Master's Degree

Corporate Cybersecurity Policy Management

tech global university

tech global university

Master's Degree

Corporate Cybersecurity Policy Management

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

Website: www.techtitute.com/us/information-technology/master-degree/master-corporate-cybersecurity-policy-management

Index

01

Introduction

The increased reliance of many businesses and industries on virtual environments has, in turn, led to the proliferation of cybercrime and cyberattacks on all types of organizations. Regardless of size or location, cybersecurity threats pose a real danger that can result in significant loss of time, money and data. Therefore, the figure of the computer scientist with specific knowledge in Cybersecurity Policy Management is gaining more and more weight in the business sector, with ample opportunities for both professional and personal growth. This program offers the IT professional an unbeatable opportunity to boost their career with the support of a team of professionals who have extensive experience in the field. The 100% online format of the program also makes it a fully compatible option with all kinds of activities and responsibilities.

Enroll now and get access to specialized content on Incident Management Policies, Software and Hardware Security and Practical Security Disaster Recovery"

Thousands of cybercriminals attack companies around the world every day, and they can do so from thousands of miles away, which has made cybersecurity a major concern in the modern business landscape. Vulnerabilities in organizations that rely on virtual environments can be exploited by criminals of all kinds, stealing sensitive data or preventing access to it in exchange for a ransom.

That is why proper Corporate Cybersecurity Policy Management entails great responsibility, as this is a highly prestigious position of responsibility, and one with considerable economic projection for specialized IT professionals. Therefore, taking the plunge and studying units such as auditing systems to locate threats or secure communication protocols is a direct boost to a key position in any organization.

For this Master's Degree, a group of teachers carefully selected by TECH has prepared first-class educational content. Throughout 10 comprehensive modules, computer scientists will expand their skills in Physical and Environmental Security Policy Implementation, Information Security Management System, monitoring tools and many more competencies that will make transform them into a valuable asset for any institution.

All of this with the undeniable advantage of not having to attend classes or preset schedules, as the entire program is taught online. The educational content is available to download from any device with an internet connection, even serving as a reference guide once the program has been completed. Computer scientists will have the freedom to adapt the teaching load to their own pace, allowing them to balance it with their usual professional activity or more demanding responsibilities.

This **Master's Degree in Corporate Cybersecurity Policy Management** contains the most complete and up-to-date educational program on the market. The most important features include:

- Case studies presented by experts in Computer Cybersecurity
- The graphic, schematic and practical contents of the book provide technical and practical information on those disciplines that are essential for professional practice
- Practical exercises where self-assessment can be used to improve learning
- Its special emphasis on innovative methodologies
- 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

Position yourself as a competent Cybersecurity Policy Manager, being able to adapt to all kinds of situations and unforeseen events in terms of IT Security"

Incorporate the most effective attack security policy practices into your daily work, perfected by a teaching team of specialists in the field"

Access a multimedia-rich syllabus, reinforced with specific units on management security policies, IT risk classification and Hijacking.

You will be able to choose when, where and how to take on the entire course load, having total freedom to advance through the syllabus at your own pace.

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

Its 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 immersion education programmed to learn in real situations.

The design of this program focuses on Problem-Based Learning, by means of which the professional must try to solve the different professional practice situations that are presented throughout the academic course. For this purpose, the student will be assisted by an innovative interactive video system created by renowned experts.

02

Objectives

With cybersecurity being such an important subject in today's business world, this program assumes the role of the computer scientist as a central part of dealing with such problems. For this reason, the objectives pursued throughout the syllabus are diverse, prioritizing to offer an up-to-date theoretical content based on the latest advances in computer security.

You will have at your disposal a reference guide on Cybersecurity Policy Management that will help you boost your career as an expert computer scientist in digital security"

General Objectives

- Study the key concepts of information security in depth
- Develop the necessary measures to ensure good information security practices.
- Develop the different methodologies for conducting a comprehensive threat analysis
- Install and learn about the different tools used in the treatment and prevention of incidents

TECH's pedagogical methodology will allow you to reach your most ambitious goals even sooner than you expect"

Specific Objectives

Module 1. Information Security Management System (ISMS)

- Analyze the regulations and standards currently applicable to ISMS
- Develop the necessary phases to implement an ISMS in an entity
- Analyze information security incident management and implementation procedures

Module 2. Organizational Aspects of Information Security Policy

- Implementing an ISMS in the company
- Determine which departments should be covered by the implementation of the safety management system
- Implement necessary security countermeasures in the operation

Module 3. Security Policies for the Analysis of Threats in Computer Systems

- Analyze the meaning of threats
- Determine the phases of preventive threat management
- Compare different threat management methodologies

Module 4. Practical Implementation of Software and Hardware Security Policies

- Determine what authentication and identification are
- Analyze the different authentication methods available and their practical implementation
- Implement the correct access control policy to software and systems
- Establish the main current identification technologies
- Generate specialized knowledge on the different methodologies that exist for system hardening

Module 5. Security Incident Management Policies

- Develop specialized knowledge on how to manage incidents caused by IT security events
- Determine the operation of a security incident handling team
- Analyze the different phases of an IT security event management
- Review standardized protocols for handling security incidents

Module 6. Implementation of Physical and Environmental Safety Policies in the Company

- Analyze the term 'safe area' and 'safe perimeter
- Examine Biometrics and Biometric Systems
- Implement correct security policies for physical security
- Develop the current regulations on secure areas of computer systems

Module 7. Secure Communications Policies in the Company

- Securing a communications network by partitioning the network
- Analyze the different encryption algorithms used in communication networks.
- Implement various encryption techniques on the network such as TLS, VPN or SSH

Module 8. Practical Implementation of Security Policies against Attacks

- Determine the different real attacks to our information system
- Evaluate the various security policies to mitigate attacks
- Technically implement measures to mitigate major threats

Module 9. Information Systems Security Policy Monitoring Tools

- Develop the concept of Metrics Monitoring and Implementation
- Configure audit trails on systems and monitor networks
- Compile the best system monitoring tools currently available on the market

Module 10. Practical Security Disaster Recovery Policy

- Generate specialized knowledge on the concept of information security continuity
- Develop a business continuity plan
- Analyze an ICT continuity plan
- Design a disaster recovery plan

03

Skills

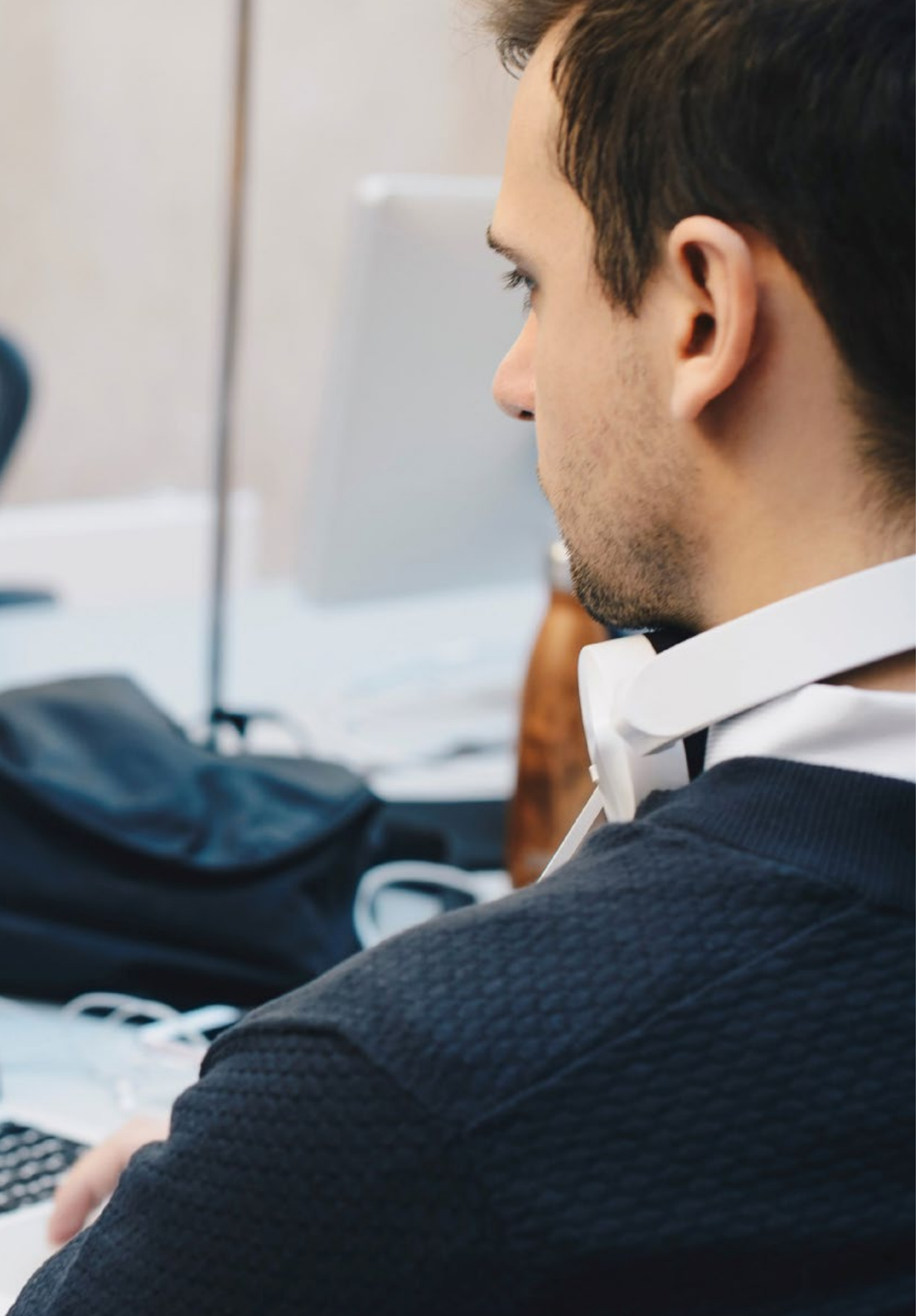
In order to develop the advanced and specialized skills that a computer scientist with expertise in Cybersecurity Policy must possess, TECH has drawn on an exceptional teaching staff. Thanks to a practical combination of their professional experience and the most recent developments in digital security, the computer scientist will gain a much greater contextualization of each unit covered, with ample examples and multimedia resources.

You will gain a skill set that will highlight the key importance in any cyber strategy plan in your organization"

General Skills

- Implement and develop a Business Continuity Plan according to each type of entity and its needs
- Develop a Business Process Analysis
- Analyze Audit methodologies
- Assess the need for a Computer Forensic Analysis for an in-depth study of the recorded incidents

You will be able to increase your career and salary projection thanks to a specialization in the unit that is currently becoming increasingly important in Cybersecurity"



Specific Skills

- Determine the involvement of an ISMS in the internal organization of the entity, as well as its status
- Establish security policies in the company
- Determine what measures we need to implement with suppliers and maintenance of information systems
- Build specialized knowledge on threat control
- Determine the phases of preventive threat management
- Develop methodologies for computer threat analysis
- Classify threats by impact and severity
- Design a proprietary methodology for the analysis and preventive control of threats
- Implement a correct access control policy to networks and services
- Analyze the importance of a correct treatment of security incidents
- Compile the different biometric systems that exist
- Examine Biometrics and Biometric Systems
- Implement the correct physical security policies and physical access control systems in data centers
- Implementing a secure network
- Examine the vulnerabilities of mobile and IoT platforms and how to avoid them
- Establish the types of social engineering and learn how to mitigate them
- Analyze the concept of monitoring and the implementation of metrics
- Determining the need for information security continuity

04

Course Management

All the professionals selected by TECH for this Master's Degree have extensive experience in the field of IT service management, always with a focus on cybersecurity and correct execution of protocols. It is precisely this experience that confers a higher quality aspect to the entire syllabus, since its eminently practical nature means that the computer scientist can adopt all the new knowledge immediately, improving his or her skills even before completing the degree.

You will have the support and help of a teaching team committed to the maximum in your professional development towards Cybersecurity Policy Management"

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
- Degree in Computer Engineering from the University of Alcalá de Henares, Madrid
- Master in DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Professors

Mr. Solana Villarias, Fabián

- Information Technology Consultant
- Developer and administrator of survey services at Investigación, Planificación y Desarrollo, S.A.
- Financial markets and IT systems maintenance specialist at Iberia Financial Software.
- Web developer and accessibility specialist at Indra
- Degree in Systems Engineering at the University of Wales/CESINE
- Diploma in Technical Engineering in Computer Systems Engineering from the University of Wales/ CESINE

Ms. López García, Rosa María

- Management Information Specialist
- Teacher at Linux Professional Institute
- Collaborator at Incibe Hacker Academy
- Cybersecurity Talent Captain at Teamciberhack
- Administrative and accounting and financial manager at Integra2Transportes
- Administrative assistant in purchasing at the Education Center Cardenal Marcelo Espínola
- Higher Technician in Cybersecurity and Ethical Hacking
- Member of Ciberpatrulla

Mr. Oropesiano Carrizosa, Francisco

- Computer Engineer
- Microcomputing, Networking and Security Technician at Cas-Training
- Web Services, CMS, e-Commerce, UI and UX Developer at Fersa Reparaciones
- Web services, content, mail and DNS manager at Oropesia Web & Network
- Graphic and web applications designer at Xarxa Sakai Projectes
- Diploma in Computer Systems at the University of Alcalá de Henares
- Master in DevOps: Docker and Kubernetes at Cyber Business Center
- Network and Computer Security Technician from the University of the Balearic Islands
- Expert in Graphic Design from the Polytechnic University of Madrid

Mr. Ortega López, Florencio

- Security Consultant (Identity Management) at SIA Group
- ICT and Security Consultant as an independent professional
- Teacher trainer in the IT sector
- Graduate in Technical Industrial Engineering at the University of Alcalá de Henares
- Master's Degree for Teachers by UNIR
- MBA in Business Administration and Management by IDE-CESEM
- Master's Degree in Information Technology Direction and Management by IDE-

Mr. Peralta Alonso, Jon

- Senior Consultant - Data Protection and Cybersecurity. Altia
- Lawyer / Legal advisor. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Legal Advisor / Intern. Professional office: Oscar Padura
- Law Degree. Public University of the Basque Country
- Master's Degree in Data Protection Officer. Escuela innovadora EIS
- Master's Degree in Law. Public University of the Basque Country
- Master's Degree in Civil Litigation Practice. Isabel I de Castilla International University
- Professor in Master's Degree in Personal Data Protection, Cybersecurity and ICT Law

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

05

Structure and Content

TECH has used the *Relearning* methodology to develop all the contents of this program. This means that the most important key concepts in Cybersecurity Policy Management are taught progressively throughout the syllabus, resulting in a much more effective and faster learning process. The computer scientist will have access to numerous detailed videos, self-knowledge exercises and complementary readings made and selected specifically for each unit of the program.

All the multimedia material contained in this Master's Degree will help you to specialize much more quickly and comprehensively"

Module 1. Information security management system (ISMS)

1.1. Information Security Key Aspects
- 1.1.1. Information Security
  - 1.1.1.1. Confidentiality
  - 1.1.1.2. Integrity
  - 1.1.1.3. Availability
  - 1.1.1.4. Information Security Measurements

1.2. Information Security Management Systems
- 1.2.1. Information Security Management Models
- 1.2.2. Documents to Implement an ISMS
- 1.2.3. Levels and Controls of an ISMS

1.3. International Norms and Standards
- 1.3.1. International Standards in Information Security
- 1.3.2. Origin and Evolution of the Standard
- 1.3.3. International Information Security Management Standards
- 1.3.4. Other Reference Standards

1.4. ISO/IEC 27,000 Standards
- 1.4.1. Purpose and Areas of Application
- 1.4.2. Structure of the Standard
- 1.4.3. Certification
- 1.4.4. Accreditation Phases
- 1.4.5. Benefits of ISO/IEC 27,000 Standards

1.5. Design and Implementation of a General Information Security System
- 1.5.1. Phases of Implementation of a General Information Security System
- 1.5.2. Business Continuity Plans

1.6. Phase I: Diagnosis
- 1.6.1. Preliminary Diagnosis
- 1.6.2. Identification of the Stratification Level
- 1.6.3. Level of Compliance with Standards/Norms

1.7. Phase II: Preparation
- 1.7.1. Context of the Organization
- 1.7.2. Analysis of Applicable Safety Regulations
- 1.7.3. Scope of the General Information Security System
- 1.7.4. General Information Security System Policy
- 1.7.5. Objectives of the General Information Security System

1.8. Phase III: Planning
- 1.8.1. Asset Classification
- 1.8.2. Risk Assessment
- 1.8.3. Identification of Threats and Risks

1.9. Phase IV: Implementation and Follow-up
- 1.9.1. Analysis of Results
- 1.9.2. Assigning Responsibilities
- 1.9.3. Timing of the Action Plan
- 1.9.4. Monitoring and Audits

1.10. Incident Management Security Policies
- 1.10.1. Phases
- 1.10.2. Incident Categorization
- 1.10.3. Incident Management and Procedures

Module 2. Organizational Aspects of Information Security Policy

2.1. Internal Organization
- 2.1.1. Assigning Responsibilities
- 2.1.2. Segregation of Duties
- 2.1.3. Contacts with Authorities
- 2.1.4. Information Security in Project Management

2.2. Asset Management
- 2.2.1. Liability for Assets
- 2.2.2. Classification of Information
- 2.2.3. Handling of Storage Media

2.3. Security Policies in Business Processes
  2.3.1. Analysis of the Vulnerabilities of Business Processes
  2.3.2. Business Impact Analysis
  2.3.3. Classification of Processes with Respect to Business Impact
2.4. Security Policies Linked to Human Resources
  2.4.1. Before Hiring
  2.4.2. During Contracting
  2.4.3. Termination or Change of Position
2.5. Management Security Policies
  2.5.1. Management Guidelines on Information Security
  2.5.2. BIA - Analyzing the Impact
  2.5.3. Recovery Plan as a Security Policy
2.6. Acquisition and Maintenance of Information Systems
  2.6.1. Information Systems Security Requirements
  2.6.2. Development and Support Data Security
  2.6.3. Test Data
2.7. Security with Suppliers
  2.7.1. IT Security with Suppliers
  2.7.2. Management of Service Delivery with Assurance
  2.7.3. Supply Chain Security
2.8. Operational Safety
  2.8.1. Operational Responsibilities
  2.8.2. Protection Against Malicious Code
  2.8.3. Backup Copies
  2.8.4. Activity and Supervision Records
2.9. Safety and Regulatory Management
  2.9.1. Compliance with Legal Requirements
  2.9.2. Information Security Reviews
2.10. Business Continuity Management Security
  2.10.1. Continuity of Information Security
  2.10.2. Redundancies

Module 3. Security Policies for the Analysis of Threats in Computer Systems

3.1. Threat Management in Security Policies
  3.1.1. Risk Management
  3.1.2. Security Risk
  3.1.3. Threat Management Methodologies
  3.1.4. Implementation of Methodologies
3.2. Phases of Threat Management
  3.2.1. Identification
  3.2.2. Analysis
  3.2.3. Localisation
  3.2.4. Safeguard Measures
3.3. Audit Systems for Threat Localization
  3.3.1. Classification and Information Flow
  3.3.2. Analysis of Vulnerable Processes
3.4. Risk Classification
  3.4.1. Types of Risk
  3.4.2. Calculation of Threat Probability
  3.4.3. Residual Risk
3.5. Risk Treatment
  3.5.1. Implementation of Safeguard Measures
  3.5.2. Transfer or Assume
3.6. Control Risks
  3.6.1. Continuous Risk Management Process
  3.6.2. Implementation of Security Metrics
  3.6.3. Strategic Model of Information Security Metrics
3.7. Practical Methodologies for Threat Analysis and Control
  3.7.1. Threat Catalog
  3.7.2. Catalog of Control Measures
  3.7.3. Safeguards Catalog

3.8. ISO 27005
- 3.8.1. Risk Identification
- 3.8.2. Risk Analysis
- 3.8.3. Risk Evaluation

3.9. Risk, Impact and Threat Matrix
- 3.9.1. Data, Systems and Personnel
- 3.9.2. Threat Probability
- 3.9.3. Magnitude of Damage

3.10. Design of Phases and Processes in Threat Analysis
- 3.10.1. Identification of Critical Organizational Elements
- 3.10.2. Determination of Threats and Impacts
- 3.10.3. Impact and Risk Analysis
- 3.10.4. Methods

Module 4. Practical Implementation of Software and Hardware Security Policies

4.1. Practical Implementation of Software and Hardware Security Policies
- 4.1.1. Implementation of Identification and Authorization
- 4.1.2. Implementation of Identification Techniques
- 4.1.3. Technical Authorization Measures

4.2. Identification and Authorization Technologies
- 4.2.1. Identifier and OTP
- 4.2.2. *USB Token* or PKI Smart Card
- 4.2.3. The "Confidential Defense" Key
- 4.2.4. Active RFID

4.3. Software and Systems Access Security Policies
- 4.3.1. Implementation of Access Control Policies
- 4.3.2. Implementation of Communications Access Policies
- 4.3.3. Types of Security Tools for Access Control

4.4. User Access Management
- 4.4.1. Access Rights Management
- 4.4.2. Segregation of Roles and Access Functions
- 4.4.3. Implementation of Access Rights in Systems

4.5. Access Control to Systems and Applications
- 4.5.1. Minimum Access Rule
- 4.5.2. Secure Logon Technologies
- 4.5.3. Password Security Policies

4.6. Identification Systems Technologies
- 4.6.1. Active Directory
- 4.6.2. OTP
- 4.6.3. PAP, CHAP
- 4.6.4. KERBEROS, DIAMETER, NTLM

4.7. CIS Controls for Systems Hardening
- 4.7.1. Basic CIS Controls
- 4.7.2. Fundamental CIS Controls
- 4.7.3. Organizational CIS Controls

4.8. Operational Safety
- 4.8.1. Protection Against Malicious Code
- 4.8.2. Backup Copies
- 4.8.3. Activity Log and Supervision

4.9. Management of Technical Vulnerabilities
- 4.9.1. Technical Vulnerabilities
- 4.9.2. Technical Vulnerability Management
- 4.9.3. Restrictions on Software Installation

4.10. Implementation of Security Policy Practices
- 4.10.1. Logical Vulnerabilities
- 4.10.2. Implementation of Defense Policies

Module 5. Security Incident Management Policies

5.1. Information Security Incident Management Policies and Enhancements
- 5.1.1. Incident Management
- 5.1.2. Responsibilities and Procedures
- 5.1.3. Event Notification

5.2. Intrusion Detection and Prevention Systems (IDS/IPS)
- 5.2.1. System Operating Data
- 5.2.2. Types of Intrusion Detection Systems
- 5.2.3. Criteria for IDS/IPS Placement

5.3. Security Incident Response
- 5.3.1. Data Collection Procedure
- 5.3.2. Intrusion Verification Process
- 5.3.3. CERT Organizations

5.4. Intrusion Attempt Notification and Management Process
- 5.4.1. Responsibilities in the Notification Process
- 5.4.2. Classification of Incidents
- 5.4.3. Resolution and Recovery Process

5.5. Forensic Analysis as a Security Policy
- 5.5.1. Volatile and Non-Volatile Evidence
- 5.5.2. Analysis and Collection of Electronic Evidence
  - 5.5.2.1. Analysis of Electronic Evidence
  - 5.5.2.2. Collection of Electronic Evidence

5.6. Intrusion Detection and Prevention Systems (IDS/IPS) Tools
- 5.6.1. *Snort*
- 5.6.2. Suricata
- 5.6.3. Solar-Winds

5.7. Event Centralizing Tools
- 5.7.1. SIM
- 5.7.2. SEM
- 5.7.3. SIEM

5.8. CCN-STIC Security Guide 817
- 5.8.1. Cyber Incident Management
- 5.8.2. Metrics and Indicators

5.9. NIST SP800-61
- 5.9.1. Computer Security Incident Response Capability
- 5.9.2. Handling an Incident
- 5.9.3. Coordination and Information Sharing

5.10. ISO 27035
- 5.10.1. ISO 27035 Standard. Incident Management Principles
- 5.10.2. Incident Management Plan Preparation Guidelines
- 5.10.3. Incident Response Operations Guides

Module 6. Implementation of Physical and Environmental Safety Policies in the Company

6.1. Security Areas
- 6.1.1. Physical Security Perimeter
- 6.1.2. Working in Safe Areas
- 6.1.3. Security of Offices, Offices and Resources

6.2. Physical Input Controls
- 6.2.1. Physical Access Control Policies
- 6.2.2. Physical Input Control Systems

6.3. Physical Access Vulnerabilities
- 6.3.1. Main Physical Vulnerabilities
- 6.3.2. Implementation of Safeguards Measures

6.4. Physiological Biometric Systems
- 6.4.1. Fingerprint
- 6.4.2. Facial Recognition
- 6.4.3. Iris and Retinal Recognition
- 6.4.4. Other Physiological Biometric Systems

6.5. Biometric Behavioral Systems
- 6.5.1. Signature Recognition
- 6.5.2. Writer Recognition
- 6.5.3. Voice Recognition
- 6.5.4. Other Biometric Behavioral Systems

6.6. Biometrics Risk Management
- 6.6.1. Implementation of Biometric Systems
- 6.6.2. Vulnerabilities of Biometric Systems

6.7. Implementation of Policies in *Hosts*
- 6.7.1. Installation of Supply and Security Cabling
- 6.7.2. Equipment Location
- 6.7.3. Exit of the Equipment Outside the Premises
- 6.7.4. Unattended Computer Equipment and Clear Post Policy

6.8. Environmental Protection
- 6.8.1. Fire Protection Systems
- 6.8.2. Earthquake Protection Systems
- 6.8.3. Earthquake Protection Systems

6.9. Data Processing Center Security
- 6.9.1. Security Doors
- 6.9.2. Video Surveillance Systems (CCTV)
- 6.9.3. Safety Control

6.10. International Physical Security Regulations
- 6.10.1. IEC 62443-2-1 (European)
- 6.10.2. NERC CIP-005-5 (USA)
- 6.10.3. NERC CIP-014-2 (USA)

Module 7. Secure Communications Policies in the Company

7.1. Network Security Management
- 7.1.1. Network Control and Monitoring
- 7.1.2. Segregation of Networks
- 7.1.3. Network Security Systems

7.2. Secure Communication Protocols
- 7.2.1. TCP/IP Model
- 7.2.2. IPSEC Protocol
- 7.2.3. TLS Protocol

7.3. Protocol TLS 1.3
- 7.3.1. Phases of a TLS1.3 Process
- 7.3.2. *Handshake* Protocol
- 7.3.3. Registration Protocol
- 7.3.4. Differences with TLS 1.2

7.4. Cryptographic Algorithms
- 7.4.1. Cryptographic Algorithms Used in Communications
- 7.4.2. *Cipher-Suites*
- 7.4.3. Cryptographic Algorithms allowed for TLS 1.3

7.5. *Digest* Functions
- 7.5.1. MD6
- 7.5.2. SHA

7.6. PKI. Public Key Infrastructure
- 7.6.1. PKI and its Entities
- 7.6.2. Digital Certificate
- 7.6.3. Types of Digital Certificates

7.7. Tunnel and Transport Communications
- 7.7.1. Tunnel Communications
- 7.7.2. Transport Communications
- 7.7.3. Encrypted Tunnel Implementation

7.8. SSH. *Secure Shell*
- 7.8.1. SSH. Safe Capsule
- 7.8.2. SSH Functions
- 7.8.3. SSH Tools

7.9. Audit of Cryptographic Systems
- 7.9.1. Integration Test
- 7.9.2. Cryptographic System Testing

7.10. Cryptographic Systems
- 7.10.1. Cryptographic Systems Vulnerabilities
- 7.10.2. Cryptographic Safeguards

Module 8. Practical Implementation of Security Policies against Attacks

8.1. *System Hacking*
- 8.1.1. Risks and Vulnerabilities
- 8.1.2. Countermeasures

8.2. DoS Attack
- 8.2.1. Risks and Vulnerabilities
- 8.2.2. Countermeasures

8.3. *Session Hijacking*
- 8.3.1. The process of *Hijacking*
- 8.3.2. *Hijacking* Countermeasures

8.4. Evading IDS, *Firewalls and Honeypots*
- 8.4.1. Avoidance Techniques
- 8.4.2. Implementation of Countermeasures

8.5. *Hacking Web Servers*
- 8.5.1. Attacks on Web Servers
- 8.5.2. Implementation of Defense Measures

8.6. *Hacking Web Applications*
- 8.6.1. Attacks on Web Applications
- 8.6.2. Implementation of Defense Measures

8.7. *Hacking Wireless Networks*
- 8.7.1. Vulnerabilities in Wi-Fi Networks
- 8.7.2. Implementation of Defense Measures

8.8. *Hacking Mobile Platforms*
- 8.8.1. Vulnerabilities of Mobile Platforms
- 8.8.2. Implementation of Countermeasures

8.9. *Ramsonware*
- 8.9.1. *Ramsonware* Vulnerabilities
- 8.9.2. Implementation of Countermeasures

8.10. Social Engineering
- 8.10.1. Types of Social Engineering
- 8.10.2. Countermeasures for Social Engineering

Module 9. Information Systems Security Policy Monitoring Tools

9.1. Information Systems Monitoring Policies
- 9.1.1. System Monitoring
- 9.1.2. Metrics
- 9.1.3. Types of Metrics

9.2. Systems Auditing and Registration
- 9.2.1. Systems Auditing and Registration
- 9.2.2. Windows Auditing and Logging
- 9.2.3. Linux Auditing and Logging

9.3. SNMP Protocol. *Simple Network Management Protocol*
- 9.3.1. SNMP Protocol
- 9.3.2. SNMP Functions
- 9.3.3. SNMP Tools

9.4. Network Monitoring
- 9.4.1. Network Monitoring in Control Systems
- 9.4.2. Monitoring Tools for Control Systems

9.5. Nagios. Network Monitoring System
- 9.5.1. Nagios
- 9.5.2. Operation of Nagios
- 9.5.3. Nagios Installation

9.6. Zabbix. Network Monitoring System
- 9.6.1. Zabbix.
- 9.6.2. How Zabbix Works
- 9.6.3. Zabbix Installation

9.7. Cacti. Network Monitoring System
- 9.7.1. Cacti
- 9.7.2. How Cacti Works
- 9.7.3. Installation of Cacti

9.8. Pandora. Network Monitoring System
- 9.8.1. Pandora.
- 9.8.2. Operation of Pandora
- 9.8.3. Pandora Installation

9.9. *SolarWinds*. Network Monitoring System
- 9.9.1. *SolarWinds*
- 9.9.2. Operation of *SolarWinds*
- 9.9.3. Installation of *SolarWinds*

9.10. Monitoring Regulations
- 9.10.1. CIS Controls Over Auditing and Record Keeping
- 9.10.2. NIST 800-123 (U.S.A.)

Module 10. Practical Security Disaster Recovery Policy

10.1. DRP. Disaster Recovery Plan
- 10.1.1. Objective of a DRP
- 10.1.2. Benefits of a DRP
- 10.1.3. Consequences of a Missing and Not up-to-Date DRP

10.2. Guidance for Defining a DRP (Disaster Recovery Plan)
- 10.2.1. Scope and Objectives
- 10.2.2. Recuperation Strategy Design
- 10.2.3. Assignment of Roles and Responsibilities
- 10.2.4. Inventory of Hardware, Software and Services
- 10.2.5. Tolerance for Downtime and Data Loss
- 10.2.6. Establishment of the Specific Types of DRP Required
- 10.2.7. Implementation of a Training, Awareness and Communication Plan.

10.3. Scope and Objectives of a DRP (Disaster Recovery Plan)
- 10.3.1. Response Guarantee
- 10.3.2. Technological Components
- 10.3.3. Scope of the Continuity Policy

10.4. Disaster Recovery Plan (DRP) Strategy Design
- 10.4.1. Disaster Recovery Strategy
- 10.4.2. Budget
- 10.4.3. Human and Physical Resources
- 10.4.4. Management Positions at Risk
- 10.4.5. Technology
- 10.4.6. Date:

10.5. Continuity of Information Processes
- 10.5.1. Continuity Planning
- 10.5.2. Continuity Implementation
- 10.5.3. Verification of Continuity Assessment

10.6. Scope of a BCP (Business Continuity Plan)
- 10.6.1. Determination of the Most Critical Processes
- 10.6.2. Asset-Based Approach
- 10.6.3. Process Approach

10.7. Implementation of Guaranteed Business Processes
- 10.7.1. Priority Activities (PA)
- 10.7.2. Ideal Recovery Times (IRT)
- 10.7.3. Survival Strategies

10.8. Organizational Analysis
- 10.8.1. Acquisition of information
- 10.8.2. Business Impact Analysis (BIA)
- 10.8.3. Risk Analysis in the Organization

10.9. Response to Contingency
- 10.9.1. Crisis Plan
- 10.9.2. Operational Environment Recovery Plans
- 10.9.3. Technical Work or Incident Procedures

10.10. International Standard ISO 27031 BCP
- 10.10.1. Objectives
- 10.10.2. Terms and Definitions
- 10.10.3. Operation

06

Methodology

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

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

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

Case Study to contextualize all content

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

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

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

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

A learning method that is different and innovative

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

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

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

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

Relearning Methodology

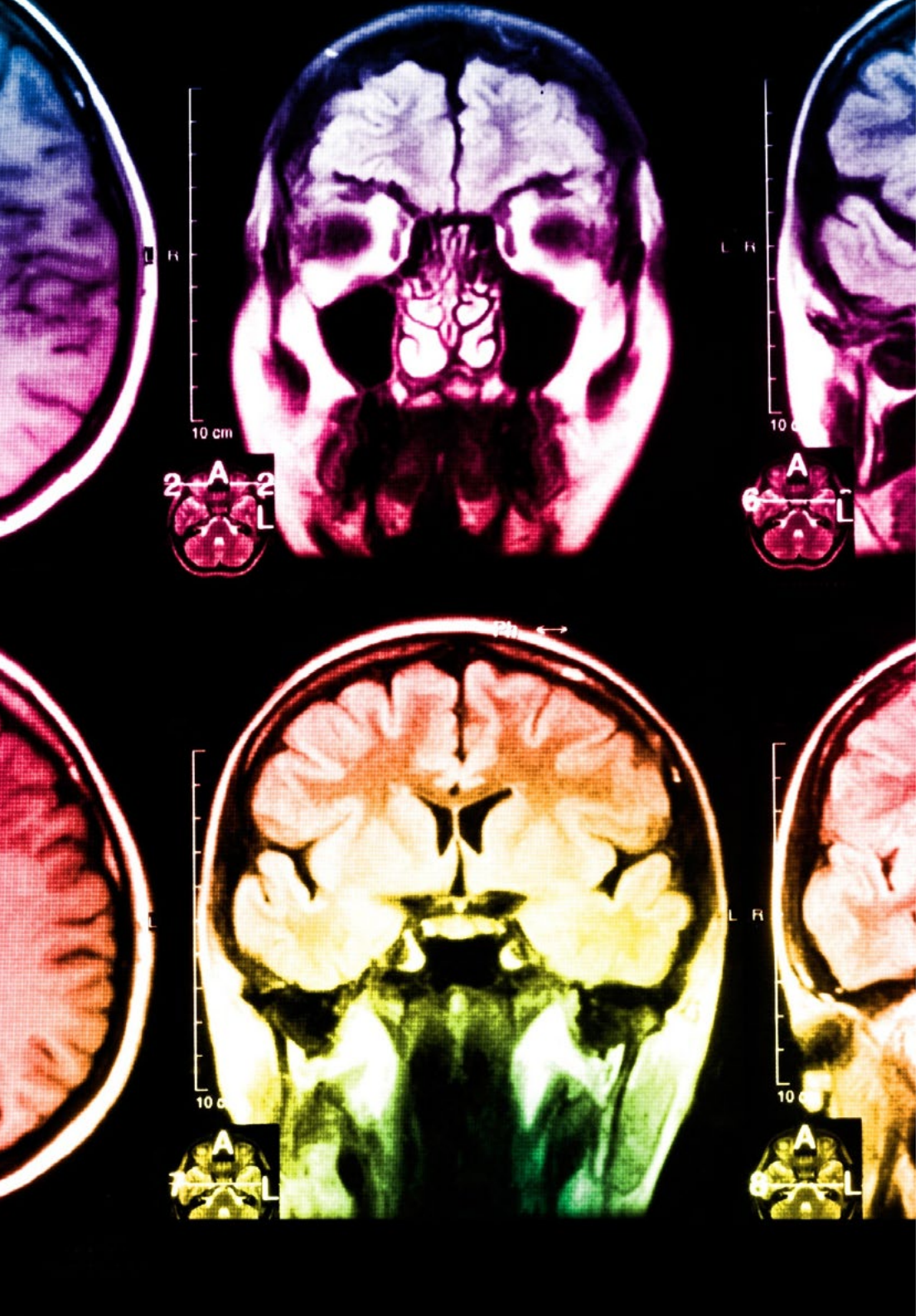
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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

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

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

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



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

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

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

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

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

Study Material

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

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

Classes

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

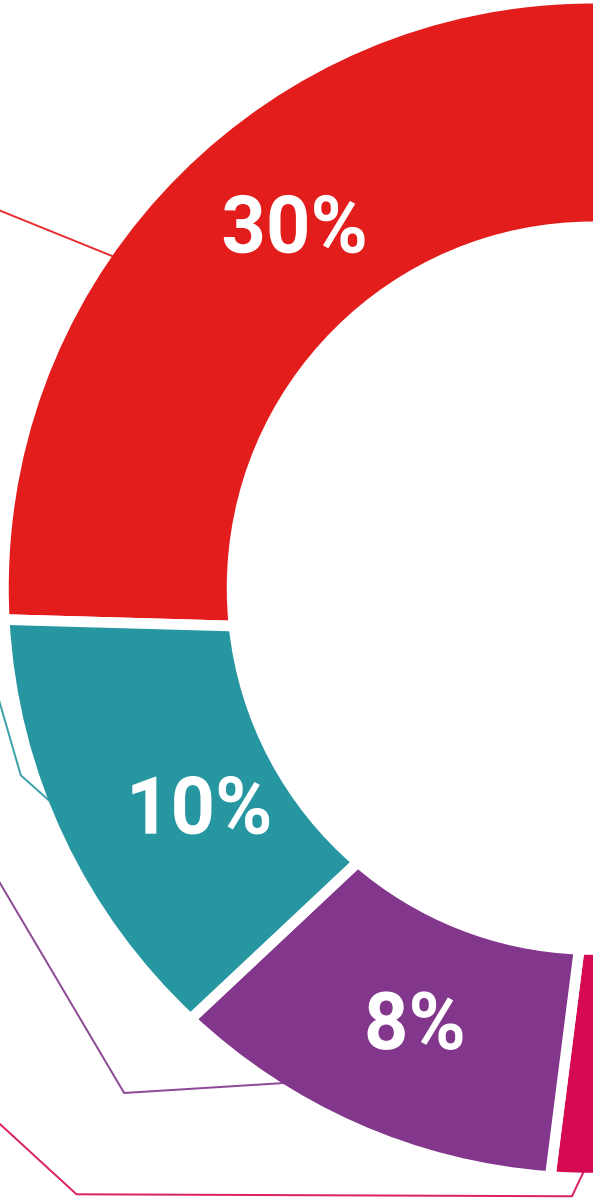
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

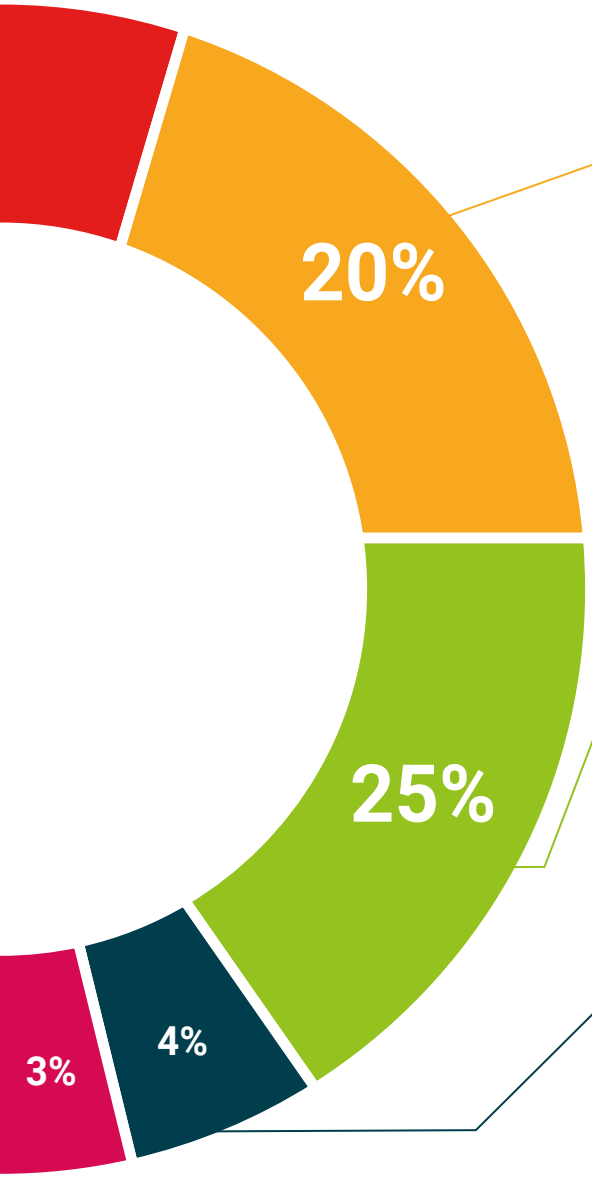
Practising Skills and Abilities

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

Additional Reading

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





Case Studies

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

Interactive Summaries

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

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

Testing & Retesting

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

07

Certificate

This Master's Degree in Corporate Cybersecurity Policy Management guarantees students, in addition to the most rigorous and up-to-date education, access to a Hybrid 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 program will allow you to obtain your **Master's Degree diploma in Corporate Cybersecurity Policy Management** endorsed by **TECH Global University**, the world's largest online university.

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

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

Title: **Master's Degree in Corporate Cybersecurity Policy Management**

Modality: **online**

Duration: **12 months**

Accreditation: **60 ECTS**


tech global university

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

Master's Degree diploma in Corporate Cybersecurity Policy Management

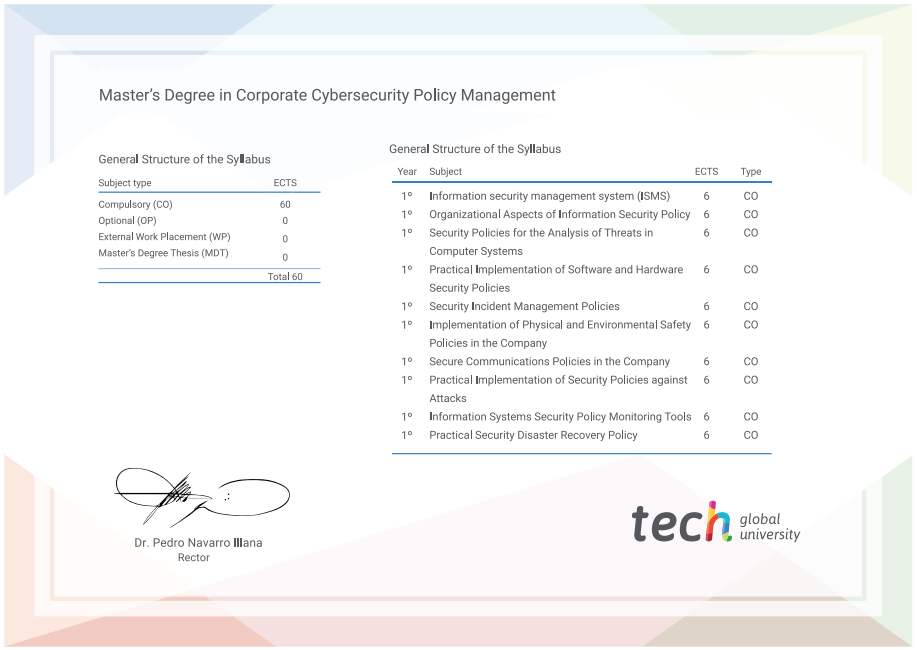
This is a program of 1,500 hours of duration equivalent to 60 ECTS, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

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

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

Dr. Pedro Navarro Illana
Rector

Unique TECH Code: AFWORD23S techtitute.com/certificates


Master's Degree in Corporate Cybersecurity Policy Management

General Structure of the Syllabus

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

General Structure of the Syllabus

Year	Subject	ECTS	Type
1º	Information security management system (ISMS)	6	CO
1º	Organizational Aspects of Information Security Policy	6	CO
1º	Security Policies for the Analysis of Threats in Computer Systems	6	CO
1º	Practical Implementation of Software and Hardware Security Policies	6	CO
1º	Security Incident Management Policies	6	CO
1º	Implementation of Physical and Environmental Safety Policies in the Company	6	CO
1º	Secure Communications Policies in the Company	6	CO
1º	Practical Implementation of Security Policies against Attacks	6	CO
1º	Information Systems Security Policy Monitoring Tools	6	CO
1º	Practical Security Disaster Recovery Policy	6	CO

Dr. Pedro Navarro Illana
Rector

tech global university

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

tech global university

Master's Degree

Corporate Cybersecurity Policy Management

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

Master's Degree

Corporate Cybersecurity Policy Management

tech global university