Professional Master's Degree
Telematics

tech technological university

tech technological university

Professional Master's Degree

Telematics

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

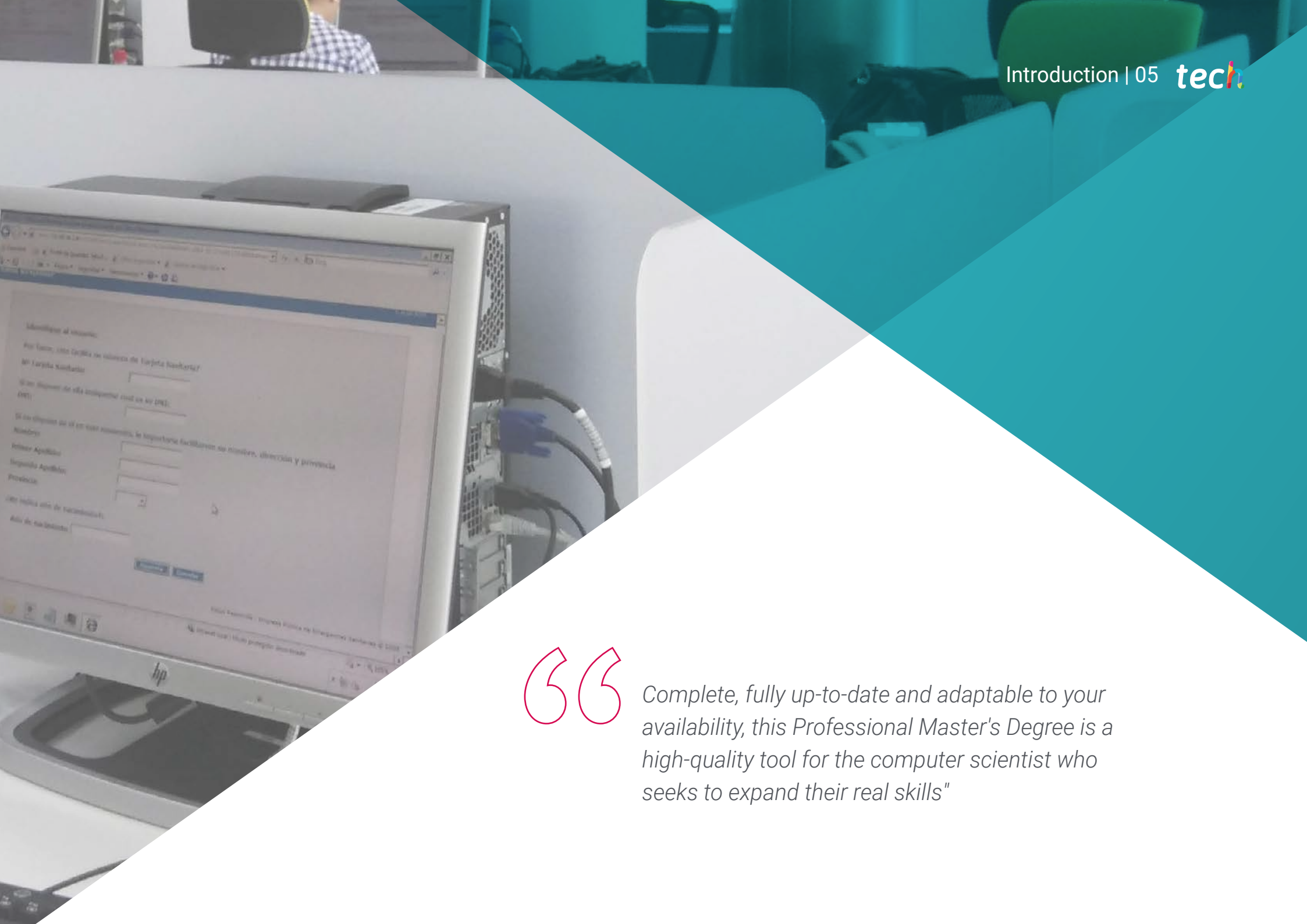
Website: www.techtitute.com/us/information-technology/professional-master-degree/master-telematics

Index

01

Introduction

Computer science and communication technology are combined in Telematics to respond to the development and implementation of techniques, processes, knowledge and devices that allow the efficient sending and receiving of data. This field of work, the constant incorporation of technological advances requires a permanent and very broad update. This program offers you that update or the quality specialization you need with an up-to-date and highly qualified program. A high-quality course that will allow you to advance in your profession.



Complete, fully up-to-date and adaptable to your availability, this Professional Master's Degree is a high-quality tool for the computer scientist who seeks to expand their real skills"

Advances in telecommunications are constantly occurring, as this is one of the fastest evolving areas. Therefore, it is necessary to have experts in Computer Science who can adapt to these changes and know first-hand the new tools and techniques that arise in this field.

The Professional Master's Degree in Telematics addresses the complete range of topics involved in this field. Its syllabus has a clear advantage over other Professional Master's Degree that focus on specific blocks, which prevents the student from knowing the interrelationship with other areas included in the multidisciplinary field of telecommunications. In addition, the teaching team of this program has made a careful selection of each of the topics of this qualification to offer the student an opportunity to study as complete as possible and always linked to current events.

This program is aimed at those interested in attaining a higher level of knowledge in Telematics. The main objective is to educate students to apply the knowledge acquired in this Professional Master's Degree in the real world, in a work environment that reproduces the conditions that can be found in their future, in a rigorous and realistic way.

In addition, as it is a 100% online Professional Master's Degree, the student is not conditioned by fixed schedules or the need to move to another physical location, but can access the contents at any time of the day, balancing their work or personal life with their academic life.

This **Professional Master's Degree in Telematics** ccontains the most complete and up-to-date program on the market. The most important features include:

- Practical cases presented by experts in Telematics
- 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 in Telematics
- 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

It includes in your skills, the ability to intervene in the different fields of Telematics, with a learning path that will boost your professional development"

This Professional Master's Degree is the best investment you can make when selecting a refresher program to update your knowledge in Telematics"

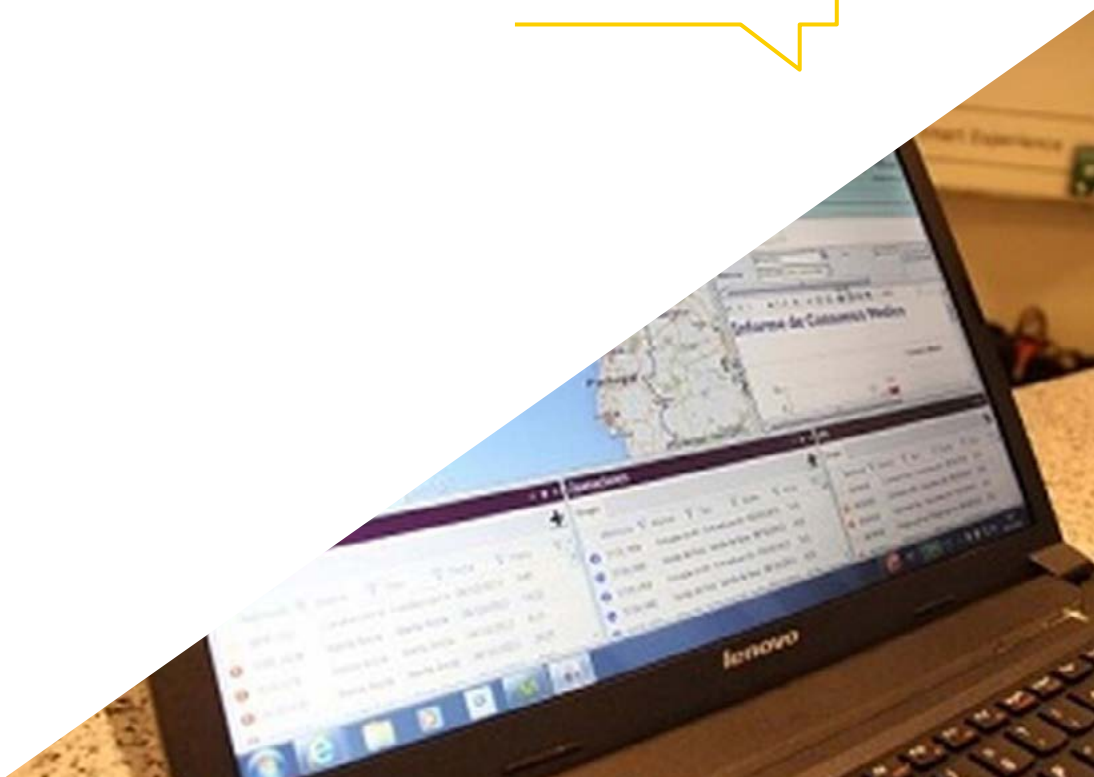
The teaching material with which you will develop your study is a compendium of high quality that will allow you to advance in a comfortable and simple way.

This 100% online Professional Master's Degree will allow you to balance your studies with your professional work.

It includes in its teaching staff professionals belonging to the field of telecommunications informatics, who pour into this program the experience of their work, in addition to recognized specialists from reference societies and prestigious universities.

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

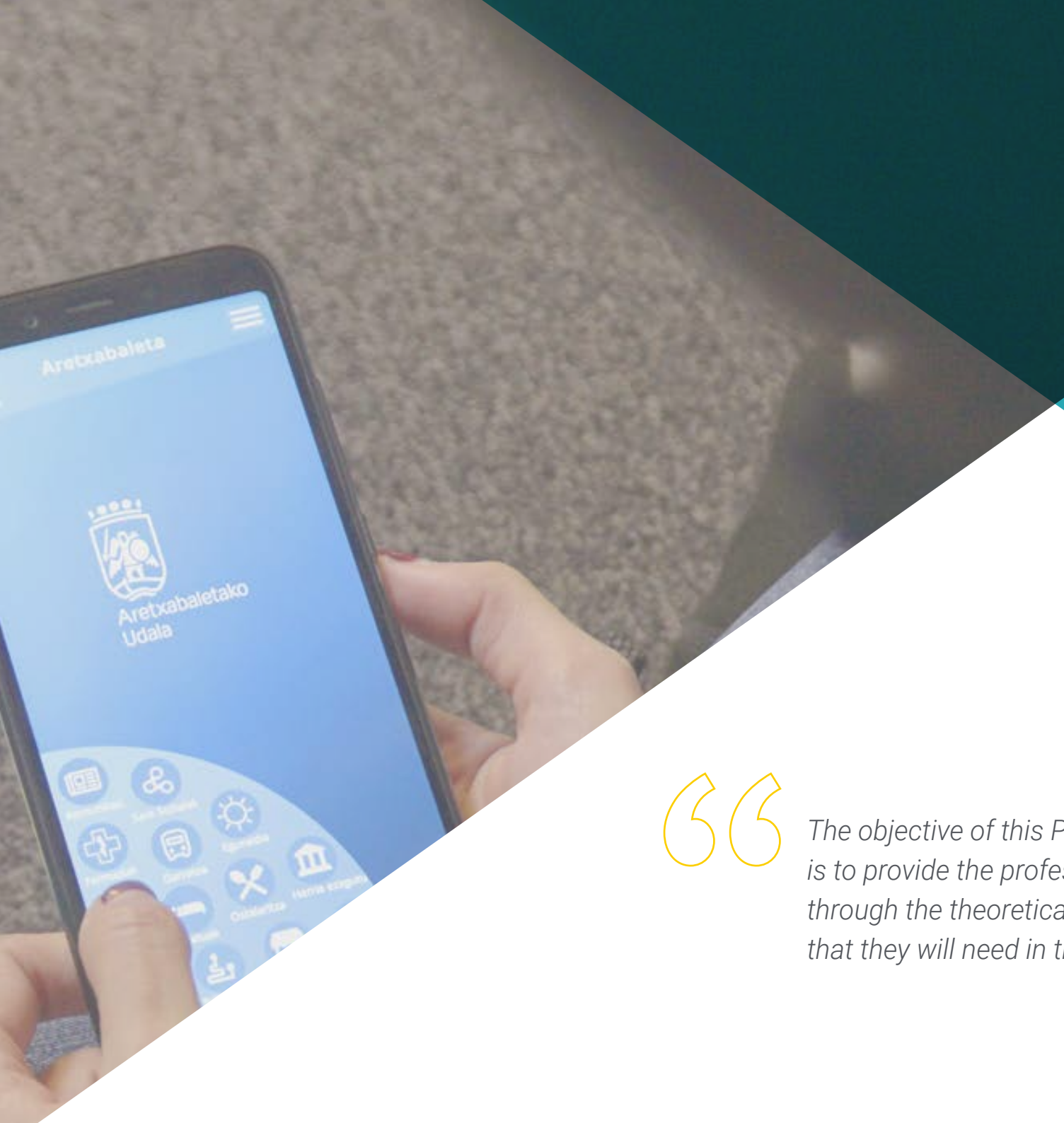
This program is designed around Problem-Based Learning, whereby the professional must try to solve the different professional practice situations that arise during the academic year For this purpose, the professional will be assisted by an innovative interactive video system developed by renowned and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



02

Objectives

The Professional Master's Degree in Telematics aims to offer IT professionals a complete and up-to-date study of all the areas involved in the intervention in Telematics. With the confidence and quality of a Professional Master's Degree created with a criterion of total excellence.



The objective of this Professional Master's Degree is to provide the professional with a complete tour through the theoretical and practical knowledge that they will need in the field of Telematics"

General Objective

- Prepare students to be able to develop telematic applications, analyze data or carry out digital security tasks, among other aspects

An opportunity created for professionals who are looking for an intensive and effective course, with which to take a significant step in the practice of their profession"

Specific Objectives

Module 1. Computer Networks

- Acquire the essential knowledge of computer networks on the Internet
- Understand the functioning of the different layers that define a networked system, such as the application, transport, network and link layers
- Understand the composition of LANs, their topology and their network elements and interconnection
- Learn how IP addressing and subnetting works
- Understand the structure of wireless and mobile networks, including the new 5G network
- Know the different network security mechanisms, as well as the different Internet security protocols

Module 2. Distributed Systems

- Master the basic principles of distributed systems
- Learn to characterize and classify distributed systems according to a number of basic parameters
- Understand the different types of models used in distributed systems
- Know the current architectures that implement the concept of distributed file systems
- Be able to analyze process and object synchronization algorithms, the definition of logical clocks and temporal consistency of information
- Understand the naming system used on the Internet, known as DNS (Domain Name System)

Module 3. Security in Communication Systems and Networks

- Obtain a global perspective on security, cryptography and classical cryptanalysis
- Understand the fundamentals of symmetric cryptography and asymmetric cryptography, as well as their main algorithms
- Analyze the nature of network attacks and the different types of security architectures
- Understand the various techniques of system protection and secure code development
- Know the essential components of botnets and spam, as well as malware and malicious code
- Lay the foundations for forensic analysis in the world of software and computer audits

Module 4. Corporate Networks and Infrastructures

- Master advanced aspects of infrastructure interconnection, essential when designing and planning high-speed networks
- Know the main characteristics and technologies of transport networks
- Understand the architectures of: Classic WAN, All-Ethernet, MPLS, VPNs
- Analyze the fundamental aspects of the evolution of networks to NGN (Next Generation Networks)
- Understand advanced QoS, routing and congestion control and reliability requirements
- Know and apply international network standards

Module 5. Security Architectures

- Understand the basic principles of IT security
- Master IT security standards and certification processes
- Analyze the organizational and cryptographic fundamentals underlying security technologies

- Identify the main threats and vulnerabilities of the different elements involved in ICT, as well as their causes
- Know in depth the tools for network security and their specific functions specific functions
- Know how to apply the technologies that make up an ICT Security Architecture, in its different perspectives

Module 6. Data Centers, Network Operation and Services

- Be able to design, operate, manage and maintain networks, services and content provided through a data center
- Know all the essential elements that make up a data center and the existing standards and certifications
- Analyze the economic impact of a data center infrastructure in terms of performance and efficiency
- Identify in real infrastructures the hardware elements of a data center
- Understand the security implications of the different solutions for offering services by market providers
- Know how the virtualization process works
- Understand the advantages, benefits and adoption models of the cloud

Module 7. Advanced Programming

- Deepen the knowledge of programming, especially as it relates to object-oriented programming, and the different types of relationships between existing classes
- Know the different design patterns for object-oriented problems
- Learning about event-driven programming and user interface development with Qt
- Acquire the essential knowledge of concurrent programming, processes and threads
- Learn how to manage the use of threads and synchronization, as well as the resolution of common problems within Concurrent Programming
- Understand the importance of documentation and testing in software development

Module 8. Systems Engineering and Network Services

- Master the fundamental concepts of service engineering
- Know the basic principles of configuration management of evolving software systems
- Know the technologies and tools for the provision of telematic services
- Know the different architectural styles of a software system, understand their differences and know how to choose the most appropriate one according to the system requirements
- Understand validation and verification processes and their relationships with other phases of the life cycle

- Be able to integrate systems for the capture, representation, processing, storage, management and presentation of multimedia information for the construction of telecommunication services and telematic applications
- Know common elements for the detailed design of a software system
- Acquire the ability to program, simulate and validate telematic, networked and distributed services and applications
- Understand the process and activities of transition, configuration, deployment and operation
- Understand network management, automation and optimization processes

Module 9. Information Systems Auditing

- Master the main concepts, standards and methodologies of systems auditing
- Be aware of the organizational elements and the legal framework of audits
- Obtain a reference guide for the design of new IT internal control systems
- Understand and determine the risks associated with technological development
- Detect how different information systems meet or do not meet the desired security requirements
- Be able to carry out a process of continuous improvement of cybersecurity

Module 10. Project Management

- Know the fundamental concepts of project management and the project management life cycle
- Understand the different stages of project management such as initiation, planning, stakeholder management and scoping
- Learning schedule development for time management, budget development and risk response
- Understand how quality management works in projects, including planning, assurance, control, statistical concepts and available tools
- Understand the functioning of the processes of procurement, execution, monitoring, control and closure of a project
- Acquire the essential knowledge related to the professional responsibility derived from project management

03

Skills

After passing the evaluations of the Professional Master's Degree in Telematics, you will have acquired the necessary skills to work in a safe and up-to-date way in the different fields of work that Telematics develops Enhancing your skills which will make a difference in your professional career.

Acquire the skills of a Telematics specialist and start working in this field with the vision of a cutting-edge professional"

General Skill

- Develop telematic applications and perform digital security tasks

Specialize with the best and be at the forefront of professional intervention"

Specific Skills

- Know all the structure of computer networks
- Master distributed systems and know how to classify them
- Perform security tasks on communication systems and networks
- Apply international standards for networks
- Master all computer security procedures
- Design and manage data centers
- Perform programming tasks, detect possible problems and solve them
- Know the entire system design process
- Perform systems audits and improve cyber security
- Know all the stages of project management and its life cycle to know how to manage them

04

Structure and Content

The structure of the contents has been designed by the best professionals in the telecommunications IT sector. An intensive and complete program that includes all the aspects that the Computer Scientist working in Telematics must handle safely, developed in a structured and efficient way for the student.

We have the most complete and up-to-date program on the market. We strive for excellence and for you to achieve it too"

Module 1. Computer Networks

1.1. Computer Networks on the Internet
- 1.1.1. Networks and Internet
- 1.1.2. Protocol Architecture

1.2. The Application Layer
- 1.2.1. Model and Protocols
- 1.2.2. FTP and SMTP Services
- 1.2.3. DNS Service
- 1.2.4. HTTP Operation Model
- 1.2.5. HTTP Message Formats
- 1.2.6. Interaction with Advanced Methods

1.3. The Transport Layer
- 1.3.1. Communication Between Processes
- 1.3.2. Connection-Oriented Transportation: TCP and SCTP

1.4. The Network Layer
- 1.4.1. Circuit and Packet Switching
- 1.4.2. IP Protocol (v4 and v6)
- 1.4.3. Routing Algorithms

1.5. The Link Layer
- 1.5.1. Link Layer and Error Detection and Correction Techniques
- 1.5.2. Multiple Access Links and Protocols
- 1.5.3. Link Level Addressing

1.6. LAN Networks
- 1.6.1. Network Topologies
- 1.6.2. Network and Interconnection Elements

1.7. IP Addressing
- 1.7.1. IP Addressing and Subnetting
- 1.7.2. Overview: An HTTP Request

1.8. Wireless and Mobile Networks
- 1.8.1. 2G, 3G and 4G Mobile Networks and Services
- 1.8.2. 5G Networks

1.9. Network Security
- 1.9.1. Fundamentals of Communications Security
- 1.9.2. Access Control
- 1.9.3. System Security
- 1.9.4. Fundamentals of Cryptography
- 1.9.5. Digital Signature

1.10. Internet Security Protocols
- 1.10.1. IP Security and Virtual Private Networks (VPN)
- 1.10.2. Web Security with SSL/TLS

Module 2. Distributed Systems

2.1. Introduction to Distributed Computing
- 2.1.1. Basic Concepts
- 2.1.2. Monolithic, Distributed, Parallel and Cooperative Computing
- 2.1.3. Advantages, Drawbacks and Challenges of Distributed Systems
- 2.1.4. Preliminary Concepts About Operating Systems: Processes and Concurrency
- 2.1.5. Preliminary Concepts About Networking
- 2.1.6. Previous Concepts About Software Engineering
- 2.1.7. Organization of this Manual

2.2. Distributed Computing Paradigms and Inter-Process Communication
- 2.2.1. Communication Between Processes
- 2.2.2. Event Synchronization
  - 2.2.2.1. Assumption 1: Synchronous Sending and Synchronous Receiving
  - 2.2.2.2. Assumption 2: Asynchronous Sending and Synchronous Receiving
  - 2.2.2.3. Scenario 3: Synchronous Sending and Asynchronous Receiving
  - 2.2.2.4. Scenario 4: Asynchronous Sending and Asynchronous Receiving

2.2.3. Interlocks and Timers
2.2.4. Data Representation and Encoding
2.2.5. Classification and Description of Distributed Computing Paradigms
2.2.6. Java as a Distributed Systems Development Environment
2.3. Sockets API
2.3.1. Socket API, Types and Differences
2.3.2. Datagram Type Sockets
2.3.3. Stream Type Sockets
2.3.4. Solution to Interlocks: Timers and Non-Blocking Events
2.3.5. Socket Security
2.4 Client-Server Communications Paradigm
2.4.1. Characteristics and Fundamental Concepts of Distributed Client-Server Systems
2.4.2. Client-Server System Design and Implementation Process
2.4.3. Non-Connection Oriented Addressing Problems with Anonymous Clients
2.4.4. Iterative and Concurrent Servers
2.4.5. Status and Session Information
2.4.5.1. Session Information
2.4.5.2. Global Status Information
2.4.6. Complex Clients Receiving Asynchronous Responses from the Server Side
2.4.7. Complex Servers Acting as Intermediaries Between Multiple Clients
2.5. Group Communication
2.5.1. Introduction to Multicast and Common Uses
2.5.2. Reliability and Management in Multicast Systems
2.5.3. Java Implementation of Multicast Systems
2.5.4. Example of Using Peer-to-peer Group Communication
2.5.5. Reliable Multicast Implementations
2.5.6. Multi-Transmission at Application Level
2.6. Distributed Objects
2.6.1. Introduction to Distributed Objects
2.6.2. Architecture of an Application Based on Distributed Objects
2.6.3. Distributed Object Systems Technologies
2.6.4. Client-Side and Server-Side Java RMI Software Layers
2.6.5. Java RMI API for Distributed Objects
2.6.6. Steps to Build an RMI Application
2.6.7. Use of Callback in RMI
2.6.8. Dynamic Offloading of Remote Object Tokens and RMI Security Manager
2.7. Internet Applications I: HTML, XML, HTTP
2.7.1. Introduction Internet Applications I
2.7.2. HTML Language
2.7.3. XML Language
2.7.4. Internet Protocol: HTTP
2.7.5. Use of Dynamic Content: Forms Management and CGI
2.7.6. Handling of State and Session Data on the Internet
2.8. CORBA
2.8.1. Introduction to CORBA
2.8.2. CORBA Architecture
2.8.3. Interface Description Language in CORBA
2.8.4. GIOP Interoperability Protocols
2.8.5. IOR Remote Object References
2.8.6. CORBA Naming Service
2.8.7. Example in IDL Java
2.8.8. Design, Compilation and Execution Steps in IDL Java
2.9. Internet Applications II: Applets, Servlets and SOA
2.9.1. Introduction to Internet Applications II
2.9.2. Applets
2.9.3. Introduction to Servlets
2.9.4. HTTP Servlets and How They Work

2.9.5. Maintaining State Information in Servlets
2.9.5.1. Hidden form Fields
2.9.5.2. Cookies
2.9.5.3. Servlet Variables
2.9.5.4. Object Session
2.9.6. Web Services
2.9.7. SOAP Protocol
2.9.8. Brief Overview of the REST Architecture
2.10. Advanced Paradigms
2.10.1. Introduction to Advanced Paradigms
2.10.2. MOM Paradigm
2.10.3. Mobile Software Agent Paradigm
2.10.4. Object Space Paradigm
2.10.5. Collaborative Computing
2.10.6. Future Trends in Distributed Computing

Module 3. Security in Communication Systems and Networks

3.1. A global Perspective on Security, Cryptography and Classical Cryptanalysis
3.1.1. Computer Security: Historical Perspective
3.1.2. But What Exactly is Meant by Security?
3.1.3. History of Cryptography
3.1.4. Substitution Ciphers
3.1.5. Case Study: The Enigma Machine
3.2. Symmetric Cryptography
3.2.1. Introduction and Basic Terminology
3.2.2. Symmetric Encryption
3.2.3. Modes of Operation
3.2.4. DES
3.2.5. The New AES Standard
3.2.6. Encryption in Flow
3.2.7. Cryptanalysis
3.3. Asymmetric Cryptography
3.3.1. Origins of Public Key Cryptography
3.3.2. Basic Concepts and Operation
3.3.3. The RSA Algorithm
3.3.4. Digital Certificates
3.3.5. Key Storage and Management
3.4. Network Attacks
3.4.1. Network Threats and Attacks
3.4.2. Enumeration
3.4.3. Traffic Interception: Sniffers
3.4.4. Denial of Service Attacks
3.4.5. ARP Poisoning Attacks
3.5. Security Architectures
3.5.1. Traditional Security Architectures
3.5.2. Secure Socket Layer: SSL
3.5.3. SSH Protocol
3.5.4. Virtual Private Networks (VPNs)
3.5.5. External Storage Unit Protection Mechanisms
3.5.6. Hardware Protection Mechanisms
3.6. System Protection Techniques and Secure Code Development
3.6.1. Operational Safety
3.6.2. Resources and Controls
3.6.3. Monitoring
3.6.4. Intrusion Detection Systems
3.6.5. Host IDS
3.6.6. Network IDS
3.6.7. Signature-Based IDS
3.6.8. Lure Systems
3.6.9. Basic Security Principles in Code Development
3.5.10. Failure Management
3.5.11. Public Enemy Number 1: Buffer Overflows
3.5.12. Cryptographic Botches

3.7. Botnets and Spam
- 3.7.1. Origin of the Problem
- 3.7.2. Spam Process
- 3.7.3. Sending Spam
- 3.7.4. Refinement of Mailing Lists
- 3.7.5. Protection Techniques
- 3.7.6. Anti-Spam Service offered by Third Parties
- 3.7.7. Study Cases
- 3.7.8. Exotic Spam

3.8. Web Auditing and Attacks
- 3.8.1. Information Gathering
- 3.8.2. Attack Techniques
- 3.8.3. Data Science

3.9. Malware and Malicious Code
- 3.9.1. What is Malware?
- 3.9.2. Types of Malware
- 3.9.3. Virus
- 3.9.4. Cryptovirus
- 3.9.5. Worms
- 3.9.6. Adware
- 3.9.7. Spyware
- 3.9.8. Hoaxes
- 3.9.9. Phishing
- 3.9.10. Trojans
- 3.9.11. The Economy of Malware
- 3.9.12. Possible Solutions

3.10. Forensic Analysis
- 3.10.1. Evidence Collection
- 3.10.2. Evidence Analysis
- 3.10.3. Anti-Forensic Techniques
- 3.10.4. Case Study

Module 4. Corporate Networks and Infrastructures

4.1. Transport Networks
- 4.1.1. Functional Architecture of Transport Networks
- 4.1.2. Network Node Interface in SDH
- 4.1.3. Network Element
- 4.1.4. Network Quality and Availability
- 4.1.5. Management of Transportation Networks
- 4.1.6. Evolution of Transmission Networks

4.2. Classical WAN Architectures
- 4.2.1. WAN Wide Area Networks
- 4.2.2. WAN Standards
- 4.2.3. WAN Encapsulation
- 4.2.4. WAN Devices
  - 4.2.4.1. Router
  - 4.2.4.2. Modem
  - 4.2.4.3. Switch
  - 4.2.4.4. Communication Servers
  - 4.2.4.5. Gateway
  - 4.2.4.6. Firewall
  - 4.2.4.7. Proxy
  - 4.2.4.8. Proxy
- 4.2.5. Types of Connection
  - 4.2.5.1. Point-to-Point Links
  - 4.2.5.2. Circuit Switching
  - 4.2.5.3. Packet Switching
  - 4.2.5.4. WAN Virtual Circuits

4.3. Networks Based on ATM
- 4.3.1. Introduction, Characteristics and Layer Model
- 4.3.2. ATM Physical Access Layer
  - 4.3.2.1. PM Physical Media Dependent Sublayer
  - 4.3.2.2. Transmission Convergence Sublayer TC
- 4.3.3. ATM Cell
  - 4.3.3.1. Header
  - 4.3.3.2. Virtual Connection
  - 4.3.3.3. ATM Switching Node
  - 4.3.3.4. Flow Control (Link Loading)
- 4.3.4. Adaptation of AAL Cells
  - 4.3.4.1. Types of AAL Services

4.4. Advanced Queuing Models
- 4.4.1. Introduction
- 4.4.2. Fundamentals of Queuing Theory
- 4.4.3. Queuing Theory Basic Systems
  - 4.4.3.1. M/M/1, M/M/m and M/M/∞ Systems
  - 4.4.3.2. M/M/1/k and M/M/m/m/m Systems
- 4.4.4. Queuing Theory Advanced Systems
  - 4.4.4.1. M/G/1 System
  - 4.4.4.2. M/G/1 System with Priorities
  - 4.4.4.3. Queuing Networks
  - 4.4.4.4. Modeling of Communication Networks

4.5. Quality of Service in Corporate Networks
- 4.5.1. Fundamentals
- 4.5.2. QoS Factors in Converged Networks
- 4.5.3. QoS Concepts
- 4.5.4. QoS Policies
- 4.5.5. Methods for Implementing QoS
- 4.5.6. QoS Models
- 4.5.7. Mechanisms for the Deployment of DiffServ QoS
- 4.5.8. Application Examples

4.6. Corporate Networks and All-Ethernet Infrastructures
- 4.6.1. Ethernet Network Topologies
  - 4.6.1.1. Bus Topology
  - 4.6.1.2. Star Topology
- 4.6.2. Ethernet and IEEE 802.3 Frame Format
- 4.6.3. Switched Ethernet Network
  - 4.6.3.1. VLAN Virtual Networks
  - 4.6.3.2. Port Aggregation
  - 4.6.3.3. Connection Redundancy
  - 4.6.3.4. QoS Management
  - 4.6.3.5. Safety Functions
- 4.6.4. Fast Ethernet
- 4.6.5. Gigabit Ethernet

4.7. MPLS. Infrastructures
- 4.7.1. Introduction
- 4.7.2. MPLS
  - 4.7.2.1. Background to MPLS and Evolution
  - 4.7.2.2. MPLS Architecture
  - 4.7.2.3. Forwarding of Labeled Packets
  - 4.7.2.4. Label Distribution Protocol (LDP)
- 4.7.3. MPLS VPN
  - 4.7.3.1. Definition of a VPN
  - 4.7.3.2. VPN Models
  - 4.7.3.3. MPLS VPN Model
  - 4.7.3.4. MPLS VPN Architecture
  - 4.7.3.5. Virtual Routing Forwarding (VRF)
  - 4.7.3.6. RD
  - 4.7.3.7. Route Target (RT)
  - 4.7.3.8. VPNv4 Route Propagation in an MPLS VPN
  - 4.7.3.9. Packet Forwarding in a VPN MPLS Network
  - 4.7.3.10. BGP
  - 4.7.3.11. Extended BGP Community: RT

4.7.3.12. Label Transport with BGP
4.7.3.13. Route Reflector (RR)
4.7.3.14. Group RR
4.7.3.15. BGP Route Selection
4.7.3.16. Packet Forwarding
4.7.4. Common Routing Protocols in MPLS Environments
4.7.4.1. Vector Distance Routing Protocols
4.7.4.2. Link State Type Routing Protocols
4.7.4.3. OSPF
4.7.4.4. ISIS
4.8. Operator Services and VPNs
4.8.1. Introduction
4.8.2. Basic Requirements of a VPN
4.8.3. Types of VPN
4.8.3.1. Remote Access VPN
4.8.3.2. Point-to-Point VPN
4.8.3.3. Internal VPN (over LAN):
4.8.4. Protocols Used in VPN
4.8.5. Implementations and Connection Types
4.9. NGN (Next Generation Networks)
4.9.1. Introduction
4.9.2. Background
4.9.2.1. Definition and Characteristics of a NGN Network
4.9.2.2. Migration to Next Generation Networks
4.9.3. NGN Architecture
4.9.3.1. Primary Connectivity Layer
4.9.3.2. Access Layer
4.9.3.3. Service Layer
4.9.3.4. Management Layer
4.9.4. IMS
4.9.5. Standard-Setting Organizations
4.9.6. Regulatory Trends
4.10. Review of ITU and IETF Standards
4.10.1. Introduction
4.10.2. Standardization
4.10.3. Some Standard Organizations
4.10.4. WAN Physical Layer Protocols and Standards
4.10.5. Examples of Medium-Oriented Protocols

Module 5. Security Architectures

5.1. Basic Principles of IT Security
5.1.1. What Is IT Security?
5.1.2. Objectives of IT Security
5.1.3. IT Security Services
5.1.4. Consequences of Lack of Security
5.1.5. Principle of "Defense in Security
5.1.6. Security Policies, Plans and Procedures
5.1.6.1. User Account Management
5.1.6.2. User Identification and Authentication
5.1.6.3. Authorization and Logical Access Control
5.1.6.4. Server Monitoring
5.1.6.5. Data Protection
5.1.6.6. Security in Remote Connections
5.1.7. The Importance of the Human Factor
5.2. Standardization and Certification in IT Security
5.2.1. Safety Standards
5.2.1.1. Purpose of the Standards
5.2.1.2. Responsible Bodies
5.2.2. Standards in the USA
5.2.2.1. TCSEC
5.2.2.2. Federal Criteria
5.2.2.3. FISCAM
5.2.2.4. NIST SP 800

5.2.3. European Standards
5.2.3.1. ITSEC
5.2.3.2. ITSEM
5.2.3.3. European Network and Information Security Agency
5.2.4. International Standards
5.2.5. Accreditation Process
5.3. Threats to Computer Security: Vulnerabilities and Malware
5.3.1. Introduction
5.3.2. System Vulnerabilities
5.3.2.1. Network Security Incidents
5.3.2.2. Causes of Vulnerabilities in Computer Systems
5.3.2.3. Types of Vulnerabilities
5.3.2.4. Responsibilities of the Software Manufacturers
5.3.2.5. Vulnerability Assessment Tools
5.3.3. Computer Security Threats
5.3.3.1. Classification of Network Intruders
5.3.3.2. Motivations of Attackers
5.3.3.3. Phases of an Attack
5.3.3.4. Types of Attacks
5.3.4. Computer Viruses
5.3.4.1. General Characteristics
5.3.4.2. Types of Viruses
5.3.4.3. Damage Caused by Viruses
5.3.4.4. How to Combat Viruses
5.4. Cyberterrorism and Incident Response
5.4.1. Introduction
5.4.2. The Threat of Cyberterrorism and Cyberwarfare
5.4.3. Consequences of Mistakes and Attacks on Businesses
5.4.4. Espionage in Computer Networks
5.5. User Identification and Biometric Systems
5.5.1. Introduction to Authentication, Authorization and User Registration
5.5.2. AAA Security Model
5.5.3. Access Control
5.5.4. User Identification
5.5.5. Verification of Passwords
5.5.6. Authentication with Digital Certificates
5.5.7. Remote User Identification
5.5.8. Single Sign-On
5.5.9. Password Managers
5.5.10. Biometric Systems
5.5.10.1. General Characteristics
5.5.10.2. Types of Biometric Systems
5.5.10.3. Implementation of the Systems
5.6. Fundamentals of Cryptography and Cryptographic Protocols
5.6.1. Introduction to Cryptography
5.6.1.1. Cryptography, Cryptanalysis and Cryptology
5.6.1.2. Operation of a Cryptographic System
5.6.1.3. History of Cryptographic Systems
5.6.2. Cryptanalysis
5.6.3. Classification of Cryptographic Systems
5.6.4. Symmetric and Asymmetric Cryptographic Systems
5.6.5. Authentication with Cryptographic Systems
5.6.6. Electronic Signature
5.6.6.1. What Is the Electronic Signature?
5.6.6.2. Characteristics of the Electronic Signature
5.6.6.3. Certification Authorities
5.6.6.4. Digital Certificates
5.6.6.5. Systems Based on the Trusted Third Party
5.6.6.6. Use of Electronic Signature
5.6.6.7. Electronic ID
5.6.6.8. Electronic Invoice

5.7. Tools for Network Security
- 5.7.1. The Problem of Security in the Internet Connection
- 5.7.2. Security in the External Network
- 5.7.3. The Role of Proxy Servers
- 5.7.4. The Role of Firewalls
- 5.7.5. Authentication Servers for Remote Connections
- 5.7.6. The Analysis of Activity Logs
- 5.7.7. Intrusion Detection Systems
- 5.7.8. Decoys

5.8. Security in Virtual and Wireless Private Networks
- 5.8.1. Security in Virtual Private Networks
  - 5.8.1.1 The Role of VPNs
  - 5.8.1.2 Protocols for VPNs
- 5.8.2. Traditional Security in Wireless Networks
- 5.8.3. Possible Attacks on Wireless Networks
- 5.8.4. The WEP Protocol
- 5.8.5. Standards for Wireless Network Security
- 5.8.6. Recommendations for Strengthening Security

5.9. Security in the Use of Internet Services
- 5.9.1. Safe Web Browsing
  - 5.9.1.1. The WWW Service
  - 5.9.1.2. Security Problems in WWW
  - 5.9.1.3. Safety Recommendations
  - 5.9.1.4. Protection of Privacy on the Internet
- 5.9.2. E-Mail Security
  - 5.9.2.1. E-Mail Characteristics
  - 5.9.2.2. E-Mail Security Problems
  - 5.9.2.3. E-Mail Security Recommendations
  - 5.9.2.4. Advanced E-Mail Services
  - 5.9.2.5. Use of E-Mail by Employees
- 5.9.3. SPAM
- 5.9.4. Phishing

5.10. Content Control
- 5.10.1. The Distribution of Contents Through the Internet
- 5.10.2. Legal Measures to Combat Illegal Content
- 5.10.3. Filtering, Cataloguing and Blocking Content
- 5.10.4. Damage to Image and Reputation

Module 6. Data Centers, Network Operation and Services

6.1. Data Center: Basic Concepts and Components
- 6.1.1. Introduction
- 6.1.2. Basic Concepts
  - 6.1.2.1. DC Definition
  - 6.1.2.2. Classification and Importance
  - 6.1.2.3. Catastrophes and Losses
  - 6.1.2.4. Evolutionary Trend
  - 6.1.2.5. Complexity Costs
  - 6.1.2.6. Pillars and Layers of Redundancy
- 6.1.3. Design Philosophy
  - 6.1.3.1. Objectives
  - 6.1.3.2. Location Selection
  - 6.1.3.3. Availability
  - 6.1.3.4. Critical Elements
  - 6.1.3.5. Assessment and Cost Analysis
  - 6.1.3.6. IT Budget
- 6.1.4. Basic Components
  - 6.1.4.1. Technical Floor
  - 6.1.4.2. Types of Tiles
  - 6.1.4.3. General Considerations
  - 6.1.4.4. Size of DC
  - 6.1.4.5. Racks
  - 6.1.4.6. Servers and Communication Equipment
  - 6.1.4.7. Monitoring

6.2. Data Center: Control Systems
- 6.2.1. Introduction
- 6.2.2. Power Supply
  - 6.2.2.1. Electric Network
  - 6.2.2.2. Electrical Power
  - 6.2.2.3. Electricity Distribution Strategies
  - 6.2.2.4. UPS
  - 6.2.2.5. Generators
  - 6.2.2.6. Electrical Problems
- 6.2.3. Environmental Control
  - 6.2.3.1. Temperature
  - 6.2.3.2. Humidity
  - 6.2.3.3. Air Conditioning
  - 6.2.3.4. Caloric Estimation
  - 6.2.3.5. Cooling Strategies
  - 6.2.3.6. Corridor Design Air Circulation
  - 6.2.3.7. Sensors and Maintenance
- 6.2.4. Fire Safety and Prevention
  - 6.2.4.1. Physical Security
  - 6.2.4.2. Fire and its Classification
  - 6.2.4.3. Classification and Types of Extinction Systems

6.3. Data Center: Design and Organization
- 6.3.1. Introduction
- 6.3.2. Network Design
  - 6.3.2.1. Typology
  - 6.3.2.2. Structured Cabling
  - 6.3.2.3. Backbone
  - 6.3.2.4. UTP and STP Network Cables
  - 6.3.2.5. Telephony Cables
  - 6.3.2.6. Terminal Elements
  - 6.3.2.7. Fiber Optic Cables
  - 6.3.2.8. Coaxial Cable
  - 6.3.2.9. Wireless Transmission
  - 6.3.2.10. Recommendations and Labeling
- 6.3.3. Organization
  - 6.3.3.1. Introduction
  - 6.3.3.2. Basic Measurements
  - 6.3.3.3. Strategies for Cable Management
  - 6.3.3.4. Policies and Procedures
- 6.3.4. DC Management
- 6.3.5. Data Center Standards

6.4. Data Center: Models and Business Continuity
- 6.4.1. Introduction
- 6.4.2. Optimization
  - 6.4.2.1. Optimization Techniques
  - 6.4.2.2. Green Data Centers
  - 6.4.2.3. Current Challenges
  - 6.4.2.4. Modular Data Centers
  - 6.4.2.5. Housing
  - 6.4.2.6. Data Center Consolidation
  - 6.4.2.7. Monitoring
- 6.4.3. Business Continuity
  - 6.4.3.1. BCP Business Continuity Plans Key Points
  - 6.4.3.2. DR Disaster Recovery Plan
  - 6.4.3.3. DR Implementation
  - 6.4.3.4. Backup and Strategy
  - 6.4.3.5. Backup Data Center
- 6.4.4. Best Practices
  - 6.4.4.1. Recommendations
  - 6.4.4.2. Use of ITIL Methodology
  - 6.4.4.3. Availability Metrics
  - 6.4.4.4. Environmental Control
  - 6.4.4.5. Risk Management
  - 6.4.4.6. Responsible for DC
  - 6.4.4.7. Data Science
  - 6.4.4.8. Implementation Tips
  - 6.4.4.9. Characterization

6.5. Cloud Computing: Introduction and Basic Concepts
- 6.5.1. Introduction
- 6.5.2. Basic Concepts and Terminology
- 6.5.3. Objectives and Benefits
  - 6.5.3.1. Availability
  - 6.5.3.2. Reliability
  - 6.5.3.3. Scales
- 6.5.4. Risks and Challenges
- 6.5.5. Roles Provider Consumer
- 6.5.6. Features of a CLOUD
- 6.5.7. Service Delivery Models
  - 6.5.7.1. IaaS
  - 6.5.7.2. PaaS
  - 6.5.7.3. SaaS
- 6.5.8. Types of Cloud
  - 6.5.8.1. Public
  - 6.5.8.2. Private
  - 6.5.9.3. Hybrid
- 6.5.9. Cloud Enabling Technologies
  - 6.5.9.1. Network Architectures
  - 6.5.9.2. Broadband Networks Interconnectivity
  - 6.5.9.3. Data Center Technologies
    - 6.5.9.3.1. Computing
    - 6.5.9.3.2. Storage
    - 6.5.9.3.3. Networking
    - 6.5.9.3.4. High Availability
    - 6.5.9.3.5. Backup Systems
    - 6.5.9.3.6. Balancers
  - 6.5.9.4. Virtualization
  - 6.5.9.5. Web Technologies
  - 6.5.9.6. Multi-Tenant Technology

6.5.9.7. Service Technologies
6.5.9.8. Cloud Security
6.5.9.8.1. Terms and Concepts
6.5.9.8.2. Integrity, Authentication
6.5.9.8.3. Security Mechanisms
6.5.9.8.4. Security Threats
6.5.9.8.5. Cloud Security Attacks
6.5.9.8.6. Case Study

6.6. Cloud Computing: Cloud Technology and Security
6.6.1. Introduction
6.6.2. Cloud Infrastructure Mechanisms
6.6.2.1. Network Perimeter
6.6.2.2. Storage
6.6.2.3. Server Environment
6.6.2.4. Cloud Monitoring
6.6.2.5. High Availability
6.6.3. Cloud Security Mechanisms (Part I)
6.6.3.1. Automation
6.6.3.2. Load Balancers
6.6.3.3. SLA Monitor
6.6.3.4. Pay-as-You-Go Mechanisms
6.6.4. Cloud Security Mechanisms (part II)
6.6.4.1. Traceability and Auditing Systems
6.6.4.2. Failover Systems
6.6.4.3. Hypervisor
6.6.4.4. Clustering
6.6.4.5. Multitenant Systems

6.7. Cloud Computing: Infrastructure. Control and Security Mechanisms
6.7.1. Introduction to the Cloud Management Mechanisms
6.7.2. Remote Management Systems
6.7.3. Resource Management Systems
6.7.4. Service Level Agreement Management Systems
6.7.5. Billing Management Systems
6.7.6. Cloud Security Mechanisms
6.7.6.1. Encryption
6.7.6.2. Hashing
6.7.6.3. Digital Signature
6.7.6.4. PKI
6.7.6.5. Identity and Access Management
6.7.6.6. SSO
6.7.6.7. Cloud-Based Security Groups
6.7.6.8. Bastion Systems

6.8. Cloud Computing: Cloud Architecture
6.8.1. Introduction
6.8.2. Basic Cloud Architecture
6.8.2.1. Workload Distribution Architectures
6.8.2.2. Resource Usage Architectures
6.8.2.3. Scalable Architectures
6.8.2.4. Load Balancing Architectures
6.8.2.5. Redundant Architectures
6.8.2.6. Examples:
6.8.3. Advanced Cloud Architecture
6.8.3.1. Hypervisor Cluster Architectures
6.8.3.2. Virtual Load Balancing Architectures
6.8.3.3. Non-Stop Architectures
6.8.3.4. High-Availability Architectures
6.8.3.5. Bare-Metal Architectures
6.8.3.6. Redundant Architectures
6.8.3.7. Hybrid Architectures

6.8.4. Specialized Cloud Architectures
6.8.4.1. Direct I/O Access Architectures
6.8.4.2. LUN Direct Access Architectures
6.8.4.3. Elastic Network Architectures
6.8.4.4. SDDC Architecture
6.8.4.5. Special Architectures
6.8.4.6. Examples:
6.9. Cloud Computing: Service Provision Models
6.9.1. Introduction
6.9.2. Provision of Cloud Services
6.9.3. Service Provider Perspective
6.9.4. Consumer Perspective of these Services
6.9.5. Study Cases
6.10. Cloud Computing: Contracting Models, Metrics and Service Providers
6.10.1. Introduction to Billing Models and Metrics
6.10.2. Billing Models
6.10.3. Pay-Per-Use Metrics
6.10.4. Cost Management Considerations
6.10.5. Introduction to Quality-of-Service Metrics and SLAs
6.10.6. Service Quality Metrics
6.10.7. Service Performance Metrics
6.10.8. Service Scalability Metrics
6.10.9. Service Model SLAs
6.10.10. Study Cases

Module 7. Advanced Programming

7.1. Introduction to Object-Oriented Programming
7.1.1. Introduction to Object-Oriented Programming
7.1.2. Class Design
7.1.3. Introduction to UML for Problem Modeling
7.2. Relationships Between Classes
7.2.1. Abstraction and Inheritance
7.2.2. Advanced Inheritance Concepts
7.2.3. Polymorphism
7.2.4. Composition and Aggregation
7.3. Introduction to Design Patterns for Object-Oriented Problems
7.3.1. What are Design Patterns?
7.3.2. Factory Pattern
7.3.3. Singleton Pattern
7.3.4. Observer Pattern
7.3.5. Composite Pattern
7.4. Exceptions
7.4.1. What are Exceptions?
7.4.2. Exception Catching and Handling
7.4.3. Throwing Exceptions
7.4.4. Exception Creation
7.5. User Interfaces
7.5.1. Introduction to Qt
7.5.2. Positioning
7.5.3. What Are Events?
7.5.4. Events: Definition and Catching
7.5.5. User Interface Development

7.6. Introduction to Concurrent Programming
- 7.6.1. Introduction to Concurrent Programming
- 7.6.2. The Concept of Process and Thread
- 7.6.3. Interaction Between Processes or Threads
- 7.6.4. Threads in C++
- 7.6.5. Advantages and Disadvantages of Concurrent Programming

7.7. Thread Management and Synchronization
- 7.7.1. Life Cycle of a Thread
- 7.7.2. Thread Class
- 7.7.3. Thread Planning
- 7.7.4. Thread Groups
- 7.7.5. Daemon Threads
- 7.7.6. Synchronization
- 7.7.7. Locking Mechanisms
- 7.7.8. Communication Mechanisms
- 7.7.9. Monitors

7.8. Common Problems in Concurrent Programming
- 7.8.1. The Problem of Consuming Producers
- 7.8.2. The Problem of Readers and Writers
- 7.8.3. The Problem of the Philosophers' Dinner Party

7.9. Software Documentation and Testing
- 7.9.1. Why is it Important to Document Software?
- 7.9.2. Design Documentation
- 7.9.3. Documentation Tool Use

7.10. Software Testing
- 7.10.1. Introduction to Software Testing
- 7.10.2. Types of Tests
- 7.10.3. Unit Test
- 7.10.4. Integration Test
- 7.10.5. Validation Test
- 7.10.6. System Test

Module 8. Systems Engineering and Network Services

8.1. Introduction to Systems Engineering and Network Services
- 8.1.1. Concept of Computer System and Computer Engineering
- 8.1.2. Software and its Characteristics
  - 8.1.2.1. Software Features
- 8.1.3. Software Evolution
  - 8.1.3.1. The Dawn of Software Development
  - 8.1.3.2. The Software Crisis
  - 8.1.3.3. Software Engineering
  - 8.1.3.4. The Software Tragedy
  - 8.1.3.5. The Actuality of Software
- 8.1.4. The Myths of Software
- 8.1.5. The new Software Challenges
- 8.1.6. Professional Ethics of Software Engineering
- 8.1.7. SWEBOK. The Software Engineering Body of Knowledge

8.2. The Development Process
- 8.2.1. Problem Solving Process
- 8.2.2. The Software Development Process
- 8.2.3. Software Process vs. Life Cycle
- 8.2.4. Life cycles. Process Models (Traditional)
  - 8.2.4.1. Waterfall Model
  - 8.2.4.2. Prototype-Based Models
  - 8.2.4.3. Incremental Development Model
  - 8.2.4.4. Rapid Application Development (RAD)
  - 8.2.4.5. Spiral Model
  - 8.2.4.6. Unified Development Process or Rational Unified Process (RUP)
  - 8.2.4.7. Component-Based Software Development

8.2.5. The Agile Manifesto. Agile Methods
8.2.5.1. Extreme Programming (XP)
8.2.5.2. Scrum
8.2.5.3. Feature Driven Development (FDD)
8.2.6. Software Process Standards
8.2.7. Definition of a Software Process
8.2.8. Software Process Maturity
8.3. Agile Project Planning and Management
8.3.1. What is Agile
8.3.1.1. History of Agile
8.3.1.2. Agile Manifesto
8.3.2. Fundamentals of Agile
8.3.2.1. The Agile Mindset
8.3.2.2. The Agile Fit
8.3.2.3. Product Development Life Cycle
8.3.2.4. The "Iron Triangle"
8.3.2.5. Working with Uncertainty and Volatility
8.3.2.6. Defined Processes and Empirical Processes
8.3.2.7. The Myths of Agile
8.3.3. The Agile Environment
8.3.3.1. Operating Model
8.3.3.2. Agile Roles
8.3.3.3. Agile Techniques
8.3.3.4. Agile Practices
8.3.4. Agile Frameworks
8.3.4.1. E-Xtreme Programming (XP)
8.3.4.2. Scrum
8.3.4.3. Dynamic Systems Development Method (DSDM)
8.3.4.4. Agile Project Management
8.3.4.5. Kanban
8.3.4.6. Lean Software Development
8.3.4.7. Lean Start-Up
8.3.4.8. Scaled Agile Framework (SAFe)

8.4. Configuration Management and Collaborative Repositories
- 8.4.1. Basic Concepts of Software Configuration Management
  - 8.4.1.1. What is Software Configuration Management?
  - 8.4.1.2. Software Configuration and Software Configuration Elements
  - 8.4.1.3. Baselines
  - 8.4.1.4. Versions, Revisions, Variants and Releases
- 8.4.2. Configuration Management Activities
  - 8.4.2.1. Configuration Identification
  - 8.4.2.2. Configuration Change Control
  - 8.4.2.3. Generation of Status Reports
  - 8.4.2.4. Configuration Audit
- 8.4.3. The Configuration Management Plan
- 8.4.4. Configuration Management Tools
- 8.4.5. Configuration Management in the Metric v.3 Methodology
- 8.4.6. Configuration Management in SWEBOK

8.5. Systems and Services Testing
- 8.5.1. General Testing Concepts
  - 8.5.1.1. Verify and Validate
  - 8.5.1.2. Definition of Test
  - 8.5.1.3. Principles of Testing
- 8.5.2. Approaches to Testing
  - 8.5.2.1. White box Testing
  - 8.5.2.2. Black Box Testing
- 8.5.3. Static Testing or Revisions
  - 8.5.3.1. Formal Technical Reviews
  - 8.5.3.2. Walkthroughs
  - 8.5.3.3. Code Inspections
- 8.5.4. Dynamic Testing
  - 8.5.4.1. Unit Testing
  - 8.5.4.2. Integration Tests
  - 8.5.4.3. System Testing
  - 8.5.4.4. Acceptance Testing
  - 8.5.4.5. Regression Testing

8.5.5. Alpha Testing and Beta Testing
8.5.6. The Testing Process
8.5.7. Error, Defect and Failure
8.5.8. Automatic Testing Tools
8.5.8.1. Junit
8.5.8.2. LoadRunner
8.6. Modeling and Design of Network Architectures
8.6.1. Introduction
8.6.2. System Characteristics
8.6.2.1. Description of the Systems
8.6.2.2. Description and Characteristics of the Services 1.3. Performance Requirements
8.6.2.3. Operability Requirements
8.6.3. Requirements Analysis
8.6.3.1. User Requirements
8.6.3.2. Application Requirements
8.6.3.3. Network Requirements
8.6.4. Design of Network Architectures
8.6.4.1. Reference Architecture and Components
8.6.4.2. Architecture Models
8.6.4.3. System and Network Architectures
8.7. Modeling and Design of Distributed Systems
8.7.1. Introduction
8.7.2. Addressing and Routing Architecture
8.7.2.1. Routing Strategy
8.7.2.2. Routing Strategy
8.7.2.3. Design Considerations
8.7.3. Network Design Concepts
8.7.4. Design Process
8.8. Platforms and Deployment Environments
8.8.1. Introduction
8.8.2. Distributed Computer Systems
8.8.2.1. Basic Concepts
8.8.2.2. Models of Computation
8.8.2.3. Advantages, Disadvantages and Challenges
8.8.2.4. Operating Systems Basics
8.8.3. Virtualized Network Deployments
8.8.3.1. Need for Change
8.8.3.2. Transformation of Networks: From "All-IP" to the Cloud
8.8.3.3. Network Deployment in the Cloud
8.8.4. Example: Network Architecture in Azure
8.9. E2E Performance: Delay and Bandwidth QoS
8.9.1. Introduction
8.9.2. Performance Analysis
8.9.3. QoS
8.9.4. Traffic Prioritization and Management
8.9.5. Service Level Agreements
8.9.6. Design Considerations
8.9.6.1. Performance Assessment
8.9.6.2. Relationships and Interactions
8.10. Network Automation and Optimization
8.10.1. Introduction
8.10.2. Network Management
8.10.2.1. Management and Configuration Protocols
8.10.2.2. Network Management Architectures
8.10.3. Orchestration and Automation
8.10.3.1. ONAP Architecture
8.10.3.2. Controllers and Functions
8.10.3.3. Politics
8.10.3.4. Network Inventory
8.10.4. Optimization

Module 9. Information Systems Auditing

9.1. Information Systems Auditing. Standards of Good Practice
- 9.1.1. Introduction
- 9.1.2. Auditing and COBIT
- 9.1.3. ICT Management Systems Auditing
- 9.1.4. Certifications

9.2. Systems Audit Concepts and Methodologies
- 9.2.1. Introduction
- 9.2.2. Systems Assessment Methodologies: Quantitative and Qualitative
- 9.2.3. IT Audit Methodologies
- 9.2.4. The Audit Plan

9.3. Audit Contract
- 9.3.1. Legal Nature of the Contract
- 9.3.2. Parties to an Audit Contract
- 9.3.3. Subject Matter of the Audit Contract
- 9.3.4. Audit Report

9.4. Organizational Elements of Audits
- 9.4.1. Introduction
- 9.4.2. Mission of the Audit Department
- 9.4.3. Audit Planning
- 9.4.4. IS Audit Methodology

9.5. Legal Framework for Audits
- 9.5.1. Protection of Personal Data
- 9.5.2. Legal Protection of Software
- 9.5.3. Technological Crimes
- 9.5.4. Contracting, Signature and Electronic ID

9.6. Outsourcing Audit and Reference Frameworks
- 9.6.1. Introduction
- 9.6.2. Basic Concepts of Outsourcing
- 9.6.3. IT Outsourcing Audit
- 9.6.4. Reference Frameworks: CMMI, ISO27001, ITIL

9.7. Security Audit
- 9.7.1. Introduction
- 9.7.2. Physical and Logical Security
- 9.7.3. Environment Security
- 9.7.4. Physical Security Audit Planning and Execution

9.8. Network and Internet Audit
- 9.8.1. Introduction
- 9.8.2. Network Vulnerabilities
- 9.8.3. Principles and Internet Rights
- 9.8.4. Controls and Data Processing

9.9. Auditing of Computer Applications and Systems
- 9.9.1. Introduction
- 9.9.2. Reference Models
- 9.9.3. Application Quality Assessment
- 9.9.4. Audit of the Organization and Management of the Development and Maintenance Area

9.10. Audit of Personal Data
- 9.10.1. Introduction
- 9.10.2. Data Protection Laws and Regulations
- 9.10.3. Development of the Audit
- 9.10.4. Violations and Penalties

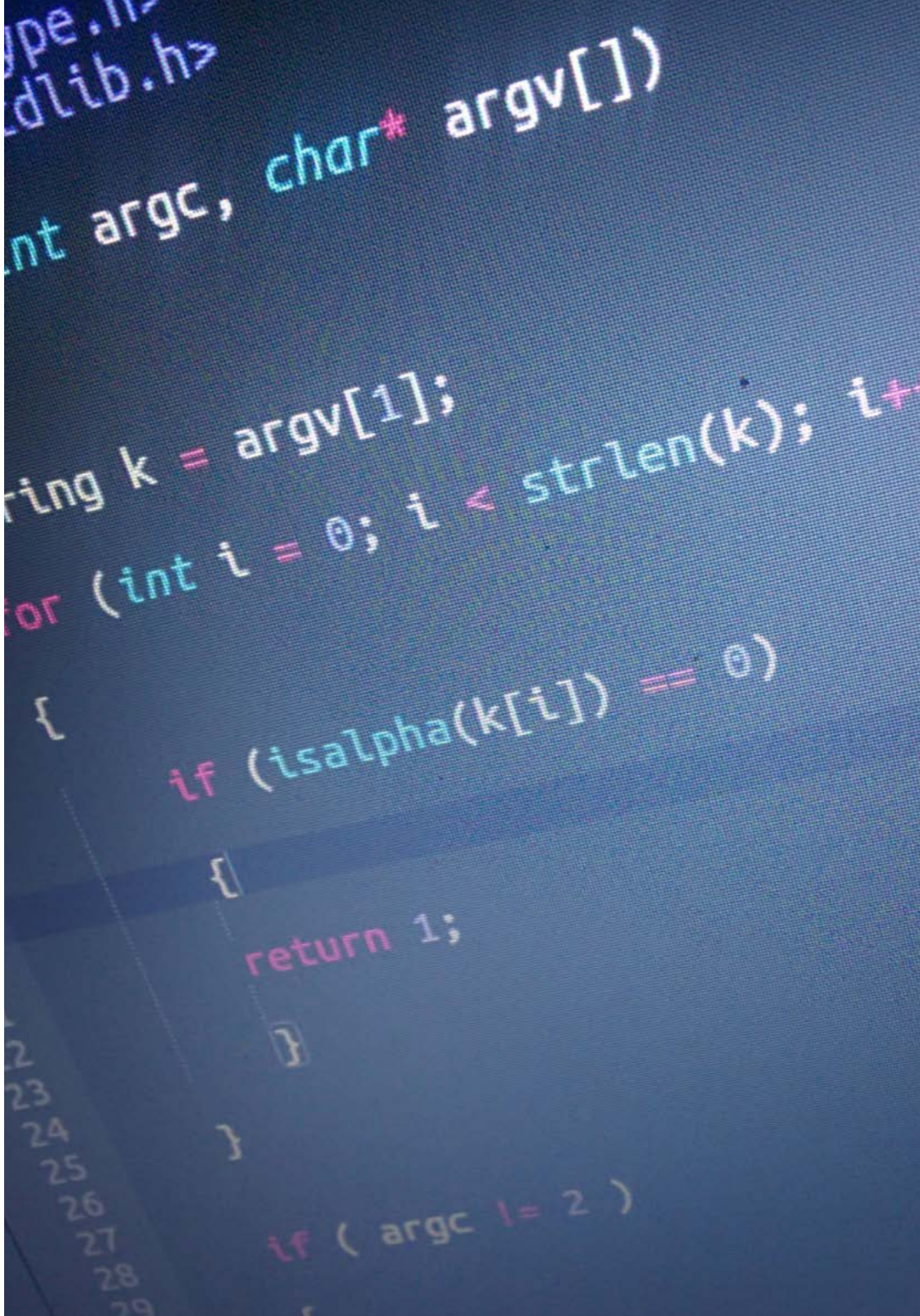
Module 10. Project Management

10.1. Fundamental Concepts of Project Management and the Project Management Lifecycle
- 10.1.1. What is a Project?
- 10.1.2. Common Methodology
- 10.1.3. What is Project Management?
- 10.1.4. What is a Project Plan?
- 10.1.5. Benefits
- 10.1.6. Project Life Cycle
- 10.1.7. Process Groups or Project Management Life Cycle
- 10.1.8. The Relationship between Process Groups and Knowledge Areas
- 10.1.9. Relationships between Product and Project Life Cycle

10.2. Start-Up and Planning
- 10.2.1. From the Idea to the Project
- 10.2.2. Development of the Project Record
- 10.2.3. Project Kick-Off Meeting
- 10.2.4. Tasks, Knowledge and Skills in the Startup Process
- 10.2.5. The Project Plan
- 10.2.6. Development of the Basic Plan. Steps
- 10.2.7. Tasks, Knowledge and Skills in the Planning Process

10.3. Stakeholders and Outreach Management
- 10.3.1. Identify Stakeholders
- 10.3.2. Develop Plan for Stakeholder Management
- 10.3.3. Manage Stakeholder Engagement
- 10.3.4. Control Stakeholder Engagement
- 10.3.5. The Objective of the Project
- 10.3.6. Scope Management and its Plan
- 10.3.7. Gathering Requirements
- 10.3.8. Define the Scope Statement
- 10.3.9. Create the WBS
- 10.3.10. Verify and Control the Scope

10.4. The Development of the Time-Schedule
- 10.4.1. Time Management and its Plan
- 10.4.2. Define Activities
- 10.4.3. Establishment of the Sequence of Activities
- 10.4.4. Estimated Resources for Activities
- 10.4.5. Estimated Duration of Activities
- 10.4.6. Development of the Time-Schedule and Calculation of the Critical Path
- 10.4.7. Schedule Control



10.5. Budget Development and Risk Response
- 10.5.1. Estimate Costs
- 10.5.2. Develop Budget and S-Curve
- 10.5.3. Cost Control and Earned Value Method
- 10.5.4. Risk Concepts
- 10.5.5. How to Perform a Risk Analysis
- 10.5.6. The Development of the Response Plan

10.6. Quality Management
- 10.6.1. Quality Planning
- 10.6.2. Assuring Quality
- 10.6.3. Quality Control
- 10.6.4. Basic Statistical Concepts
- 10.6.5. Quality Management Tools

10.7. Communication and Human Resources
- 10.7.1. Planning Communications Management
- 10.7.2. Communications Requirements Analysis
- 10.7.3. Communication Technology
- 10.7.4. Communication Models
- 10.7.5. Communication Methods
- 10.7.6. Communications Management Plan
- 10.7.7. Manage Communications
- 10.7.8. Management of Human Resources
- 10.7.9. Main Stakeholders and their Roles in the Projects
- 10.7.10. Types of Organization
- 10.7.11. Project Organization
- 10.7.12. The Work Equipment

10.8. Procurement
- 10.8.1. The Procurement Process
- 10.8.2. Planning
- 10.8.3. Search for Suppliers and Request for Quotations
- 10.8.4. Contract Allocation
- 10.8.5. Contract Administration
- 10.8.6. Contracts
- 10.8.7. Types of Contracts
- 10.8.8. Contract Negotiation

10.9. Execution, Monitoring and Control and Closure
- 10.9.1. Process Groups
- 10.9.2. Project Execution
- 10.9.3. Project Monitoring and Control
- 10.9.4. Project Closure

10.10. Professional Responsibility
- 10.10.1. Professional Responsibility
- 10.10.2. Characteristics of Social and Professional Responsibility
- 10.10.3. Project Leader Code of Ethics
- 10.10.4. Liability vs. PMP®
- 10.10.5. Examples of Liability
- 10.10.6. Benefits of Professionalization

A process of professional and personal growth that will become a boost of enormous quality for your competitiveness"

05

Methodology

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

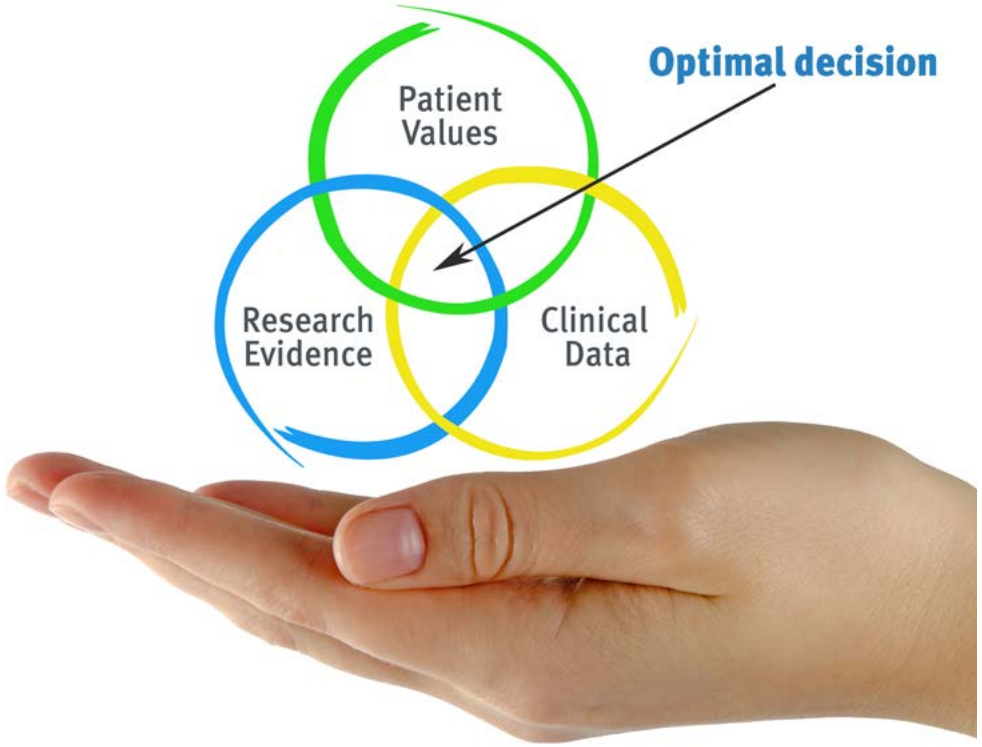
This teaching system is used, for example, in the most prestigious medical schools in the world, and major publications such as the **New England Journal of Medicine** have considered it to be one of the most effective.

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

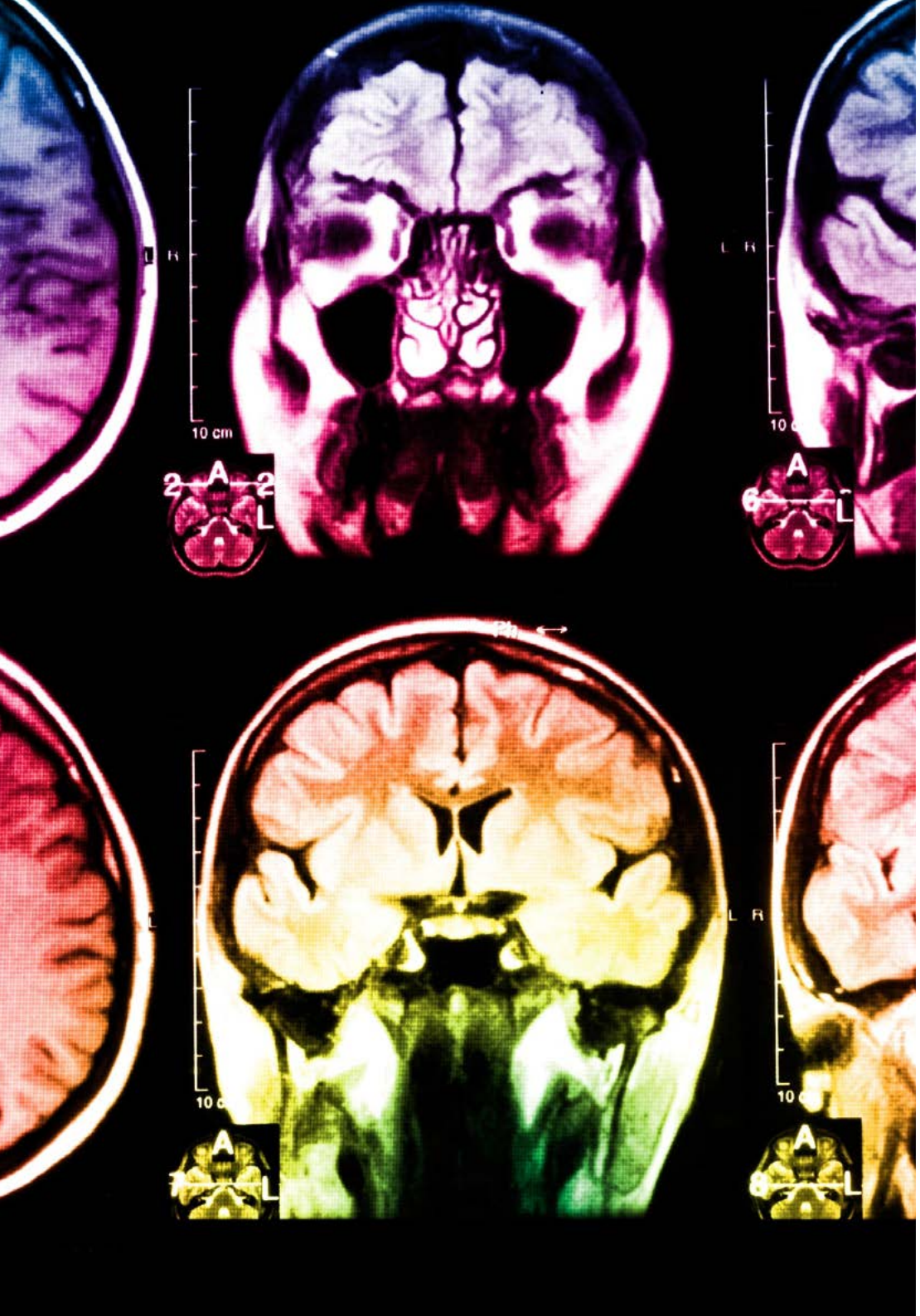
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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.

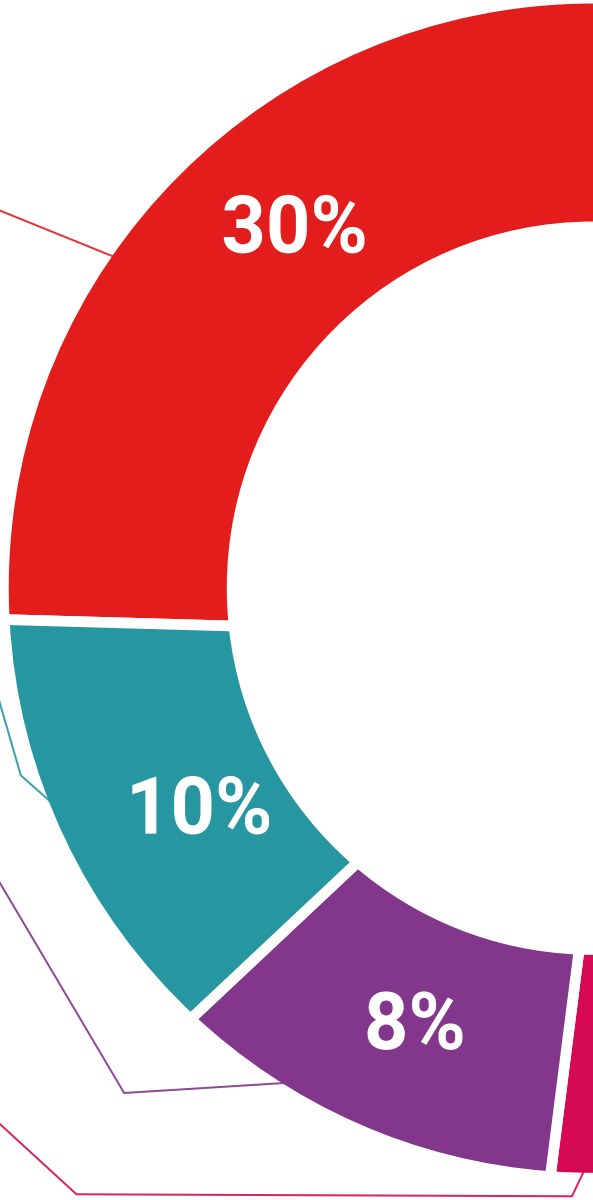
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

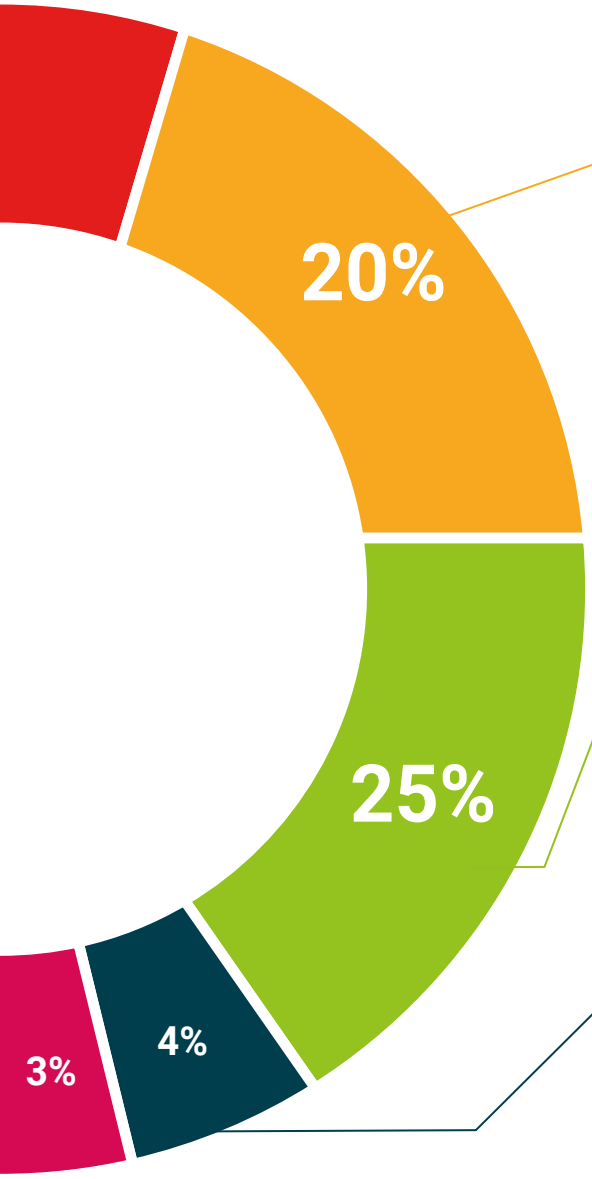
Practising Skills and Abilities

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.

06

Certificate

The Professional Master's Degree in Telematics 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 Postgraduate Certificate without having to travel or fill out laborious paperwork"

This **Professional Master's Degree in Telematics** contains the most complete and up-to-date program on the market.

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

The diploma 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 Telematics**

Official Nº of Hours: **1500 h.**


tech technological university

Awards the following

DIPLOMA

to

Mr./Ms. _____, with identification number _____.

For having successfully passed and accredited the following program

PROFESSIONAL MASTER'S DEGREE

in

Telematics

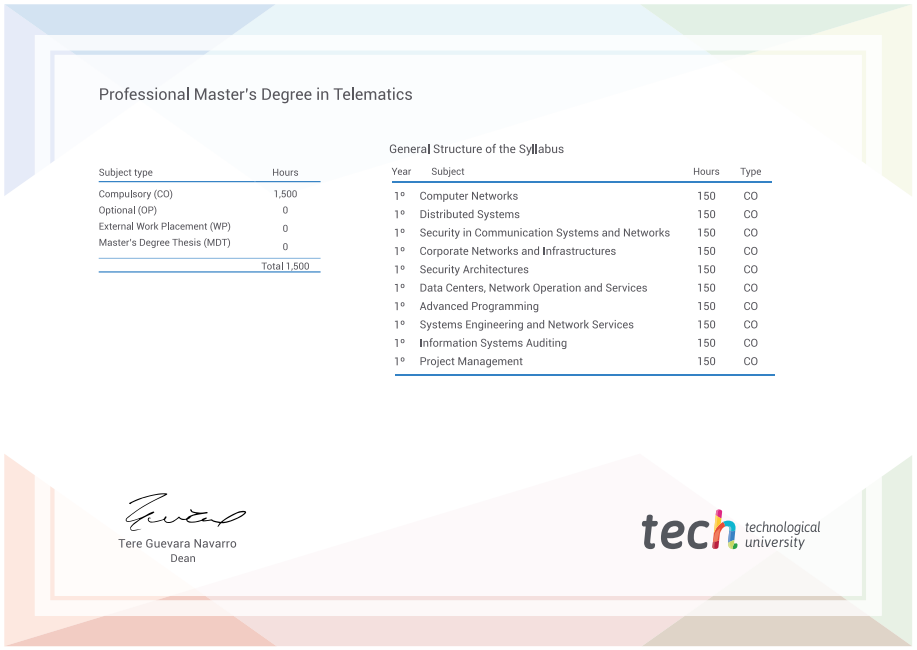
This is a qualification awarded by this University, equivalent to 1,500 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

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

June 17, 2020

Tere Guevara Navarro
Dean

Unique TECH Code: AFWORD23S techtitute.com/certificates


Professional Master's Degree in Telematics

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	Computer Networks	150	CO
1º	Distributed Systems	150	CO
1º	Security in Communication Systems and Networks	150	CO
1º	Corporate Networks and Infrastructures	150	CO
1º	Security Architectures	150	CO
1º	Data Centers, Network Operation and Services	150	CO
1º	Advanced Programming	150	CO
1º	Systems Engineering and Network Services	150	CO
1º	Information Systems Auditing	150	CO
1º	Project Management	150	CO

Tere Guevara Navarro
Dean

tech technological university

*Apostille Convention. In the event that the student wishes to have their paper diploma 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

Telematics

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

Professional Master's Degree
Telematics

tech technological university