Professional Master's Degree
Advanced Cybersecurity Management

tech technological university

tech technological university

Professional Master's Degree
Advanced Cybersecurity Management

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

Website: **www.techtitute.com/in/information-technology/professional-master-degree/master-advanced-cybersecurity-management**

Index

01 Introduction p. 4

02 Objectives p. 8

03 Skills p. 14

04 Course Management p. 18

05 Structure and Content p. 24

06 Methodology p. 36

07 Certificate p. 44

01

Introduction

Today's world is moving towards complete digitalization. More and more processes, operations and basic tasks of all kinds are being performed through an electronic device. But this progress also has certain risks, as computers, *smartphones*, *tablets* and all kinds of digital applications can be susceptible to cyber-attacks. For that reason, many companies are looking for experts who can effectively lead and manage the cybersecurity of their services. Thus, this new professional profile is in great demand, so this program has been designed to provide the latest knowledge and techniques to the computer scientist, who will be prepared to be the director of cybersecurity in any company that requires it.

This program will prepare you intensively to specialize in cybersecurity management, the most demanded professional profile in the IT field today"

In recent years, the digitization process has accelerated, driven by the continuous advances in information technology. Thus, not only technology has enjoyed great improvements, but also the digital tools themselves with which many tasks are performed today. For example, these advances have made it possible for many banking operations to be carried out from a mobile application. There have also been new developments in the healthcare field, in appointment systems or in access to medical records. In addition, thanks to these technologies, it is possible to consult invoices or request services from companies in areas such as telephony.

But these advances have also led to an increase in computer vulnerabilities. Thus, while the options for performing various activities and tasks have expanded, attacks on the security of devices, applications and websites have increased proportionally. As a result, more and more companies are looking for cybersecurity professionals who are able to provide them with adequate protection against all types of cyber-attacks.

Thus, the profile of Cybersecurity Manager is one of the most sought after by companies that operate on the Internet or have services in the digital environment. And to respond to this demand, TECH has designed this Professional Master's Degree in Advanced Cybersecurity Management, which will provide the computer scientist with all the necessary tools to exercise this position effectively and taking into account the latest developments in protection and vulnerabilities in this technological field.

In this program, you will be able to delve deeper into aspects such as security in the development and design of systems, techniques or security in *Cloud Computing* environments. It will do so through a 100% online methodology with which you will be able to combine your professional work with your studies, without rigid schedules or uncomfortable trips to an academic center. In addition, you will enjoy numerous multimedia teaching resources, taught by the most prestigious and specialized faculty in the field of cybersecurity.

This **Professional Master's Degree in Advanced Cybersecurity Management** contains the most complete and up to date scientific program on the market. Its most notable features are:

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

> *Get to know, first hand, the best security techniques applied to Cloud Computing environments or Blockchain technology"*

You will enjoy numerous multimedia contents to speed up your learning process, while receiving the support of a faculty of great prestige in the field of cybersecurity"

TECH's online methodology will allow you to choose the time and place to study, without hindering your professional work.

You will be able to become the Cybersecurity Manager of the best companies in your field.

The program includes, in its teaching staff, professionals from the sector who bring to this training the experience of their work, in addition to recognized specialists from prestigious reference societies and universities.

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

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

02

Objectives

The rapid development of information technologies has brought great advances, providing numerous services to the population as a whole. However, the number of vulnerabilities and cyber-attacks has also increased, so the main objective of this Professional Master's Degree is to turn the computer scientist into a true specialist in cybersecurity management, guaranteeing them a huge and immediate professional progress. Your new skills will provide you with the opportunity to gain access to large companies operating digitally in various sectors.

> *The objective of this program is to make you a professional prepared to lead the cybersecurity department of a large company"*

General Objectives

- Generate specialized knowledge about an information system, types and security aspects that must be taken into account
- Identify the vulnerabilities of an information system
- Develop legal regulations and criminalization of the crime attacking an information system
- Evaluate the different security architecture models to establish the most appropriate model for the organization
- Identify the regulatory frameworks of application and their regulatory bases
- Analyze the organizational and functional structure of an information security area (the CISO's office)
- Analyze and develop the concept of risk and uncertainty within the environment in which we live
- Examine the Risk Management Model based on ISO 31.000
- Examine the science of cryptology and the relationship to its branches: cryptography, cryptanalysis, steganography and stegoanalysis
- Analyze the types of cryptography according to the type of algorithm and according to its use
- Examine digital certificates
- Examine the Public Key Infrastructure (PKI)
- Develop the concept of identity management
- Identify authentication methods
- Generate specialized knowledge about the IT security ecosystem
- Assessing knowledge in terms of cybersecurity
- Identify the areas of *Cloud* security
- Analyze the services and tools in each of the security areas
- Develop security specifications for each LPWAN technology
- Analyze comparatively the security of LPWAN technologies

> *Your professional goals are now within your reach thanks to this Professional Master's Degree, which provides the most advanced knowledge in cybersecurity"*

Specific Objectives

Module 1. Security in System Design and Development

- Evaluate the security of an information system in all its components and layers
- Identify current security threat types and trends
- Establish security guidelines by defining security and contingency policies and plans
- Analyze strategies and tools to ensure the integrity and security of information systems
- Apply specific techniques and tools for each type of attack or security vulnerability
- Protect sensitive information stored in the information system
- Have the legal framework and typification of the crime, completing the vision with the typification of the offender and his victim

Module 2. Information Security Architectures and Models

- Align the Safety Management Plan with the strategic objectives of the organization
- Establish an ongoing risk management framework as an integral part of the Security Management Plan
- Determine appropriate indicators for monitoring the implementation of the ISMS
- Establish a policy-based security strategy
- Analyze the objectives and procedures associated with the employee, supplier and partner awareness plan
- Identify, within the regulatory framework, the regulations, certifications and laws applicable in each organization
- Develop the fundamental elements required by the ISO 27001:2013 standard
- Implement a privacy management model in line with the European GDPR/RGPD regulation

Module 3. IT Security Management

- Identify the different structures that an information security area can have
- Develop a security model based on three lines of defence
- Present the different periodic and extraordinary committees in which the cybersecurity area is involved
- Specify the technological tools that support the main functions of the security operations team (SOC)
- Evaluate vulnerability control measures appropriate to each scenario
- Develop the security operations framework based on the NIST CSF
- Specify the scope of the different types of audits (*Red Team*, *Pentesting*, *Bug Bounty*, etc.)
- Propose the activities to be carried out after a security incident
- Set up an information security command center that encompasses all relevant stakeholders (authorities, customers, suppliers, etc.)

Module 4. Risk Analysis and IT Security Environment

- Examine, with a holistic vision, the environment in which we move
- Identify the main risks and opportunities that may affect the achievement of our objectives
- Analyze risks based on the best practices available to us
- Assessing the potential impact of these risks and opportunities
- Develop techniques to deal with risks and opportunities in a way that maximizes value contribution
- Examine in depth the different risk and value transfer techniques
- Generate value from the design of proprietary models for agile risk management
- Examine results to propose continuous improvements in project and process management based on *risk-driven* management models
- Innovate and transform general data into relevant information for risk-based decision making

Module 5. Cryptography in IT

- Compile the fundamental operations (XOR, large numbers, substitution and transposition) and the various components (One-Way functions, Hash, random number generators)
- Analyze cryptographic techniques
- Develop the different cryptographic algorithms
- Demonstrate the use of digital signatures and their application in digital certificates
- Assess key management systems and the importance of cryptographic key lengths
- Examine key derivation algorithms
- Analyze the life cycle of keys
- Evaluate block cipher and stream cipher modes
- Determine pseudorandom number generators
- Develop real-world cryptography application cases, such as Kerberos, PGP or smart cards
- Examine related associations and organizations, such as ISO, NIST or NCSC
- Determine the challenges in quantum computing cryptography

Module 6. Identity and Access Management in IT Security

- Develop the concept of digital identity
- Assessing physical access control to information
- Foundation of biometric authentication and MFA authentication
- Assess attacks related to information confidentiality
- Analyze the federation of identities
- Establish network access control

Module 7. Security in Communications and Software Operation

- Develop specialized physical and logical security knowledge
- Demonstrate knowledge of communications and networks
- Identify major malicious attacks
- Establish a secure development framework
- Demonstrate knowledge of the main information security management system regulations
- Support the operation of a cybersecurity operations center
- Demonstrate the importance of having cybersecurity practices for organizational disasters

Module 8. Security in *Cloud* Environments

- Identifying risks of a public *cloud* infrastructure deployment
- Define security requirements
- Developing a security plan for a *cloud* deployment
- Identify the *cloud* services to be deployed for the execution of a security plan
- Determine the operations necessary for the prevention mechanisms
- Establish guidelines for a *logging* and monitoring system
- Propose incident response actions

Module 9. Security in IoT Device Communications

- Introduce the simplified IoT architecture
- Substantiate the differences between generalist connectivity technologies and connectivity technologies for IoT
- Establish the concept of the iron triangle of IoT connectivity
- Analyze the security specifications of LoRaWAN technology, NB-IoT technology and WiSUN technology
- Justify the choice of the appropriate IoT technology for each project

Module 10. Business Continuity Plan Associated with Security

- Present the key elements of each phase and analyze the characteristics of the Business Continuity Plan (BCP)
- Substantiate the need for a Business Continuity Plan
- Determine the success and risk maps for each phase of the Business Continuity Plan
- Specify how to establish an Action Plan for implementation
- Assess the completeness of a Business Continuity Plan (BCP)
- Develop a plan for the successful implementation of a Business Continuity Plan

03
Skills

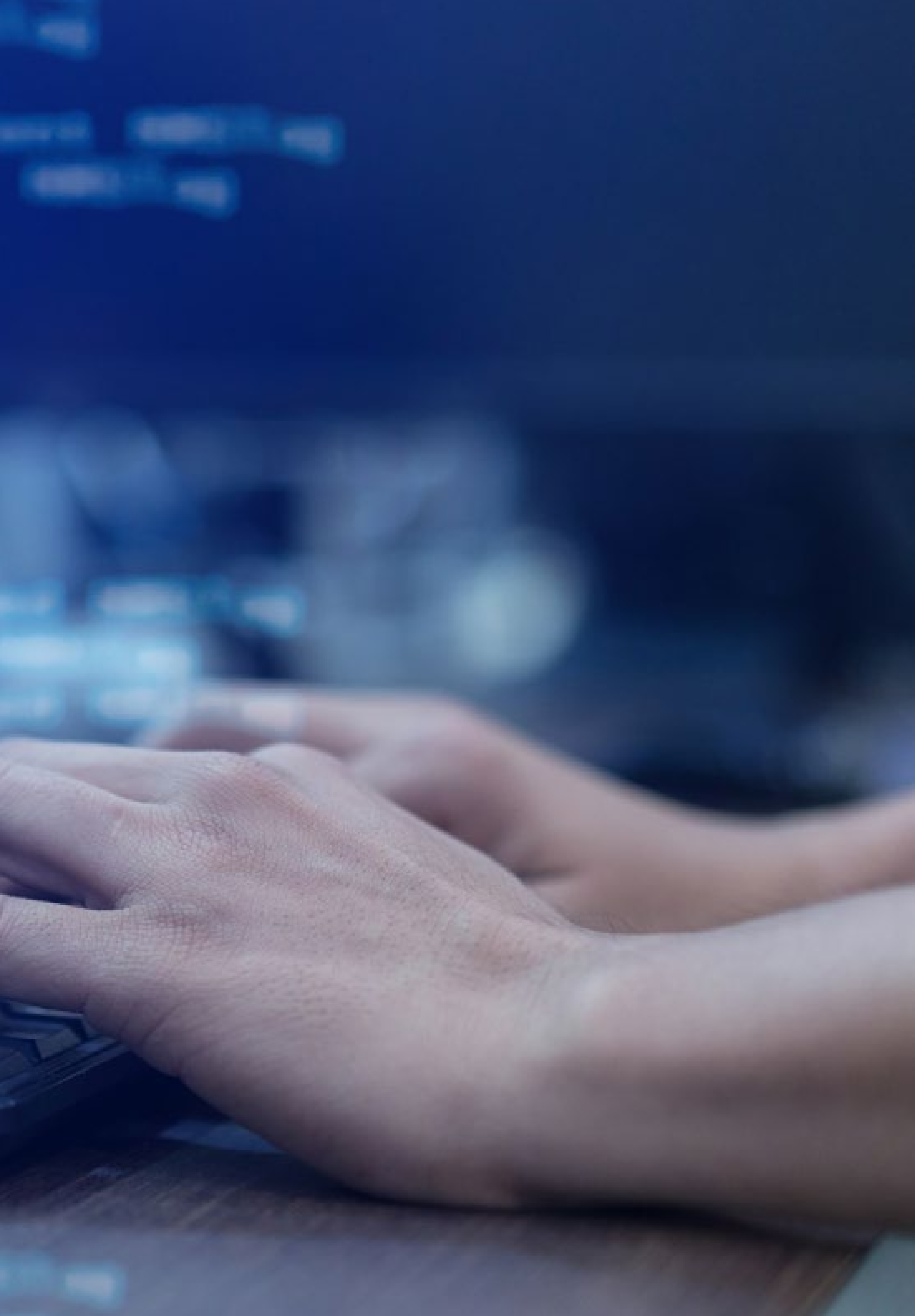
Thanks to this Professional Master's Degree, the professional will acquire numerous new skills in the field of cybersecurity. The emergence in the last few years of technologies such as the *Blockchain*, *Cloud Computing* or artificial intelligence has led to the development of new areas of cybersecurity. For that reason, this program has been specially designed to provide the professional with all the necessary skills to adapt to these booming technologies.

> *The skills that this Professional Master's Degree will provide you with will allow you to update and adapt to the new IT environment, where technologies such as Blockchain or artificial intelligence have burst onto the scene"*

General Skills

- Apply the most appropriate security measures depending on the threats
- Determine the security policy and plan for a company's information system, completing the design and implementation of the Contingency Plan
- Establish an audit program that meets the organization's cybersecurity self assessment needs
- Develop a vulnerability scanning and monitoring program and a cybersecurity incident response plan
- Maximize the opportunities presented and eliminate exposure to all potential risks from the design itself
- Compile key management systems
- Assessing a company's information security
- Analyze information access systems
- Develop best practices in secure development
- Present the risks for companies of not having an IT security environment

> *Not only will you improve your cybersecurity skills, but you will prepare yourself to lead this department in any large internet or digitally operated company"*



Specific Skills

- Develop an Information Security Management System (ISMS)
- Identify the key elements that make up an ISMS
- Apply the MAGERIT methodology to evolve the model and take it a step further
- Design new risk management methodologies based on the *agile risk management* concept
- Identify, analyze, evaluate and treat the risks faced by the professional from a new business perspective based on a *risk-driven* model that allows not only to survive in its own environment, but also to boost the contribution of its own value
- Examine the process of designing a security strategy when deploying corporate *cloud*services
- Assess the differences in the concrete implementations of different public *cloud* vendors
- Assess IoT connectivity options to address a project, with special emphasis on LPWAN technologies
- Present the basic specifications of the main LPWAN technologies for the IoT

04

Course Management

The sheer complexity of today's cybersecurity demands thorough and detailed learning. For this reason, TECH has taken it upon itself to bring together the best faculty specialized in this area. Thus, the professional will enjoy the accompaniment and supervision of a teaching staff that is up to date with the latest advances in this area, so that they will be able to incorporate the best cybersecurity techniques into their daily work, while acquiring the necessary management skills in this area.

You will have real cybersecurity specialists at your disposal. This is the opportunity you were looking for"

Management

Mr. Olalla Bonal, Martín

- *Blockchain Technical Specialist* at IBM SPGI
- *Blockchain* Architect
- Infrastructure Architect in Banking
- Project management and implementation of solutions
- Digital Electronics Technician
- Teacher *Hyperledger Fabric* Training to Companies
- Teacher Business-oriented companies *Blockchain* training

Professors

Mr. Tobal Redondo, Javier

- HUAWEI Application Innovation Program Manager
- Information Security Manager of the Payment Division Amadeus IT Group
- Chief Information Security Officer FINTONIC, Financial Services
- Services Engineer and Architect in the Services and Security Planning and Architecture Area at Amena / Orange Spain
- Degree in Computer Science from the University of Deusto (Bilbao, Spain)
- Postgraduate degree in Industrial Computing Industrial Engineering School Bilbao

Mr. Gonzalo Alonso, Félix

- CEO and Founder of Smart REM Solutions
- Founding Partner and Head of Risk Engineering and Innovation Dynargy
- Manager and Founding Partner Risknova (Specialized Expert Technology Office)
- Degree in Industrial Organization Engineering from Comillas Pontifical University ICAI
- Graduate in Industrial Technical Engineering, specializing in Industrial Electronics, Comillas Pontifical University ICAI
- Master's Degree in Insurance Management from ICEA (Institute for the Collaboration between Insurance Companies)

Mr. Sevillano Izquierdo, Javier

- Global Cyber Security Architect Vodafone Spain
- Chief Technology Security Office (CTSO) Vodafone Spain
- Responsible for Technological Security Bankia
- Responsible for Technological Security Caja Madrid
- Security Manager 4B System
- SEINCA - Senior Analyst
- Superior Technician in Business Computing by Instituto Cibernos

Mr. Entrenas, Alejandro

- Entelgy Innotec
- Degree in Technical Engineering in Computer Systems from the University of Cordoba
- Master's Degree in Information Security Management at the Polytechnic University of Madrid

Mr. Nogales Ávila, Javier

- Enterprise Cloud and sourcing senior consultant. Quint
- Cloud and Technology Consultant. Indra
- Associate Technology Consultant. Accenture
- Graduate by Jaen University y University of Technology and Economics of Budapest (BME)
- Degree in Industrial Organization Engineering

Mr. Gómez Rodríguez, Antonio

- Cloud Solutions Engineer at Oracle
- Project Manager at Sopra Group
- Project Manager at Everis
- Project Manager at Empresa pública de Gestion de Programas Culturales. Department of Culture of Andalusia
- Information Systems Analyst. Sopra Group
- Degree in Telecommunications Engineering from the Polytechnic University of Catalonia
- Postgraduate Degree in Information Technologies and Systems, Catalan Institute of Technology
- E-Business Master, La Salle School of Business

Mr. del Valle Arias, Jorge

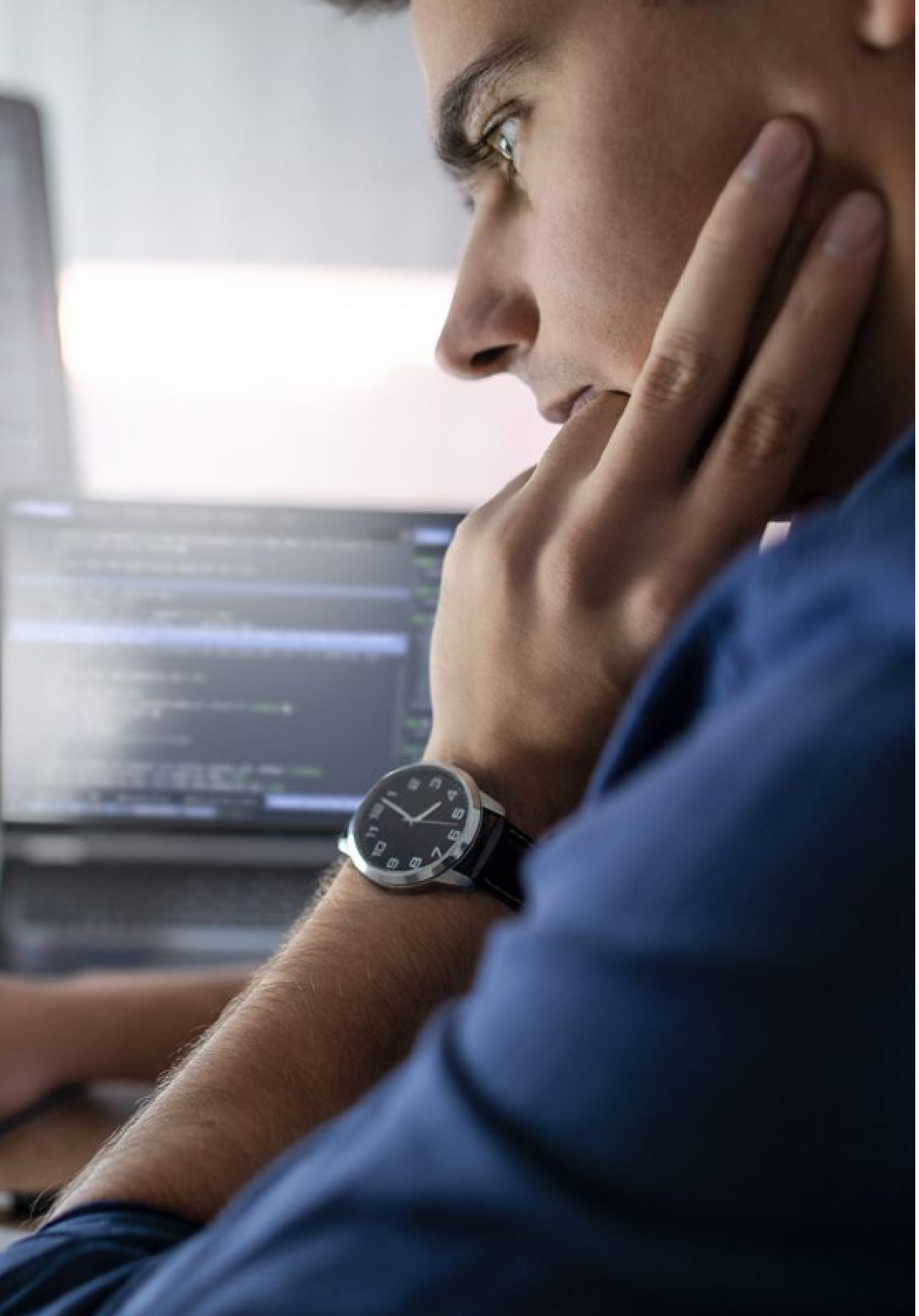
- Smart Cities Business Growth Manager Spain en Itron Inc.
- IoT Consultor
- IoT Division Director at Diode Spain
- Sales Manager IoT & Celular at Aicox Solutions
- Founder and CEO of Sensor Intelligence
- Operations Manager at Codium Networks
- Head of Electronics at Aitemin
- Telecommunications Engineer from the Polytechnic University of Madrid
- Executive MBA from the International Graduate School of La Salle in Madrid

Mr. Gozalo Fernández, Juan Luis

- Computer Engineer
- Blockchain Director DevOps in Alastria
- Tinkerlink Mobile Application Development Manager at Cronos Telecom
- IT Manager at Banco Santander
- IT Service Management Technology Director at Barclays Bank Spain
- Degree in Computer Engineering from the National Distance Education University (UNED)

Ms. Jurado Jabonero, Lorena

- Head of Information Security (CISO) at Grupo Pascual
- Graduate in Computer Engineering from Alfonso X El Sabio University
- Technical Computer Engineer from Polytechnical University of Madrid
- Knowledge: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, etc.



> You will be able to respond appropriately to all types of cybersecurity threats. Enroll and become a great specialist"

05

Structure and Content

This program is structured in 10 specialized modules that will allow the professional to deepen in aspects such as digital identification, access control systems, information security architecture, the structure of the security area, information security management systems in communications and software operation or the development of the business continuity plans associated with security. This will enable the IT specialist to gain a comprehensive understanding of all the relevant issues of today's cybersecurity.

> *You won't find more complete and innovative content than this to specialize in advanced cybersecurity management"*

Module 1. Security in System Design and Development

1.1. Information Systems

1.1.1. Information System Domains

1.1.2. Information System Components

1.1.3. Information System Activities

1.1.4. Life Cycle of an Information System

1.1.5. Information System Resources

1.2. IT Systems Types

1.2.1. Types of Information Systems

1.2.1.1. Corporate

1.2.1.2. Strategic

1.2.1.3. According to the Area of Application

1.2.1.4. Specific

1.2.2. Information Systems Real Examples

1.2.3. Evolution of Information Systems: Stages

1.2.4. Methods of Information Systems

1.3. Information System Security Legal Implications

1.3.1. Access to Data

1.3.2. Security Threats: Vulnerabilities

1.3.3. Legal Implications: Criminal Offenses

1.3.4. Maintenance Procedures of an Information System

1.4. Information System Security Security Protocol

1.4.1. Information System Security

1.4.1.1. Integrity

1.4.1.2. Confidentiality

1.4.1.3. Availability

1.4.1.4. Authentication

1.4.2. Security Services

1.4.3. Information Security Protocols Types

1.4.4. Information System Sensitivity

1.5. Information System Security Access Control Measures and Systems

1.5.1. Security Measures

1.5.2. Type of Security Measures

1.5.2.1. Prevention

1.5.2.2. Detection

1.5.2.3. Correction

1.5.3. Access Control Systems Types

1.5.4. Cryptography

1.6. Network and Internet Security

1.6.1. Firewalls

1.6.2. Digital Identification

1.6.3. Viruses and Worms

1.6.4. *Hacking*

1.6.5. Examples and Real Cases

1.7. Computer Crimes

1.7.1. Computer Crimes

1.7.2. Computer Crimes Types

1.7.3. Computer Crimes Attack Types

1.7.4. The Case for Virtual Reality

1.7.5. Profiles of Offenders and Victims Criminalization of the Crime

1.7.6. Computer Crimes Examples and Real Cases

1.8. Security Plans in Information Systems

1.8.1. Security Plan Objectives

1.8.2. Security Plan Plan

1.8.3. Risk Plan Analysis

1.8.4. Security Policy Implementation in the Organization

1.8.5. Security Plan Implementation in the Organization

1.8.6. Security Procedures Types

1.8.7. Security Plan Examples:

1.9. Contingency Plan
   1.9.1. Contingency Plan Functions
   1.9.2. Emergency Plan Elements and Objectives
   1.9.3. Contingency Plan in the Organization Implementation
   1.9.4. Contingency Plans Examples:
1.10. Information Systems Security Governance
   1.10.1. Legal Regulations
   1.10.2. Standards
   1.10.3. Certifications
   1.10.4. Technologies

Module 2. Information Security Architectures and Models

2.1. Information Security Architecture
   2.1.1. ISMSI / PDS
   2.1.2. Strategic Alignment
   2.1.3. Risk Management
   2.1.4. Performance Measurement
2.2. Information Security Models
   2.2.1. Based on Security Policies
   2.2.2. Based on Protection Tools
   2.2.3. Bases on Teamwork
2.3. Security Model Key Components
   2.3.1. Risk Identification
   2.3.2. Definition of Controls
   2.3.3. Continuous Assessment of Risk Levels
   2.3.4. Awareness Plan for Employees, Suppliers, Partners, etc.
2.4. Risk Management Process
   2.4.1. Asset Identification
   2.4.2. Threat Identification
   2.4.3. Risk Assessment
   2.4.4. Prioritization of Controls
   2.4.5. Reassessment and Residual Risk
2.5. Business Processes and Information Security
   2.5.1. Business Processes
   2.5.2. Risk Assessment Based on Business Parameters
   2.5.3. Business Impact Analysis
   2.5.4. Business Operations and Information Security
2.6. Continuous Improvement Process
   2.6.1. Deming's Cycle
      2.6.1.1. Planning
      2.6.1.2. Do
      2.6.1.3. Verify
      2.6.1.4. Act
2.7. Security Architectures
   2.7.1. Selection and Homogenization of Technologies
   2.7.2. Identity Management Authentication
   2.7.3. Access Management Authorization
   2.7.4. Network Infrastructure Security
   2.7.5. Encryption Technologies and Solutions
   2.7.6. Endpoint Detection and Response (EDR)
2.8. Regulatory Framework
   2.8.1. Sectoral Regulations
   2.8.2. Certifications
   2.8.3. Legislations
2.9. The ISO 27001 Standard
   2.9.1. Implementation
   2.9.2. Certification
   2.9.3. Audits and Penetration Tests
   2.9.4. Continuous Risk Management
   2.9.5. Classification of Information

2.10. Privacy Legislation GDPR
- 2.10.1. Scope of General Data Protection Regulation (GDPR)
- 2.10.2. Personal Data
- 2.10.3. Roles in the Processing of Personal Data
- 2.10.4. ARCO Rights
- 2.10.5. DPO Functions

Module 3. IT Security Management

3.1. Safety Management
- 3.1.1. Security Operations
- 3.1.2. Legal and Regulatory Appearance
- 3.1.3. Business Authorization
- 3.1.4. Risk Management
- 3.1.5. Identity and Access Management

3.2. Structure of the Security Area The CISO's office
- 3.2.1. Organisational Structure. Position of the CISO in the Structure
- 3.2.2. Lines of Defence
- 3.2.3. CISO Office Organization Chart
- 3.2.4. Budget Management

3.3. Government Security
- 3.3.1. Security Committee
- 3.3.2. Risk Monitoring Committee
- 3.3.3. Audit Committee
- 3.3.4. Crisis Committee

3.4. Government Security Functions
- 3.4.1. Policies and Standards
- 3.4.2. Security Management Plan
- 3.4.3. Control Panels
- 3.4.4. Awareness and Training
- 3.4.5. Supply Chain Security

3.5. Security Operations
- 3.5.1. Identity and Access Management
- 3.5.2. Configuration of Network Security Rules *Firewalls*
- 3.5.3. IDS/IPS Platform Management
- 3.5.4. Vulnerability Analysis

3.6. Cybersecurity Framework NIST CSF
- 3.6.1. NIST Methodology
  - 3.6.1.1. Log In
  - 3.6.1.2. Protect
  - 3.6.1.3. Detect
  - 3.6.1.4. Respond
  - 3.6.1.5. Recover

3.7. Security Operations Center (SOC) Functions
- 3.7.1. Protection *Red Team, Pentesting, Threat Intelligence*
- 3.7.2. Detection SIEM, *User Behavior Analytics, Fraud Prevention*
- 3.7.3. Response

3.8. Security Audits
- 3.8.1. Intrusion Test
- 3.8.2. *Red Team* Exercises
- 3.8.3. Source Code Audits Secure Development
- 3.8.4. Component Safety (*Software Supply Chain*))
- 3.8.5. Forensic Analysis

3.9. Incident Response
- 3.9.1. Preparation
- 3.9.2. Detection, Analysis and Reporting
- 3.9.3. Containment, Eradication and Recovery
- 3.9.4. Post-Incident Activity
  - 3.9.4.1. Retention of Evidence
  - 3.9.4.2. Forensic Analysis
  - 3.9.4.3. Gap Management
- 3.9.5. Official Cyber Incident Management Guides

3.10. Vulnerability Management

3.10.1. Vulnerability Analysis

3.10.2. Vulnerability Assessment

3.10.3. System Basing

3.10.4. Day 0 Vulnerabilities *Zero-Day*

Module 4. Risk Analysis and IT Security Environment

4.1. Analysis of the environment

4.1.1. Analysis of the Economic Situation

4.1.1.1. VUCA Environment

4.1.1.1.1. Volatile

4.1.1.1.2. Unsure

4.1.1.1.3. Complex

4.1.1.1.4. Ambiguous

4.1.1.2. BANI Environment

4.1.1.2.1. Broken

4.1.1.2.2. Anxious

4.1.1.2.3. Non-Linear

4.1.1.2.4. Incomprehensible

4.1.2. General Environment Analysis PESTLE

4.1.2.1. Politics

4.1.2.2. Economics

4.1.2.3. Social

4.1.2.4. Technological

4.1.2.5. Ecological/Environmental

4.1.2.6. Legal

4.1.3. Analysis of the Internal Situation SWOT Analysis

4.1.3.1. Objectives

4.1.3.2. Threats

4.1.3.3. Opportunities

4.1.3.4. Strengths

4.2. Risk and Uncertainty

4.2.1. Risk

4.2.2. Risk Management

4.2.3. Risk Management Standards

4.3. ISO 31.000:2018 Risk Management Guidelines

4.3.1. Object

4.3.2. Principles

4.3.3. Frame of Reference

4.3.4. Process

4.4. Methodology for Analysis and Management of Information Systems Risks (MAGERIT)

4.4.1. MAGERIT Methodology

4.4.1.1. Objectives

4.4.1.2. Method

4.4.1.3. Components

4.4.1.4. Techniques

4.4.1.5. Available Tools (PILAR)

4.5. Cyber Risk Transfer

4.5.1. Risk Transfer

4.5.2. Cyber Risks Types

4.5.3. Cyber Risk Insurance

4.6. Agile Methodologies for Risk Management

4.6.1. Agile Methodologies

4.6.2. Scrum for Risk Management

4.6.3. *Agile Risk Management*

4.7. Technologies for Risk Management

4.7.1. Artificial Intelligence Applied to Risk Management

4.7.2. *Blockchain* and Cryptography Value Preservation Methods

4.7.3. Quantum Computing Opportunity or Risk

4.8. IT Risk Mapping Based on Agile Methodologies

4.8.1. Representation of Probability and Impact in Agile Environments

4.8.2. Risk as a Threat to Value

4.8.3. Re-Evolution in Project Management and Agile Processes Based on KRIs

4.9. *Risk-Driven* in Risk Management
- 4.9.1. *Risk Driven*
- 4.9.2. *Risk-Driven* in Risk Management
- 4.9.3. Development of a Risk-Driven Business Management Model

4.10. Innovation and Digital Transformation in IT Risk Management
- 4.10.1. Agile Risk Management as a Source of Business Innovation
- 4.10.2. Transforming Data into Useful Information for Decision Making
- 4.10.3. Holistic View of the Company through Risk

Module 5. Cryptography in IT

5.1. Cryptography
- 5.1.1. Cryptography
- 5.1.2. Fundamentals of Mathematics

5.2. Cryptology
- 5.2.1. Cryptology
- 5.2.2. Cryptanalysis
- 5.2.3. Steganography and Stegoanalysis

5.3. Cryptographic Protocols
- 5.3.1. Basic Blocks
- 5.3.2. Basic Protocols
- 5.3.3. Intermediate Protocols
- 5.3.4. Advanced Protocols
- 5.3.5. Exoteric Protocols

5.4. Cryptographic Techniques
- 5.4.1. Length of Passwords
- 5.4.2. Password Management
- 5.4.3. Types of Algorithms
- 5.4.4. Summary of Functions *Hash*
- 5.4.5. Pseudo-Random Number Generators
- 5.4.6. Use of Algorithms

5.5. Symmetric Cryptography
- 5.5.1. Block Ciphers
- 5.5.2. DES (*Data Encryption Standard*)
- 5.5.3. RC4 Algorithm
- 5.5.4. AES (*Advanced Encryption Standard*)
- 5.5.5. Combination of Block Ciphers
- 5.5.6. Password Derivation

5.6. Asymmetric Cryptography
- 5.6.1. Diffie-Hellman
- 5.6.2. DSA (*Digital Signature Algorithm*)
- 5.6.3. RSA (Rivest, Shamir and Adleman)
- 5.6.4. Elliptic Curve
- 5.6.5. Asymmetric Cryptography Types

5.7. Digital Certificates
- 5.7.1. Digital Signature
- 5.7.2. X509 Certificates
- 5.7.3. Public Key Infrastructure (PKI)

5.8. Implementations
- 5.8.1. Kerberos
- 5.8.2. IBM CCA
- 5.8.3. *Pretty Good Privacy* (PGP)
- 5.8.4. ISO *Authentication Framework*
- 5.8.5. SSL and TLS
- 5.8.6. Europay, MasterCard, and Visa (EMV)
- 5.8.7. Mobile Telephony Protocols
- 5.8.8. *Blockchain*

5.9. Steganography
- 5.9.1. Steganography
- 5.9.2. Stegoanalysis
- 5.9.3. Applications and Uses

5.10. Quantum Cryptography
- 5.10.1. Quantum Algorithms
- 5.10.2. Algorithm Protection Against Quantum Computing
- 5.10.3. Quantum Key Distribution

Module 6. Identity and Access Management in IT Security

- 6.1. Identity and Access Management (IAM)
  - 6.1.1. Digital Identity
  - 6.1.2. Identity Management
  - 6.1.3. Identity Federation
- 6.2. Physical Access Control
  - 6.2.1. Protection Systems
  - 6.2.2. Security of the Areas
  - 6.2.3. Recovery Facilities
- 6.3. Logical Access Control
  - 6.3.1. Authentication Types
  - 6.3.2. Authentication Protocols
  - 6.3.3. Authentication Attacks
- 6.4. Logical Access Control. MFA Authentication
  - 6.4.1. Logical Access Control. MFA Authentication
  - 6.4.2. Passwords Importance
  - 6.4.3. Authentication Attacks
- 6.5. Logical Access Control. Biometric Authentication
  - 6.5.1. Logical Access Control Biometric Authentication
    - 6.5.1.1. Biometric Authentication Requirements
  - 6.5.2. Operation
  - 6.5.3. Models and Techniques
- 6.6. Authentication Management Systems
  - 6.6.1. *Single Sign On*
  - 6.6.2. Kerberos
  - 6.6.3. AAA Systems
- 6.7. Authentication Management Systems: AAA Systems
  - 6.7.1. TACACS
  - 6.7.2. RADIUS
  - 6.7.3. DIAMETER
- 6.8. Access Control Services
  - 6.8.1. FW- Firewalls
  - 6.8.2. VPN - Virtual Private Networks
  - 6.8.3. IDS - Intrusion Detection System
- 6.9. Network Access Control Systems
  - 6.9.1. NAC
  - 6.9.2. Architecture and Elements
  - 6.9.3. Operation and Standardization
- 6.10. Access to Wireless Networks
  - 6.10.1. Types of Wireless Networks
  - 6.10.2. Wireless Network Security
  - 6.10.3. Wireless Network Attacks

Module 7. Security in Communications and Software Operation

- 7.1. Computer Security in Communications and Software Operation
  - 7.1.1. IT Security
  - 7.1.2. Cybersecurity
  - 7.1.3. Cloud Security
- 7.2. IT Security in Communications and Software Operation Types
  - 7.2.1. Physical Security
  - 7.2.2. Logical Security
- 7.3. Communications Security
  - 7.3.1. Main Elements
  - 7.3.2. Network Security
  - 7.3.3. Best Practices
- 7.4. Cyberintelligence
  - 7.4.1. Social Engineering
  - 7.4.2. *Deep Web*
  - 7.4.3. *Phishing*
  - 7.4.4. *Malware*

7.5. Secure Development in Communications and Software Operation
- 7.5.1. Secure Development HTTP Protocol
- 7.5.2. Secure Development Life Cycle
- 7.5.3. Secure Development PHP Security
- 7.5.4. Secure Development NET Security
- 7.5.5. Secure Development Best Practices

7.6. Information Security Management Systems in Communications and Software Operation
- 7.6.1. GDPR
- 7.6.2. ISO 27021
- 7.6.3. ISO 27017/18

7.7. SIEM Technologies
- 7.7.1. SIEM Technologies
- 7.7.2. SOC Operations
- 7.7.3. SIEM *Vendors*

7.8. The Role of Security in Organizations
- 7.8.1. Roles in Organizations
- 7.8.2. Role of IoT Specialists in Companies
- 7.8.3. Recognized Certifications in the Market

7.9. Forensic Analysis
- 7.9.1. Forensic Analysis
- 7.9.2. Forensic Analysis Methodology
- 7.9.3. Forensic Analysis Tools and Implementation

7.10. Cybersecurity Today
- 7.10.1. Main Cyber Attacks
- 7.10.2. Employability Forecasts
- 7.10.3. Challenges

Module 8. Security in *Cloud* Environments

8.1. Security in *Cloud Computing* Environments
- 8.1.1. Security in *Cloud Computing* Environments
- 8.1.2. Security in *Cloud Environments* Security Threats and Risks
- 8.1.3. Security in *Cloud Computing* Key Security Aspects

8.2. Types of *Cloud* Infrastructure
- 8.2.1. Public
- 8.2.2. Private
- 8.2.3. Hybrid

8.3. Shared Management Model
- 8.3.1. Security Elements Managed by Supplier
- 8.3.2. Elements Managed by the Client
- 8.3.3. Definition of the Security Strategy

8.4. Prevention Mechanisms
- 8.4.1. Authentication Management Systems
- 8.4.2. Authorization Management System: Access Policies
- 8.4.3. Key Management Systems

8.5. Securing Systems
- 8.5.1. Securing Storage Systems
- 8.5.2. Protection of Database Systems
- 8.5.3. Securing Data in Transit

8.6. Infrastructure Protection
- 8.6.1. Secure Network Design and Implementation
- 8.6.2. Security in Computing Resources
- 8.6.3. Tools and Resources to Protect the Infrastructure

8.7. Detection of Threats and Attacks
- 8.7.1. Auditing, *Logging* and Monitoring Systems
- 8.7.2. Event and Alarm Systems
- 8.7.3. SIEM Systems

8.8. Incident Response
- 8.8.1. Incident Response Plan
- 8.8.2. Business Continuity
- 8.8.3. Forensic Analysis and Remediation of Incidents of the Same Nature.

8.9. Security in Public *Clouds*
- 8.9.1. AWS (Amazon Web Services)
- 8.9.2. Microsoft Azure
- 8.9.3. Google GCP
- 8.9.4. Oracle Cloud

8.10. Regulations and Compliance
- 8.10.1. Compliance with Safety Regulations
- 8.10.2. Risk Management
- 8.10.3. People and Process in the Organizations

Module 9. Security in IoT Device Communications

9.1. From Telemetry to IoT
- 9.1.1. Telemetry
- 9.1.2. M2M Connectivity
- 9.1.3. Democratization of Telemetry

9.2. IoT Reference Models
- 9.2.1. IoT Reference Models
- 9.2.2. IoT Simplified Architecture

9.3. IoT Security Vulnerabilities
- 9.3.1. IoT Devices
- 9.3.2. IoT Devices Usage Case Studies
- 9.3.3. IoT Devices Vulnerabilities

9.4. Connectivity to IoT
- 9.4.1. PAN, LAN, WAN Networks
- 9.4.2. Non IoT Wireless Technologies
- 9.4.3. LPWAN Wireless Technologies

9.5. LPWAN Technologies
- 9.5.1. The Iron Triangle of LPWAN Networks
- 9.5.2. Free Frequency Bands vs. Licensed Bands
- 9.5.3. LPWAN Technology Options

9.6. LoRaWAN Technology
- 9.6.1. LoRaWAN Technology
- 9.6.2. LoRaWAN Use Cases Ecosystem
- 9.6.3. Security in LoRaWAN

9.7. Sigfox Technology
- 9.7.1. Sigfox Technology
- 9.7.2. Sigfox Use Cases Ecosystem
- 9.7.3. Security in Sigfox

9.8. IoT Cellular Technology
- 9.8.1. IoT Cellular Technology (NB-IoT and LTE-M)
- 9.8.2. Cellular IoT Use Cases Ecosystem
- 9.8.3. IoT Cellular Security

9.9. WiSUN Technology
- 9.9.1. WiSUN Technology
- 9.9.2. WiSUN Use Cases Ecosystem
- 9.9.3. Security in WiSUN

9.10. Other IoT Technologies
- 9.10.1. Other IoT Technologies
- 9.10.2. Use Cases and Ecosystem of Other IoT Technologies
- 9.10.3. Security in Other IoT Technologies

Module 10. Business Continuity Plan Associated with Security

10.1. Business Continuity Plans
- 10.1.1. Business Continuity Plans (BCP)
- 10.1.2. Business Continuity Plans (BCP) Key Aspects
- 10.1.3. Business Continuity Plan (BCP) for Company Valuation

10.2. Metrics in Business Continuity Plans (BCP)
- 10.2.1. *Recovery Time Objective* (RTO) and *Recovery Point Objective* (RPO)
- 10.2.2. Maximum Tolerable Downtime (MTD)
- 10.2.3. Minimum Recovery Levels (ROL)
- 10.2.4. Recovery Point Objective (RPO)

10.3. Continuity Projects Types
- 10.3.1. Business Continuity Plans (BCP)
- 10.3.2. ICT Continuity Plan (ICTCP)
- 10.3.3. Disaster Recovery Plan (DRP)

10.4. Risk Management Associated with the BCP
- 10.4.1. Business Impact Analysis
- 10.4.2. Benefits of Implementing a BCP
- 10.4.3. Risk-Based Mentality

10.5. Life Cycle of a Business Continuity Plan
- 10.5.1. Phase 1: Analysis of the Organization
- 10.5.2. Phase 2: Determining the Continuity Strategy
- 10.5.3. Phase 3: Response to Contingency
- 10.5.4. Phase 4: Tests, Maintenance and Review

10.6. Organizational Analysis Phase of a BCP
- 10.6.1. Identification of Processes in the Scope of the BCP
- 10.6.2. Identification of Critical Business Areas
- 10.6.3. Identification of Dependencies between Areas and Processes
- 10.6.4. Determination of Appropriate BAT
- 10.6.5. Deliverables Creating a Plan

10.7. Phase of Determination of the Continuity Strategy in a BCP
- 10.7.1. Roles in the Strategy Determination Phase
- 10.7.2. Tasks of the Strategy Determination Phase
- 10.7.3. Deliverables

10.8. Contingency Response Phase in a BCP
- 10.8.1. Roles in the Response Phase
- 10.8.2. Tasks in this Phase
- 10.8.3. Deliverables

10.9. Testing, Maintenance and Revision Phase of a BCP
- 10.9.1. Roles in the Testing, Maintenance and Revision Phase
- 10.9.2. Tasks in the Testing, Maintenance and Revision Phase
- 10.9.3. Deliverables

10.10. ISO Standards Associated with Business Continuity Plans (BCP)
- 10.10.1. ISO 22301:2019
- 10.10.2. ISO 22313:2020
- 10.10.3. Other Related ISO and International Standards

> *The best teaching staff and its innovative teaching system are combined with the most complete and up to date syllabus: you have a great opportunity to progress as a computer scientist”*

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.

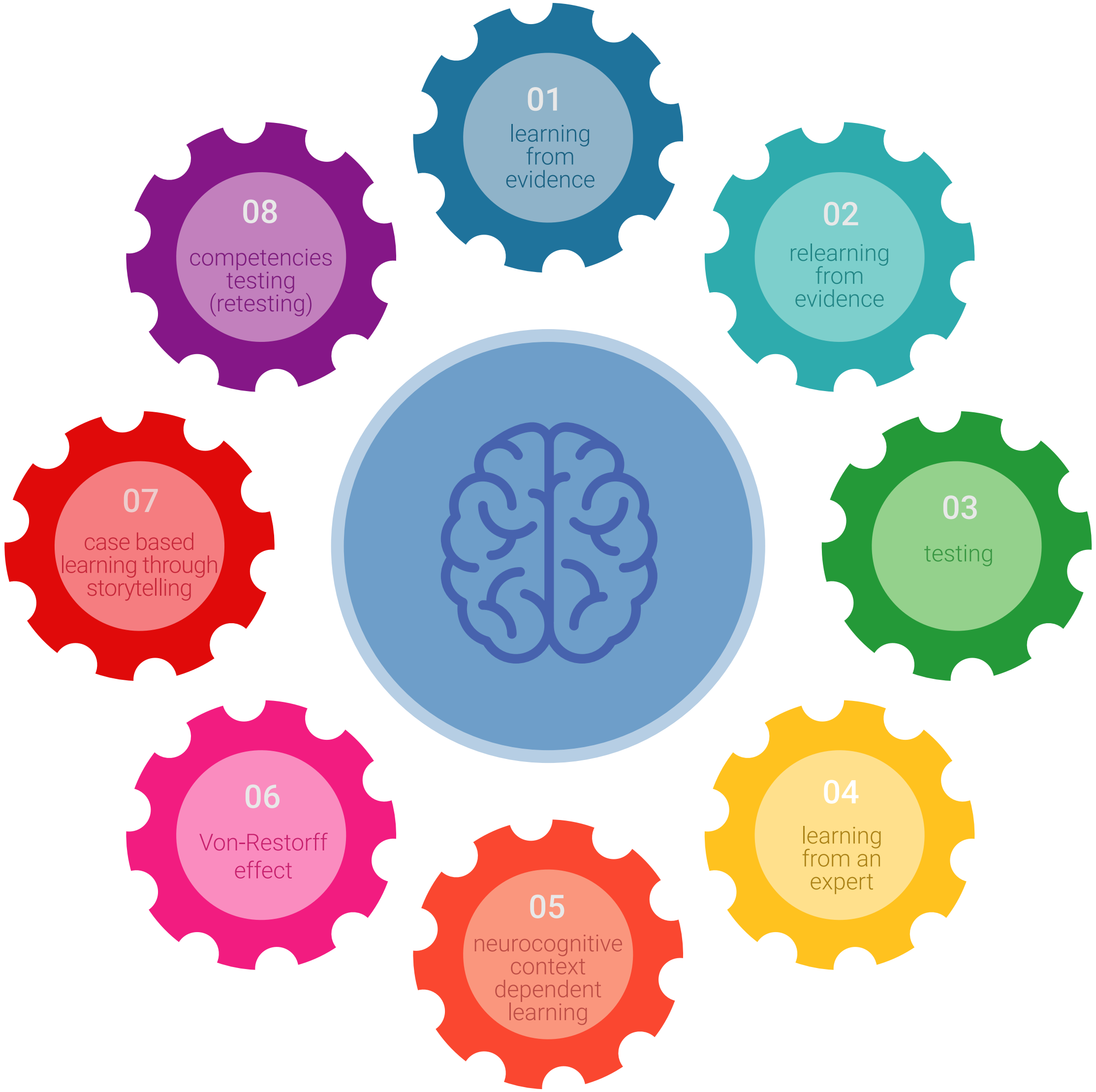
What should a professional do in a given situation? This is the question that you are presented with in the case method, an action-oriented learning method. Throughout the course, students will be presented with multiple real cases. They will have to combine all their knowledge and research, and argue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

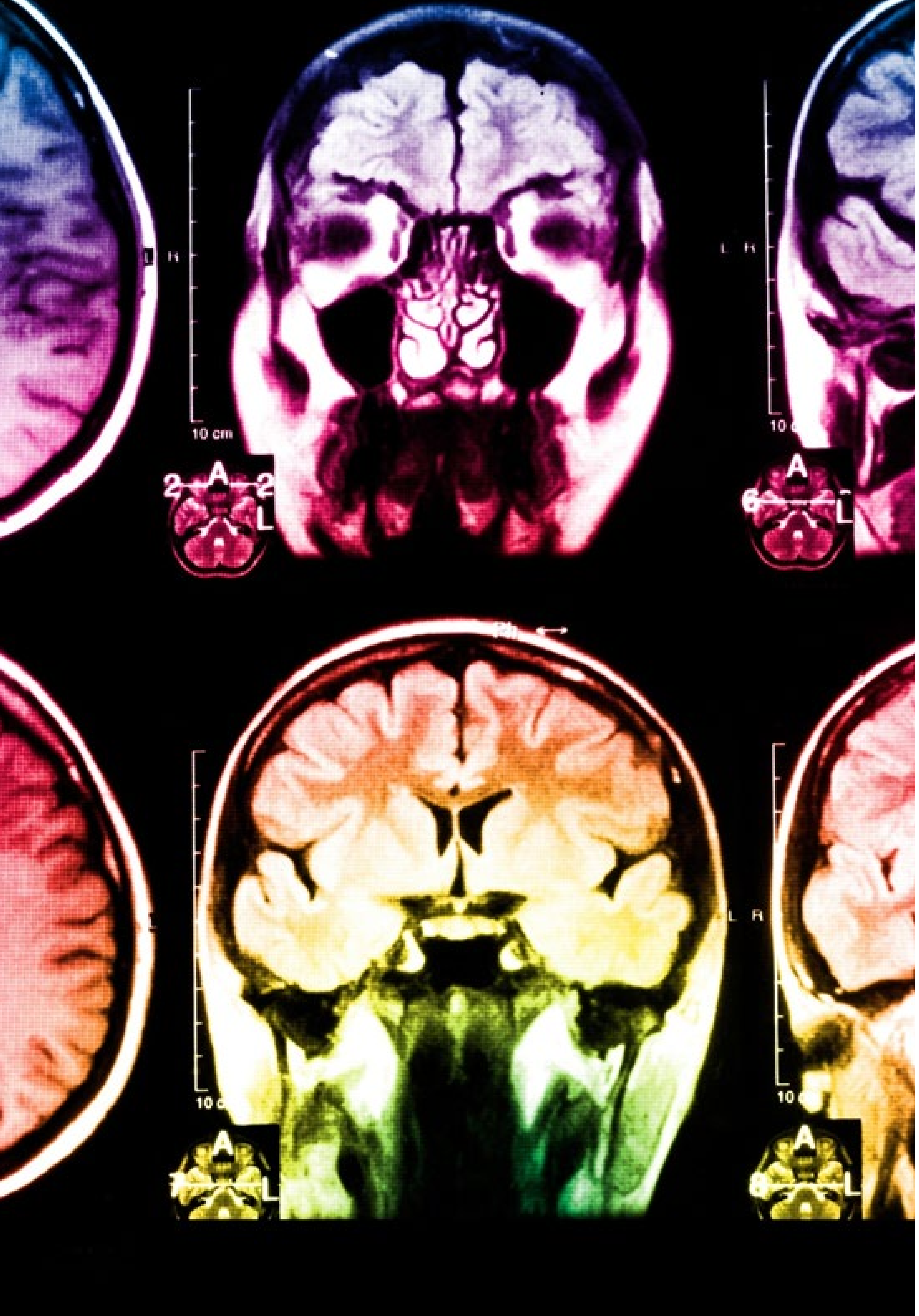
We enhance the Case Study with the best 100% online teaching method: Relearning.

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


01
learning from evidence
02
relearning from evidence
03
testing
04
learning from an expert
05
neurocognitive context dependent learning
06
Von-Restorff effect
07
case based learning through storytelling
08
competencies testing (retesting)

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

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



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

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

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

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

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

Study Material

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

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

Classes

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

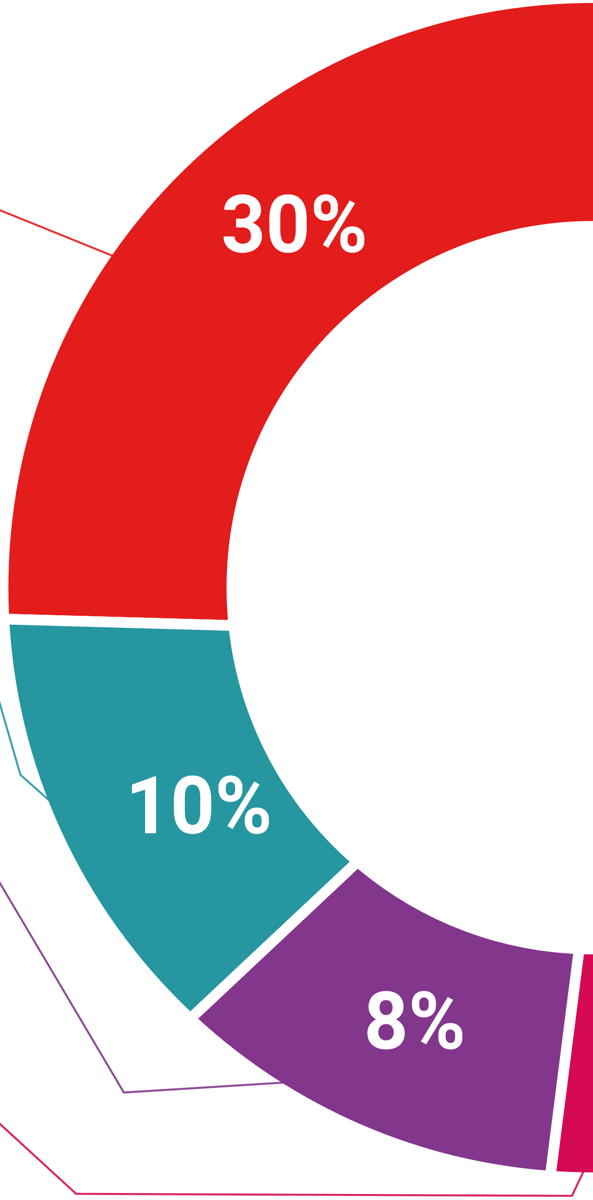
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

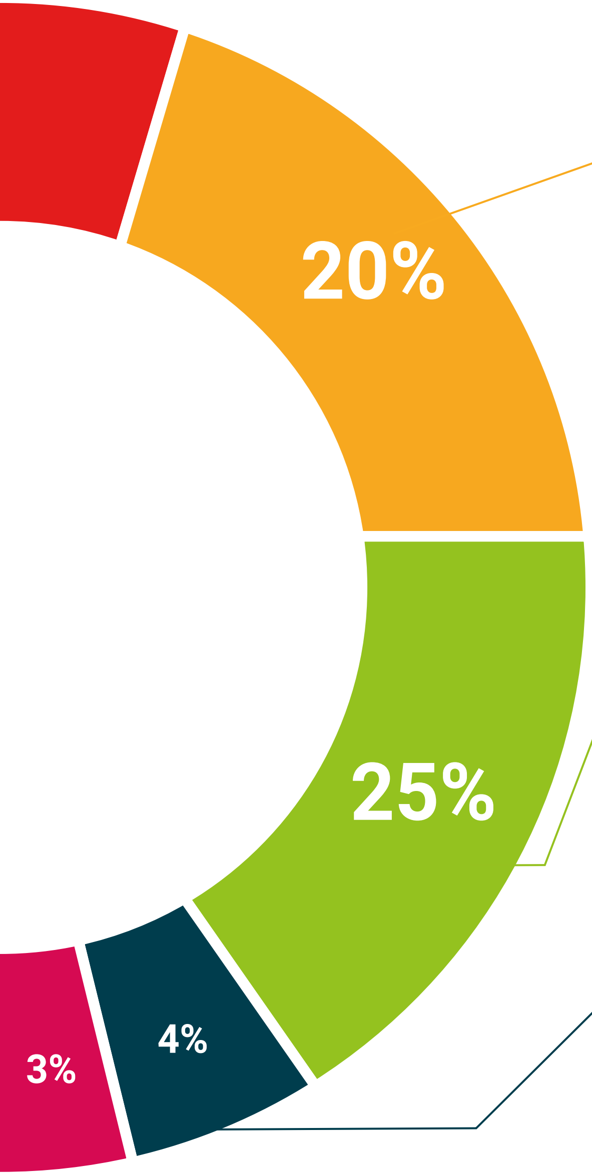
Practising Skills and Abilities

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

Additional Reading

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





Case Studies

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

Interactive Summaries

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

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

Testing & Retesting

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

07

Certificate

The Professional Master's Degree in Advanced Cybersecurity Management guarantees students, in addition to the most rigorous and up to date education, access to a Professional Master's Degree issued by TECH Technological University.

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

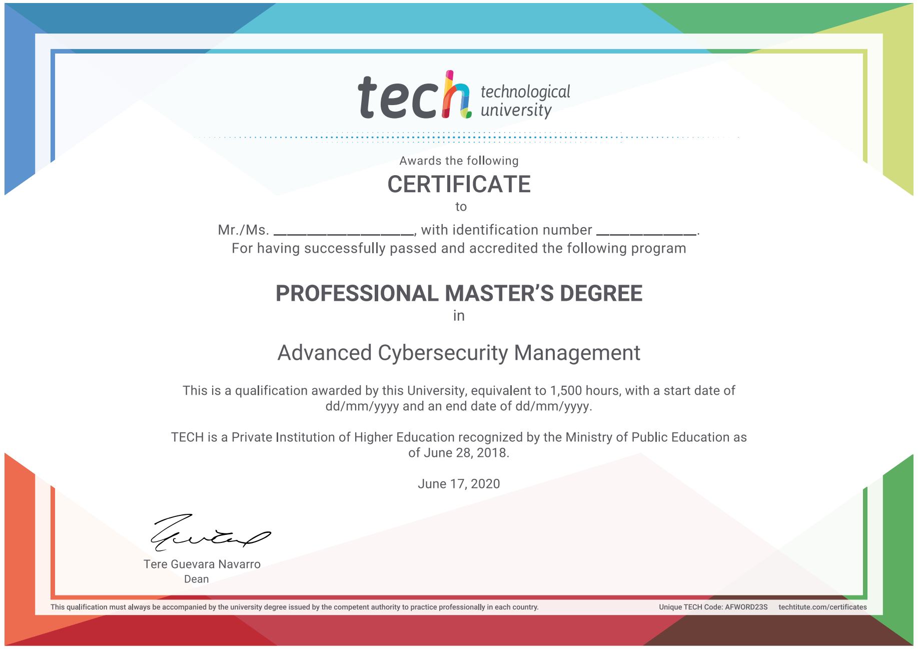
This **Professional Master's Degree in Advanced Cybersecurity Management** contains the most complete and up to date scientific program on the market.

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

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

Title: **Professional Master's Degree in Advanced Cybersecurity Management**

Official Nº of hours: **1,500 h.**



tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. _______________, with identification number ___________.

For having successfully passed and accredited the following program

PROFESSIONAL MASTER'S DEGREE

in

Advanced Cybersecurity Management

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

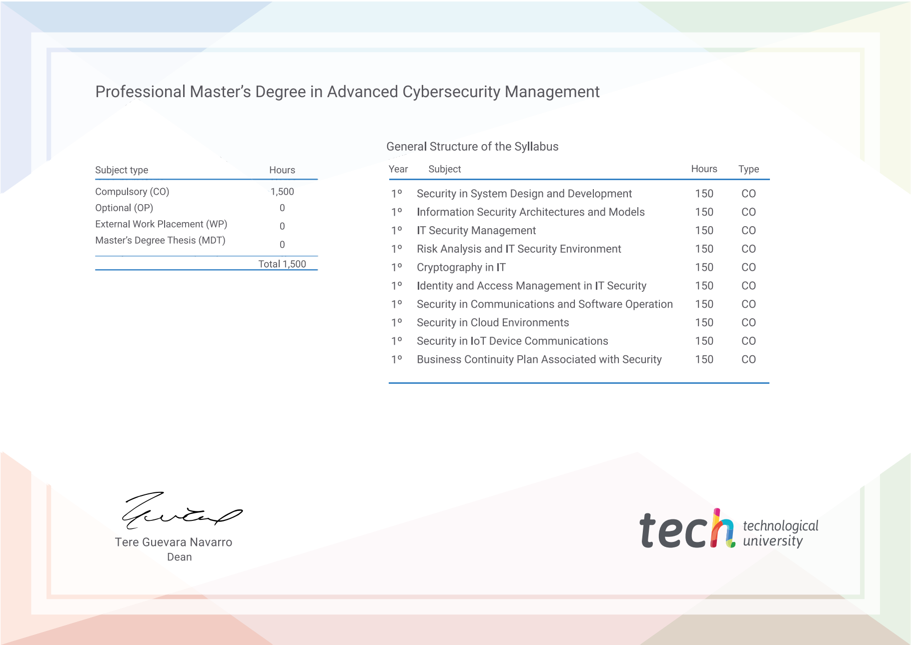
TECH is a Private Institution of Higher Education recognized by the Ministry of Public Education as of June 28, 2018.

June 17, 2020

Tere Guevara Navarro
Dean

This qualification must always be accompanied by the university degree issued by the competent authority to practice professionally in each country.

Unique TECH Code: AFWORD23S techtitute.com/certificates



Professional Master's Degree in Advanced Cybersecurity Management

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

General Structure of the Syllabus

Year	Subject	Hours	Type
1º	Security in System Design and Development	150	CO
1º	Information Security Architectures and Models	150	CO
1º	IT Security Management	150	CO
1º	Risk Analysis and IT Security Environment	150	CO
1º	Cryptography in IT	150	CO
1º	Identity and Access Management in IT Security	150	CO
1º	Security in Communications and Software Operation	150	CO
1º	Security in Cloud Environments	150	CO
1º	Security in IoT Device Communications	150	CO
1º	Business Continuity Plan Associated with Security	150	CO

Tere Guevara Navarro
Dean

tech technological university

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

tech technological university

Professional Master's Degree
Advanced Cybersecurity Management

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

Professional Master's Degree
Advanced Cybersecurity Management

tech technological university