Postgraduate Diploma

Computer Security for Communications

tech technological university

tech technological university

Postgraduate Diploma
Computer Security for Communications

- Modality: **online**
- Duration: **6 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/pk/information-technology/postgraduate-diploma/postgraduate-diploma-computer-security-communications

Index

01

Introduction

Unauthorized and improper use of networks is one of the main problems that users may face. It is essential to carry out computer security actions, since a large amount of private and confidential information circulates throughout the Internet. This Postgraduate Diploma brings students closer to the field of computer security for communications, with an up-to-date and quality program. It is a comprehensive preparation course that seeks to prepare students for success in their profession.

If you are looking for quality education that will help you specialize in one of the fields with the most professional prospects, this is your best option"

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

Within this area, computer security must be one of the aspects that companies must take the greatest care of, since all their information is on the network, so uncontrolled access by a user to carry out illicit tasks can be a serious problem for the organization, either financially or in terms of reputation.

The Postgraduate Diploma in Computer Security for Communications addresses the complete range of topics involved in this field. Its study has a clear advantage over other programs that focus on specific blocks, which prevents students from knowing the interrelation with other areas included in the multidisciplinary field of telecommunications. In addition, the teaching team of this educational program has made a careful selection of each of the topics of this program in order to offer students the most complete study opportunity possible and always linked to current events.

This program is aimed at those people interested in achieving a higher level of knowledge about Computer Security for Communications. The main objective of this Postgraduate Diploma is for students to specialize their knowledge in simulated work environments and conditions in a rigorous and realistic manner so that they can later apply it in the real world.

In addition, as it is a 100% online Postgraduate Diploma, the student is not constrained by fixed timetables or the need to move to another physical location, but can access the contents at any time of the day, balancing their professional or personal life with their academic life.

This **Postgraduate Diploma in Computer Security for Communications** contains the most complete and up-to-date program on the market. Its most notable features are:

- The development of case studies presented by computer security 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 self-assessment can be used to improve learning
- Its special emphasis on innovative methodologies in information security for communications
- 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

Do not miss the opportunity to take with us this Postgraduate Diploma in Computer Security for Communications. It's the perfect opportunity to advance your career"

This Postgraduate Diploma is the best investment you can make when selecting a refresher program to update your existing knowledge in Computer Security for Communications"

This program comes with the best educational material, providing you with a contextual approach that will facilitate your learning.

This 100% online Postgraduate Diploma will allow you to combine your studies with your professional work. You choose where and when to study.

The teaching staff includes professionals from the field of design, who bring their experience to this specialization program, as well as renowned specialists from leading 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, professionals will be assisted by an innovative interactive video system developed by renowned and experienced Computer Security experts.

02

Objectives

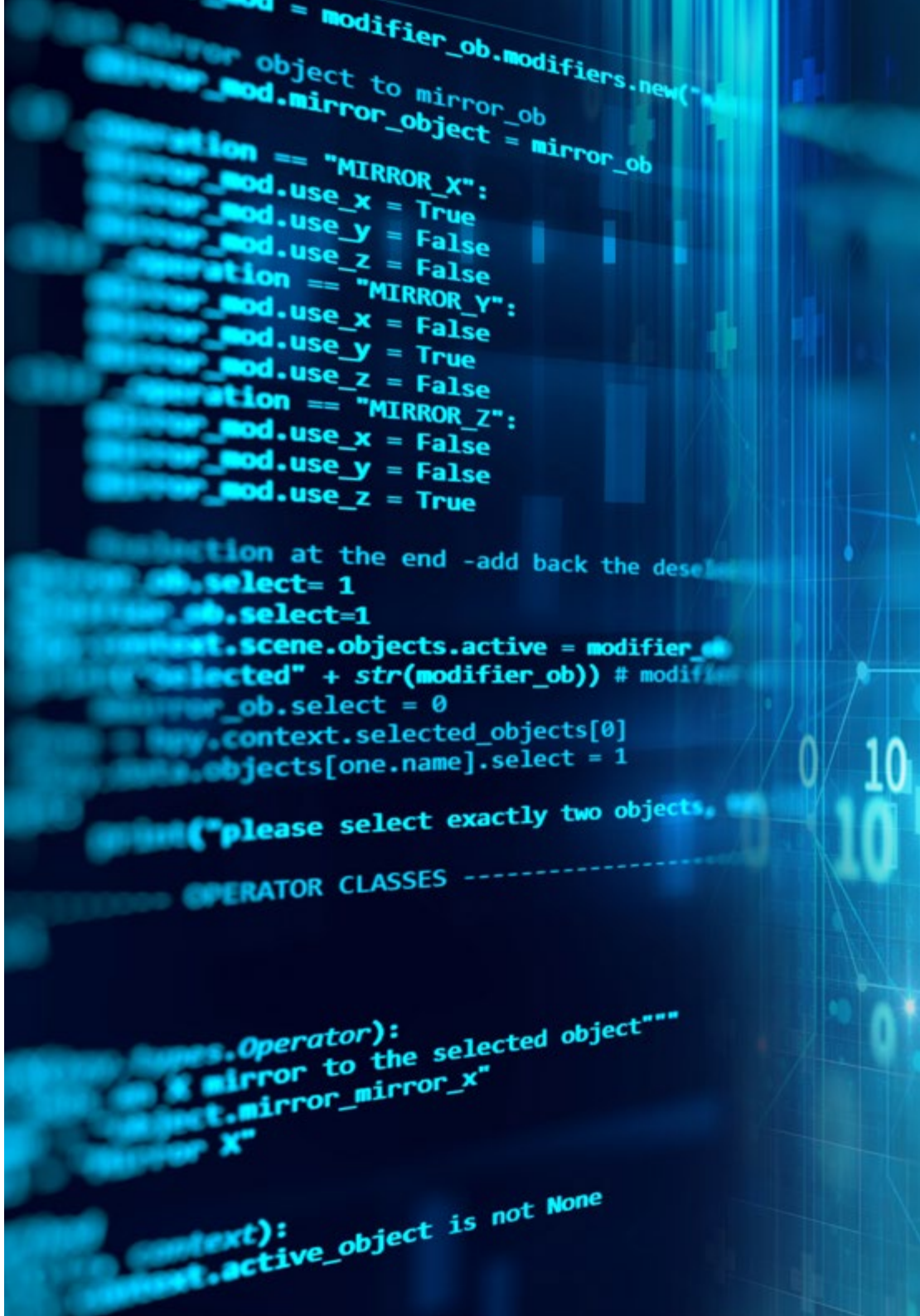
This Postgraduate Diploma in Computer Security for Communications is designed to facilitate professional performance in the field to acquire knowledge of the main developments in the sector.

Our goal is to make you the best professional in your sector. For this, we have the best methodology and content"

General Objective

- Prepare students to be able to develop their work with total security and quality in the field of Communication

Specialize at the one of the world's leading private online universities"



Specific Objectives

Module 1: Communication Systems and Network Security

- Understand and know how to apply the fundamentals of programming in networks, systems and telecommunication services
- Master the rules and regulations of protocols and networks of international standardization organizations
- Understand the concepts of symmetric and asymmetric cryptography, digital signature, hash functions and securitization of each level of a communications architecture
- Understand the different security mechanisms and protocols based on access control: authentication and perimeter defence
- Understand the operation of technical and human threats to the security of telecommunication networks and systems
- Appropriately categorize the different security services for networks and systems, based on the assets they protect
- Apply network and service management systems to telecommunication networks and services for their configuration, operation, supervision and pricing
- Know how to manage the security of telecommunication networks and services by implementing tunneling, firewalls, encryption and authentication protocols, and content protection mechanisms
- Be able to understand and apply the main techniques of secure programming

Module 2: Security Architectures

- Understand the basic principles of computer security
- Master computer security standards and certification processes
- Analyze the organizational and cryptographic foundations on which security technologies are based
- Identify the main threats and vulnerabilities of the different elements involved in ICT, as well as their causes
- Gain an in-depth knowledge of network security tools and their specific functions
- Know how to apply the technologies that make up an ICT security architecture, in its different perspectives

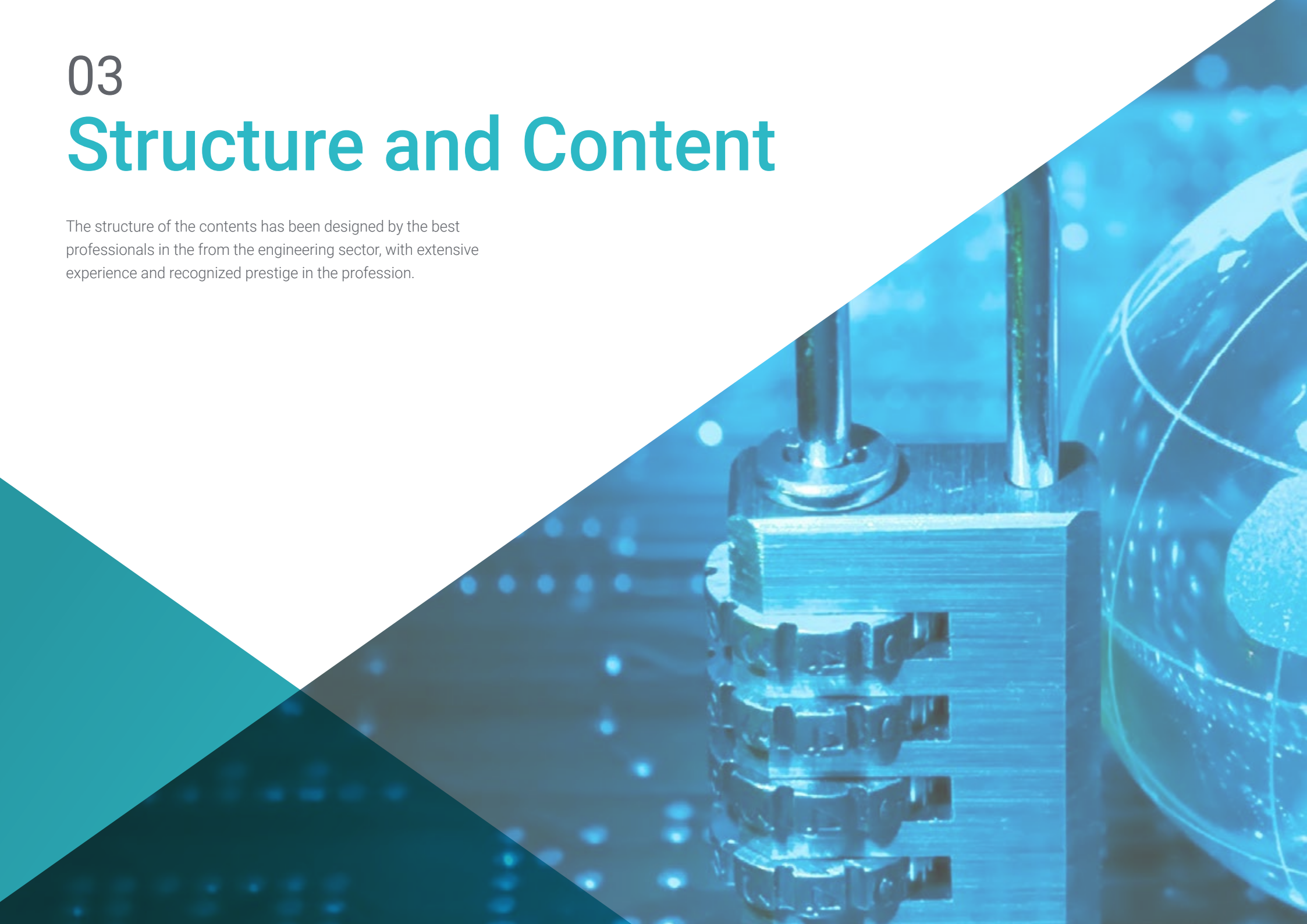
Module 3: Information System Auditing

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

03

Structure and Content

The structure of the contents has been designed by the best professionals in the from the engineering sector, with extensive experience and recognized prestige in the profession.



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

Module 1. Communication Systems and Network Security

1.1. A global Perspective on Security, Cryptography and Classical Cryptanalysis
- 1.1.1. Computer Security: Historical Perspective
- 1.1.2. But What Exactly is Meant by Security?
- 1.1.3. History of Cryptography
- 1.1.4. Substitution Ciphers
- 1.1.5. Case Study: The Enigma Machine

1.2. Symmetric Cryptography
- 1.2.1. Introduction and Basic Terminology
- 1.2.2. Symmetric Encryption
- 1.2.3. Modes of Operation
- 1.2.4. DES
- 1.2.5. The New AES Standard
- 1.2.6. Encryption in Flow
- 1.2.7. Cryptanalysis

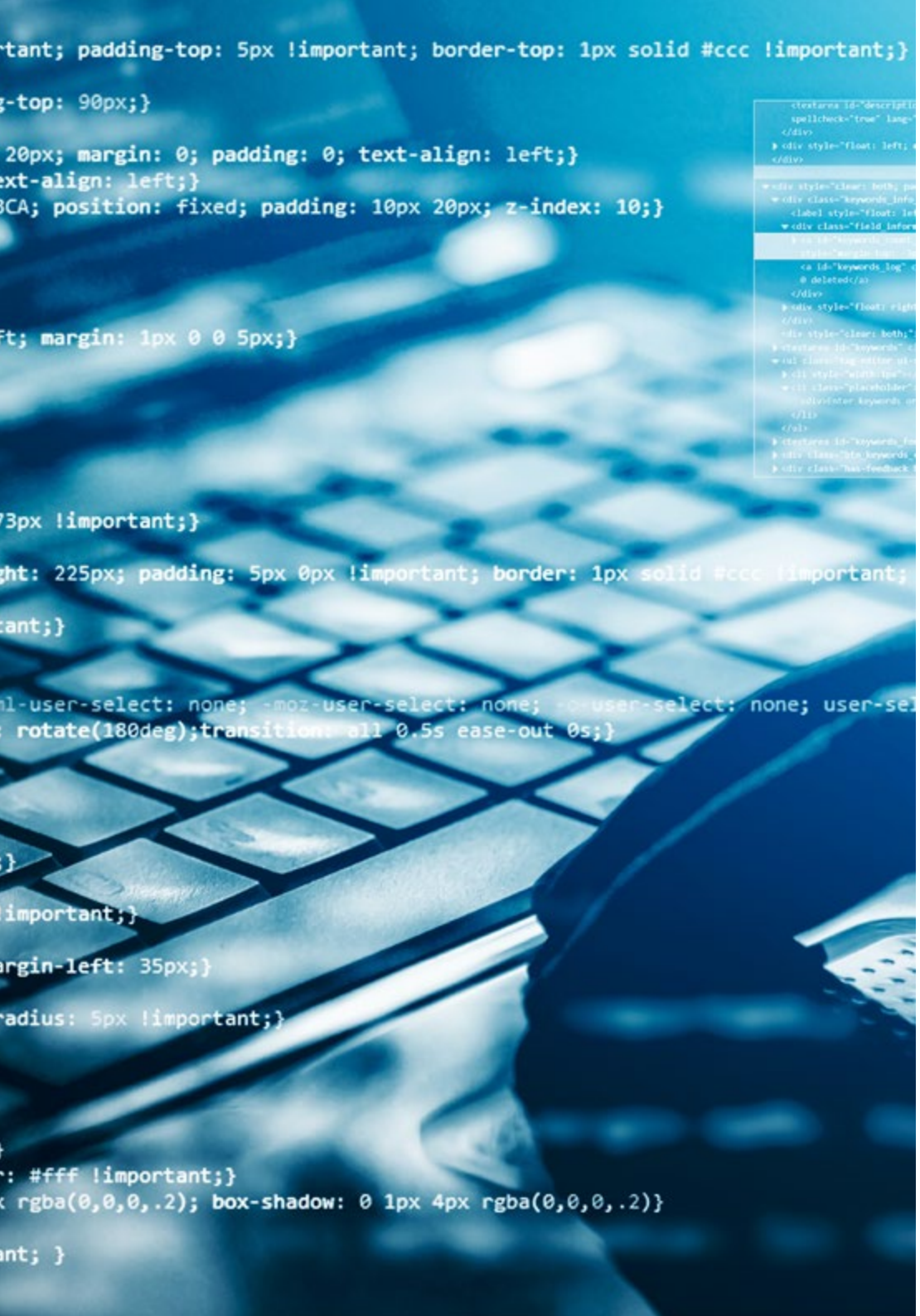
1.3. Asymmetric Cryptography
- 1.3.1. Origins of Public Key Cryptography
- 1.3.2. Basic Concepts and Operation
- 1.3.3. The RSA Algorithm
- 1.3.4. Digital Certificates
- 1.3.5. Key Storage and Management

1.4. Network Attacks
- 1.4.1. Network Threats and Attacks
- 1.4.2. Enumeration
- 1.4.3. Traffic Interception: Sniffers
- 1.4.4. Denial of Service Attacks
- 1.4.5. ARP Poisoning Attacks

1.5. Security Architectures
- 1.5.1. Traditional Security Architectures
- 1.5.2. Secure Socket Layer: SSL
- 1.5.3. SSH Protocol
- 1.5.4. Virtual Private Networks (VPNs)
- 1.5.5. External Storage Unit Protection Mechanisms
- 1.5.6. Hardware Protection Mechanisms

1.6. System Protection Techniques and Secure Code Development
- 1.6.1. Operational Security
- 1.6.2. Resources and Controls
- 1.6.3. Monitoring
- 1.6.4. Intrusion Detection Systems
- 1.6.5. Host IDS
- 1.6.6. Network IDS
- 1.6.7. Signature-Based IDS
- 1.6.8. Lure Systems
- 1.6.9. Basic Security Principles in Code Development
- 1.6.10. Failure Management
- 1.6.11. Public Enemy Number 1: Buffer Overflows
- 1.6.12. Cryptographic Botches

1.7. Botnets and Spam
- 1.7.1. Origin of the Problem
- 1.7.2. Spam Process
- 1.7.3. Sending Spam
- 1.7.4. Refinement of Mailing Lists
- 1.7.5. Protection Techniques
- 1.7.6. Third-Party Antispam Services
- 1.7.7. Study Cases
- 1.7.8. Exotic Spam



1.8. Web Auditing and Attacks
- 1.8.1. Information Gathering
- 1.8.2. Attack Techniques
- 1.8.3. Tools

1.9. Malware and Malicious Code
- 1.9.1. What is Malware?
- 1.9.2. Types of Malware
- 1.9.3. Virus
- 1.9.4. Cryptovirus
- 1.9.5. Worms
- 1.9.6. Adware
- 1.9.7. Spyware
- 1.9.8. Hoaxes
- 1.9.9. Phishing
- 1.9.10. Trojans
- 1.9.11. The Economy of Malware
- 1.9.12. Possible Solutions

1.10. Forensic Analysis
- 1.10.1. Evidence Collection
- 1.10.2. Evidence Analysis
- 1.10.3. Antiforensic Techniques
- 1.10.4. Case Study

Module 2. Security Architectures

2.1. Basic Principles of Computer Security
- 2.1.1. What is Meant by Computer Security?
- 2.1.2. Computer Security Objectives
- 2.1.3. Computer Security Services
- 2.1.4. Lack of Security Consequences
- 2.1.5. "Defence in Security" Principle
- 2.1.6. Security Policies, Plans and Procedures
  - 2.1.6.1. User Account Management
  - 2.1.6.2. User Identification and Authentication
  - 2.1.6.3. Authorization and Logical Access Control
  - 2.1.6.4. Server Monitoring
  - 2.1.6.5. Data Protection
  - 2.1.6.6. Remote Connection Security
- 2.1.7. The Importance of the Human Factor

2.2. Standardization and Certification in Computer Security
- 2.2.1. Safety Standards
  - 2.2.1.1. Purpose of Standards
  - 2.2.1.2. Responsible Bodies
- 2.2.2. U.S. Standards
  - 2.2.2.1. TCSEC
  - 2.2.2.2. Federal Criteria
  - 2.2.2.3. FISCAM
  - 2.2.2.4. NIST SP 800
- 2.2.3. European Standards
  - 2.2.3.1. ITSEC
  - 2.2.3.2. ITSEM
  - 2.2.3.3. European Network and Information Security Agency
- 2.2.4. International Standards
- 2.2.5. Accreditation Process

2.3. Threats to Computer Security: Vulnerabilities and Malware
- 2.3.1. Introduction
- 2.3.2. System Vulnerabilities
  - 2.3.2.1. Network Security Incidents
  - 2.3.2.2. Causes of Computer System Vulnerabilities
  - 2.3.2.3. Vulnerability Types
  - 2.3.2.4. Software Manufacturers' Responsibilities
  - 2.3.2.5. Vulnerability Assessment Tools
- 2.3.3. Computer Security Threats
  - 2.3.3.1. Network Intruder Classification
  - 2.3.3.2. Attacker Motivations
  - 2.3.3.3. Phases of the Attacks
  - 2.3.3.4. Types of Attack
- 2.3.4. Computer Viruses
  - 2.3.4.1. General Characteristics
  - 2.3.4.2. Types of Viruses
  - 2.3.4.3. Damage Caused by Viruses
  - 2.3.4.4. How to Combat Viruses

2.4. Cyberterrorism and Incident Response
- 2.4.1. Introduction
- 2.4.2. The Threat of Cyberterrorism and IT Warfare
- 2.4.3. Consequences of Failures and Attacks on Businesses
- 2.4.4. Computer Network Espionage

2.5. User Identification and Biometric Systems
- 2.5.1. Introduction to User Authentication, Authorization and Registration
- 2.5.2. AAA Safety Model
- 2.5.3. Access Control
- 2.5.4. User Identification
- 2.5.5. Password Verification

2.5.6. Digital Certificate Authentication
2.5.7. Remote User Identification
2.5.8. Single Sign-In
2.5.9. Password Managers
2.5.10. Biometric Systems
2.5.10.1. General Characteristics
2.5.10.2. Types of Biometric Systems
2.5.10.3. System Implementation
2.6. Cryptography and Cryptographic Protocol Fundamentals
2.6.1. Cryptography Introduction
2.6.1.1. Cryptography, Cryptoanalysis and Cryptology
2.6.1.2. Operation of a Cryptographic System
2.6.1.3. History of Cryptographic Systems
2.6.2. Cryptanalysis
2.6.3. Cryptographic Systems Classification
2.6.4. Symmetric and Asymmetric Cryptographic Systems
2.6.5. Authentication with Cryptographic Systems
2.6.6. Electronic Signature
2.6.6.1. What is an Electronic Signature?
2.6.6.2. Electronic Signature Characteristics
2.6.6.3. Certification Authorities
2.6.6.4. Digital Certificates
2.6.6.5. Systems Based on Trusted Third Parties
2.6.6.6. Electronic Signature Use
2.6.6.7. Electronic ID
2.6.6.8. Electronic Invoice
2.7. Network Security Tools
2.7.1. The Internet Connection Security Problem
2.7.2. External Network Security
2.7.3. The Role of Proxy Servers
2.7.4. The Role of Firewalls
2.7.5. Authentication Servers for Remote Connections
2.7.6. Analysis of Activity Records
2.7.7. Intrusion Detection Systems
2.7.8. Decoys
2.8. Wireless and Virtual Private Network Security
2.8.1. Virtual Private Network Security
2.8.1.1 The Role of VPNs
2.8.1.2 VPN Protocols
2.8.2. Traditional Wireless Network Security
2.8.3. Possible Attacks on Wireless Networks
2.8.4. The WEP Protocol
2.8.5. Wireless Network Security Standards
2.8.6. Recommendations to Reinforce Security
2.9. Internet Service Security
2.9.1. Safe Web Browsing
2.9.1.1. The WWW
2.9.1.2. Security Problems on the WWW
2.9.1.3. Safety Recommendations
2.9.1.4. Internet Privacy Protection
2.9.2. Email Security
2.9.2.1. Email Characteristics
2.9.2.2. Email Security Issues
2.9.2.3. Email Security Recommendations
2.9.2.4. Advanced Email Services
2.9.2.5. Use of Email by Employees
2.9.3. SPAM
2.9.4. Phishing
2.10. Content Control
2.10.1. Content Distribution over the Internet
2.10.2. Legal Measures to Combat Illegal Content
2.10.3. Filtering, Cataloging and Content Blocking
2.10.4. Damage to Image and Reputation

Module 3. Information System Auditing

3.1. Information System Auditing. Standards of Good Practice
- 3.1.1. Introduction
- 3.1.2. Auditing and COBIT
- 3.1.3. ICT Management System Auditing
- 3.1.4. Certifications

3.2. Concepts and Methodologies of System Auditing
- 3.2.1. Introduction
- 3.2.2. System Evaluation Methodologies: Quantitative and Qualitative
- 3.2.3. IT Audit Methodologies
- 3.2.4. The Audit Plan

3.3. Audit Contract
- 3.3.1. Legal Nature of the Contract
- 3.3.2. Parts of an Audit Contract
- 3.3.3. Subject Matter of the Audit Contract
- 3.3.4. Audit Report

3.4. Organizational Elements of Audits
- 3.4.1. Introduction
- 3.4.2. Audit Department Mission
- 3.4.3. Audit Planning
- 3.4.4. IS Audit Methodology

3.5. Legal Framework of Audits
- 3.5.1. Personal Data Protection
- 3.5.2. Legal Software Protection
- 3.5.3. Technological Crimes
- 3.5.4. Contracting, Signature and Electronic ID

3.6. Outsourcing Audit and Frameworks
- 3.6.1. Introduction
- 3.6.2. Basic Concepts of Outsourcing
- 3.6.3. IT Outsourcing Audit
- 3.6.4. Leading Frameworks: CMMI, ISO27001, ITIL

3.7. Security Audit
- 3.7.1. Introduction
- 3.7.2. Physical and Logical Security
- 3.7.3. Environment Safety
- 3.7.4. Physical Security Audit Planning and Execution

3.8. Network and Internet Auditing
- 3.8.1. Introduction
- 3.8.2. Network Vulnerabilities
- 3.8.3. Principles and Rights on the Internet
- 3.8.4. Controls and Data Processing

3.9. Computer System and Application Auditing
- 3.9.1. Introduction
- 3.9.2. Reference Models
- 3.9.3. Application Quality Assessment
- 3.9.4. Auditing the Organization and Management of the Development and Maintenance Area

3.10. Personal Data Auditing
- 3.10.1. Introduction
- 3.10.2. Data Protection Laws and Regulations
- 3.10.3. Audit Development
- 3.10.4. Violations and Penalties

This program will allow you to advance in your career comfortably"

04

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

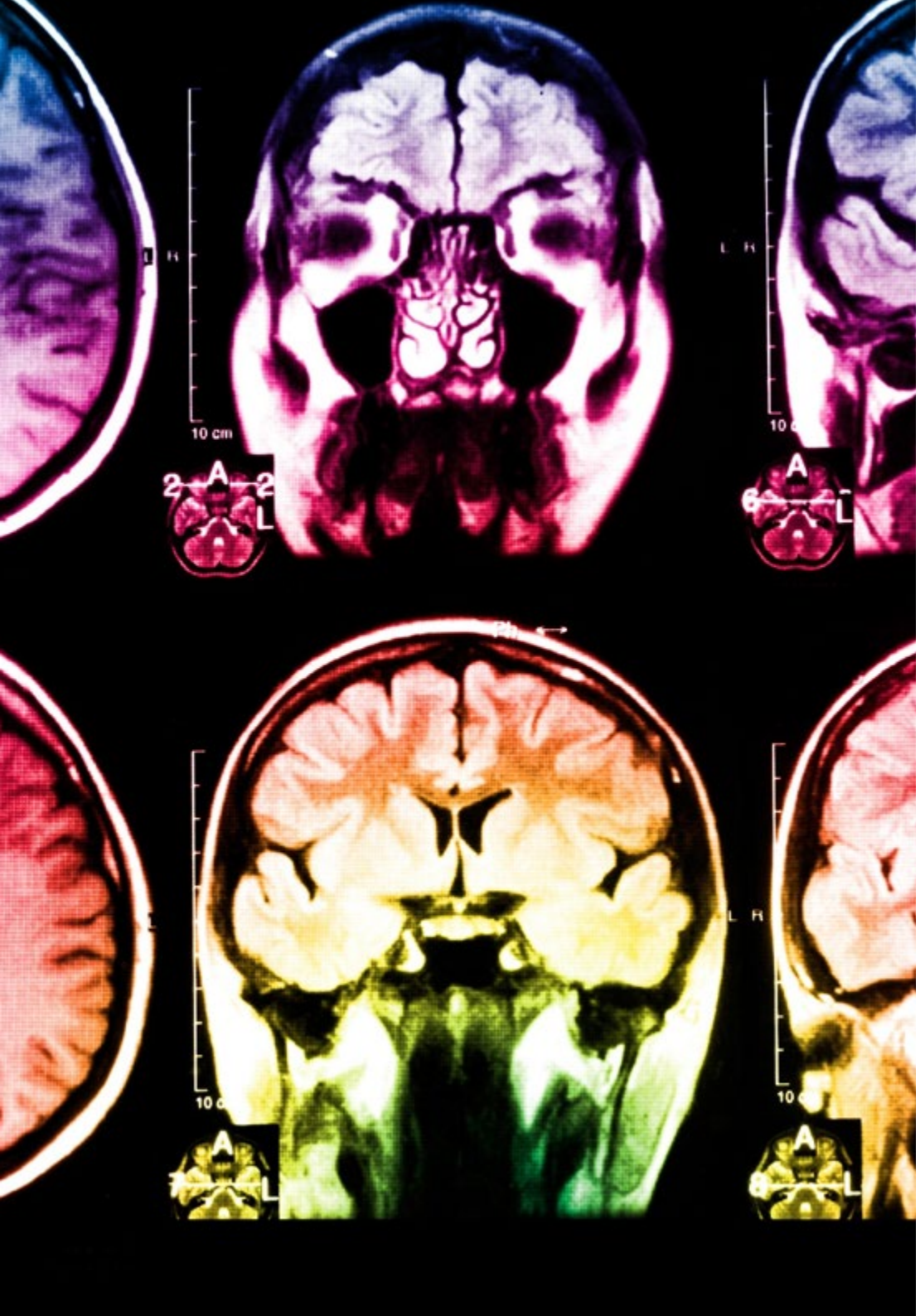
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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.

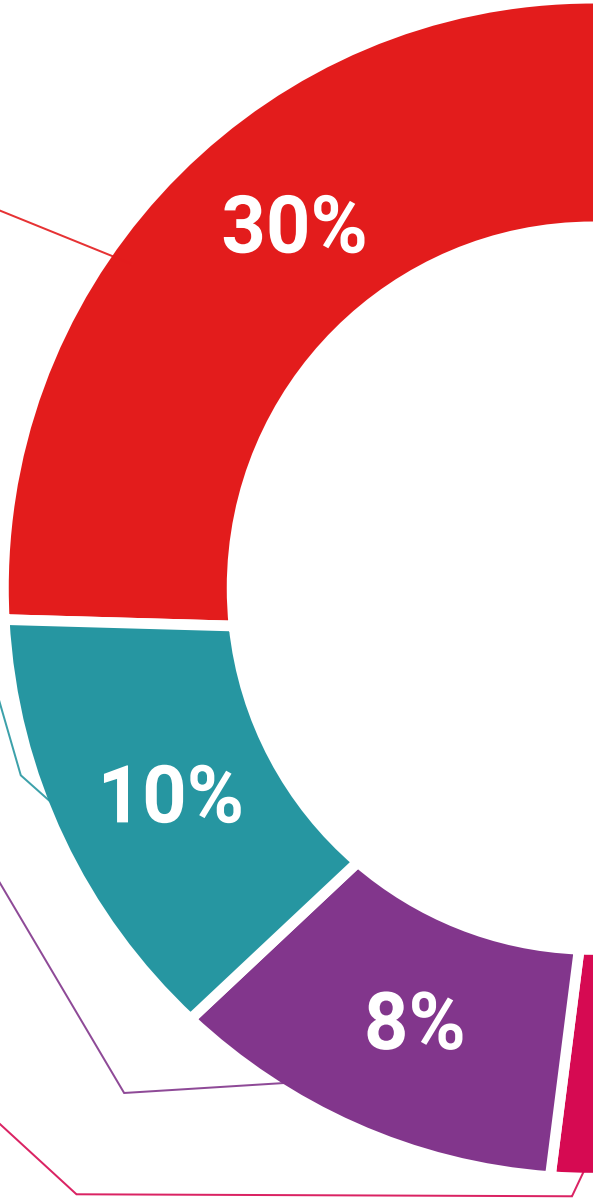
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

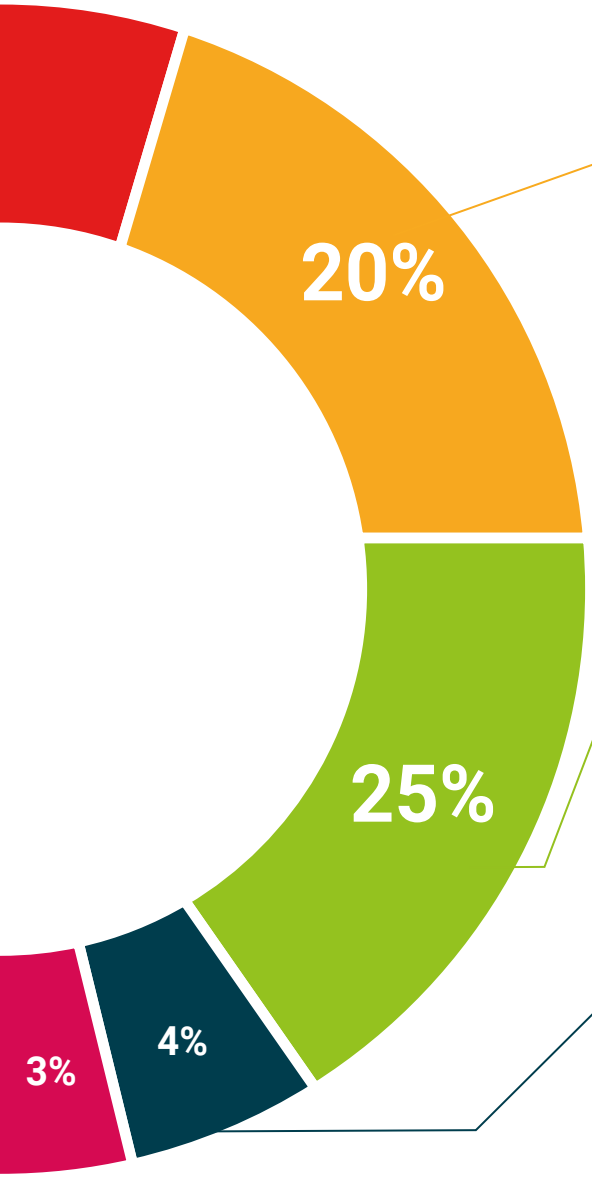
Practising Skills and Abilities

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.

05

Certificate

This Postgraduate Diploma in Computer Security for Communications guarantees students, in addition to the most rigorous and up-to-date education, access to a Postgraduate Diploma issued by TECH Technological University.

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

This **Postgraduate Diploma in Computer Security for Communications** contains the most complete and up-to-date program on the market.

After the student has passed the evaluations, they will receive their corresponding **Postgraduate Diploma** issued by **TECH Technological University** via tracked delivery*.

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

Title: **Postgraduate Diploma in Computer Security for Communications**

Official Nº of Hours: **450 h.**


tech technological university

Awards the following

CERTIFICATE

to

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

For having passed and accredited the following program

POSTGRADUATE DIPLOMA

in

Computer Security for Communications

This is a qualification awarded by this University, equivalent to 450 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

*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

Postgraduate Diploma
Computer Security for Communications

- Modality: **online**
- Duration: **6 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Postgraduate Diploma

Computer Security for Communications

tech technological university