Executive Master's Degree

Cybersecurity Management (CISO, Chief Information Security Officer)

MCNVDAAAA

tech technological university

tech technological university

Executive Master's Degree

Cybersecurity Management (CISO, Chief Information Security Officer)

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Website: **www.techtitute.com/in/school-of-business/professional-master-degree/master-cybersecurity-management-ciso-chief-information-security-officer**

Index

01 Welcome — p. 4

02 Why Study at TECH? — p. 6

03 Why Our Program? — p. 10

04 Objectives — p. 14

05 Skills — p. 20

06 Structure and Content — p. 26

07 Methodology — p. 38

08 Our Students' Profiles — p. 46

09 Course Management — p. 50

10 Impact on Your Career — p. 58

11 Benefits for Your Company — p. 62

12 Certificate — p. 66

01

Welcome

Modern society is hyperconnected. The information age allows citizens to access any piece of data at the click of a button. But this has also meant that digital threats are the order of the day, so companies are more at risk than ever of receiving malicious software that damages their production and security, or even exposes customer and employee personal data, in turn exposing their IT weaknesses. Although protection in this area is the job of IT specialists, more and more Chief Revenue Officers and other managers are deciding to specialize in this field in order to try to stop cybercriminals and avoid being the target of their attacks. For all those reasons, TECH has created this program for business professionals to have access to the most relevant information available, through a syllabus that will be easy for students to understand.

Executive Master's Degree in Cybersecurity Management (CISO Chief Information Security Officer). TECH Technological University

Specializing in cybersecurity will give you the opportunity to improve your management skills and position yourself as Chief Information Security Officer in large companies"

02

Why Study at TECH?

TECH is the world's largest 100% online business school. It is an elite business school, with a model based on the highest academic standards. A world-class centre for intensive managerial skills training.

TECH is a university at the forefront of technology, and puts all its resources at the student's disposal to help them achieve entrepreneurial success"

At TECH Technological University

Innovation

The university offers an online learning model that combines the latest educational technology with the most rigorous teaching methods. A unique method with the highest international recognition that will provide students with the keys to develop in a rapidly-evolving world, where innovation must be every entrepreneur's focus.

"Microsoft Europe Success Story", for integrating the innovative, interactive multi-video system.

The Highest Standards

Admissions criteria at TECH are not economic. Students don't need to make a large investment to study at this university. However, in order to obtain a qualification from TECH, the student's intelligence and ability will be tested to their limits. The institution's academic standards are exceptionally high...

95% | **of TECH students successfully complete their studies**

Networking

Professionals from countries all over the world attend TECH, allowing students to establish a large network of contacts that may prove useful to them in the future.

100,000+
executives trained each year

200+
different nationalities

Empowerment

Students will grow hand in hand with the best companies and highly regarded and influential professionals. TECH has developed strategic partnerships and a valuable network of contacts with major economic players in 7 continents.

500+ | **collaborative agreements with leading companies**

Talent

This program is a unique initiative to allow students to showcase their talent in the business world. An opportunity that will allow them to voice their concerns and share their business vision.

After completing this program, TECH helps students show the world their talent.

Multicultural Context

While studying at TECH, students will enjoy a unique experience. Study in a multicultural context. In a program with a global vision, through which students can learn about the operating methods in different parts of the world, and gather the latest information that best adapts to their business idea.

TECH students represent more than 200 different nationalities.

Learn with the best

In the classroom, TECH's teaching staff discuss how they have achieved success in their companies, working in a real, lively, and dynamic context. Teachers who are fully committed to offering a quality specialization that will allow students to advance in their career and stand out in the business world.

Teachers representing 20 different nationalities.

"At TECH, you will have access to the most rigorous and up-to-date case studies in the academic community"

TECH strives for excellence and, to this end, boasts a series of characteristics that make this university unique:

Analysis

TECH explores the student's critical side, their ability to question things, their problem-solving skills, as well as their interpersonal skills.

Academic Excellence

TECH offers students the best online learning methodology. The university combines the Relearning method (a postgraduate learning methodology with the highest international rating) with the Case Study. A complex balance between tradition and state-of-the-art, within the context of the most demanding academic itinerary.

Economy of Scale

TECH is the world's largest online university. It currently boasts a portfolio of more than 10,000 university postgraduate programs. And in today's new economy, **volume + technology = a ground-breaking price**. This way, TECH ensures that studying is not as expensive for students as it would be at another university.

03

Why Our Program?

Studying this TECH program means increasing the chances of achieving professional success in senior business management.

It is a challenge that demands effort and dedication, but it opens the door to a promising future. Students will learn from the best teaching staff and with the most flexible and innovative educational methodology.

We have highly qualified teachers and the most complete syllabus on the market, which allows us to offer you training of the highest academic level"

This program will provide students with a multitude of professional and personal advantages, particularly the following:

01

A significant career boost

By studying at TECH, students will be able to take control of their future and develop their full potential. By completing this program, students will acquire the skills required to make a positive change in their career in a short period of time.

70% of participants achieve positive career development in less than 2 years.

02

Develop a strategic and global vision of companies

TECH offers an in-depth overview of general management to understand how each decision affects each of the company's different functional areas.

Our global vision of companies will improve your strategic vision.

03

Consolidate the student's senior management skills

Studying at TECH means opening the doors to a wide range of professional opportunities for students to position themselves as senior executives, with a broad vision of the international environment.

You will work on more than 100 real senior management cases.

04

Take on new responsibilities

The program will cover the latest trends, advances and strategies, so that students can carry out their professional work in a changing environment.

45% of graduates are promoted internally.

05

Access to a powerful network of contacts

TECH connects its students to maximize opportunities. Students with the same concerns and desire to grow. Therefore, partnerships, customers or suppliers can be shared.

You will find a network of contacts that will be instrumental for professional development.

06

Thoroughly develop business projects

Students will acquire a deep strategic vision that will help them develop their own project, taking into account the different areas in companies.

20% of our students develop their own business idea.

07

Improve soft skills and management skills

TECH helps students apply and develop the knowledge they have acquired, while improving their interpersonal skills in order to become leaders who make a difference.

Improve your communication and leadership skills and enhance your career.

08

Be part of an exclusive community

Students will be part of a community of elite executives, large companies, renowned institutions, and qualified professors from the most prestigious universities in the world: the TECH Technological University community.

We give you the opportunity to train with a team of world renowned teachers.

04

Objectives

This TECH Executive Master's Degree has been designed to strengthen the professional skills of business executives, who, in addition to being widely specialized in their area of activity, will find in this program a unique opportunity to improve in a highly relevant field, since they will learn to prevent potential Internet threats that can cause serious damage to businesses. This way, they will become professional experts in different branches, so they will be able to protect all areas of the company from cyberattacks, thereby becoming a Chief Information Security Officer.

Increase your training and achieve your work objectives thanks to the superior training offered by TECH with this Executive Master's Degree"

Your goals are our goals.
We work together to help you achieve them.

This **Executive Master's Degree in Cybersecurity Management (CISO, Chief Information Security Officer)** trains students to:

01 Analyze the role played by cybersecurity analysts

02 Study social engineering and its methods in depth

03 Explore the OSINT, HUMINT, OWASP, PTEC OSSTM, OWISAM methodologies

04 Become familiar with risk metrics and conduct risk analyses

05 Determine the appropriate use of anonymity and networks such as TOR, I2P and Freenet

06 Compile the current regulations on cyber security

07 Generate specialized knowledge to perform security audits

08 Develop appropriate usage policies

09 Examine the most important threat prevention and detection systems

10 Assess new threat detection systems and their evolution from more traditional solutions

11 Analyze the main mobile platforms today, features and use

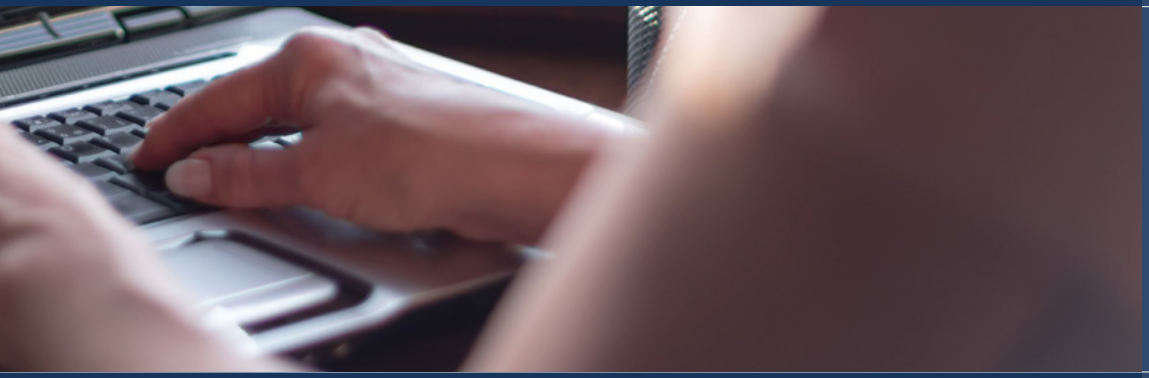
12 Identify, analyze and assess security risks involved in IoT project parts

13 Assess the information obtained and develop prevention and hacking mechanisms

14 Apply reverse engineering to cybersecurity environments

15 Specify the tests to be carried out on the software developed

16 Collect all the existing evidence and data to carry out forensic reports



17 Duly submit forensic reports

18 Analyze the current and future state of computer security

19 Examine the risks of new emerging technologies

20 Compile various technologies in relation to IT security

05

Skills

This Executive Master's Degree in Cybersecurity Management (CISO, Chief Information Security Officer) has been designed to improve the competitiveness of professionals in the business sector. Upon completing the program, students will have acquired the skills required to perform quality and up-to-date work based on the most innovative teaching methodology. Undoubtedly, a program that will improve their training and will allow them to be more competitive in their daily work, by unifying all the relevant safety aspects of computer security that managers must know and put into practice.

Delve into the study of computer security and improve your skills to protect from potential network threats”

01 Become familiar with the methodologies used in cybersecurity

02 Assess each type of threat in order to offer an optimal solution in each case

03 Generate comprehensive intelligent solutions to automate behaviors in case of incidents

04 Assess the risks associated with vulnerabilities both internal and external to the enterprise

05 Understand the evolution and impact of IoT over time

06 Test system vulnerability, attack it for preventive purposes and solve the problems that arise

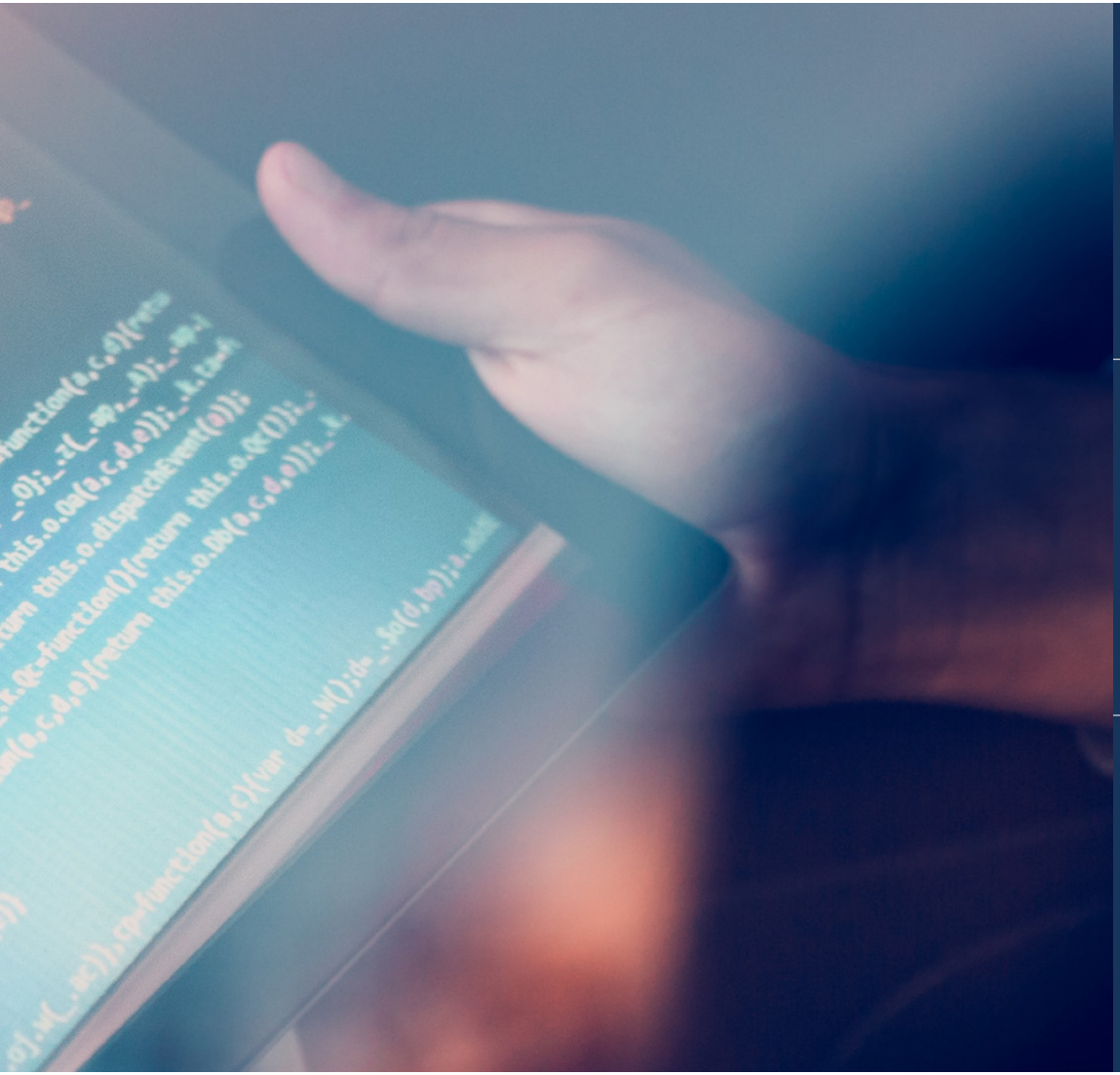
07 Know how to apply Sandboxing in different environments

08 Know the guidelines that a good developer must follow to comply with security requirements

09 Conduct defensive security operations

10 Have a deep and specialized understanding of computer security

11 Apply security processes for smartphones and handheld devices



12 Identify the means to perform so-called ethical Hacking to protect a company from cyberattacks

13 Investigate cybersecurity incidents

14 Differentiate between existing attacks and defense techniques

06

Structure and Content

This TECH program has been designed to meet the specialization needs of business professionals who wish to expand their knowledge of computer security, a fundamental qualification to protect from potential threats that can pose great risks to any company. Therefore, this Executive Master's Degree will allow them to acquire specific knowledge that they can apply to their work practice. And, to do so, they will use a totally online methodology so they can balance their studies with the rest of their daily obligations.

This program will be essential to detect possible cyberattacks on your company"

Syllabus

The TECH Executive Master's Degree in Cybersecurity Management (CISO, Chief Information Security Officer) is an intensive program that prepares students to face challenges and business decisions in computer security. Its content is designed to promote the development of managerial skills that enable more rigorous decision-making in uncertain environments.

Throughout 1,500 hours of study, you will analyze a multitude of practical cases through individual work, which will allow you to acquire the necessary skills to develop successfully in your daily practice. It is, therefore, an authentic immersion in real business situations.

This program deals with the different areas of a company in depth, and it is designed for managers to understand cybersecurity from a strategic, international and innovative perspective.

A plan designed for students, focused on their professional development, which prepares them to achieve excellence in the field of computer security management and administration. A program that understands your needs and those of your company through innovative content based on the latest trends, and supported by the best educational methodology and an exceptional faculty, which will provide you with the competencies to solve critical situations in a creative and efficient way.

This Executive Master's Degree takes place over 12 months and is divided into 10 modules:

Module 1	Cyberintelligence and Cybersecurity
Module 2	Host Security
Module 3	Network Security (Perimeter)
Module 4	Smartphones Security
Module 5	IoT Security
Module 6	Ethical Hacking
Module 7	Inverse Engineering
Module 8	Secure Development
Module 9	Forensic Analysis
Module 10	Current and Future Challenges in Computer Security

Where, When and How is it Taught?

TECH offers the possibility of developing this Executive Master's Degree in Cybersecurity Management (CISO , Chief Information Security Officer) completely online. Over the course of 12 months, you will be able to access all the contents of this program at any time, allowing you to self-manage your study time.

A unique, key and decisive educational experience to boost your professional development and make the definitive leap.

Module 1. Cyberintelligence and Cybersecurity

1.1. Cyberintelligence
1.1.1. Cyberintelligence
1.1.2. Intelligence Analysts

1.2. Cybersecurity
1.2.1. Security Layers
1.2.2. Identifying Cyber Threats
1.2.3. Adverse Actions

1.3. Intelligence Techniques and Tools
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. OWISAP
1.3.7. PTES
1.3.8. OSSTM

1.4. Evaluation Methodologies
1.4.1. Intelligence Analyses
1.4.2. Techniques to Organize Acquired Information
1.4.3. Reliability and Credibility of Information Sources
1.4.4. Analysis Methodologies
1.4.5. Presenting Intelligence Results

1.5. Audits and Documentation
1.5.1. Computer Security Auditing
1.5.2. Auditing Documentation and Permissions
1.5.3. Types of Audits
1.5.4. Deliverables

1.6. Online Anonymity
1.6.1. Anonymity Use
1.6.2. Anonymity Techniques (Proxy, VPNs)
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. Mobile Device Security

1.8. Regulations and Compliance
1.8.1. GDPR
1.8.3. ISO/IEC 27000-Series
1.8.4. NIST Cybersecurity Framework
1.8.5. PIC 9
1.8.6. ISO 27032
1.8.7. *Cloud* Regulations
1.8.8. SOX
1.8.9. PCI

1.9. Risk Analysis and Metrics
1.9.1. Extent of the Risks
1.9.2. Assets
1.9.3. Threats
1.9.4. Vulnerabilities
1.9.5. Risk Assessment
1.9.6. Risk Treatment

1.10. Relevant Cybersecurity Agencies
1.10.1. NIST
1.10.4. OEA
1.10.5. 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 Antiviruses
2.2.1. Types of Antiviruses
2.2.2. Antiviruses for Windows
2.2.3. Antiviruses for Linux
2.2.4. Antiviruses for MacOS
2.2.5. Antivirus for Smartphones

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

2.4. Local Firewalls
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. StickyPassword
2.5.5. RoboForm

2.6. Phishing Detection
2.6.1. Manual Phishing Detection
2.6.2. Antiphishing Tools

2.7. Spyware
2.7.1. Avoidance Mechanisms
2.7.2. Antispyware Tools

2.8. Trackers
2.8.1. System Protection Measures
2.8.2. Anti-Tracking Tools

2.9. Endpoint Detection and Response (EDR)
2.9.1. EDR System Behavior
2.9.2. Differences between EDRs and Antiviruses
2.9.3. The Future of EDR Systems

2.10. Control over Software Installations
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 Prevention and Detection Systems
3.1.1. General Framework for Security Incidents
3.1.2. Current Defense Systems: Defense in Depth and SOC
3.1.3. Current Network Architectures
3.1.4. Types of Incident Prevention and Detection Tools
3.1.5. Instance/Hosts, Container and Serverless Communication and Detection

3.2. Firewalls
3.2.1. Types of Firewalls
3.2.2. Attacks and Mitigation
3.2.3. Common Firewalls in the Linux Kernel
3.2.4. Log-Based Detection Systems

3.3. Intrusion Prevention and Detection Systems (IDS/ IPS)
3.3.1. Attacks on IDS/IPS
3.3.2. IDS/IPS Systems

3.4. Next Generation Firewalls (NGFW)
3.4.1. Differences between NGFW and Traditional Firewall
3.4.2. Main Capabilities
3.4.3. Business Solutions
3.4.4. Firewalls for Cloud Services

3.5. Proxy
3.5.1. Types of Proxy
3.5.2. Proxy Use: Advantages and Disadvantages

3.6. Antivirus Engines
3.6.1. General Context of Malware and IOCS
3.6.2. Problems with Antivirus Engines

3.7. Email Protection Systems
3.7.1. Antispam
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 in SIEM Systems

3.9. SOAR
3.9.1. SOAR and SIEM: Friends or Foes
3.9.2. The Future of SOAR Systems

3.10. Other 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 Projects
4.2.2. Communications, Networks and Connections

4.3. Mobile Devices in Business Environments
4.3.1. Risks
4.3.2. Security Policies
4.3.3. Device Monitoring
4.3.4. Mobile Device Management (MDM)

4.4. User Privacy and Data Security
4.4.1. Information Status
4.4.3. Secure Data Storage
4.4.4. Best Practices in Application Development

4.5. Vulnerabilities and Attack Vectors
4.5.1. Vulnerabilities
4.5.2. Attack Vectors

4.6. Main Threats
4.6.1. Untrained Users
4.6.2. 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. Weak Passwords
4.6.10. Weak or Non-Existent Security Settings
4.6.11. Physical Access
4.6.12. Device Loss or Theft
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 Methods
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
4.8.3. Hacking iOS Devices: Mechanisms and Tools
4.8.4. Hacking 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. Protection and Security
4.10.1. Security Settings
4.10.2. Security Measures
4.10.3. Protection Tools

Module 5. IoT Security

5.1. Devices
5.1.1. Types of Devices
5.1.2. Standardized Architectures
5.1.3. Application Protocols
5.1.4. Connectivity Technologies

5.2. IoT Devices: Application Areas
5.2.1. Smart Home
5.2.2. Smart City
5.2.3. Transport
5.2.4. Wearables
5.2.5. Healthcare Sector
5.2.6. Industrial Internet of Things (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. Smart Home
5.4.1. Home Automation
5.4.2. Networks
5.4.3. Household Appliances
5.4.4. Surveillance and Security

5.5. Smart City
5.5.1. Lighting
5.5.2. Meteorology
5.5.3. Security

5.6. Transport
5.6.1. Localization
5.6.2. Making Payments and Obtaining Services
5.6.3. Connectivity

5.7. Wearables
5.7.1. Smart Clothes
5.7.2. Smart Jewels
5.7.3. Smart Watches

5.8. Healthcare Sector
5.8.1. Exercise/Heart Rate Monitoring
5.8.2. Monitoring Patients and Elderly People
5.8.3. Implantation
5.8.4. Surgical Robots

5.9. Connectivity
5.9.1. Wi-Fi/Gateway
5.9.2. Bluetooth
5.9.3. Built-In Connectivity

5.10. Securization
5.10.1. Dedicated Networks
5.10.2. Password Managers
5.10.3. Use of Encrypted Protocols
5.10.4. Application Tips

Module 6. Ethical Hacking

6.1. Work Environment
6.1.1. Linux Distributions
6.1.2. Virtualization Systems
6.1.3. Sandboxes
6.1.4. Laboratory Deployment

6.2. Methods
6.2.1. OSSTM
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. Data Breach and Vulnerability Scanning
6.3.3. Use of Passive Tools

6.4. Network Scanning
6.4.1. Scanning Tools
6.4.2. Scanning Techniques
6.4.3. Firewall and IDS Avoidance Techniques
6.4.4. Banner Grabbing
6.4.5. Network Diagrams

6.5. Enumeration
6.5.1. SMTP Enumeration
6.5.2. DNS User 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
6.6.2. Vulnerability Scoring Systems

6.7. Attacks on Wireless Networks
6.7.1. Hacking Methodology in Wireless Networks
6.7.2. Wireless Security Tools

6.8. Web Server Hacking
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

6.10. Persistence
6.10.1. Installing Rootkits
6.10.2. Using Ncat
6.10.3. Use of Scheduled Tasks for Backdoors
6.10.4. Creating Users
6.10.5. HIDS Detection

Module 7. Reverse Engineering

7.1. Compilers
7.1.1. Types of Code
7.1.2. Compiler Phases
7.1.3. Symbol Table
7.1.4. Error Handler
7.1.5. GCC Compiler

7.2. Types of Compiler Analyses
7.2.1. Lexical Analysis
7.2.2. Syntactic Analysis
7.2.3. Semantic Analysis

7.3. Data Structures in Assemblers
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
7.4.2. Iteration Structures
7.4.3. Functions

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

7.6. ARM Hardware Architecture
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. Interactive Disassembler (IDA)
7.7.3. Code Reconstructors

7.8. Dynamic Code Analysis
7.8.1. Behavioral Analysis
7.8.2. Linux Code Debuggers
7.8.3. Windows Code Debuggers

7.9. Sandbox
7.9.1. Sandbox Architecture
7.9.2. Sandbox Avoidance
7.9.3. Detection Techniques
7.9.4. Avoidance Techniques
7.9.5. Countermeasures
7.9.6. Sandbox on Linux
7.9.7. Sandbox on 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
7.10.3. Malware Analysis Tools

Module 8. Secure Development

8.1. Secure Development
8.1.1. Quality, Functionality and Security
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. Roles and Privileges Control
8.2.3. Risk-Oriented Requirements
8.2.4. Privilege Approvals

8.3. Analysis and Design Phase
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. Adequate Error Handling
8.3.6. Separating Functions

8.4. Implementation and Coding Phase
8.4.1. Securing Development Environments
8.4.2. Preparing Technical Documentation
8.4.3. Secure Codification
8.4.4. Communications Security

8.5. Best Secure Coding Practices
8.5.1. Input Data Validation
8.5.2. Output Data Coding
8.5.3. Programming Styles
8.5.4. Changelog 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. Managing Users, Groups and Roles on Servers
8.6.2. Software Installation
8.6.3. Server Hardening
8.6.4. Robust Configuration of Application Environments

8.7. Preparing Databases and Hardening
8.7.1. Database Engine Optimization
8.7.2. Creating Personal User Accounts on Applications
8.7.3. Assigning Specific User Privileges
8.7.4. Database Hardening

8.8. Testing Phase
8.8.1. Quality Control in Security Controls
8.8.2. Code Inspection by Phases
8.8.3. Configuration Management Check
8.8.4. Black Box Testing

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

8.10. Maintenance Phase
8.10.1. Risk-Based Assurance
8.10.2. White Box Safety Maintenance Testing
8.10.3. Black Box Safety Maintenance Testing

Module 9. Forensic Analysis

9.1. Data Acquisition and Duplication
9.1.1. Volatile Data Acquisition
9.1.2. Static Data Acquisition
9.1.3. Methods to Validate Acquired Data

9.2. Anti-Forensic Techniques Assessment and Defeat
9.2.1. Anti-Forensic Techniques Objectives
9.2.2. Data Erasure
9.2.3. Password Protection
9.2.4. Steganography
9.2.5. Secure Device Wiping
9.2.6. Encryption

9.3. Operating System Forensic Analysis
9.3.1. Windows Forensic Analysis
9.3.2. Linux Forensics
9.3.3. Mac and iOS Forensic Analysis

9.4. Network Forensics
9.4.1. Log Analysis
9.4.2. Data Correlation
9.4.3. Network Investigation
9.4.4. Steps in Network Forensics

9.5. Web Forensics
9.5.1. Web Attack Investigations
9.5.2. Attack Detection
9.5.3. IP Address Localization

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

9.7. *Cloud* Forensic Analysis
9.7.1. Types of Crimes on the Cloud
9.7.2. Challenges in Forensic Analysis on the Cloud
9.7.3. Researching Storage Services on the Cloud
9.7.4. Forensic Analysis Tools for the Cloud

9.8. E-Mail Crime Investigation
9.8.1. E-Mail Systems
9.8.2. E-Mail Crimes
9.8.3. E-Mail Messages
9.8.4. Steps in the Investigation of these Crimes
9.8.5. Forensic Tools for E-Mail

9.9. Mobile Forensic Analysis
9.9.1. Cellular Networks
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 Drafting and Submission
9.10.1. Important Aspects of Forensic Reports
9.10.2. Classification and Types of Reports
9.10.3. Guide to Draft a Report
9.10.4. Report Submission

Module 10. Current and Future Challenges in Computer Security

10.1. Technology Blockchain
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. Deepfakes
10.3.1. Impact in the Media
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. Data Value on the Network
10.5.2. Data Use on 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 Cyberattacks on the General Population
10.6.3. Types of Cybercriminals: Protection Measures

10.7. Remote Work
10.7.1. Remote Work Revolution during and post COVID-19
10.7.2. Access Bottlenecks
10.7.3. Attack Surface Variation
10.7.4. Employee Needs

10.8. Emerging *Wireless* Technologies
10.8.1. WPA3
10.8.2. 5G
10.8.3. Millimeter Waves
10.8.4. Trend toward "Get Smart" Rather Than "Get More"

10.9. The Future of Network Addressing
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. Population Resistance to Learning
10.10.3. Training Plans for Companies

This program will open doors to a new professional world"

07

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"

TECH Business School uses the 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"

This program prepares you to face business challenges in uncertain environments and achieve business success.

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

A learning method that is different and innovative

This TECH program is an intensive educational program, created from scratch to present executives with challenges and business decisions at the highest level, whether at the national or international level. 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 business reality is taken into account.

> *You will learn, through collaborative activities and real cases, how to solve complex situations in real business environments"*

The case method has been the most widely used learning system among the world's leading business 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 we face in the case method, an action-oriented learning method. Throughout the program, the studies will be presented with multiple real cases. They must integrate all their knowledge, research, argue and defend their ideas and decisions.

Relearning Methodology

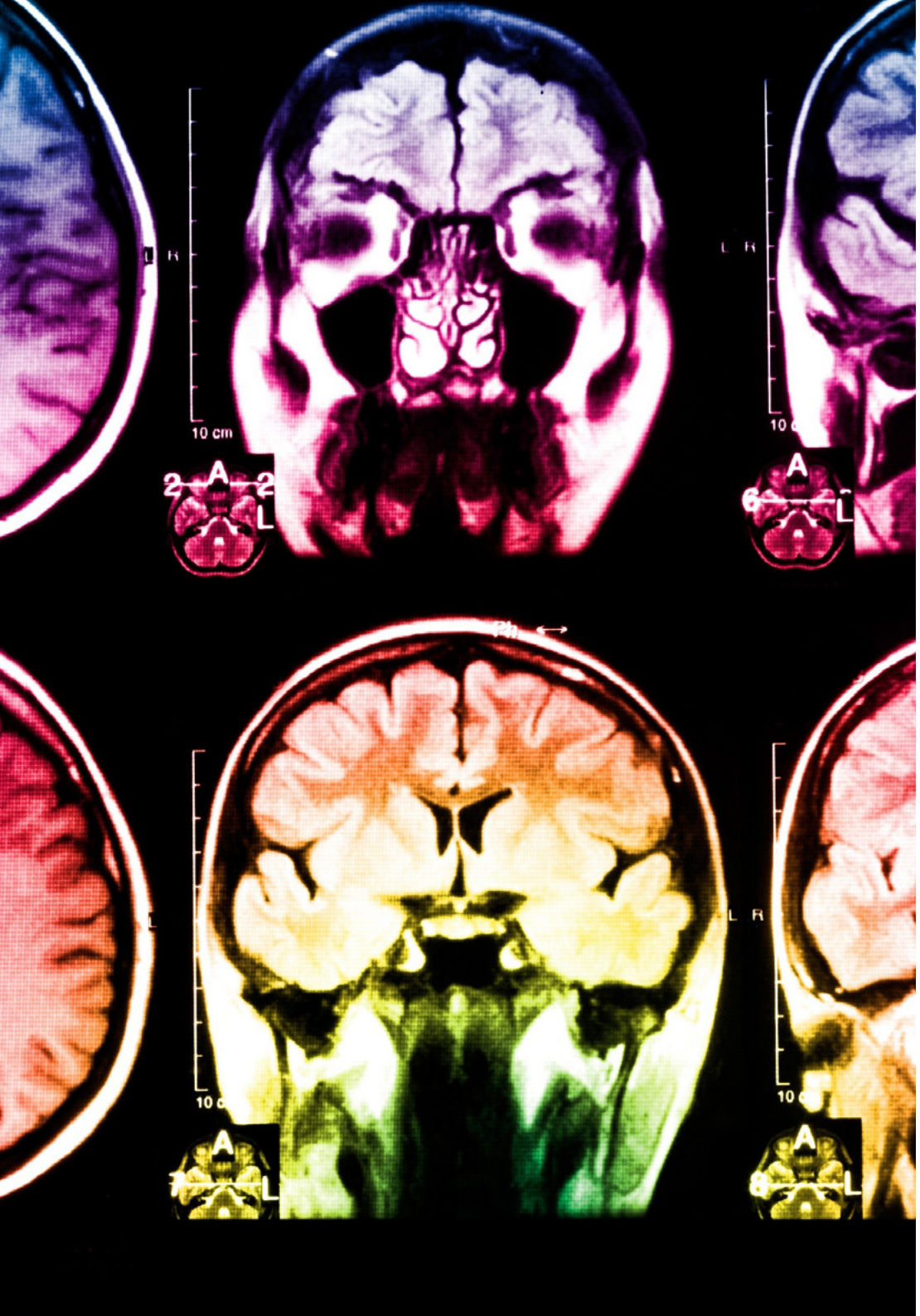
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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

Our online system will allow you to organize your time and learning pace, adapting it to your schedule. You will be able to access the contents from any device with an internet connection.

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 online business school is the only one in the world licensed to incorporate 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. With this methodology we have 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, markets, and financial 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 specialization, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation to 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.

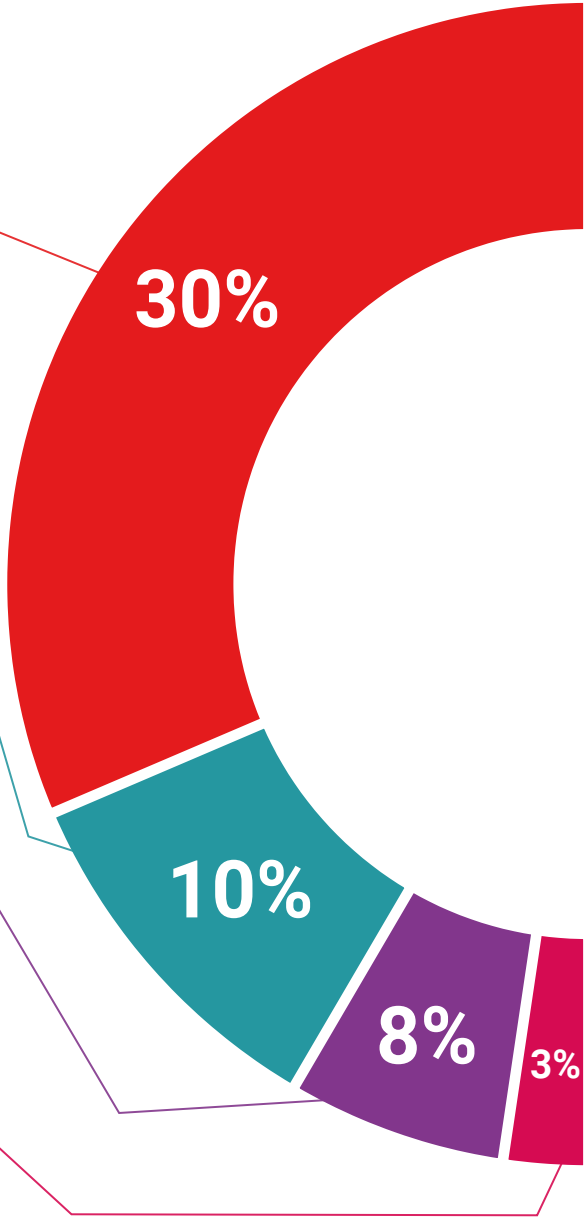
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

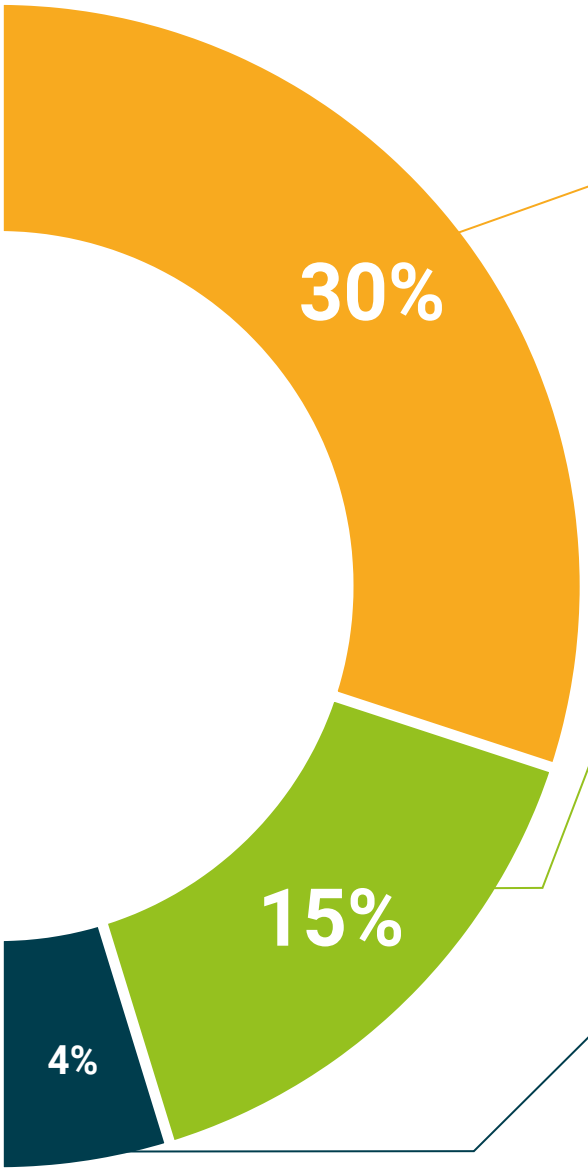
Management Skills Exercises

They will carry out activities to develop specific executive competencies in each thematic area. Practices and dynamics to acquire and develop the skills and abilities that a high-level manager needs to develop in the context of the globalization we live in.

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 senior management 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.

08

Our Students’ Profiles

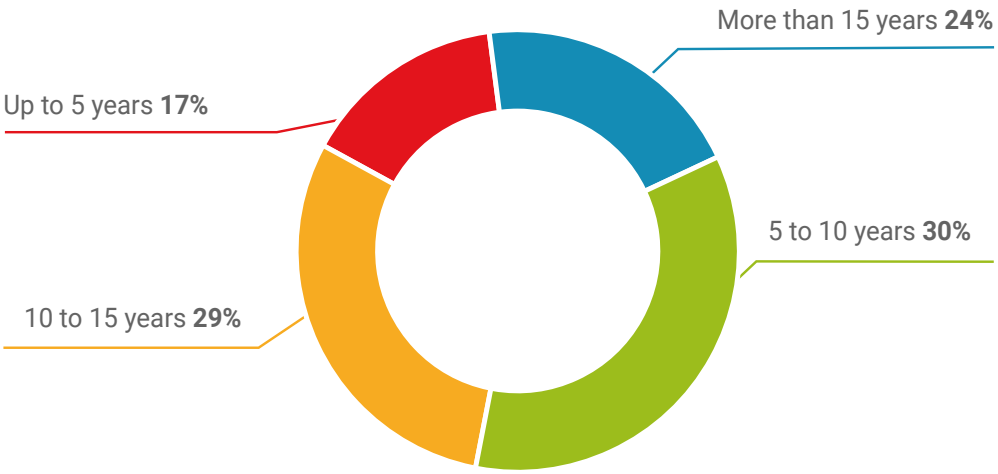
The Executive Master’s Degree in Cybersecurity Management (CISO, Chief Information Security Officer) is a program aimed at professionals who wish to improve their training through quality education. Students who want to broaden their knowledge in another business-related field such as IT, but more specifically, IT security. A program aimed at professionals with experience, but who believe in higher specialization as a way of improving on a personal and professional level.

TECH students are professionals with extensive experience who are looking for a better job"

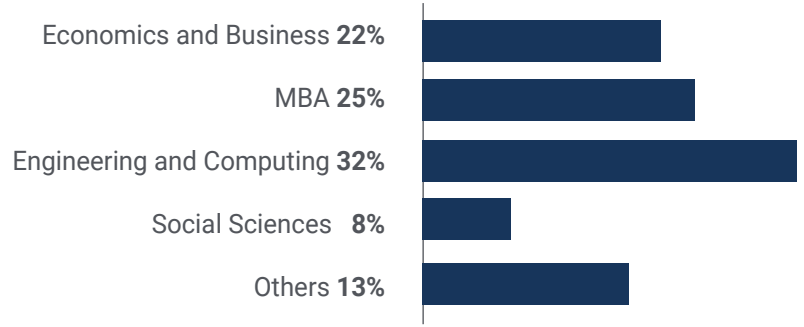
Average Age

Between **35** and **45** years old

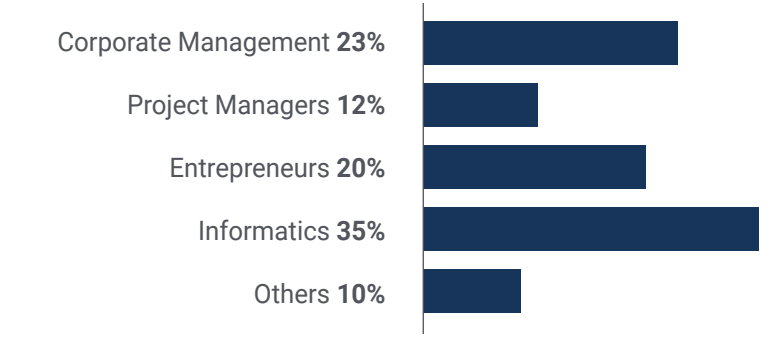
Years of Experience



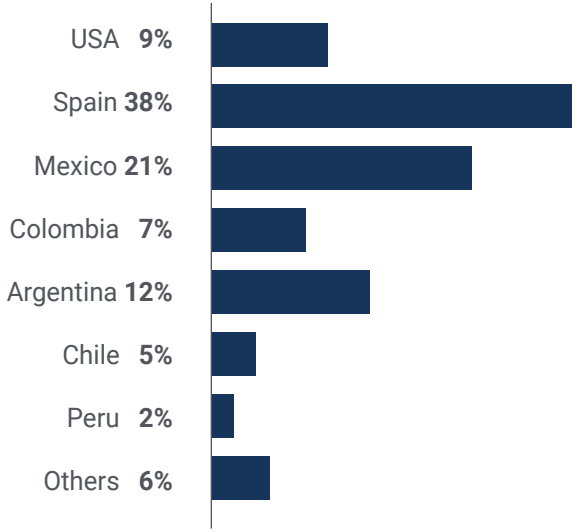
Training



Academic Profile



Geographical Distribution



Jaime Díaz

Chief Revenue Officer

"In the business environment I work in, we handle a large amount of confidential information and data that, in the wrong hands, could generate lead to serious problems for the company. For this reason, I had been thinking for some time about expanding my knowledge in cybersecurity, with the aim of learning how to safeguard all the processes that are susceptible to cyber-attacks. Thanks to this TECH program, I managed to improve my training and work more confidently"

09

Course Management

The professors on this Executive Master's Degree in Cybersecurity Management (CISO, Chief Information Security Officer) are professionals with extensive experience in the sector, both professionally and educationally. Their specialization in this field allows them to have the necessary qualifications to offer students a complete and high-quality study on subjects that will be useful in their daily work in the business environment. Undoubtedly, people who believe in higher education as a method to advance in their profession and improve the competitiveness of their business.

An experienced teaching staff to help you specialize in cybersecurity"

International Guest Director

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 National Reference Center of Getafe in Informatics and Telecommunications Madrid
- Certified E-Council Instructor Madrid
- Trainer in the following certifications: EXIN Ethical Hacking Foundation and EXIN Cyber & IT Security Foundation Madrid
- Accredited Expert Trainer, CAM; 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)
- External Collaborator CSO/SSA (Chief Security Officer/Senior Security Architect) University of the Balearic Islands
- IT Engineer Alcalá de Henares University. Madrid
- Master in DevOps: Docker and Kubernetes Cas-Training Madrid
- Microsoft Azure Security Techonologies E-Council Madrid

Professors

Mr. Catalá Barba, José Francisco

- Middle management in MINISDEF Different tasks and responsibilities within GOE III, such as internal network administration and incident management, customized program development in different areas, training courses for network users and group personnel in general
- Electronic Technician, Ford Factory located in Almusafes, Valencia, programming robots, PLC's, repair and maintenance
- Electronic Technician
- Application Developer 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 Telematic Engineering, Polytechnic University of Madrid
- Master's Degree in Cybersecurity and Ethical Hacking, CICE
- Advanced Course in Cybersecurity, Deusto Training

Ms. Marcos Sbarbaro, Victoria Alicia

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

Mr. Peralta Alonso, Jon

- Lawyer, DPO Altia Consultores S.A.
- Lecturer, 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 Counsel / Intern Professional Office: Oscar Padura
- Law Degree Public University of the Basque Country
- Master's Degree in Data Protection Delegate EIS Innovative School
- Master's Degree in Law Public University of the Basque Country
- Master's Degree in Civil Litigation Practice Isabel I of Castile International University

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 Grupo Zener, Castilla y León
- Telecommunications Equipment and Services Installer Lican Comunicaciones SL, Castilla y León
- Certified in Computer Security CFTIC Getafe, Madrid
- Senior Technician: Telecommunications and Computer Systems IES Trinidad Arroyo High School, Palencia
- Senior Technician: MV and LV Electrotechnical Installations IES Trinidad Arroyo High School, Palencia
- Training in reverse engineering, stenography, encryption Incibe Hacker Academy (Incibe Talents)

TECH has carefully selected the teaching staff for this program so you can learn from today's top specialists"

10

Impact on Your Career

The completion of this Executive Master's Degree in Cybersecurity Management (CISO, Chief Information Security Officer) will be an added value to your professional business qualifications, by offering all the knowledge that, although it may seem totally alien to daily work, can be very useful to control computer processes that may harbor harmful external elements that can affect the entire organization. For this reason, higher specialization in this field proves essential, both at a personal and professional level for students, but also for the companies where they work.

TECH puts all of its academic resources at the disposal of its students so they acquire the necessary skills that will lead them to success"

The completion of this Executive Master's Degree will allow students to acquire the necessary competitiveness to make a radical change in their careers.

Are you ready to take the leap? Excellent professional development awaits you

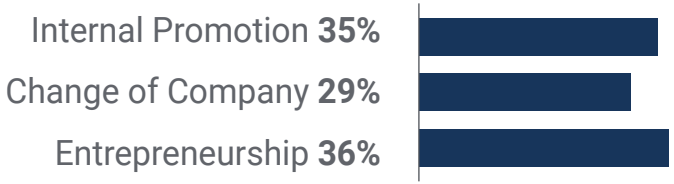
The TECH Technological University Executive Master's Degree in Cybersecurity Management (CISO, Chief Information Security Officer) is an intensive and highly valuable program aimed at improving students' professional skills in an area of extensive competition. Undoubtedly, it is a unique opportunity to improve professionally, but also personally, as it involves effort and dedication.

Those who wish to improve themselves, achieve a positive change at a professional level and interact with the best, will find their place at TECH.

A program of high academic standing to lead your career to success.

When the change occurs

Type of change



Salary increase

This program represents a salary increase of more than **25.22%** for our students.

11

Benefits for Your Company

The Executive Master's Degree in Cybersecurity Management (CISO, Chief Information Security Officer) helps raise the organization's talent to its maximum potential by training high-level leaders. That way, business professionals will be able to bring added value to their company by having the necessary skills to control Cybersecurity processes. A program that adapts to students so they acquire the necessary tools that, later on, they will be able to apply in their daily practice, achieving great benefits for their company.

A must-have program for business professionals who want to monitor and manage potential Cybersecurity"

Developing and retaining talent in companies is the best long-term investment.

01

Intellectual Capital and Talent Growth

Bring new concepts, strategies and perspectives to the company that can bring about relevant changes in the organization.

02

Retaining high-potential executives to avoid talent drain

This program strengthens the link between the company and the executive and opens new avenues for professional growth within the company.

03

Building agents of change

You will be able to make decisions in times of uncertainty and crisis, helping the organization overcome obstacles.

04

Increased international expansion possibilities

Thanks to this program, the company will come into contact with the main markets in the world economy.

05

Project Development

The professional will be work on a current project or develop new projects in the field of R&D or Business Development within their company.

06

Increased competitiveness

This program will equip students with the skills to take on new challenges and drive the organization forward.

12

Certificate

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

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

This **Executive Master's Degree in Cybersecurity Management (CISO Chief Information Security Officer)** contains the most complete and up-to-date program on the market.

After the student has passed the assessments, they will receive their corresponding **Executive Master's Degree** diploma issued by **TECH Technological University** via tracked delivery*.

The certificate issued by **TECH Technological University** will reflect the qualification obtained in the Executive Master's Degree, and meets the requirements commonly demanded by labor exchanges, competitive examinations and professional career evaluation committees.

Title: **Executive Master's Degree in Cybersecurity Management (CISO , Chief Information Security Officer)**
Official Number of Hours: **1,500 h.**


tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. _____, with identification number _____.
For having successfully passed and accredited the following program

EXECUTIVE MASTER'S DEGREE
in

Cybersecurity Management (CISO , Chief Information Security Officer)

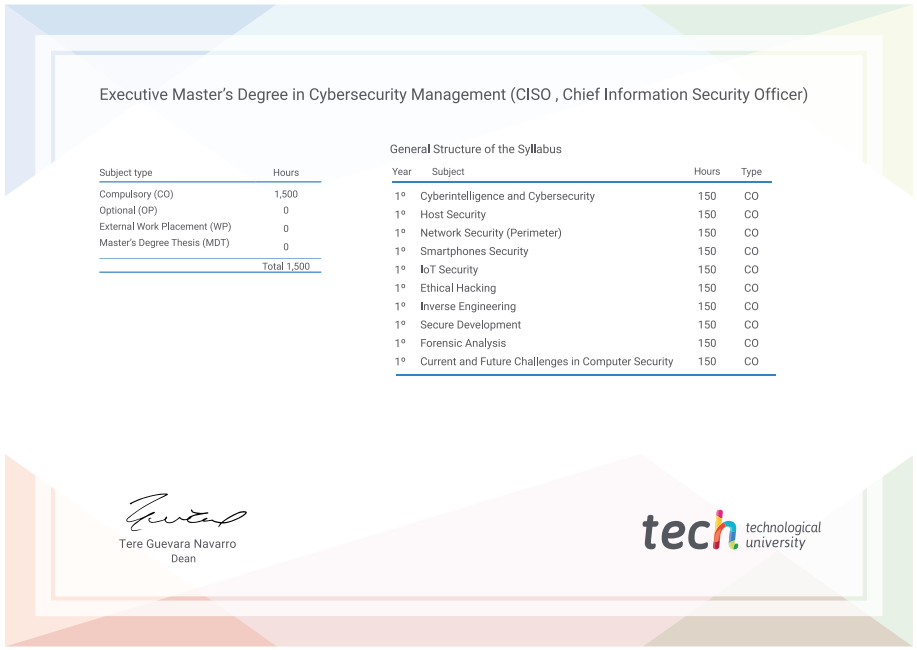
This is a qualification awarded by this University, equivalent to 1,500 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH is a Private Institution of Higher Education recognized by the Ministry of Public Education as of June 28, 2018.

June 17, 2020

Tere Guevara Navarro
Dean

Unique TECH Code: AFWORD23S techtitute.com/certificates


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

Subject type	Hours
Compulsory (CO)	1,500
Optional (OP)	0
External Work Placement (WP)	0
Master's Degree Thesis (MDT)	0
	Total 1,500

General Structure of the Syllabus

Year	Subject	Hours	Type
1º	Cyberintelligence and Cybersecurity	150	CO
1º	Host Security	150	CO
1º	Network Security (Perimeter)	150	CO
1º	Smartphones Security	150	CO
1º	IoT Security	150	CO
1º	Ethical Hacking	150	CO
1º	Inverse Engineering	150	CO
1º	Secure Development	150	CO
1º	Forensic Analysis	150	CO
1º	Current and Future Challenges in Computer Security	150	CO

Tere Guevara Navarro
Dean

tech technological university

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

tech technological university

Executive Master's Degree

Cybersecurity Management (CISO, Chief Information Security Officer)

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Executive Master's Degree

Cybersecurity Management (CISO, Chief Information Security Officer)

tech technological university