4. Pre-production Testing

8.10. Maintenance Phase
- 8.10.1. Risk-based Assurance
- 8.10.2. White Box Security Maintenance Testing
- 8.10.3. Black box Safety Maintenance Tests

Module 9. Forensic Analysis

9.1. Data Acquisition and Duplication
- 9.1.1. Volatile Data Acquisition
  - 9.1.1.1. System Information
  - 9.1.1.2. Network Information
  - 9.1.1.3. Volatility Order
- 9.1.2. Static Data Acquisition
  - 9.1.2.1. Creating a Duplicate Image
  - 9.1.2.2. Preparation of a Chain of Custody Document
- 9.1.3. Methods for Validation of Acquired Data
  - 9.1.3.1. Methods for Linux
  - 9.1.3.2. Methods for Windows

9.2. Evaluation and Defeat of Antiforensic Techniques
- 9.2.1. Objectives of Antiforensic Techniques
- 9.2.2. Data Deletion
  - 9.2.2.1. Deletion of Data and Files
  - 9.2.2.2. File Recovery
  - 9.2.2.3. Recovery of Deleted Partitions
- 9.2.3. Password Protection
- 9.2.4. Steganography
- 9.2.5. Secure Device Wiping
- 9.2.6. Encryption

9.3. Operating System Forensics
- 9.3.1. Windows Forensics
- 9.3.2. Linux Forensics
- 9.3.3. Mac Forensics

9.4. Network Forensics
- 9.4.1. Log Analysis
- 9.4.2. Data Correlation
- 9.4.3. Network Research
- 9.4.4. Steps to Follow in Network Forensic Analysis

9.5. Web Forensics
- 9.5.1. Investigation of Web Attacks
- 9.5.2. Attack Detection
- 9.5.3. IP Address Location

9.6. Forensic Database Analysis
- 9.6.1. Forensic Analysis in MSSQL
- 9.6.2. MySQL Forensic Analysis
- 9.6.3. PostgreSQL Forensic Analysis
- 9.6.4. Forensic Analysis in MongoDB

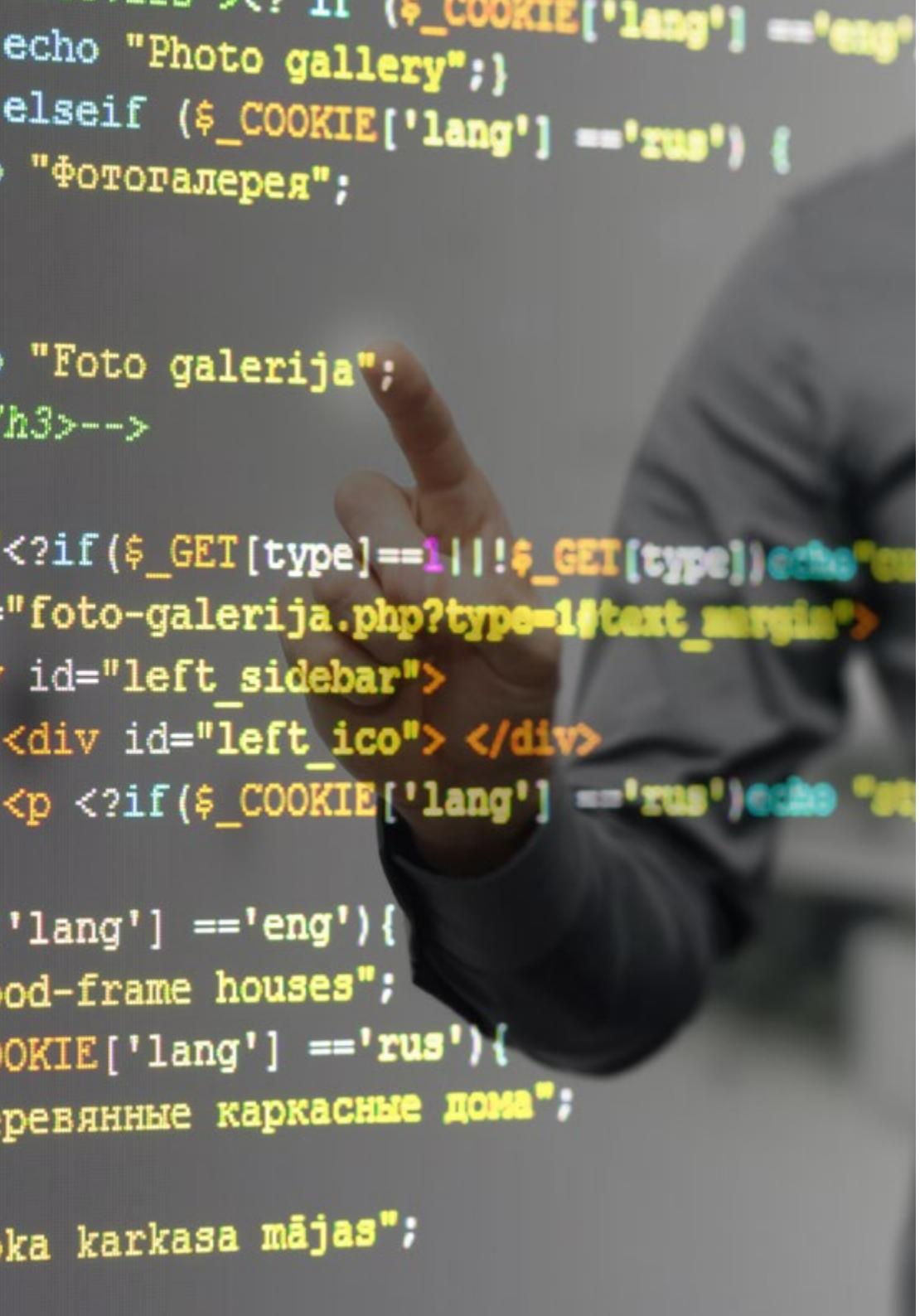
9.7. Cloud Forensics
- 9.7.1. Types of Crimes in the Cloud
  - 9.7.1.1. Cloud as Subject
  - 9.7.1.2. Cloud as an Object
  - 9.7.1.3. Cloud as a Tool
- 9.7.2. Challenges of Cloud Forensics
- 9.7.3. Research on Cloud Storage Services
- 9.7.4. Forensic Analysis Tools for Cloud

9.8. Investigation of Email Crimes
- 9.8.1. Mailing Systems
  - 9.8.1.1. Mail Clients
  - 9.8.1.2. Mail Server
  - 9.8.1.3. SMTP Server
  - 9.8.1.4. POP3 Server
  - 9.8.1.5. IMAP4 Server

9.8.2. Mailing Crimes
9.8.3. Mail Message
9.8.3.1. Standard Headers
9.8.3.2. Extended Headers
9.8.4. Steps for the Investigation of these Crimes
9.8.5. E-Mail Forensic Tools
9.9. Mobile Forensic Analysis
9.9.1. Cellular Networks
9.9.1.1. Types of Networks
9.9.1.2. CDR Contents
9.9.2. Subscriber Identity Module (SIM)
9.9.3. Logical Acquisition
9.9.4. Physical Acquisition
9.9.5. File System Acquisition
9.10. Forensic Report Writing and Reporting
9.10.1. Important Aspects of a Forensic Report
9.10.2. Classification and Types of Reports
9.10.3. Guide to Writing a Report
9.10.4. Presentation of the Report
9.10.4.1. Prior Preparation for Testifying
9.10.4.2. Deposition
9.10.4.3. Dealing with the Media

Module 10. Current and Future IT Security Challenges

10.1. Blockchain Technology
10.1.1. Scope of Application
10.1.2. Confidentiality Guarantee
10.1.3. Non-Repudiation Guarantee
10.2. Digital Money
10.2.1. Bitcoins
10.2.2. Cryptocurrencies
10.2.3. Cryptocurrency Mining
10.2.4. Pyramid Schemes
10.2.5. Other Potential Crimes and Problems
10.3. Deepfake
10.3.1. Media Impact
10.3.2. Dangers to Society
10.3.3. Detection Mechanisms
10.4. The Future of Artificial Intelligence
10.4.1. Artificial Intelligence and Cognitive Computing
10.4.2. Uses to Simplify Customer Service
10.5. Digital Privacy
10.5.1. Value of Data in the Network
10.5.2. Use of Data in the Network
10.5.3. Privacy and Digital Identity Management
10.6. Cyberconflicts, Cybercriminals and Cyberattacks
10.6.1. The Impact of Cybersecurity on International Conflicts
10.6.2. Consequences of Cyber-attacks on the General Population.
10.6.3. Types of Cybercriminals. Protective Measures
10.7. Telework
10.7.1. Telework Revolution During and After COVID-19
10.7.2. Access Bottlenecks
10.7.3. Variation of the Attacking Surface
10.7.4. Workers' Needs
10.8. Emerging Wireless Technologies
10.8.1. WPA3
10.8.2. 5G
10.8.3. Millimeter Waves
10.8.4. Trend in "Get Smart" instead of "Get more"



10.9. Future Addressing in Networks
- 10.9.1. Current Problems with IP Addressing
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Advantages of IPv4+ Over IPv4
- 10.9.5. Advantages of IPv6 Over IPv4

10.10. The Challenge of Raising Awareness of Early and Continuing Education in the Population
- 10.10.1. Current Government Strategies
- 10.10.2. Resistance of the Population to Learning
- 10.10.3. Training Plans to be Adopted by Companies

TECH has prepared a series of contents that make a global review of all the units that influence Cybersecurity Management (Chief Information Security Officer)"

06

Methodology

This academic program offers students a different way of learning. Our methodology uses a cyclical learning approach: **Relearning.**

This teaching system is used, for example, in the most prestigious medical schools in the world, and major publications such as the **New England Journal of Medicine** have considered it to be one of the most effective.

Discover Relearning, a system that abandons conventional linear learning, to take you through cyclical teaching systems: a way of learning that has proven to be extremely effective, especially in subjects that require memorization"

Case Study to contextualize all content

Our program offers a revolutionary approach to developing skills and knowledge. Our goal is to strengthen skills in a changing, competitive, and highly demanding environment.

At TECH, you will experience a learning methodology that is shaking the foundations of traditional universities around the world"

You will have access to a learning system based on repetition, with natural and progressive teaching throughout the entire syllabus.

The student will learn to solve complex situations in real business environments through collaborative activities and real cases.

A learning method that is different and innovative

This TECH program is an intensive educational program, created from scratch, which presents the most demanding challenges and decisions in this field, both nationally and internationally. This methodology promotes personal and professional growth, representing a significant step towards success. The case method, a technique that lays the foundation for this content, ensures that the most current economic, social and professional reality is taken into account.

> *Our program prepares you to face new challenges in uncertain environments and achieve success in your career"*

The case method has been the most widely used learning system among the world's leading Information Technology schools for as long as they have existed. The case method was developed in 1912 so that law students would not only learn the law based on theoretical content. It consisted of presenting students with real-life, complex situations for them to make informed decisions and value judgments on how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

What should a professional do in a given situation? This is the question that you are presented with in the case method, an action-oriented learning method. Throughout the course, students will be presented with multiple real cases. They will have to combine all their knowledge and research, and argue and defend their ideas and decisions.

Relearning Methodology

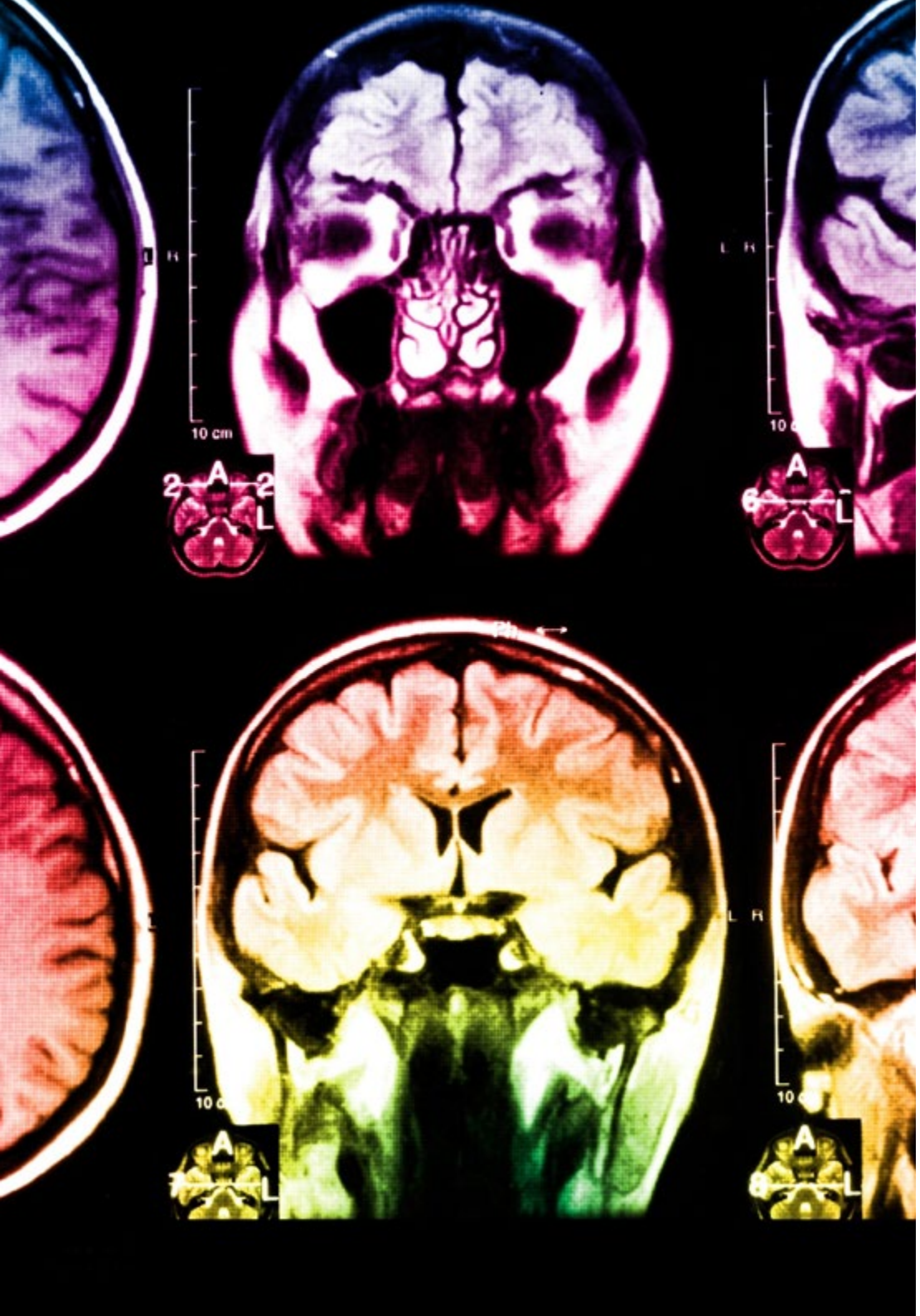
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

We enhance the Case Study with the best 100% online teaching method: Relearning.

In 2019, we obtained the best learning results of all online universities in the world.

At TECH you will learn using a cutting-edge methodology designed to train the executives of the future. This method, at the forefront of international teaching, is called Relearning.

Our university is the only one in the world authorized to employ this successful method. In 2019, we managed to improve our students' overall satisfaction levels (teaching quality, quality of materials, course structure, objectives...) based on the best online university indicators.



In our program, learning is not a linear process, but rather a spiral (learn, unlearn, forget, and re-learn). Therefore, we combine each of these elements concentrically. This methodology has trained more than 650,000 university graduates with unprecedented success in fields as diverse as biochemistry, genetics, surgery, international law, management skills, sports science, philosophy, law, engineering, journalism, history, and financial markets and instruments. All this in a highly demanding environment, where the students have a strong socio-economic profile and an average age of 43.5 years.

Relearning will allow you to learn with less effort and better performance, involving you more in your training, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation for success.

From the latest scientific evidence in the field of neuroscience, not only do we know how to organize information, ideas, images and memories, but we know that the place and context where we have learned something is fundamental for us to be able to remember it and store it in the hippocampus, to retain it in our long-term memory.

In this way, and in what is called neurocognitive context-dependent e-learning, the different elements in our program are connected to the context where the individual carries out their professional activity.

This program offers the best educational material, prepared with professionals in mind:

Study Material

All teaching material is produced by the specialists who teach the course, specifically for the course, so that the teaching content is highly specific and precise.

These contents are then applied to the audiovisual format, to create the TECH online working method. All this, with the latest techniques that offer high quality pieces in each and every one of the materials that are made available to the student.

Classes

There is scientific evidence suggesting that observing third-party experts can be useful.

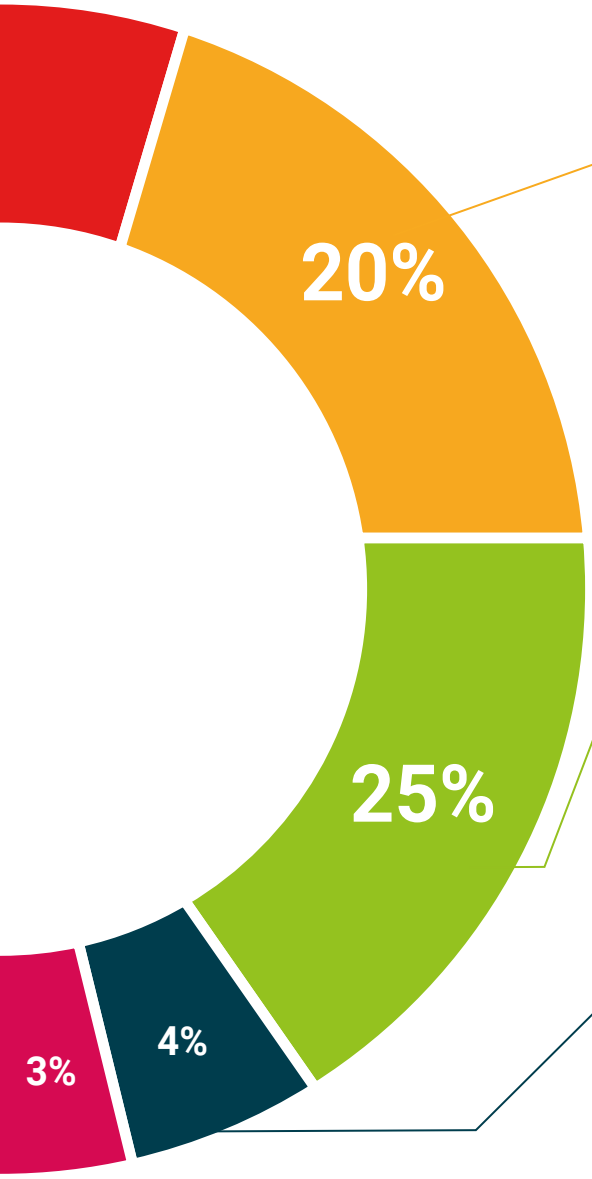
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

Practising Skills and Abilities

They will carry out activities to develop specific skills and abilities in each subject area. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop in the context of the globalization that we are experiencing.

Additional Reading

Recent articles, consensus documents and international guidelines, among others. In TECH's virtual library, students will have access to everything they need to complete their course.



Case Studies

Students will complete a selection of the best case studies chosen specifically for this program. Cases that are presented, analyzed, and supervised by the best specialists in the world.

Interactive Summaries

The TECH team presents the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

This exclusive educational system for presenting multimedia content was awarded by Microsoft as a "European Success Story".

Testing & Retesting

We periodically evaluate and re-evaluate students' knowledge throughout the program, through assessment and self-assessment activities and exercises, so that they can see how they are achieving their goals.

07

Certificate

The Professional Master's Degree in Cybersecurity Management (Chief Information Security Officer) guarantees students, in addition to the most rigorous and up-to-date education, access to a Professional Master's Degree issued by TECH Global University.

Successfully complete this program and receive your university qualification without having to travel or fill out laborious paperwork"

This program will allow you to obtain your **Professional Master's Degree diploma in Cybersecurity Management (CISO, Chief Information Security Officer)** endorsed by **TECH Global University**, the world's largest online university.

TECH Global University is an official European University publicly recognized by the Government of Andorra (***official bulletin***). Andorra is part of the European Higher Education Area (EHEA) since 2003. The EHEA is an initiative promoted by the European Union that aims to organize the international training framework and harmonize the higher education systems of the member countries of this space. The project promotes common values, the implementation of collaborative tools and strengthening its quality assurance mechanisms to enhance collaboration and mobility among students, researchers and academics.

This **TECH Global University** title is a European program of continuing education and professional updating that guarantees the acquisition of competencies in its area of knowledge, providing a high curricular value to the student who completes the program.

Title: **Professional Master's Degree in Cybersecurity Management (CISO, Chief Information Security Officer)**

Modality: **online**

Duration: **12 months**

Accreditation: **60 ECTS**


tech global university

Mr./Ms. _____, with identification document _____
has successfully passed and obtained the title of:

Professional Master's Degree in Cybersecurity Management (CISO, Chief Information Security Officer)

This is a program of 1,500 hours of duration equivalent to 60 ECTS, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH Global University is a university officially recognized by the Government of Andorra on the 31st of January of 2024, which belongs to the European Higher Education Area (EHEA).

In Andorra la Vella, on the 28th of February of 2024

Dr. Pedro Navarro Illana
Rector

Unique TECH Code: AFWORD23S techtitute.com/certificates


Professional Master's Degree in Cybersecurity Management
(CISO, Chief Information Security Officer)

General Structure of the Syllabus

Subject type	ECTS
Compulsory (CO)	60
Optional (OP)	0
External Work Placement (WP)	0
Master's Degree Thesis (MDT)	0
	Total 60

General Structure of the Syllabus

Year	Subject	ECTS	Type
1º	Cyberintelligence and Cybersecurity	6	CO
1º	Host Security	6	CO
1º	Network Security (Perimeter)	6	CO
1º	Smartphone Security	6	CO
1º	IoT Security	6	CO
1º	Ethical Hacking	6	CO
1º	Inverse Engineering	6	CO
1º	Secure Development	6	CO
1º	Forensic Analysis	6	CO
1º	Current and Future IT Security Challenges	6	CO

Dr. Pedro Navarro Illana
Rector

tech global university

*Apostille Convention. In the event that the student wishes to have their paper diploma issued with an apostille, TECH Global University will make the necessary arrangements to obtain it, at an additional cost.

tech global university

Professional Master's Degree

Cybersecurity Management (CISO, Chief Information Security Officer)

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Global University**
- Credits: **60 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

Professional Master's Degree

Cybersecurity Management (CISO, Chief Information Security Officer)

tech global university