Advanced Master's Degree

Senior Cybersecurity Management (CISO, Chief Information Security Officer)

tech global university

tech global university

Advanced Master's Degree

Senior Cybersecurity Management (CISO, Chief Information Security Officer)

- Modality: **online**
- Duration: **2 years**
- Certificate: **TECH Global University**
- Accreditation: **120 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/us/information-technology/advanced-master-degree/advanced-master-degree-senior-cybersecurity-management-ciso-chief-information-security-officer

Index

01

Introduction

Nowadays, cybersecurity has become a fundamental pillar to protect individuals and companies against the growing number of digital threats. This discipline not only focuses on safeguarding the technological systems and critical information of organizations, but also on leading the planning, implementation and supervision of security strategies. As such, its main objective is to mitigate risks and respond effectively to cyber-attacks and incidents. Among the main responsibilities of a Cybersecurity Director are the design of security policies, the management of technological risks and the leadership of specialized teams. Faced with the challenges arising from technological progress and digitization, this program is designed specifically to address these issues. TECH not only focuses on ensuring efficiency in information protection, but also on identifying and managing new vulnerabilities. This positions the CISO as the most important element for the resilience of any organization.

With TECH, specialize and become a leader in one of the most important areas of IT"

Senior Cybersecurity Management has been fundamental to ensure the stability and continuity of organizations in a digitized and highly interconnected world. Through the implementation of robust security strategies and the adoption of advanced technologies, risks have been mitigated and attacks with catastrophic consequences have been prevented. In critical sectors such as banking, healthcare and public infrastructure, security has been strengthened through governance and compliance, driven by specialized leaders in this area.

This discipline has enabled organizations to establish more secure digital work environments, thereby strengthening the trust of customers, partners and users. Successful results have generated significant savings of millions of dollars in potential economic losses, while promoting an organizational culture in which security is a shared priority. In addition, it has proven essential to protecting the innovation, reputation and sustainability of organizations in an ever-evolving landscape.

TECH's Advanced Master's Degree is designed to specialize professionals in leading effective security strategies. Throughout the program, students will learn at their own pace, focusing on the development of management skills and strategic business acumen. In addition, you will have access to a cutting-edge specialization that prepares you to excel in a career that is in high demand in the global market. Thanks to its 100% online format, participants will be able to combine their studies with their work responsibilities, allowing them to advance without compromising their professional activity.

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

- Practical cases presented by experts in IT
- 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 Senior Cybersecurity Management (CISO, Chief Information Security Officer)
- 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

This Advanced Master's Degree positions you at the forefront of the industry and opens up endless career opportunities"

Develop the skills you need to meet the challenges of the future without neglecting your current activities"

Become the protector of technological infrastructures with the Relearning method that adapts to your learning pace.

Be part of the world's largest online university and specialize from anywhere in the world.

Its teaching staff includes professionals from the field of journalism, who bring to this program the experience of their work, as well as renowned specialists from reference 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 an immersive learning experience designed to prepare for real-life situations.

This program is designed around Problem-Based Learning, whereby the student must try to solve the different professional practice situations that arise throughout the program. For this purpose, the professional will be assisted by an innovative interactive video system created by renowned and experienced experts.

02

Why Study at TECH?

TECH is the world's largest online university. With an impressive catalog of more than 14,000 university programs, available in 11 languages, it is positioned as a leader in employability, with a 99% job placement rate. In addition, it has a huge faculty of more than 6,000 professors of the highest international prestige.

Study at the largest online university in the world and ensure your professional success. The future begins at TECH"

The world's best online university, according to FORBES

The prestigious Forbes magazine, specialized in business and finance, has highlighted TECH as "the best online university in the world" This is what they have recently stated in an article in their digital edition in which they echo the success story of this institution, "thanks to the academic offer it provides, the selection of its teaching staff, and an innovative learning method oriented to form the professionals of the future"

The best top international faculty

TECH's faculty is made up of more than 6,000 professors of the highest international prestige. Professors, researchers and top executives of multinational companies, including Isaiah Covington, performance coach of the Boston Celtics; Magda Romanska, principal investigator at Harvard MetaLAB; Ignacio Wistumba, chairman of the department of translational molecular pathology at MD Anderson Cancer Center; and D.W. Pine, creative director of TIME magazine, among others.

The world's largest online university

TECH is the world's largest online university. We are the largest educational institution, with the best and widest digital educational catalog, one hundred percent online and covering most areas of knowledge. We offer the largest selection of our own degrees and accredited online undergraduate and postgraduate degrees. In total, more than 14,000 university programs, in ten different languages, making us the largest educational institution in the world.

The most complete syllabuses on the university scene

TECH offers the most complete syllabuses on the university scene, with programs that cover fundamental concepts and, at the same time, the main scientific advances in their specific scientific areas. In addition, these programs are continuously updated to guarantee students the academic vanguard and the most demanded professional skills. and the most in-demand professional competencies. In this way, the university's qualifications provide its graduates with a significant advantage to propel their careers to success.

A unique learning method

TECH is the first university to use Relearning in all its programs. This is the best online learning methodology, accredited with international teaching quality certifications, provided by prestigious educational agencies. In addition, this innovative academic model is complemented by the "Case Method", thereby configuring a unique online teaching strategy. Innovative teaching resources are also implemented, including detailed videos, infographics and interactive summaries.

The official online university of the NBA

TECH is the official online university of the NBA. Thanks to our agreement with the biggest league in basketball, we offer our students exclusive university programs, as well as a wide variety of educational resources focused on the business of the league and other areas of the sports industry. Each program is made up of a uniquely designed syllabus and features exceptional guest hosts: professionals with a distinguished sports background who will offer their expertise on the most relevant topics.

Leaders in employability

TECH has become the leading university in employability. Ninety-nine percent of its students obtain jobs in the academic field they have studied within one year of completing any of the university's programs. A similar number achieve immediate career enhancement. All this thanks to a study methodology that bases its effectiveness on the acquisition of practical skills, which are absolutely necessary for professional development.

Google Premier Partner

The American technology giant has awarded TECH the Google Premier Partner badge. This award, which is only available to 3% of the world's companies, highlights the efficient, flexible and tailored experience that this university provides to students. The recognition not only accredits the maximum rigor, performance and investment in TECH's digital infrastructures, but also places this university as one of the world's leading technology companies.

The top-rated university by its students

Students have positioned TECH as the world's top-rated university on the main review websites, with a highest rating of 4.9 out of 5, obtained from more than 1,000 reviews. These results consolidate TECH as the benchmark university institution at an international level, reflecting the excellence and positive impact of its educational model."

03

Syllabus

The Advanced Master's Degree in Cybersecurity Senior Management (CISO) is designed to specialize strategic leaders capable of managing information security in global organizations. Through a comprehensive and up-to-date approach, the program covers key areas such as cybersecurity governance and risk management. In doing so, students will develop managerial skills to lead high-performance teams and implement security policies. In addition, while acquiring knowledge of the latest trends and emerging technologies, graduates will learn how to meet the challenges of the digital environment and lead security into the future.

TECH prepares you to be the strategist who prevents, detects and mitigates cyber threats across the global business environment"

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. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

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. IT Security Audit
- 1.5.2. Documentation and Permissions for Audit
- 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. ICP

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. ENISA
1.10.3. OEA
1.10.4. 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. Intrusion Detectors - HIDS
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. StickyPassword
2.5.5. RoboForm
2.6. Detectors for Phishing
2.6.1. Manual Detection of Phishing
2.6.2. Antiphishing Tools
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 Defense Systems: Defense 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. Fai2ban
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 Firewalls
3.4.2. Main Capabilities
3.4.3. Commercial Solutions
3.4.4. Firewalls for Cloud Services
3.4.4.1. Virtual Private Cloud (VPC) Architecture
3.4.4.2. ACLs Cloud
3.4.4.3. Security Group
3.5. *Proxy*
3.5.1. Types of Proxies
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. 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
4.2.1.1. Top 10 Vulnerabilities
4.2.2. Communications, Networks and Connection Modes

4.3. Mobile Devices in Business Environments
- 4.3.1. Risk
- 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. Statements of Information
- 4.4.2. Data Protection and Confidentiality
  - 4.4.2.1. Licenses
  - 4.4.2.2. Encryption
- 4.4.3. Secure Data Storage
  - 4.4.3.1. Secure Storage on iOS
  - 4.4.3.2. Secure Storage on Android
- 4.4.4. 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. Criptojacking 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

5.6. Transportation
- 5.6.1. Localization
- 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. Implantables
- 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. 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. 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. 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. Firewall and 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. *SQLinjection*

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 Programmed Tasks for Backdoors
- 6.10.4. User Creation
- 6.10.5. HIDS Detection

Module 7. Reverse 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 (Left To Right) Analyzers
    - 7.2.2.4.2. LALR Analyzers
- 7.2.3. Semantic Analysis
  - 7.2.3.1. Attribute Grammars
  - 7.2.3.2. S-Attributed
  - 7.2.3.3. L-Attributed

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 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. IDA
- 7.7.3. Code Rebuilders

7.8. Dynamic Code Analysis
- 7.8.1. Behavioral Analysis
  - 7.8.1.1. Communications
  - 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 in 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 Databases
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. Preparation of the Production Step
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. Practical Implementation of Software and Hardware Security Policies

9.1. Practical Implementation of Software and Hardware Security Policies
- 9.1.1. Implementation of Identification and Authorization
- 9.1.2. Implementation of Identification Techniques
- 9.1.3. Technical Authorization Measures

9.2. Identification and Authorization Technologies
- 9.2.1. Identifier and OTP
- 9.2.2. USB Token or PKI Smart Card
- 9.2.3. The "Confidential Defense" Key
- 9.2.4. Active RFID

9.3. Software and Systems Access Security Policies
- 9.3.1. Implementation of Access Control Policies
- 9.3.2. Implementation of Communications Access Policies
- 9.3.3. Types of Security Tools for Access Control

9.4. User Access Management
- 9.4.1. Access Rights Management
- 9.4.2. Segregation of Roles and Access Functions
- 9.4.3. Implementation of Access Rights in Systems

9.5. Access Control to Systems and Applications
- 9.5.1. Minimum Access Rule
- 9.5.2. Secure Log-On Technologies
- 9.5.3. Password Security Policies

9.6. Identification Systems Technologies
- 9.6.1. Active Directory
- 9.6.2. OTP
- 9.6.3. PAP, CHAP
- 9.6.4. KERBEROS, DIAMETER, NTLM

9.7. CIS Controls for Systems Hardening
- 9.7.1. Basic CIS Controls
- 9.7.2. Fundamental CIS Controls
- 9.7.3. Organizational CIS Controls

9.8. Operational Safety
- 9.8.1. Protection Against Malicious Code
- 9.8.2. Backup Copies
- 9.8.3. Activity Log and Supervision

9.9. Management of Technical Vulnerabilities
- 9.9.1. Technical Vulnerabilities
- 9.9.2. Technical Vulnerability Management
- 9.9.3. Restrictions on Software Installation

9.10. Implementation of Security Policy Practices
- 9.10.1. Logical Vulnerabilities
- 9.10.2. Implementation of Defense Policies

Module 10. Forensic Analysis

10.1. Data Acquisition and Duplication
- 10.1.1. Volatile Data Acquisition
  - 10.1.1.1. System Information
  - 10.1.1.2. Network Information
  - 10.1.1.3. Volatility Order
- 10.1.2. Static Data Acquisition
  - 10.1.2.1. Creating a Duplicate Image
  - 10.1.2.2. Preparation of a Chain of Custody Document
- 10.1.3. Methods for Validation of Acquired Data
  - 10.1.3.1. Methods for Linux
  - 10.1.3.2. Methods for Windows

10.2. Evaluation and Defeat of Antiforensic Techniques
- 10.2.1. Objectives of Antiforensic Techniques
- 10.2.2. Data Deletion
  - 10.2.2.1. Deletion of Data and Files
  - 10.2.2.2. File Recovery
  - 10.2.2.3. Recovery of Deleted Partitions
- 10.2.3. Password Protection
- 10.2.4. Steganography
- 10.2.5. Secure Device Wiping
- 10.2.6. Encryption

10.3. Operating System Forensics
- 10.3.1. Windows Forensics
- 10.3.2. Linux Forensics
- 10.3.3. Mac Forensics

10.4. Network Forensics
- 10.4.1. Logs Analysis
- 10.4.2. Data Correlation
- 10.4.3. Network Research
- 10.4.4. Steps to Follow in Network Forensic Analysis

10.5. Web Forensics
- 10.5.1. Investigation of Web Attacks
- 10.5.2. Attack Detection
- 10.5.3. IP Address Location

10.6. Forensic Database Analysis
- 10.6.1. Forensic Analysis in MSSQL
- 10.6.2. MySQL Forensic Analysis
- 10.6.3. PostgreSQL Forensic Analysis
- 10.6.4. Forensic Analysis in MongoDB

10.7. Cloud Forensics
- 10.7.1. Types of Crimes in the Cloud
  - 10.7.1.1. Cloud as Subject
  - 10.7.1.2. Cloud as an Object
  - 10.7.1.3. Cloud as a Tool
- 10.7.2. Challenges of Cloud Forensics
- 10.7.3. Research on Cloud Storage Services
- 10.7.4. Forensic Analysis Tools for Cloud

10.8. Investigation of Email Crimes
- 10.8.1. Mailing Systems
  - 10.8.1.1. Mail Clients
  - 10.8.1.2. Mail Server
  - 10.8.1.3. SMTP Server
  - 10.8.1.4. POP3 Server
  - 10.8.1.5. IMAP4 Server
- 10.8.2. Mailing Crimes
- 10.8.3. Mail Message
  - 10.8.3.1. Standard Headers
  - 10.8.3.2. Extended Headers
- 10.8.4. Steps for the Investigation of These Crimes
- 10.8.5. E-Mail Forensic Tools

10.9. Mobile Forensic Analysis
- 10.9.1. Cellular Networks
  - 10.9.1.1. Types of Networks
  - 10.9.1.2. CDR Contents
- 10.9.2. Subscriber Identity Module (SIM)
- 10.9.3. Logical Acquisition
- 10.9.4. Physical Acquisition
- 10.9.5. File System Acquisition

10.10. Forensic Report Writing and Reporting
- 10.10.1. Important Aspects of a Forensic Report
- 10.10.2. Classification and Types of Reports
- 10.10.3. Guide to Writing a Report
- 10.10.4. Presentation of the Report
  - 10.10.4.1. Prior Preparation for Testifying
  - 10.10.4.2. Deposition
  - 10.10.4.3. Dealing with the Media

Module 11. Security in System Design and Development

11.1. Information Systems
- 11.1.1. Information System Domains
- 11.1.2. Components of an Information System
- 11.1.3. Activities of an Information System
- 11.1.4. Life Cycle of an Information System
- 11.1.5. Information System Resources

11.2. IT Systems. Typology
- 11.2.1. Types of Information Systems
  - 11.2.1.1. Enterprise
  - 11.2.1.2. Strategic
  - 11.2.1.3. According to the Scope of Application
  - 11.2.1.4. Specific
- 11.2.2. Information Systems Real Examples
- 11.2.3. Evolution of Information Systems: Stages
- 11.2.4. Information Systems Methodologies

11.3. Security of Information Systems. Legal Implications
- 11.3.1. Access to Data
- 11.3.2. Security Threats Vulnerabilities
- 11.3.3. Legal Implications: Crimes
- 11.3.4. Information System Maintenance Procedures

11.4. Security of an Information System. Security Protocols
- 11.4.1. Security of an Information System
  - 11.4.1.1. Integrity
  - 11.4.1.2. Confidentiality
  - 11.4.1.3. Availability
  - 11.4.1.4. Authentication
- 11.4.2. Security Services
- 11.4.3. Information Security Protocols. Typology
- 11.4.4. Sensitivity of an Information System

11.5. Security in an Information System. Access Control Measures and Systems
- 11.5.1. Safety Measures
- 11.5.2. Type of Security Measures
  - 11.5.2.1. Prevention
  - 11.5.2.2. Detection
  - 11.5.2.3. Correction
- 11.5.3. Access Control Systems. Typology
- 11.5.4. Cryptography

11.6. Network and Internet Security
- 11.6.1. Firewalls
- 11.6.2. Digital Identification
- 11.6.3. Viruses and Worms
- 11.6.4. Hacking
- 11.6.5. Examples and Real Cases

11.7. Computer Crimes
- 11.7.1. Computer Crime
- 11.7.2. Computer Crimes. Typology
- 11.7.3. Computer Crimes. Attacks. Typology
- 11.7.4. The Case for Virtual Reality
- 11.7.5. Profiles of Offenders and Victims. Typification of the Crime
- 11.7.6. Computer Crimes. Examples and Real Cases

11.8. Security Plan in an Information System
- 11.8.1. Security Plan. Objectives
- 11.8.2. Security Plan. Planning
- 11.8.3. Risk Plan. Analysis
- 11.8.4. Security Policy. Implementation in the Organization
- 11.8.5. Security Plan. Implementation in the Organization
- 11.8.6. Security Procedures. Types
- 11.8.7. Security Plans. Examples

11.9. Contingency Plan
- 11.9.1. Contingency Plan. Functions
- 11.9.2. Emergency Plan Elements and Objectives
- 11.9.3. Contingency Plan in the Organization. Implementation
- 11.9.4. Contingency Plans. Examples

11.10. Information Systems Security Governance
- 11.10.1. Standards
- 11.10.2. Certifications
- 11.10.3. Technologies

Module 12. Information Security Architectures and Models

12.1. Information Security Architecture
- 12.1.1. ISMSI / PDS
- 12.1.2. Strategic Alignment
- 12.1.3. Risk Management
- 12.1.4. Performance Measurement

12.2. Information Security Models
- 12.2.1. Based on Security Policies
- 12.2.2. Based on Protection Tools
- 12.2.3. Based on Work Teams

12.3. Safety Model. Key Components
- 12.3.1. Identification of Risks
- 12.3.2. Definition of Controls
- 12.3.3. Continuous Assessment of Risk Levels
- 12.3.4. Awareness-Raising Plan for Employees, Suppliers, Partners, etc.

12.4. Risk Management Process
- 12.4.1. Asset Identification
- 12.4.2. Threat Identification
- 12.4.3. Risk Assessment
- 12.4.4. Prioritization of Controls
- 12.4.5. Re-Evaluation and Residual Risk

12.5. Business Processes and Information Security
- 12.5.1. Business Processes
- 12.5.2. Risk Assessment Based on Business Parameters
- 12.5.3. Business Impact Analysis
- 12.5.4. Business Operations and Information Security

12.6. Continuous Improvement Process
- 12.6.1. The Deming Cycle
  - 12.6.1.1. Plan
  - 12.6.1.2. Do
  - 12.6.1.3. Verify
  - 12.6.1.4. Act

12.7. Security Architectures
- 12.7.1. Selection and Homogenization of Technologies
- 12.7.2. Identity Management. Authentication
- 12.7.3. Access Management. Authorization
- 12.7.4. Network Infrastructure Security
- 12.7.5. Encryption Technologies and Solutions
- 12.7.6. Endpoint Detection Response (EDR)

12.8. Regulatory Framework
- 12.8.1. Sectoral Regulations
- 12.8.2. Certifications
- 12.8.3. Legislation

12.9. The ISO 27001 Standard
- 12.9.1. Implementation
- 12.9.2. Certification
- 12.9.3. Audits and Penetration Tests
- 12.9.4. Continuous Risk Management
- 12.9.5. Classification of Information

12.10. Privacy Legislation. GDPR
- 12.10.1. Scope of General Data Protection Regulation (GDPR)
- 12.10.2. Personal Data
- 12.10.3. Roles in the Processing of Personal Data
- 12.10.4. ARCO Rights
- 12.10.5. El DPO. Functions

Module 13. Information Security Management System (ISMS)

13.1. Information Security. Key Aspects
- 13.1.1. Information Security
  - 13.1.1.1. Confidentiality
  - 13.1.1.2. Integrity
  - 13.1.1.3. Availability
  - 13.1.1.4. Information Security Measurements

13.2. Information Security Management Systems
- 13.2.1. Information Security Management Models
- 13.2.2. Documents to Implement an ISMS
- 13.2.3. Levels and Controls of an ISMS

13.3. International Norms and Standards
- 13.3.1. International Standards in Information Security
- 13.3.2. Origin and Evolution of the Standard
- 13.3.3. International Information Security Management Standards
- 13.3.4. Other Reference Standards

13.4. ISO/IEC 27,000 Standards
- 13.4.1. Purpose and Areas of Application
- 13.4.2. Structure of the Standard
- 13.4.3. Certification
- 13.4.4. Accreditation Phases
- 13.4.5. Benefits of ISO/IEC 27,000 Standards

13.5. Design and Implementation of a General Information Security System
- 13.5.1. Phases of Implementation of a General Information Security System
- 13.5.2. Business Continuity Plans

13.6. Phase I: Diagnosis
- 13.6.1. Preliminary Diagnosis
- 13.6.2. Identification of the Stratification Level
- 13.6.3. Level of Compliance with Standards/Norms

13.7. Phase II: Preparation
- 13.7.1. Context of the Organization
- 13.7.2. Analysis of Applicable Safety Regulations
- 13.7.3. Scope of the General Information Security System
- 13.7.4. General Information Security System Policy
- 13.7.5. Objectives of the General Information Security System

13.8. Phase III: Planning
- 13.8.1. Asset Classification
- 13.8.2. Risk Assessment
- 13.8.3. Identification of Threats and Risks

13.9. Phase IV: Implementation and Follow-up
- 13.9.1. Result Analysis
- 13.9.2. Assigning Responsibilities
- 13.9.3. Timing of the Action Plan
- 13.9.4. Monitoring and Audits

13.10. Incident Management Security Policies
- 13.10.1. Phases
- 13.10.2. Incident Categorization
- 13.10.3. Incident Management and Procedures

Module 14. IT Security Management

14.1. Safety Management
- 14.1.1. Security Operations
- 14.1.2. Legal and Regulatory Aspects
- 14.1.3. Business Qualification
- 14.1.4. Risk Management
- 14.1.5. Identity and Access Management

14.2. Structure of the Security Area. The CISO's Office
- 14.2.1. Organizational Structure. Position of the CISO in the Structure
- 14.2.2. Lines of Defense
- 14.2.3. Organizational Chart of the CISO's Office
- 14.2.4. Budget Management

14.3. Security Governance
- 14.3.1. Safety Committee
- 14.3.2. Risk Monitoring Committee
- 14.3.3. Audit Committee
- 14.3.4. Crisis Committee

14.4. Security Governance. Functions
- 14.4.1. Policies and Standards
- 14.4.2. Security Master Plan
- 14.4.3. Control Panels
- 14.4.4. Awareness and Education
- 14.4.5. Supply Chain Security

14.5. Security Operations
- 14.5.1. Identity and Access Management
- 14.5.2. Configuration of Network Security Rules. Firewalls
- 14.5.3. IDS/IPS Platform Management
- 14.5.4. Vulnerability Analysis

14.6. Cybersecurity Framework NIST CSF
- 14.6.1. Methodology NIST
  - 14.6.1.1. Identify
  - 14.6.1.2. Protect
  - 14.6.1.3. Detect
  - 14.6.1.4. Respond
  - 14.6.1.5. Retrieve

14.7. Security Operations Center (SOC). Functions
- 14.7.1. Protection Red Team, Pentesting, Threat Intelligence
- 14.7.2. Detection. SIEM, User Behavior Analytics, Fraud Prevention
- 14.7.3. Response

14.8. Security Audits
- 14.8.1. Intrusion Test
- 14.8.2. Red Team Exercises
- 14.8.3. Source Code Audits. Secure Development
- 14.8.4. Component Safety (Software Supply Chain)
- 14.8.5. Forensic Analysis

14.9. Incident Response
- 14.9.1. Preparation
- 14.9.2. Detection, Analysis and Notification
- 14.9.3. Containment, Eradication and Recovery
- 14.9.4. Post-Incident Activity
  - 14.9.4.1. Evidence Retention
  - 14.9.4.2. Forensic Analysis
  - 14.9.4.3. Gap Management
- 14.9.5. Official Cyber-Incident Management Guidelines

14.10. Vulnerability Management
- 14.10.1. Vulnerability Analysis
- 14.10.2. Vulnerability Assessment
- 14.10.3. System Basing
- 14.10.4. Zero-Day Vulnerabilities. Zero-Day

Module 15. Security Incident Management Policies

15.1. Information Security Incident Management Policies and Enhancements
- 15.1.1. Incident Management
- 15.1.2. Responsibilities and Procedures
- 15.1.3. Event Notification

15.2. Intrusion Detection and Prevention Systems (IDS/IPS)
- 15.2.1. System Operating Data
- 15.2.2. Types of Intrusion Detection Systems
- 15.2.3. Criteria for IDS/IPS Placement

15.3. Security Incident Response
- 15.3.1. Data Collection Procedure
- 15.3.2. Intrusion Verification Process
- 15.3.3. CERT Organizations

15.4. Intrusion Attempt Notification and Management Process
- 15.4.1. Responsibilities in the Notification Process
- 15.4.2. Classification of Incidents
- 15.4.3. Resolution and Recovery Process

15.5. Forensic Analysis as a Security Policy
- 15.5.1. Volatile and Non-Volatile Evidence
- 15.5.2. Analysis and Collection of Electronic Evidence
  - 15.5.2.1. Analysis of Electronic Evidence
  - 15.5.2.2. Collection of Electronic Evidence

15.6. Intrusion Detection and Prevention Systems (IDS/IPS) Tools
- 15.6.1. Snort
- 15.6.2. Suricata
- 15.6.3. Solar-Winds

15.7. Event Centralizing Tools
- 15.7.1. SIM
- 15.7.2. SEM
- 15.7.3. SIEM

15.8. CCN-STIC Security Guide 817
- 15.8.1. Cyber Incident Management
- 15.8.2. Metrics and Indicators

15.9. NIST SP800-61
- 15.9.1. Computer Security Incident Response Capability
- 15.9.2. Handling an Incident
- 15.9.3. Coordination and Information Sharing

15.10. ISO 27035
- 15.10.1. ISO 27035 Standard. Incident Management Principles
- 15.10.2. Incident Management Plan Preparation Guidelines
- 15.10.3. Incident Response Operations Guides

Module 16. Risk Analysis and IT Security Environment

16.1. Analysis of the Environment
- 16.1.1. Analysis of the Economic Situation
  - 16.1.1.1. VUCA Environments
    - 16.1.1.1.1. Volatile
    - 16.1.1.1.2. Uncertain
    - 16.1.1.1.3. Complex
    - 16.1.1.1.4. Ambiguous

16.1.1.2. BANI Environments
16.1.1.2.1. Brittle
16.1.1.2.2. Anxious
16.1.1.2.3. Nonlinear
16.1.1.2.4. Incomprehensible
16.1.2. Analysis of the General Environment. PESTEL
16.1.2.1. Politics
16.1.2.2. Economics
16.1.2.3. Social
16.1.2.4. Technological
16.1.2.5. Ecological/Environmental
16.1.2.6. Legal
16.1.3. Analysis of the Internal Situation SWOT Analysis
16.1.3.1. Objectives
16.1.3.2. Threats
16.1.3.3. Opportunities
16.1.3.4. Strengths
16.2. Risk and Uncertainty
16.2.1. Risk
16.2.2. Risk Management
16.2.3. Risk Management Standards
16.3. ISO 31.000:2018 Risk Management Guidelines
16.3.1. Object
16.3.2. Principles
16.3.3. Frame of Reference
16.3.4. Process
16.4. Information Systems Risk Analysis and Management Methodology (MAGERIT)
16.4.1. MAGERIT Methodology
16.4.1.1. Objectives
16.4.1.2. Method
16.4.1.3. Components
16.4.1.4. Techniques
16.4.1.5. Available Tools (PILAR)
16.5. Cyber Risk Transfer
16.5.1. Risk Transfer
16.5.2. Cyber Risks. Typology
16.5.3. Cyber Risk Insurance
16.6. Agile Methodologies for Risk Management
16.6.1. Agile Methodologies
16.6.2. Scrum for Risk Management
16.6.3. *Agile Risk Management*
16.7. Technologies for Risk Management
16.7.1. Artificial Intelligence Applied to Risk Management
16.7.2. Blockchain and Cryptography. Value Preservation Methods
16.7.3. Quantum Computing Opportunity or Threat
16.8. IT Risk Mapping Based on Agile Methodologies
16.8.1. Representation of Probability and Impact in Agile Environments.
16.8.2. Risk as a Threat to Value
16.8.3. Re-Evolution in Project Management and Agile Processes based on KRIs
16.9. Risk-Driven in Risk Management
16.9.1. *Risk Driven*
16.9.2. Risk-Driven in Risk Management
16.9.3. Development of a Risk-Driven Business Management Model
16.10. Innovation and Digital Transformation in IT Risk Management
16.10.1. Agile Risk Management as a Source of Business Innovation
16.10.2. Transforming Data into Useful Information for Decision Making
16.10.3. Holistic View of the Enterprise through Risk

Module 17. Security Policies for the Analysis of Threats in Computer Systems

17.1. Threat Management in Security Policies
17.1.1. Risk Management
17.1.2. Security Risk
17.1.3. Threat Management Methodologies
17.1.4. Implementation of Methodologies

17.2. Phases of Threat Management
- 17.2.1. Identification
- 17.2.2. Analysis
- 17.2.3. Localization
- 17.2.4. Safeguard Measures

17.3. Audit Systems for Threat Localization
- 17.3.1. Classification and Information Flow
- 17.3.2. Analysis of Vulnerable Processes

17.4. Risk Classification
- 17.4.1. Types of Risk
- 17.4.2. Calculation of Threat Probability
- 17.4.3. Residual Risk

17.5. Risk Treatment
- 17.5.1. Implementation of Safeguard Measures
- 17.5.2. Transfer or Assume

17.6. Control Risks
- 17.6.1. Continuous Risk Management Process
- 17.6.2. Implementation of Security Metrics
- 17.6.3. Strategic Model of Information Security Metrics

17.7. Practical Methodologies for Threat Analysis and Control
- 17.7.1. Threat Catalog
- 17.7.2. Catalog of Control Measures
- 17.7.3. Safeguards Catalog

17.8. ISO 27005
- 17.8.1. Risk Identification
- 17.8.2. Risk Analysis
- 17.8.3. Risk Evaluation

17.9. Risk, Impact and Threat Matrix
- 17.9.1. Data, Systems and Personnel
- 17.9.2. Threat Probability
- 17.9.3. Magnitude of Damage

17.10. Design of Phases and Processes in Threat Analysis
- 17.10.1. Identification of Critical Organizational Elements
- 17.10.2. Determination of Threats and Impacts
- 17.10.3. Impact and Risk Analysis
- 17.10.4. Methods

Module 18. Practical Implementation of Security Policies in the Face of Attacks

18.1. *System Hacking*
- 18.1.1. Risks and Vulnerabilities
- 18.1.2. Countermeasures

18.2. DoS Attack
- 18.2.1. Risks and Vulnerabilities
- 18.2.2. Countermeasures

18.3. *Session Hijacking*
- 18.3.1. The Process of Hijacking
- 18.3.2. Hijacking Countermeasures

18.4. Evading IDS, Firewalls and Honeypots
- 18.4.1. Avoidance Techniques
- 18.4.2. Implementation of Countermeasures

18.5. *Hacking Web Servers*
- 18.5.1. Attacks on Web Servers
- 18.5.2. Implementation of Defense Measures

18.6. *Hacking Web Applications*
- 18.6.1. Attacks on Web Applications
- 18.6.2. Implementation of Defense Measures

18.7. *Hacking Wireless Networks*
- 18.7.1. Vulnerabilities in Wi-Fi Networks
- 18.7.2. Implementation of Defense Measures

18.8. *Hacking Mobile Platforms*
- 18.8.1. Vulnerabilities of Mobile Platforms
- 18.8.2. Implementation of Countermeasures

18.9. *Ransomware*
- 18.9.1. Ramsonware Vulnerabilities
- 18.9.2. Implementation of Countermeasures

18.10. Social Engineering
- 18.10.1. Types of Social Engineering
- 18.10.2. Countermeasures for Social Engineering

Module 19. Cryptography in IT

19.1. Cryptography
- 19.1.1. Cryptography
- 19.1.2. Fundamentals of Mathematics

19.2. Cryptology
- 19.2.1. Cryptology
- 19.2.2. Cryptanalysis
- 19.2.3. Steganography and Stegoanalysis

19.3. Cryptographic Protocols
- 19.3.1. Basic Blocks
- 19.3.2. Basic Protocols
- 19.3.3. Intermediate Protocols
- 19.3.4. Advanced Protocol
- 19.3.5. Exoteric Protocols

19.4. Cryptographic Techniques
- 19.4.1. Key Length
- 19.4.2. Key Management
- 19.4.3. Types of Algorithms
- 19.4.4. Key Management *Hash*
- 19.4.5. Pseudo-Random Number Generators
- 19.4.6. Use of Algorithms

19.5. Symmetric Cryptography
- 19.5.1. Block Ciphers
- 19.5.2. DES (Data Encryption Standard)
- 19.5.3. RC4 Algorithm
- 19.5.4. AES (Advanced Encryption Standard)
- 19.5.5. Combination of Block Ciphers
- 19.5.6. Key Derivation

19.6. Asymmetric Cryptography
- 19.6.1. Diffie-Hellman
- 19.6.2. DSA (Digital Signature Algorithm)
- 19.6.3. RSA (Rivest, Shamir and Adleman)
- 19.6.4. Elliptic Curve
- 19.6.5. Asymmetric Cryptography. Typology

19.7. Digital Certificates
- 19.7.1. Digital Signature
- 19.7.2. X509 Certificates
- 19.7.3. Public Key Infrastructure (PKI)

19.8. Implementations
- 19.8.1. Kerberos
- 19.8.2. IBM CCA
- 19.8.3. Pretty Good Privacy (PGP)
- 19.8.4. ISO Authentication Framework
- 19.8.5. SSL and TLS
- 19.8.6. Smart Cards in Means of Payment (EMV)
- 19.8.7. Mobile Telephony Protocols
- 19.8.8. *Blockchain*

19.9. Steganography
- 19.9.1. Steganography
- 19.9.2. Stegoanalysis
- 19.9.3. Applications and Uses

19.10. Quantum Cryptography
- 19.10.1. Quantum Algorithms
- 19.10.2. Protection of Algorithms from Quantum Computing
- 19.10.3. Quantum Key Distribution

Module 20. Identity and Access Management in IT Security

20.1. Identity and Access Management (IAM)
- 20.1.1. Digital Identity
- 20.1.2. Identity Management
- 20.1.3. Identity Federation

20.2. Physical Access Control
- 20.2.1. Protection Systems
- 20.2.2. Area Security
- 20.2.3. Recovery Facilities

20.3. Logical Access Control
- 20.1.1. Authentication: Typology
- 20.1.2. Authentication Protocols
- 20.1.3. Authentication Attacks

20.4. Logical Access Control. MFA Authentication
- 20.4.1. Logical Access Control. MFA Authentication
- 20.4.2. Passwords. Importance
- 20.4.3. Authentication Attacks

20.5. Logical Access Control. Biometric Authentication
- 20.5.1. Logical Access Control. Biometric Authentication
  - 20.5.1.1. Biometric Authentication. Requirements
- 20.5.2. Operation
- 20.5.3. Models and Techniques

20.6. Authentication Management Systems
- 20.6.1. *Single Sign On*
- 20.6.2. Kerberos
- 20.6.3. AAA Systems

20.7. Authentication Management Systems: AAA Systems
- 20.7.1. TACACS
- 20.7.2. RADIUS
- 20.7.3. DIAMETER

20.8. Access Control Services
- 20.8.1. FW - Firewall
- 20.8.2. VPN - Virtual Private Networks
- 20.8.3. IDS - Intrusion Detection System

20.9. Network Access Control Systems
- 20.9.1. NAC
- 20.9.2. Architecture and Elements
- 20.9.3. Operation and Standardization

20.10. Access to Wireless Networks
- 20.10.1. Types of Wireless Networks
- 20.10.2. Security in Wireless Networks
- 20.10.3. Attacks on Wireless Networks

Module 21. Security in Communications and Software Operation

21.1. Computer Security in Communications and Software Operation
- 21.1.1. IT Security
- 21.1.2. Cybersecurity
- 21.1.3. Cloud Security

21.2. IT Security in Communications and Software Operation. Typology
- 21.2.1. Physical Security
- 21.2.2. Logical Security

21.3. Communications Security
- 21.3.1. Main Elements
- 21.3.2. Network Security
- 21.3.3. Best Practices

21.4. Cyberintelligence
- 21.4.1. Social Engineering
- 21.4.2. *Deep Web*
- 21.4.3. *Phishing*
- 21.4.4. *Malware*

21.5. Secure Development in Communications and Software Operation
- 21.1.1. Secure Development. HTTP Protocol
- 21.1.2. Secure Development. Life Cycle
- 21.1.3. Secure Development. PHP Security
- 21.1.4. Secure Development. NET Security
- 21.1.5. Secure Development. Best Practices

21.6. Information Security Management Systems in Communications and Software Operation
- 21.6.1. GDPR
- 21.6.2. ISO 27021
- 21.6.3. ISO 27017/18

21.7. SIEM Technologies
- 21.7.1. SIEM Technologies
- 21.7.2. SOC Operation
- 21.7.3. SIEM Vendors

21.8. The Role of Security in Organizations
- 21.8.1. Roles in Organizations
- 21.8.2. Role of IoT Specialists in Companies
- 21.8.3. Recognized Certifications in the Market

21.9. Forensic Analysis
- 21.9.1. Forensic Analysis
- 21.9.2. Forensic Analysis. Study Methodology
- 21.9.3. Forensic Analysis. Tools and Implementation

21.10. Cybersecurity Today
- 21.10.1. Major Cyber-Attacks
- 21.10.2. Employability Forecasts
- 21.10.3. Challenges

Module 22. Security in Cloud Environments

22.1. Security in Cloud Computing Environments
- 22.1.1. Security in Cloud Computing Environments
- 22.1.2. Security in Cloud Computing Environments. Threats and Security Risks
- 22.1.3. Security in Cloud Computing Environments. Key Security Aspects

22.2. Types of Cloud Infrastructure
- 22.2.1. Public
- 22.2.2. Private
- 22.2.3. Hybrid

22.3. Shared Management Model
- 22.3.1. Security Elements Managed by Vendor
- 22.3.2. Elements Managed by Customer
- 22.3.3. Definition of the Security Strategy

22.4. Prevention Mechanisms
- 22.4.1. Authentication Management Systems
- 22.4.2. Authorization Management Systems: Access Policies
- 22.4.3. Key Management Systems

22.5. System Securitization
- 22.5.1. Securitization of Storage Systems
- 22.5.2. Protection of Database Systems
- 22.5.3. Securing Data in Transit

22.6. Infrastructure Protection
- 22.6.1. Secure Network Design and Implementation
- 22.6.2. Security in Computing Resources
- 22.6.3. Tools and Resources for Infrastructure Protection

22.7. Detection of Threats and Attacks
- 22.7.1. Auditing, Logging and Monitoring Systems
- 22.7.2. Event and Alarm Systems
- 22.7.3. SIEM Systems

22.8. Incident Response
- 22.8.1. Incident Response Plan
- 22.8.2. Business Continuity
- 22.8.3. Forensic Analysis and Remediation of Incidents of the Same Nature.

22.9. Security in Public Clouds
- 22.9.1. AWS (Amazon Web Services)
- 22.9.2. Microsoft Azure
- 22.9.3. Google GCP
- 22.9.4. Oracle Cloud

22.10. Regulations and Compliance
- 22.10.1. Security Compliance
- 22.10.2. Risk Management
- 22.10.3. People and Process in Organizations

Module 23. Monitoring Tools in Information Systems Security Policies

23.1. Information Systems Monitoring Policies
- 23.1.1. System Monitoring
- 23.1.2. Metrics
- 23.1.3. Types of Metrics

23.2. Systems Auditing and Registration
- 23.2.1. Windows Auditing and Logging
- 23.2.2. Linux Auditing and Logging

23.3. SNMP Protocol. *Simple Network Management Protocol*
- 23.3.1. SNMP Protocol
- 23.3.2. SNMP Functions
- 23.3.3. SNMP Tools

23.4. Network Monitoring
- 23.4.1. Network Monitoring in Control Systems
- 23.4.2. Monitoring Tools for Control Systems

23.5. Nagios. Network Monitoring System
- 23.5.1. Nagios
- 23.5.2. Operation of Nagios
- 23.5.3. Nagios Installation

23.6. Zabbix. Network Monitoring System
- 23.6.1. Zabbix
- 23.6.2. How Zabbix Works
- 23.6.3. Zabbix Installation

23.7. Cacti. Network Monitoring System
- 23.7.1. Cacti
- 23.7.2. How Cacti Works
- 23.7.3. Installation of Cacti

23.8. Pandora. Network Monitoring System
- 23.8.1. Pandora.
- 23.8.2. Operation of Pandora
- 23.8.3. Pandora Installation

23.9. SolarWinds. Network Monitoring System
- 23.9.1. SolarWinds
- 23.9.2. Operation of SolarWinds
- 23.9.3. Installation of SolarWinds

23.10. Monitoring Regulations
- 23.10.1. CIS Controls Over Auditing and Record Keeping
- 23.10.2. NIST 800-123 (U.S.A.)

Module 24. Security in IoT Device Communications

24.1. From Telemetry to IoT
- 24.1.1. Telemetry
- 24.1.2. M2M Connectivity
- 24.1.3. Democratization of Telemetry

24.2. IoT Reference Models
- 24.2.1. IoT Reference Model
- 24.2.2. Simplified IoT Architecture

24.3. IoT Security Vulnerabilities
- 24.3.1. IoT Devices
- 24.3.2. IoT Devices. Usage Case Studies
- 24.3.3. IoT Devices. Vulnerabilities

24.4. IoT Connectivity
- 24.4.1. PAN, LAN, WAN Networks
- 24.4.2. Non IoT Wireless Technologies
- 24.4.3. LPWAN Wireless Technologies

24.5. LPWAN Technologies
- 24.5.1. The Iron Triangle of LPWAN Networks
- 24.5.2. Free Frequency Bands vs. Licensed Bands
- 24.5.3. LPWAN Technology Options

24.6. LoRaWAN Technology
- 24.6.1. LoRaWAN Technology
- 24.6.2. LoRaWAN Use Cases. Ecosystem
- 24.6.3. Security in LoRaWAN

24.7. Sigfox Technology
- 24.7.1. Sigfox Technology
- 24.7.2. Sigfox Use Cases. Ecosystem
- 24.7.3. Sigfox Security

24.8. IoT Cellular Technology
- 24.8.1. IoT Cellular Technology (NB-IoT and LTE-M)
- 24.8.2. Cellular IoT Use Cases. Ecosystem
- 24.8.3. IoT Cellular Security

24.9. WiSUN Technology
- 24.9.1. WiSUN Technology
- 24.9.2. WiSUN Use Cases. Ecosystem
- 24.9.3. Security in WiSUN

24.10. Other IoT Technologies
- 24.10.1. Other IoT Technologies
- 24.10.2. Use Cases and Ecosystem of Other IoT Technologies
- 24.10.3. Security in Other IoT Technologie

Module 25. Business Continuity Plan Associated with Security

25.1. Business Continuity Plans
- 25.1.1. Business Continuity Plans (BCP)
- 25.1.2. Business Continuity Plans (BCP). Key Aspects
- 25.1.3. Business Continuity Plan (BCP) for Business Valuation

25.2. Metrics in a Business Continuity Plan (BCP)
- 25.2.1. Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- 25.2.2. Maximum Tolerable Time (MTD)
- 25.2.3. Minimum Recovery Levels (ROL)
- 25.2.4. Recovery point objective (RPO)

25.3. Continuity Projects. Typology
- 25.3.1. Business Continuity Plan (BCP)
- 25.3.2. ICT Continuity Plan (ICTCP)
- 25.3.3. Disaster Recovery Plan (DRP)

25.4. Risk Management Associated with the BCP
- 25.4.1. Business Impact Analysis
- 25.4.2. Benefits of Implementing a BCP
- 25.4.3. Risk-Based Mentality

25.5. Life Cycle of a Business Continuity Plan
- 25.5.1. Phase 1 Organizational Analysis
- 25.5.2. Phase 2 Determining the Continuity Strategy
- 25.5.3. Phase 3 Response to Contingency
- 25.5.4. Phase 4 Tests, Maintenance and Review

25.6. Organizational Analysis Phase of a BCP
- 25.6.1. Identification of Processes in the Scope of the BCP
- 25.6.2. Identification of Critical Business Areas
- 25.6.3. Identification of Dependencies Between Areas and Processes
- 25.6.4. Determination of Appropriate BAT
- 25.6.5. Deliverables. Creation of a Plan

25.7. Determination Phase of the Continuity Strategy in a BCP
- 25.7.1. Roles in the Strategy Determination Phase
- 25.7.2. Tasks in the Strategy Determination Phase
- 25.7.3. Deliverables

25.8. Contingency Response Phase of a BCP
- 25.8.1. Roles in the Response Phase
- 25.8.2. Tasks in This Phase
- 25.8.3. Deliverables

25.9. Testing, Maintenance and Revision Phase of a BCP
- 25.9.1. Roles in the Testing, Maintenance and Review Phase
- 25.9.2. Tasks in the Testing, Maintenance and Review Phase
- 25.9.3. Deliverables

25.10. ISO Standards Associated with Business Continuity Plans (BCP)
- 25.10.1. ISO 22301:2019
- 25.10.2. ISO 22313:2020
- 25.10.3. Other Related ISO and International Standards

Module 26. Practical Security Disaster Recovery Policy

26.1. DRP. Disaster Recovery Plan
- 26.1.1. Objective of a DRP
- 26.1.2. Benefits of a DRP
- 26.1.3. Consequences of a Missing and Not up-to-Date DRP

26.2. Guidance for Defining a DRP (Disaster Recovery Plan)
- 26.2.1. Scope and Objectives
- 26.2.2. Recuperation Strategy Design
- 26.2.3. Assignment of Roles and Responsibilities
- 26.2.4. Inventory of Hardware, Software and Services
- 26.2.5. Tolerance for Downtime and Data Loss
- 26.2.6. Establishment of the Specific Types of DRP Required
- 26.2.7. Implementation of a Training, Awareness and Communication Plan

26.3. Scope and Objectives of a DRP (Disaster Recovery Plan)
- 26.3.1. Response Guarantee
- 26.3.2. Technological Components
- 26.3.3. Scope of the Continuity Policy

26.4. Disaster Recovery Plan (DRP) Strategy Design
- 26.4.1. Disaster Recovery Strategy
- 26.4.2. Budget
- 26.4.3. Human and Physical Resources
- 26.4.4. Management Positions at Risk
- 26.4.5. Technology
- 26.4.6. Date:

26.5. Continuity of Information Processes
- 26.5.1. Continuity Planning
- 26.5.2. Continuity Implementation
- 26.5.3. Verification of Continuity Assessment

26.6. Scope of a BCP (Business Continuity Plan)
- 26.6.1. Determination of the Most Critical Processes
- 26.6.2. Asset-Based Approach
- 26.6.3. Process Approach

26.7. Implementation of Guaranteed Business Processes
- 26.7.1. Priority Activities (PA)
- 26.7.2. Ideal Recovery Times (IRT)
- 26.7.3. Survival Strategies

26.8. Organizational Analysis
- 26.8.1. Acquisition of information
- 26.8.2. Business Impact Analysis (BIA)
- 26.8.3. Risk Analysis in the Organization

26.9. Response to Contingency
- 26.9.1. Crisis Plan
- 26.9.2. Operational Environment Recovery Plans
- 26.9.3. Technical Work or Incident Procedures

26.10. International Standard ISO 27031 BCP
- 26.10.1. Objectives
- 26.10.2. Terms and Definitions
- 26.10.3. Operation

Module 27. Implementation of Physical and Environmental Safety Policies in the Company

27.1. Security Areas
- 27.1.1. Physical Security Perimeter
- 27.1.2. Working in Safe Areas
- 27.1.3. Security of Offices, Offices and Resources

27.2. Physical Input Controls
- 27.2.1. Physical Access Control Policies
- 27.2.2. Physical Input Control Systems

27.3. Physical Access Vulnerabilities
- 27.3.1. Main Physical Vulnerabilities
- 27.3.2. Implementation of Safeguards Measures

27.4. Physiological Biometric Systems
- 27.4.1. Fingerprint
- 27.4.2. Facial Recognition
- 27.4.3. Iris and Retinal Recognition
- 27.4.4. Other Physiological Biometric Systems

27.5. Biometric Behavioral Systems
- 27.5.1. Signature Recognition
- 27.5.2. Writer Recognition
- 27.5.3. Voice Recognition
- 27.5.4. Other Biometric Behavioral Systems

27.6. Biometrics Risk Management
- 27.6.1. Implementation of Biometric Systems
- 27.6.2. Vulnerabilities of Biometric Systems

27.7. Implementation of Policies in Hosts
- 27.7.1. Installation of Supply and Security Cabling
- 27.7.2. Equipment Location
- 27.7.3. Exit of the Equipment Outside the Premises
- 27.7.4. Unattended Computer Equipment and Clear Post Policy

27.8. Environmental Protection
- 27.8.1. Fire Protection Systems
- 27.8.2. Seismic Protection Systems
- 27.8.3. Earthquake Protection Systems

27.9. Data Processing Center Security
- 27.9.1. Security Doors
- 27.9.2. Video Surveillance Systems (CCTV)
- 27.9.3. Safety Control

27.10. International Physical Security Standards
- 27.10.1. IEC 62443-2-1 (European)
- 27.10.2. NERC CIP-005-5 (USA)
- 27.10.3. NERC CIP-014-2 (USA)

Module 28. Secure Communications Policies in the Company

28.1. Network Security Management
- 28.1.1. Network Control and Monitoring
- 28.1.2. Segregation of Networks
- 28.1.3. Network Security Systems

28.2. Secure Communication Protocols
- 28.2.1. TCP/IP Model
- 28.2.2. IPSEC Protocol
- 28.2.3. TLS Protocol

28.3. Protocol TLS 1.3
- 28.3.1. Phases of a TLS1.3 Process
- 28.3.2. Handshake Protocol
- 28.3.3. Registration Protocol
- 28.3.4. Differences with TLS 1.2

28.4. Cryptographic Algorithms
- 28.4.1. Cryptographic Algorithms Used in Communications
- 28.4.2. *Cipher-Suites*
- 28.4.3. Cryptographic Algorithms allowed for TLS 1.3

28.5. Digest Functions
- 28.5.1. MD6
- 28.5.2. SHA

28.6. PKI. Public Key Infrastructure
- 28.6.1. PKI and its Entities
- 28.6.2. Digital Certificate
- 28.6.3. Types of Digital Certificates

28.7. Tunnel and Transport Communications
- 28.7.1. Tunnel Communications
- 28.7.2. Transport Communications
- 28.7.3. Encrypted Tunnel Implementation

28.8. SSH. *Secure Shell*
- 28.8.1. SSH. Safe Capsule
- 28.8.2. SSH Functions
- 28.8.3. SSH Tools

28.9. Audit of Cryptographic Systems
- 28.9.1. Integration Test
- 28.9.2. Cryptographic System Testing

28.10. Cryptographic Systems
- 28.10.1. Cryptographic Systems Vulnerabilities
- 28.10.2. Cryptographic Safeguards

Module 29. Organizational Aspects of Information Security Policy

29.1. Internal Organization
- 29.1.1. Assigning Responsibilities
- 29.1.2. Segregation of Duties
- 29.1.3. Contacts with Authorities
- 29.1.4. Information Security in Project Management

29.2. Asset Management
- 29.2.1. Liability for Assets
- 29.2.2. Classification of Information
- 29.2.3. Handling of Storage Media

29.3. Security Policies in Business Processes
- 29.3.1. Analysis of the Vulnerabilities of Business Processes
- 29.3.2. Business Impact Analysis
- 29.3.3. Classification of Processes with Respect to Business Impact

29.4. Security Policies Linked to Human Resources
- 29.4.1. Before Hiring
- 29.4.2. During Contracting
- 29.4.3. Termination or Change of Position

29.5. Management Security Policies
- 29.5.1. Management Guidelines on Information Security
- 29.5.2. BIA - Analyzing the Impact
- 29.5.3. Recovery Plan as a Security Policy

29.6. Acquisition and Maintenance of Information Systems
- 29.6.1. Information Systems Security Requirements
- 29.6.2. Development and Support Data Security
- 29.6.3. Test Data

29.7. Security with Suppliers
- 29.7.1. IT Security with Suppliers
- 29.7.2. Management of Service Delivery with Assurance
- 29.7.3. Supply Chain Security

29.8. Operational Safety
- 29.8.1. Operational Responsibilities
- 29.8.2. Protection Against Malicious Code
- 29.8.3. Backup Copies
- 29.8.4. Activity and Supervision Records

29.9. Safety and Regulatory Management
- 29.9.1. Compliance with Legal Requirements
- 29.9.2. Information Security Reviews

29.10. Business Continuity Management Security
- 29.10.1. Continuity of Information Security
- 29.10.2. Redundancies

A complete TECH curriculum will teach you how to be a visionary leader who ensures the long-term protection of the organization"

04

Teaching Objectives

The Advanced Master's Degree in Senior Cybersecurity Management (CISO) aims to train strategic leaders capable of managing information security in any type of organization. Throughout the program, participants will develop skills to identify, assess and mitigate cyber risks, implement effective security policies. In addition, they will be provided with an in-depth understanding of emerging technologies and best practices in security architecture, ensuring data protection and business continuity. The program also fosters an integrated business view of cybersecurity, aligning initiatives with corporate objectives and ensuring compliance with international regulations. Students will be prepared to be agents of change and promote an organizational culture focused on digital protection.

In this 100% online specialization you will find the most up-to-date teaching material and research in the university landscape"

General Objectives

- Develop strategic cybersecurity leaders who can manage the protection of the digital assets and technology infrastructures of global organizations
- Integrate cybersecurity within the business strategy, aligning digital protection initiatives with the organization's overall objectives
- Train in the implementation of cybersecurity policies and regulatory frameworks that ensure regulatory compliance and information protection in digital environments
- Foster leadership and management of cybersecurity teams, enhancing the ability to make strategic decisions in crisis situations and manage security projects at the organizational level

Join TECH and develop the skills necessary to become a leader who anticipates threats and strengthens opportunities"

Specific Objectives

Module 1. Cyberintelligence and Cybersecurity

- Develop the skills necessary to implement cyberintelligence and cybersecurity strategies
- Protect IT systems from cyber threats through the collection, analysis and use of digital intelligence

Module 2. Host Security

- Train in the implementation of security measures in host systems
- Ensure the protection of servers and devices against vulnerabilities, malware and unauthorized access

Module 3. Network Security (Perimeter)

- Provide the necessary knowledge to protect computer networks at the perimeter level
- Handle security techniques and tools such as firewalls, VPNs and intrusion detection systems

Module 4. Smartphone Security

- Provide a comprehensive understanding of mobile device security
- Delve into protection against threats such as malware, data loss and attacks through mobile applications

Module 5. IoT Security

- Train in the implementation of security policies for IoT devices
- Protect infrastructure and data generated by devices connected through IoT networks and platforms

Module 6. Ethical Hacking

- Develop the necessary skills to perform penetration tests and security audits using ethical hacking techniques
- Be able to identify vulnerabilities and prevent attacks

Module 7. Reverse Engineering

- Master reverse engineering techniques, allowing to analyze and understand the operation of software and hardware
- Identify potential vulnerabilities and security solutions

Module 8. Secure Development

- Teach secure software development best practices
- Apply security principles throughout the development lifecycle to minimize application risks and vulnerabilities

Module 9. Practical Implementation of Software and Hardware Security Policies

- Provide the necessary knowledge to design and implement robust software and hardware security policies
- Ensure protection against internal and external threats

Module 10. Forensic Analysis

- Develop skills in digital forensic analysis
- Analyze the collection, preservation and analysis of digital evidence in cases of computer security incidents

Module 11. Security in System Design and Development

- Address the integration of security measures from the design and development phases of IT systems
- Ensure protection against potential vulnerabilities from the beginning of the project

Module 12. Information Security Architectures and Models

- Provide the necessary knowledge of information security architectures and models
- Design and implement robust systems that protect the organization's data and resources

Module 13. Information Security Management System (ISMS)

- Implement an Information Security Management System
- Protect business information effectively, ensuring compliance with regulations and best practices

Module 14. IT Security Management

- Provide the necessary knowledge to effectively manage security in the company's technological infrastructures
- Minimize risks and ensure operational continuity

Module 15. Security Incident Management Policies

- Train in the creation and implementation of effective policies for the management of security incidents
- Establish clear protocols for detection, analysis and response to security breaches

Module 16. Risk Analysis and IT Security Environment

- Provide the necessary knowledge to perform a risk analysis in the IT environment, identifying threats and vulnerabilities
- Apply mitigation strategies to secure the technological infrastructure

Module 17. Security Policies for the Analysis of Threats in Computer Systems

- Train in the development of security policies to identify, analyze and mitigate threats to IT systems
- Use appropriate tools and methods to protect the organization's digital assets

Module 18. Practical Implementation of Security Policies in the Face of Attacks

- Implement effective security policies in the face of possible attacks
- Ensure the protection of the organization's systems and critical information

Module 19. Cryptography in IT

- Teach the fundamentals and applications of cryptography in the field of information technology
- Implement encryption and security algorithms in data transmission

Module 20. Identity and Access Management in IT Security

- Develop the skills necessary to manage identity and access in IT systems
- Establish authentication and access control policies to protect the organization's resources and data

Module 21. Security in Communications and Software Operation
- Train in the protection of digital communications and in the implementation of security measures in software operation
- Ensure confidentiality, integrity and availability of information

Module 22. Security in Cloud Environments
- Implement security policies in cloud computing environments
- Ensure that data and applications are protected from unauthorized access and attacks

Module 23. Monitoring Tools in Information Systems Security Policies
- Train in the use of monitoring tools to evaluate the effectiveness of information systems security policies
- Delve into the early detection of vulnerabilities and attacks

Module 24. Security in IoT Device Communications
- Develop skills in the implementation of security measures to protect communications between IoT devices
- Minimize risks associated with the exchange of data between connected devices

Module 25. Business Continuity Plan Associated with Security
- Develop a business continuity plan to ensure the protection and rapid recovery of systems
- Establish protocols to safeguard critical data in the event of security incidents

Module 26. Practical Security Disaster Recovery Policy
- Create disaster recovery policies
- Ensure rapid restoration of systems and protection of data in the event of major security incidents

Module 27. Implementation of Physical and Environmental Safety Policies in the Company
- Train in the implementation of physical and environmental security policies to protect the organization's physical resources
- Ensure the proper environment for the safe operation of technological systems

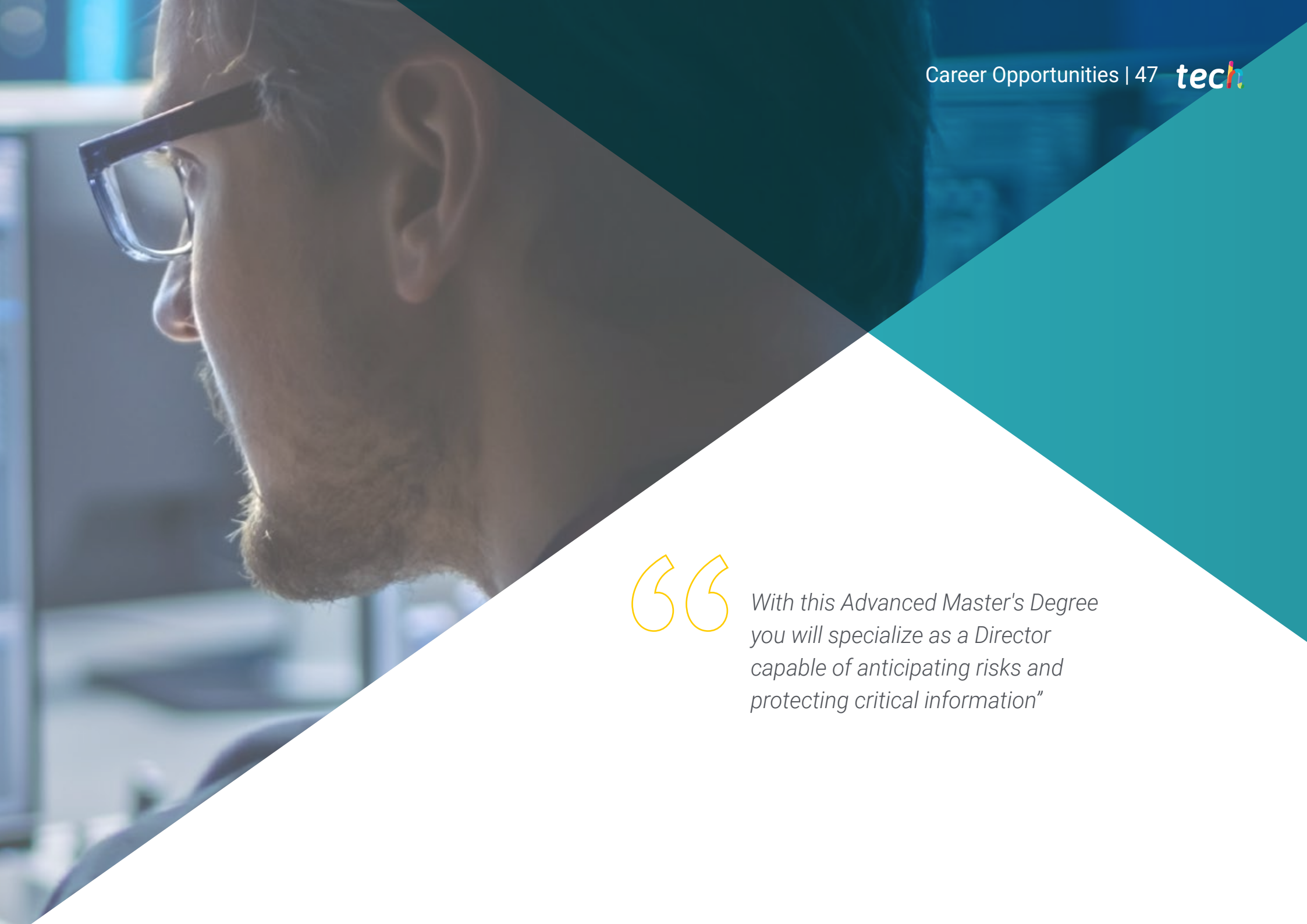
Module 28. Secure Communications Policies in the Company
- Provide the knowledge to develop secure communications policies within the organization
- Protect networks and communication channels against espionage and information leaks

Module 29. Organizational Aspects of Information Security Policy
- Provide the necessary tools to implement organizational policies in information security management
- Establish appropriate roles, responsibilities and processes to protect information assets

05

Career Opportunities

Upon completion of the Advanced Master's Degree in Senior Cybersecurity Management (CISO), graduates will be fully qualified to assume key roles in the protection and management of information security in various organizations. In addition, they will be able to lead security strategies in multinational companies, managing and mitigating cyber risks. Likewise, they will be prepared to occupy positions that require skills to lead cybersecurity initiatives and ensure the protection of digital assets in any sector.



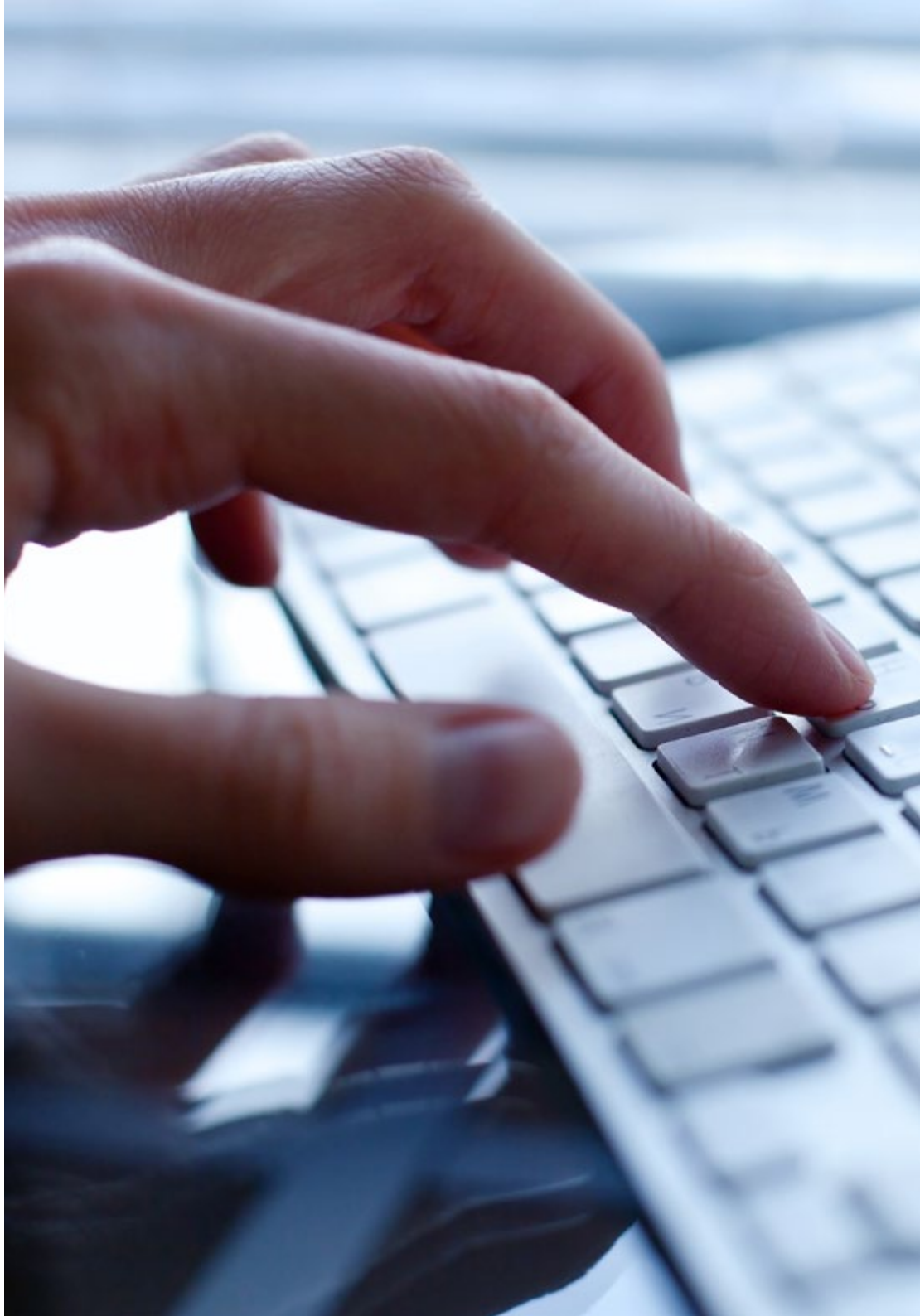
With this Advanced Master's Degree you will specialize as a Director capable of anticipating risks and protecting critical information"

Graduate Profile

The graduate of the Advanced Master's Degree in Senior Cybersecurity Management (CISO) will be a strategic leader with a deep understanding of information security in the context of global organizations. They will be able to design and implement advanced security policies and lead multidisciplinary teams. You will also have strong management and governance skills, enabling you to address cybersecurity challenges in various sectors, ensuring the protection of digital assets. This opportunity will provide you with the tools you need to stay on top of the latest technology trends and adapt to the rapidly changing digital landscape.

Prepare yourself to be one of the best professionals, minimizing the impact of cyber-attacks and getting back to normal quickly.

- **Strategic Leadership and Adaptability:** Ability to lead multidisciplinary teams and manage security policies, adapting to rapid technological and emerging changes in cybersecurity
- **Risk Management and Informed Decision Making:** Ability to identify, assess and mitigate cyber risks, making decisions based on detailed data and analysis
- **Critical Analysis and Incident Management:** Ability to identify vulnerabilities, manage security incidents and coordinate crisis response, ensuring business continuit
- **Effective Communication and Strategic Thinking:** Ability to communicate risks and solutions clearly to different stakeholders, adopting a global and strategic approach to digital asset protection



After completing the Advanced Master's Degree, you will be able to apply your knowledge and skills in the following positions:

1. **Chief Technology Security Office (CISO):** Strategic leader in charge of information protection and cybersecurity across the organization, developing policies and overseeing the digital security infrastructure.
2. **Cybersecurity Director:** Responsible for the management and supervision of the IT security teams, developing and implementing strategies to protect the company's technology infrastructure.
3. **IT Security Manager:** Responsible for managing and coordinating digital security policies, overseeing the protection of data and computer systems from potential threats.
4. **Cybersecurity Consultant:** Expert in advising companies on the best way to implement and manage cybersecurity policies, helping to mitigate risks and complying with international regulations.
5. **IT Risk Management Director:** Responsible for identifying, assessing and mitigating cyber risks that may affect the security of the organization's information and technology systems.
6. **Information Security Head:** Leader in charge of overseeing and coordinating all initiatives related to the protection of data and IT systems within the organization

You are one step away from improving your professional life with this Advanced Master's Degree that only TECH offers"

06

Study Methodology

TECH is the world's first university to combine the **case study** methodology with **Relearning**, a 100% online learning system based on guided repetition.

This disruptive pedagogical strategy has been conceived to offer professionals the opportunity to update their knowledge and develop their skills in an intensive and rigorous way. A learning model that places students at the center of the educational process giving them the leading role, adapting to their needs and leaving aside more conventional methodologies.

TECH will prepare you to face new challenges in uncertain environments and achieve success in your career"

The student: the priority of all TECH programs

In TECH's study methodology, the student is the main protagonist.
The teaching tools of each program have been selected taking into account the demands of time, availability and academic rigor that, today, not only students demand but also the most competitive positions in the market.

With TECH's asynchronous educational model, it is students who choose the time they dedicate to study, how they decide to establish their routines, and all this from the comfort of the electronic device of their choice. The student will not have to participate in live classes, which in many cases they will not be able to attend. The learning activities will be done when it is convenient for them. They can always decide when and from where they want to study.

"At TECH you will NOT have live classes (which you might not be able to attend)"

The most comprehensive study plans at the international level

TECH is distinguished by offering the most complete academic itineraries on the university scene. This comprehensiveness is achieved through the creation of syllabi that not only cover the essential knowledge, but also the most recent innovations in each area.

By being constantly up to date, these programs allow students to keep up with market changes and acquire the skills most valued by employers. In this way, those who complete their studies at TECH receive a comprehensive education that provides them with a notable competitive advantage to further their careers.

And what's more, they will be able to do so from any device, pc, tablet or smartphone.

"TECH's model is asynchronous, so it allows you to study with your pc, tablet or your smartphone wherever you want, whenever you want and for as long as you want"

Case Studies and Case Method

The case method has been the learning system most used by the world's best business schools. Developed in 1912 so that law students would not only learn the law based on theoretical content, its function was also to present them with real complex situations. In this way, they could make informed decisions and value judgments about how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

With this teaching model, it is students themselves who build their professional competence through strategies such as Learning by Doing or Design Thinking, used by other renowned institutions such as Yale or Stanford.

This action-oriented method will be applied throughout the entire academic itinerary that the student undertakes with TECH. Students will be confronted with multiple real-life situations and will have to integrate knowledge, research, discuss and defend their ideas and decisions. All this with the premise of answering the question of how they would act when facing specific events of complexity in their daily work.

Relearning Methodology

At TECH, case studies are enhanced with the best 100% online teaching method: Relearning.

This method breaks with traditional teaching techniques to put the student at the center of the equation, providing the best content in different formats. In this way, it manages to review and reiterate the key concepts of each subject and learn to apply them in a real context.

In the same line, and according to multiple scientific researches, reiteration is the best way to learn. For this reason, TECH offers between 8 and 16 repetitions of each key concept within the same lesson, presented in a different way, with the objective of ensuring that the knowledge is completely consolidated during the study process.

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.

A 100% online Virtual Campus with the best teaching resources

In order to apply its methodology effectively, TECH focuses on providing graduates with teaching materials in different formats: texts, interactive videos, illustrations and knowledge maps, among others. All of them are designed by qualified teachers who focus their work on combining real cases with the resolution of complex situations through simulation, the study of contexts applied to each professional career and learning based on repetition, through audios, presentations, animations, images, etc.

The latest scientific evidence in the field of Neuroscience points to the importance of taking into account the place and context where the content is accessed before starting a new learning process. Being able to adjust these variables in a personalized way helps people to remember and store knowledge in the hippocampus to retain it in the long term. This is a model called Neurocognitive context-dependent e-learning that is consciously applied in this university qualification.

In order to facilitate tutor-student contact as much as possible, you will have a wide range of communication possibilities, both in real time and delayed (internal messaging, telephone answering service, email contact with the technical secretary, chat and videoconferences).

Likewise, this very complete Virtual Campus will allow TECH students to organize their study schedules according to their personal availability or work obligations. In this way, they will have global control of the academic content and teaching tools, based on their fast-paced professional update.

The online study mode of this program will allow you to organize your time and learning pace, adapting it to your schedule"

The effectiveness of the method is justified by four fundamental achievements:

1. Students who follow this method not only achieve the assimilation of concepts, but also a development of their mental capacity, through exercises that assess real situations and the application of knowledge.
2. Learning is solidly translated into practical skills that allow the student to better integrate into the real world.
3. Ideas and concepts are understood more efficiently, given that the example situations are based on real-life.
4. Students like to feel that the effort they put into their studies is worthwhile. This then translates into a greater interest in learning and more time dedicated to working on the course.

The university methodology top-rated by its students

The results of this innovative teaching model can be seen in the overall satisfaction levels of TECH graduates.

The students' assessment of the quality of teaching, quality of materials, course structure and objectives is excellent. Not surprisingly, the institution became the best rated university by its students on the Global Score review platform, obtaining a 4.9 out of 5.

Access the study contents from any device with an Internet connection (computer, tablet, smartphone) thanks to the fact that TECH is at the forefront of technology and teaching.

You will be able to learn with the advantages that come with having access to simulated learning environments and the learning by observation approach, that is, Learning from an expert.

As such, the best educational materials, thoroughly prepared, will be available in this program:

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.

This content is then adapted in an audiovisual format that will create our way of working online, with the latest techniques that allow us to offer you high quality in all of the material that we provide you with.

Practicing Skills and Abilities

You will carry out activities to develop specific competencies and skills in each thematic field. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop within the framework of the globalization we live in.

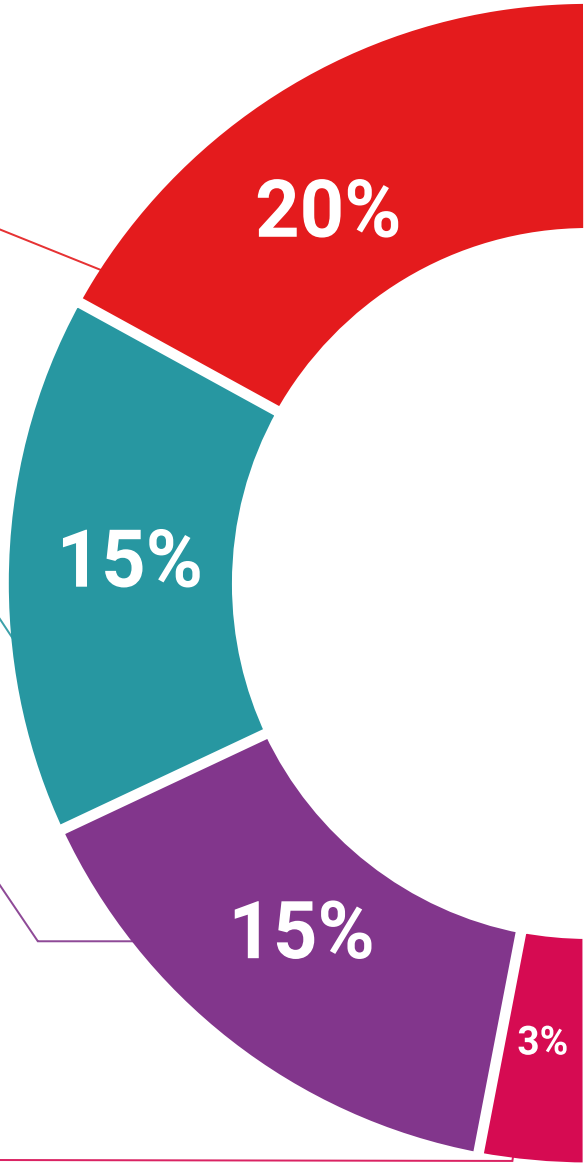
Interactive Summaries

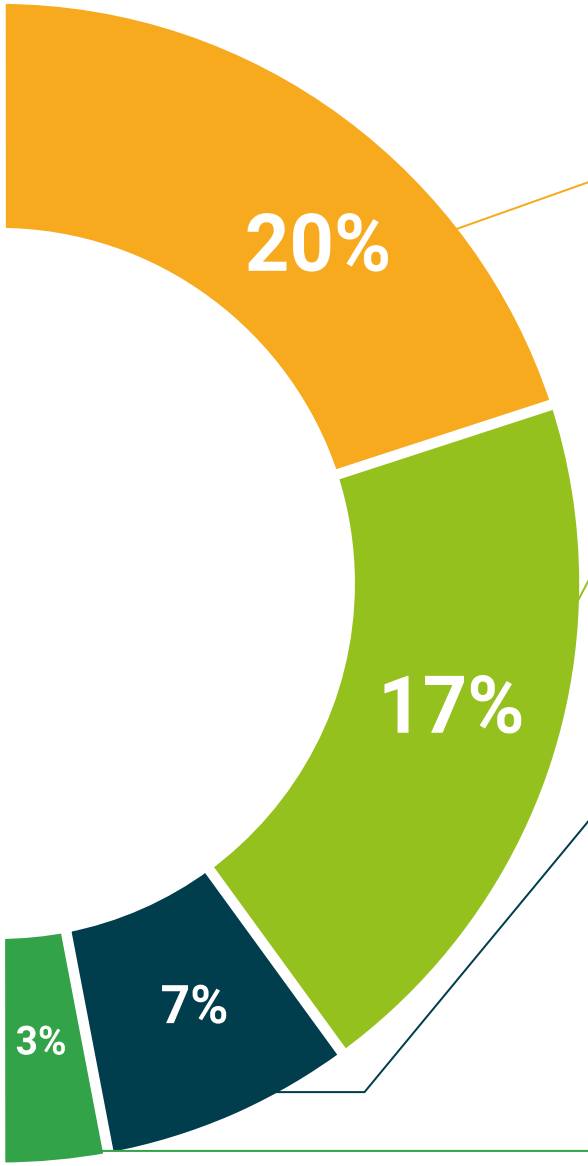
We present the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

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

Additional Reading

Recent articles, consensus documents, international guides... In our virtual library you will have access to everything you need to complete your education.





Case Studies

Students will complete a selection of the best case studies in the field. Cases that are presented, analyzed, and supervised by the best specialists in the world.

Testing & Retesting

We periodically assess and re-assess your knowledge throughout the program. We do this on 3 of the 4 levels of Miller's Pyramid.

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 for future difficult decisions.

Quick Action Guides

TECH offers the most relevant contents of the course in the form of worksheets or quick action guides. A synthetic, practical and effective way to help students progress in their learning.

07

Teaching Staff

This Advanced Master's Degree in Senior Cybersecurity Management (CISO, Chief Information Security Officer) has a teaching staff composed of active professionals who know perfectly the current state of this area, and who will transfer, therefore, all the keys of current cybersecurity to the student. In this way, it is guaranteed that the student of this program will obtain the latest advances in this field, being able to access them thanks to the prestigious faculty selected by TECH.

TECH offers you the most specialized Directors and Teachers so that your approach and learning will be the best"

International Guest Director

Dr. Frederic Lemieux is internationally recognized as an innovative expert and inspirational leader in the fields of Intelligence, National Security, Homeland 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 in several 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 of them related to **criminal intelligence, policing, cyber threats and international security.** He has also made a significant contribution to the field of Cybersecurity with the publication of numerous articles in academic journals, examining 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 various academic, private and governmental organizations, reflecting his influence and commitment to excellence in his field of expertise. In this way, 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

- Director of the Master's Degree in Cybersecurity Risk Management at Georgetown, Washington, U.S.A.
- Director of the Master's Degree in Technology Management at Georgetown University
- Director of the Master's Degree in Applied Intelligence at Georgetown University
- Professor of Internships at Georgetown University
- PhD in Criminology from the School of Criminology at the University of Montreal
- B.A. in Sociology and Minor Degree in Psychology from Laval University
- 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

- Trainer in Computer Security and Ethical Hacking at the National Reference Center of Getafe in Computer Science and Telecommunications in Madrid
- Certified E-Council instructor
- Trainer in the following certifications: EXIN Ethical Hacking Foundation and 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).
- External collaborator CSO/SSA (*Chief Security Officer/Senior Security Architect*) at the University of the Balearic Islands
- Computer Engineer by the University of Alcalá de Henares, Madrid
- Master's Degree in DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Mr. Olalla Bonal, Martín

- Senior Blockchain Practice Manager at EY
- Blockchain Client Technical Specialist for IBM
- Director of Architecture for Blocknitive
- Team Coordinator in Non-Relational Distributed Databases for WedoIT, a subsidiary of IBM
- Infrastructure Architect at Bankia
- Head of Layout Department at T-Systems
- Department Coordinator for Bing Data España SL

Professors

Ms. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applications Developer at B60. UK.
- Analyst Programmer for the Management, Coordination and Documentation of the Virtualized Environment of Security Alarms
- Analyst Programmer of Java Applications for Automatic Teller Machines (ATM)
- Software Development Professional for Signature Validation and Document Management Application
- Systems Technician for Equipment Migration and for Management, Maintenance and Training of PDA Mobile Devices
- Technical Engineer in Computer Systems from the Open University of Catalonia (UOC)
- Master's Degree in Computer Security and Ethical Hacking Official EC- Council and CompTIA from the Professional School of New Technologies CICE

Mr. Entrenas, Alejandro

- Cybersecurity Project Manager. Entelgy Innotec Security
- Cybersecurity Consultant. Entelgy
- Information Security Analyst. Innovery Spain
- Information Security Analyst. Atos
- Degree in Technical Engineering in Computer Systems from the University of Cordoba.
- Master's Degree in Information Security Management from the Polytechnic University of Madrid.
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

Mr. Catalá Barba, José Francisco

- Electronic Technician Expert in Cybersecurity
- Developer of Applications for Mobile Devices
- Electronic Technician in Intermediate Command at the Ministry of Defense of Spain
- Electronics Technician at Ford Factory in Valencia

Mr. Peralta Alonso, Jon

- Senior Data Protection and Cybersecurity Consultant at Altia
- Lawyer/Legal Advisor at Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Legal Advisor/Intern at a professional law firm: Óscar Padura
- Law Degree from the Public University of the Basque Country
- Master's Degree in Data Protection Delegate by EIS Innovative School
- Master's Degree in Law from the Public University of the Basque Country
- Specialist Master's Degree in Civil Litigation Practice from the International University Isabel I
  of Castilla
- Professor in Master's Degree in Personal Data Protection, Cybersecurity and ICT Law

Mr. Gonzalo Alonso, Félix

- CEO and Founder of Smart REM Solutions
- Head of Risk Engineering and Innovation at Dynargy
- Manager and founding partner of Risknova, a technology consultancy firm
- Master's Degree in Insurance Management from the Higher Institute for Collaboration between Insurance Companies
- Degree in Industrial Technical Engineering, specializing in Industrial Electronics from Comillas Pontifical University ICAI

Mr. Jiménez Ramos, Álvaro

- Cybersecurity Analyst
- 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
- Master's Degree in Cybersecurity and Ethical Hacking by CICE
- Advanced Course in Cybersecurity by Deusto Training

Mr. Redondo, Jesús Serrano

- Web Developer and Cybersecurity Technician
- Web Developer at Roams, Palencia
- FrontEnd Developer at Telefónica, Madrid
- FrontEnd Developer at Best Pro Consulting SL, Madrid
- Telecommunications Equipment and Services Installer at Grupo Zener, Castilla y León
- Telecommunications Equipment and Services Installer at Lican Comunicaciones SL, Castilla y León
- Certificate in Computer Security by CFTIC Getafe, Madrid
- Senior Technician in Telecommunications and Computer Systems at IES Trinidad Arroyo, Palencia
- Higher Technician in MV and LV Electrotechnical Installations by IES Trinidad Arroyo, Palencia
- Training in Reverse Engineering, Stenography and Encryption by Academia Hacker Incibe

Mr. Nogales Ávila, Javier

- Enterprise Cloud and Sourcing Senior Consultant at Quint
- Cloud and Technology Consultant at Indra
- Associate Technology Consultant at Accenture
- Graduate in Industrial Organization Engineering from the University of Jaén
- MBA in Business Administration and Management from ThePower Business School

Mr. Gómez Rodríguez, Antonio

- Principal Cloud Solutions Engineer for Oracle
- Co-organizer of Málaga Developer Meetup
- Specialist Consultant for Sopra Group and Everis
- Team Leader at System Dynamics
- Software Developer at SGO Software
- Master's Degree in E-Business from from La Salle Business School
- Postgraduate degree in Information Technologies and Systems from the Catalan Institute of Technology.
- Degree in Telecommunications Engineering from the Polytechnic University of Catalonia

Mr. Rodrigo Estébanez, Juan Manuel

- Co-founder of Ismet Tech
- Information Security Manager at Ecix Group
- Operational Security Officer at Atos IT Solutions and Services A/S
- Teacher of Cybersecurity Management in university studies
- Degree in Engineering from the University of Valladolid
- Master's Degree in Integrated Management Systems from CEU San Pablo University

Mr. Del Valle Arias, Jorge

- Telecommunications Engineer with expertise in Business Development
- Smart City Solutions & Software Business Development Manager Spain Itron, Inc
- IoT Consultant
- Interim IoT Business Director. TCOMET
- IoT, Industry 4.0 Business Unit Manager. Diode Spain
- IoT and Telecommunications Sales Area Manager. Aicox Solutions
- Chief Technical Officer (CTO) and Business Development Manager. TELYC Consulting
- Founder and CEO of Sensor Intelligence
- Head of Operations and Projects. Codio
- Operations Director at Codium Networks
- Chief Engineer of hardware and firmware design. AITEMIN
- Regional Head of RF Planning and Optimization - LMDS 3.5 GHz Network. Clearwire
- Telecommunications Engineer from Universidad Politécnica de Madrid
- Executive MBA from the International Graduate School of La Salle of Madrid
- Master's Degree in Renewable Energies. CEPYME

Mr. Gozalo Fernández, Juan Luis

- Blockchain-based Product Manager for Open Canarias
- Director Blockchain DevOps Director at Alastria
- Director of Service Level Technology at Santander Spain
- Tinkerlink Mobile Application Development Manager at Cronos Telecom
- IT Service Management Technology Director at Barclays Bank Spain
- Bachelor's Degree in Computer Engineering from UNED
- Specialization in Deep Learning at DeepLearning.ai

Ms. Jurado Jabonero, Lorena

- Head of Information Security (CISO) at Grupo Pascual
- Cybersecurity Manager at KPMG. Spain
- IT Processes and Infrastructure Control and Project Management Consultant at Bankia
- Exploitation Tools Engineer at Dalkia
- Developer at Banco Popular Group
- Applications Developer at the Polytechnic University of Madrid
- Graduate in Computer Engineering from the Alfonso X El Sabio University.
- Technical Engineer in Computer Management from the Polytechnic University of Madrid
- Certified Data Privacy Solutions Engineer (CDPSE) by ISACA

Mr. Ortega Esteban, Octavio

- Marketing and Web Development Specialist
- Freelance Computer Applications Programmer and Web Developer
- Chief Operating Officer at Smallsquid SL
- E-Commerce Administrator at Ortega y Serrano
- Lecturer in Postgraduate courses in Computer and Communications Professionalism
- Lecturer in Computer Security Postgraduate courses
- Degree in Psychology from the Open University of Catalonia
- Higher University Technician in Software Analysis, Design and Solutions
- Higher University Technician in Advanced Programming

Mr. Embid Ruiz, Mario

- Lawyer Expert in ICT and Data Protection at Martínez-Echevarría Abogados
- Legal Manager of Branddocs SL
- Risk Analyst in the SME Segment at BBVA
- Lecturer in postgraduate university studies related to law
- Degree in Law from Rey Juan Carlos University
- Degree in Business Administration and Management from the Rey Juan Carlos University
- Master's Degree in New Technologies, Internet and Audiovisual Law from the Villanueva University Study Center

Take the opportunity to learn about the latest advances in this field in order to apply it to your daily practice"

08

Certificate

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

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

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

This **TECH Global University** private qualification, 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: **Advanced Master's Degree in Senior Cybersecurity Management (CISO, Chief Information Security Officer)**

Modality: **online**

Duration: **2 years**

Accreditation: **120 ECTS**


tech global university

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

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

This is a private qualification of 3,600 hours of duration equivalent to 120 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
Dean

Unique TECH Code: AFWORD23S techtitute.com/certificates


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

General Structure of the Syllabus

Year	Subject	ECTS	Type
1º	Cyberintelligence and Cybersecurity	4	CO
1º	Host Security	4	CO
1º	Network Security (Perimeter)	4	CO
1º	Smartphone Security	4	CO
1º	IoT Security	4	CO
1º	Ethical Hacking	4	CO
1º	Reverse Engineering	4	CO
1º	Secure Development	4	CO
1º	Practical Implementation of Software and Hardware Security Policies	4	CO
1º	Forensic Analysis	4	CO
1º	Security in System Design and Development	4	CO
1º	Information Security Architectures and Models	4	CO
1º	Information Security Management System (ISMS)	4	CO
1º	IT Security Management	4	CO
1º	Security Incident Management Policies	4	CO
2º	Risk Analysis and IT Security Environment	4	CO
2º	Security Policies for the Analysis of Threats in Computer Systems	4	CO
2º	Practical Implementation of Security Policies in the Face of Attacks	4	CO
2º	Cryptography in IT	4	CO
2º	Identity and Access Management in IT Security	4	CO
2º	Security in Communications and Software Operation	4	CO
2º	Security in Cloud Environments	4	CO
2º	Monitoring Tools in Information Systems Security Policies	4	CO
2º	Security in IoT Device Communications	4	CO
2º	Business Continuity Plan Associated with Security	4	CO
2º	Practical Security Disaster Recovery Policy	5	CO
2º	Implementation of Physical and Environmental Safety Policies in the Company	5	CO
2º	Secure Communications Policies in the Company	5	CO
2º	Organizational Aspects of Information Security Policy	5	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

Advanced Master's Degree

Senior Cybersecurity Management (CISO, Chief Information Security Officer)

- Modality: **online**
- Duration: **2 years**
- Certificate: **TECH Global University**
- Accreditation: **120 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

Advanced Master's Degree

Senior Cybersecurity Management (CISO, Chief Information Security Officer)

tech global university