Postgraduate Diploma

Implementation of IT Security Policies

tech technological university

tech technological university

Postgraduate Diploma

Implementation of IT Security Policies

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

Website: www.techtitute.com/in/information-technology/postgraduate-diploma/postgraduate-diploma-implementation-it-security-policies

Index

01

Introduction

Companies focus on the security of computer equipment and the cloud to prevent the theft or loss of valuable data. However, they may neglect other equally important aspects of security in a company, such as the protection of physical and environmental equipment. In this 100% online program, IT professionals will delve into the implementation of systems with the implementation of advanced security methods to maintain access control and authorization to each user. All this, with quality content based on video summaries, specific readings and case studies that will enable specialization in a field of computer science in need of highly qualified professionals.

Learn more about the main identification and authorization technologies and implement more secure IT systems with this Postgraduate Diploma"

Investing in IT security is essential for companies and institutions, however, many are oriented to possible external cyber-attacks and forget to develop a correct physical and environmental security policy to control access to computer systems. In this Postgraduate Diploma, the IT professional will delve into the main aspects to be taken into account to implement this task, which is not an easy one.

The program, taught by professional experts in computer security, goes into how to check the security status of a computer system through CIS controls, analyzing all existing biometric access control systems, their implementation and risk management. In addition, it addresses the implementation of cryptography in communication networks with the most widely used current protocols, both symmetric and asymmetric.

Likewise, authentication and identification will have an important place in this qualification, where IT professionals will develop a PKI, learn about its structure and the use of this infrastructure to protect the network through the use of Digital Certificates.

An excellent opportunity offered by TECH to achieve specialization in a sector that requires professionals with up-to-date and innovative knowledge in the field of computer security. The 100% online teaching model allows to combine learning with other areas of personal life, since students only need a device with internet connection to access all the quality multimedia content made available to them.

This **Postgraduate Diploma in Implementation of IT Security Policies** contains the most complete and up-to-date program on the market. The most important features include:

- The development of practical cases presented by IT security experts
- The graphic, schematic and practical contents of the book provide technical and practical information on those disciplines that are essential for professional practice
- Practical exercises where self-assessment can be used to improve learning
- Its special emphasis on innovative methodologies
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- Content that is accessible from any fixed or portable device with an Internet connection

Update your knowledge in computer security against possible fires and earthquakes. Enroll in this Postgraduate Diploma"

Learn about the latest developments in fingerprint, facial, iris and retina recognition as computer security measures"

Delve into secure communication protocols and prevent high-value data theft. Enroll now.

Master the Secure Shell tool and avoids leaks of company information.

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

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 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

Upon completion of this Postgraduate Diploma, IT professionals will be able to implement security policies in software and hardware or examine biometrics and biometric systems. In addition, students will be able to apply various network encryption techniques such as TLS, VPN or SSH and control the best system monitoring tools currently available on the market. The wide range of resources and case studies will provide a learning experience very close to the reality they will have to face in their work environment.

Achieve a specialization in the field of computer security thanks to this Postgraduate Diploma. Enroll now"

General Objectives

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

Specific Objectives

Module 1. Practical Implementation of Software and Hardware Security Policies

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

Module 2. Implementation of Physical and Environmental Safety Policies in the Company

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

Module 3. Secure Communications Policies in the Company

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

Module 4. Information Systems Security Policy Monitoring Tools

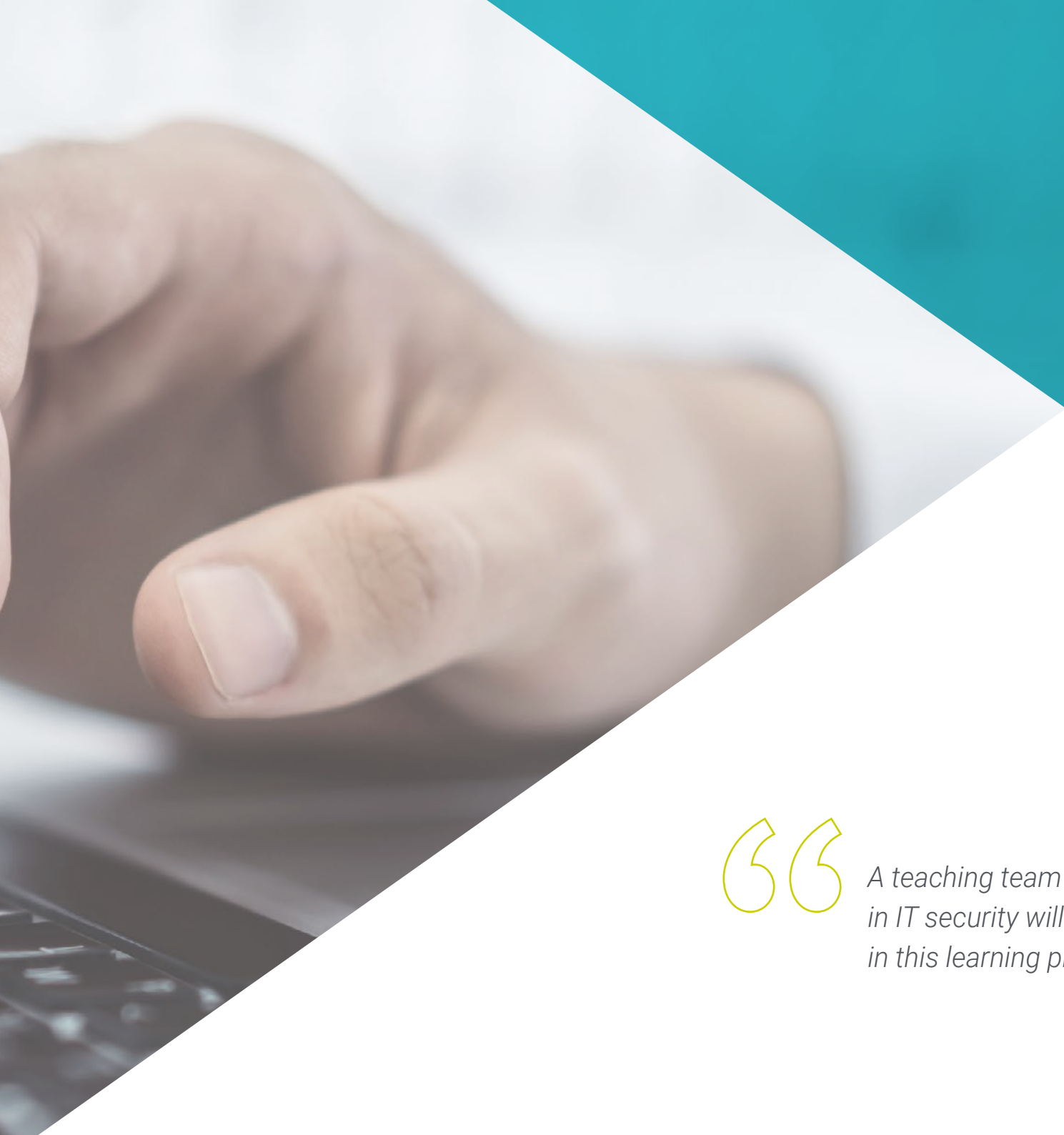
- Develop the concept of monitoring and implementation of metrics
- Configure Audit Trails on Systems and Monitor Networks
- Compile the best system monitoring tools currently available on the market

This program will provide you with the tools you need to examine biometrics and biometric systems in a company"

03

Course Management

This Postgraduate Diploma has a faculty with experience in web management and network security and service systems. Their extensive knowledge in this field of computer science has been key to their collaboration. In this way, students have the guarantee of being guided, during the six months of this course, by teachers who have the necessary academic education and daily practice in the application of tools, systems and security protocols in companies. All this, with the ultimate goal of providing quality learning, which allows the IT professional to advance in this area.



A teaching team with extensive experience in IT security will guarantee your success in this learning process"

Management

Ms. Fernández Sapena, Sonia

- Trainer in Computer Security and Ethical Hacking at the National Reference Center of Getafe in Computer Science and Telecommunications in Madrid
- Certified E-Council instructor
- Trainer in the following certifications: EXIN Ethical Hacking Foundation and EXIN Cyber & IT Security Foundation. Madrid
- Accredited expert trainer by the CAM of the following certificates of professionalism: Computer Security (IFCT0190), Voice and Data Network Management (IFCM0310), Departmental Network Administration (IFCT0410), Alarm Management in Telecommunications Networks (IFCM0410), Voice and Data Network Operator (IFCM0110), and Internet Services Administration (IFCT0509)
- External collaborator CSO/SSA (Chief Security Officer/Senior Security Architect) at the University of the Balearic Islands
- Degree in Computer Engineering from the University of Alcalá de Henares, Madrid
- Master in DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Professors

Ms. López García, Rosa María

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

Mr. Oropesiano Carrizosa, Francisco

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

04

Structure and Content

The faculty of this Postgraduate Diploma has developed a syllabus that integrates all the knowledge on the practical implementation of security policies in software and hardware, dedicating one of its modules to address in depth biometric systems and protection against environmental factors such as fire or earthquakes. In addition, this curriculum pays special attention to system monitoring tools and cryptographic algorithms. The Relearning system, based on the reiteration of content, and the eminently practical cases will allow students to acquire solid learning in a simple way.

Adapt the teaching load of this teaching is to your needs. Access content anytime, anywhere. Click and enroll"

Module 1. Practical Implementation of Software and Hardware Security Policies

1.1. Practical Implementation of Software and Hardware Security Policies
- 1.1.1. Implementation of Identification and Authorization
- 1.1.2. Implementation of Identification Techniques
- 1.1.3. Technical Authorization Measures

1.2. Identification and Authorization Technologies
- 1.2.1. Identifier and OTP
- 1.2.2. USB Token or PKI Smart Card
- 1.2.3. The "Confidential Defense" Key
- 1.2.4. Active RFID

1.3. Software and Systems Access Security Policies
- 1.3.1. Implementation of Access Control Policies
- 1.3.2. Implementation of Communications Access Policies
- 1.3.3. Types of Security Tools for Access Control

1.4. User Access Management
- 1.4.1. Access Rights Management
- 1.4.2. Segregation of Roles and Access Functions
- 1.4.3. Implementation of Access Rights in Systems

1.5. Access Control to Systems and Applications
- 1.5.1. Minimum Access Rule
- 1.5.2. Secure Logon Technologies
- 1.5.3. Password Security Policies

1.6. Identification Systems Technologies
- 1.6.1. Active Directory
- 1.6.2. OTP
- 1.6.3. PAP, CHAP
- 1.6.4. KERBEROS, DIAMETER, NTLM

1.7. CIS Controls for Systems Hardening
- 1.7.1. Basic CIS Controls
- 1.7.2. Fundamental CIS Controls
- 1.7.3. Organizational CIS Controls

1.8. Operational Safety
- 1.8.1. Protection Against Malicious Code
- 1.8.2. Backup Copies
- 1.8.3. Activity Log and Supervision

1.9. Management of Technical Vulnerabilities
- 1.9.1. Technical Vulnerabilities
- 1.9.2. Technical Vulnerability Management
- 1.9.3. Restrictions on Software Installation

1.10. Implementation of Security Policy Practices
- 1.10.1. Logical Vulnerabilities
- 1.10.2. Implementation of Defense Policies

Module 2. Implementation of Physical and Environmental Safety Policies in the Company

2.1. Security Areas
- 2.1.1. Physical Security Perimeter
- 2.1.2. Working in Safe Areas
- 2.1.3. Security of Offices, Offices and Resources

2.2. Physical Input Controls
- 2.2.1. Physical Access Control Policies
- 2.2.2. Physical Input Control Systems

2.3. Physical Access Vulnerabilities
- 2.3.1. Main Physical Vulnerabilities
- 2.3.2. Implementation of Safeguards Measures

2.4. Physiological Biometric Systems
- 2.4.1. Fingerprint
- 2.4.2. Facial Recognition
- 2.4.3. Iris and Retinal Recognition
- 2.4.4. Other Physiological Biometric Systems

2.5. Biometric Behavioral Systems
- 2.5.1. Signature Recognition
- 2.5.2. Writer Recognition
- 2.5.3. Voice Recognition
- 2.5.4. Other Biometric Behavioral Systems

2.6. Biometrics Risk Management
- 2.6.1. Implementation of Biometric Systems
- 2.6.2. Vulnerabilities of Biometric Systems

2.7. Implementation of Policies in Hosts
- 2.7.1. Installation of Supply and Security Cabling
- 2.7.2. Equipment Location
- 2.7.3. Exit of the Equipment Outside the Premises
- 2.7.4. Unattended Computer Equipment and Clear Post Policy

2.8. Environmental Protection
- 2.8.1. Fire Protection Systems
- 2.8.2. Earthquake Protection Systems
- 2.8.3. Earthquake Protection Systems

2.9. Data Processing Center Security
- 2.9.1. Security Doors
- 2.9.2. Video Surveillance Systems (CCTV)
- 2.9.3. Safety Control

2.10. International Physical Security Standards
- 2.10.1. IEC 62443-2-1 (European)
- 2.10.2. NERC CIP-005-5 (U.S. USA
- 2.10.3. NERC CIP-014-2 (U.S. USA

Module 3. Secure Communications Policies in the Company

3.1. Network Security Management
- 3.1.1. Network Control and Monitoring
- 3.1.2. Segregation of Networks
- 3.1.3. Network Security Systems

3.2. Secure Communication Protocols
- 3.2.1. TCP/IP Model
- 3.2.2. IPSEC Protocol
- 3.2.3. TLS Protocol

3.3. Protocol TLS 1.3
- 3.3.1. Phases of a TLS process 1.3
- 3.3.2. Handshake Protocol
- 3.3.3. Registration Protocol
- 3.3.4. Differences with TLS 1.2

3.4. Cryptographic Algorithms
- 3.4.1. Cryptographic Algorithms Used in Communications
- 3.4.2. Cipher-Suites
- 3.4.3. Cryptographic Algorithms allowed for TLS 1.3

3.5. Digest Functions
- 3.5.1. MD6
- 3.5.2. SHA

3.6. PKI. Public Key Infrastructure
- 3.6.1. PKI and its Entities
- 3.6.2. Digital Certificate
- 3.6.3. Types of Digital Certificates

3.7. Tunnel and Transport Communications
- 3.7.1. Tunnel Communications
- 3.7.2. Transport Communications
- 3.7.3. Encrypted Tunnel Implementation

3.8. SSH. Secure Shell
- 3.8.1. SSH. Safe Capsule
- 3.8.2. SSH Functions
- 3.8.3. SSH Tools

3.9. Audit of Cryptographic Systems
- 3.9.1. Integration Test
- 3.9.2. Cryptographic System Testing

3.10. Cryptographic Systems
- 3.10.1. Cryptographic Systems Vulnerabilities
- 3.10.2. Cryptographic Safeguards

Module 4. Information Systems Security Policy Monitoring Tools

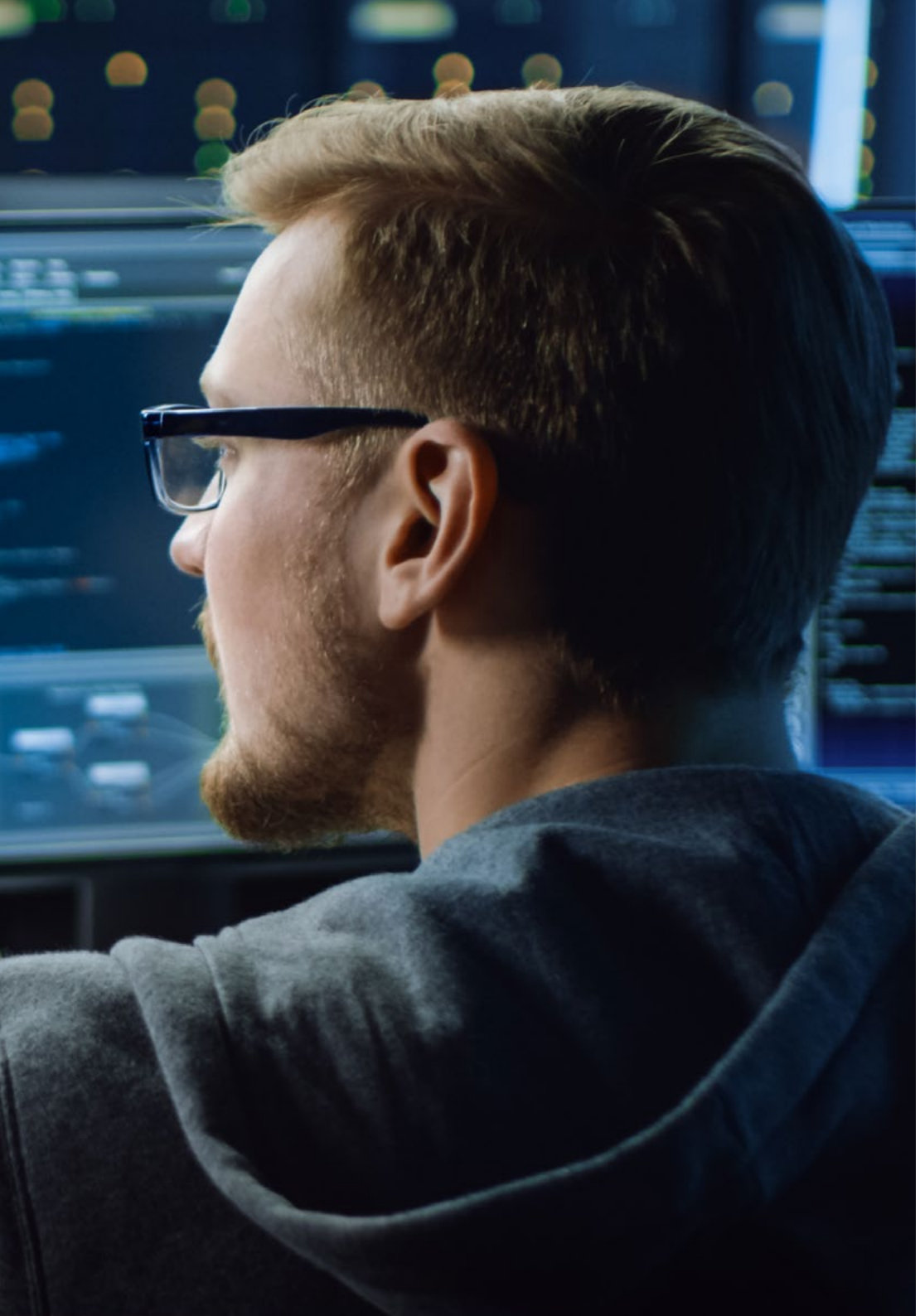
4.1. Information Systems Monitoring Policies
- 4.1.1. System Monitoring
- 4.1.2. Metrics
- 4.1.3. Types of Metrics

4.2. Systems Auditing and Logging
- 4.2.1. Windows Audit and Logging
- 4.2.2. Linux Audit and Logging

4.3. SNMP Protocol. Simple Network Management Protocol
- 4.3.1. SNMP Protocol
- 4.3.2. SNMP Functions
- 4.3.3. SNMP Tools

4.4. Network Monitoring
- 4.4.1. Network Monitoring in Control Systems
- 4.4.2. Monitoring Tools for Control Systems

4.5. Nagios. Network Monitoring System
- 4.5.1. Nagios
- 4.5.2. Operation of Nagios
- 4.5.3. Nagios Installation



4.6. Zabbix. Network Monitoring System
- 4.6.1. Zabbix
- 4.6.2. How Zabbix Works
- 4.6.3. Zabbix Installation

4.7. Cacti. Network Monitoring System
- 4.7.1. Cacti
- 4.7.2. How Cacti Works
- 4.7.3. Installation of Cacti

4.8. Pandora. Network Monitoring System
- 4.8.1. Pandora
- 4.8.2. Operation of Pandora
- 4.8.3. Pandora Installation

4.9. SolarWinds. Network Monitoring System
- 4.9.1. SolarWinds
- 4.9.2. Operation of SolarWinds
- 4.9.3. Installation of SolarWinds

4.10. Monitoring Regulations
- 4.10.1. CIS Controls Over Audit and Record Keeping
- 4.10.2. NIST 800-123 (U.S.) USA

Interactive summaries and case studies developed by the teaching team will provide you with the content you need to advance your career"

05

Methodology

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

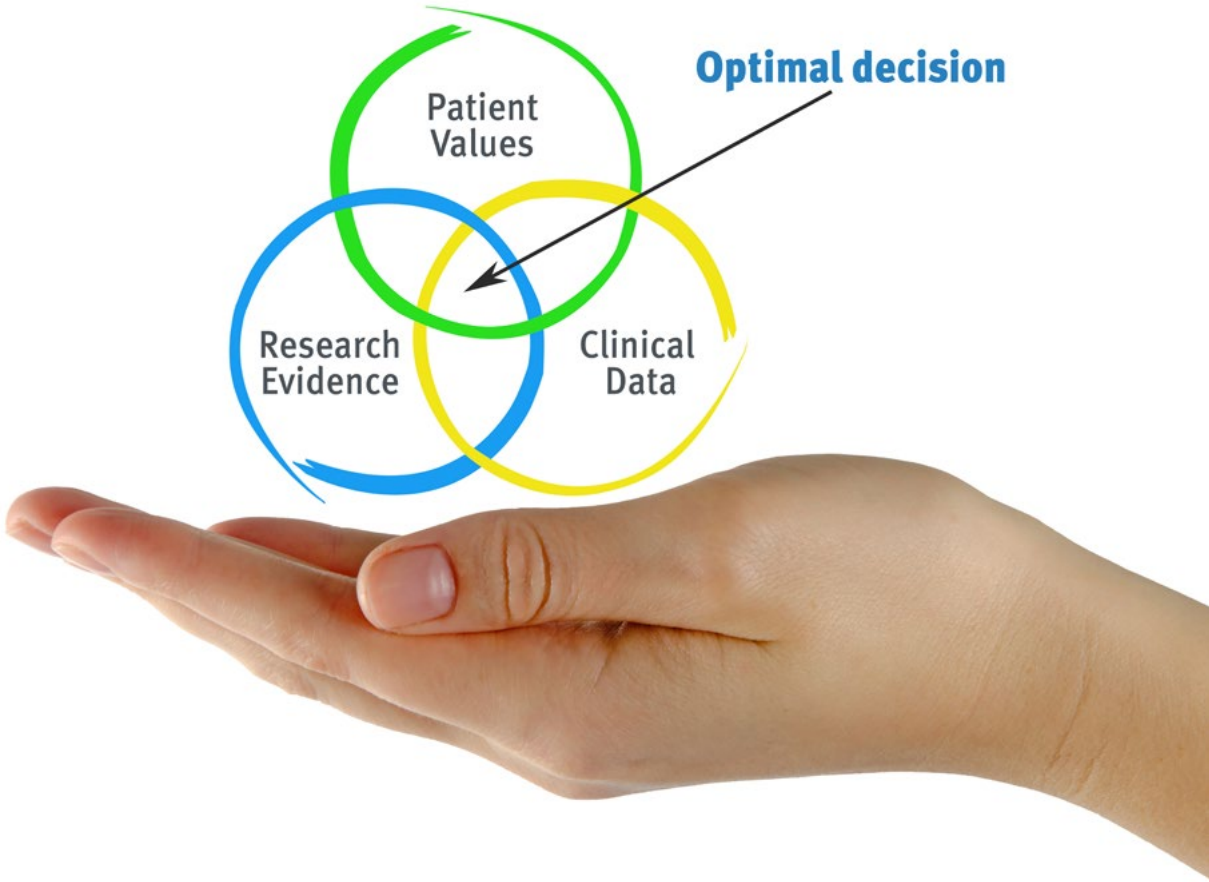
This teaching system is used, for example, in the most prestigious medical schools in the world, and major publications such as the **New England Journal of Medicine** have considered it to be one of the most effective.

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

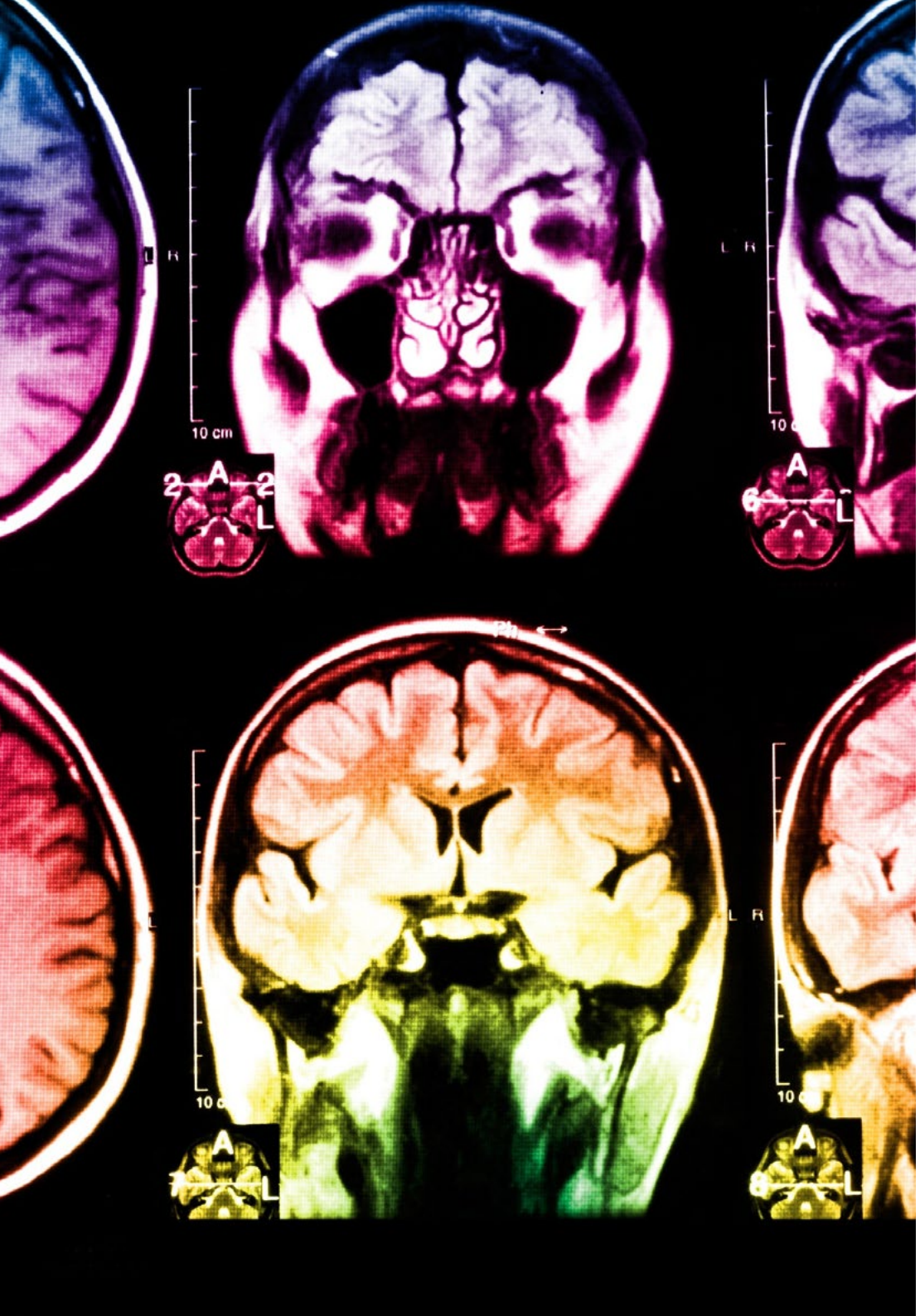
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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.

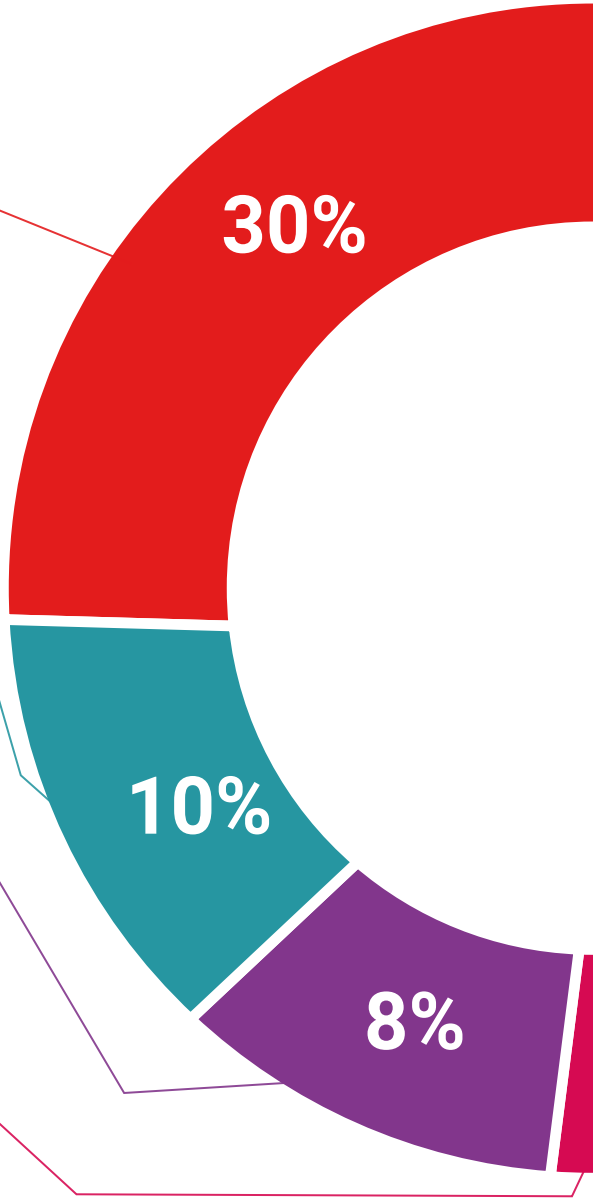
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

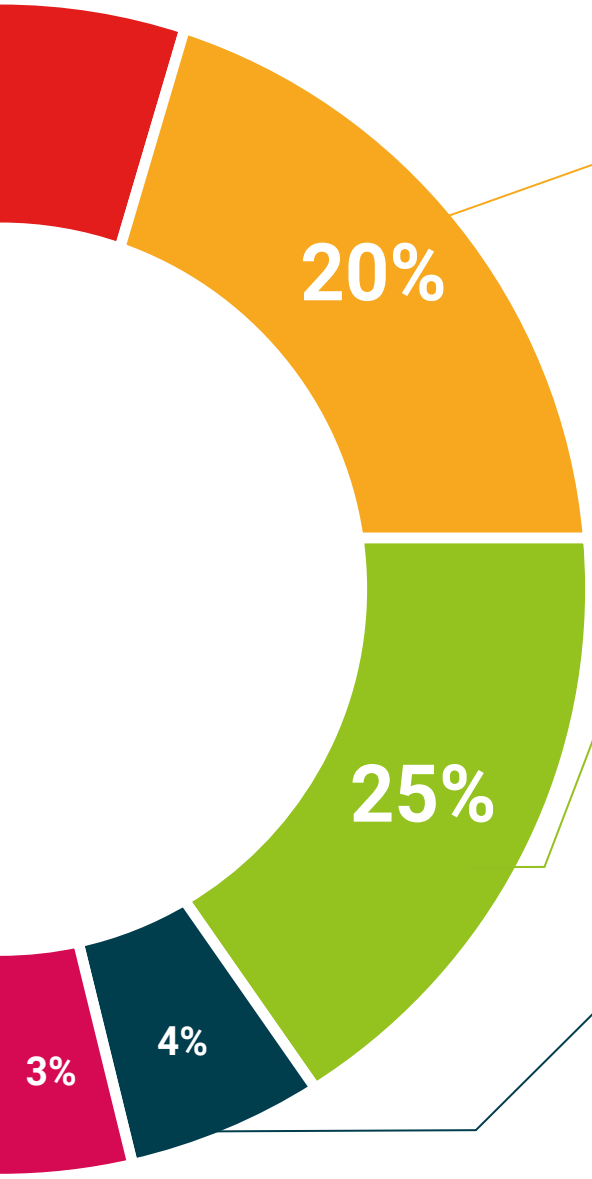
Practising Skills and Abilities

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 Postgraduate Diploma in Implementation of IT Security Policies 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"

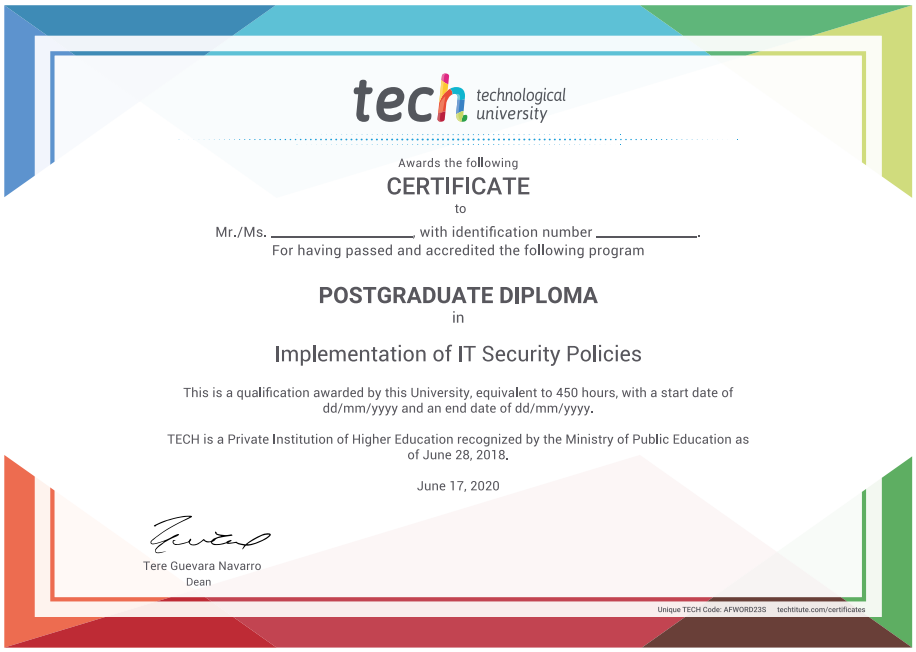
This **Postgraduate Diploma in Implementation of IT Security Policies** contains the most complete and up-to-date program on the market.

After the student has passed the assessments, 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 Implementation of IT Security Policies**

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

Implementation of IT Security Policies

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

Implementation of IT Security Policies

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

Postgraduate Diploma

Implementation of IT Security Policies

tech technological university