Postgraduate Diploma
Defensive Cybersecurity

tech technological university

tech technological university

Postgraduate Diploma
Defensive Cybersecurity

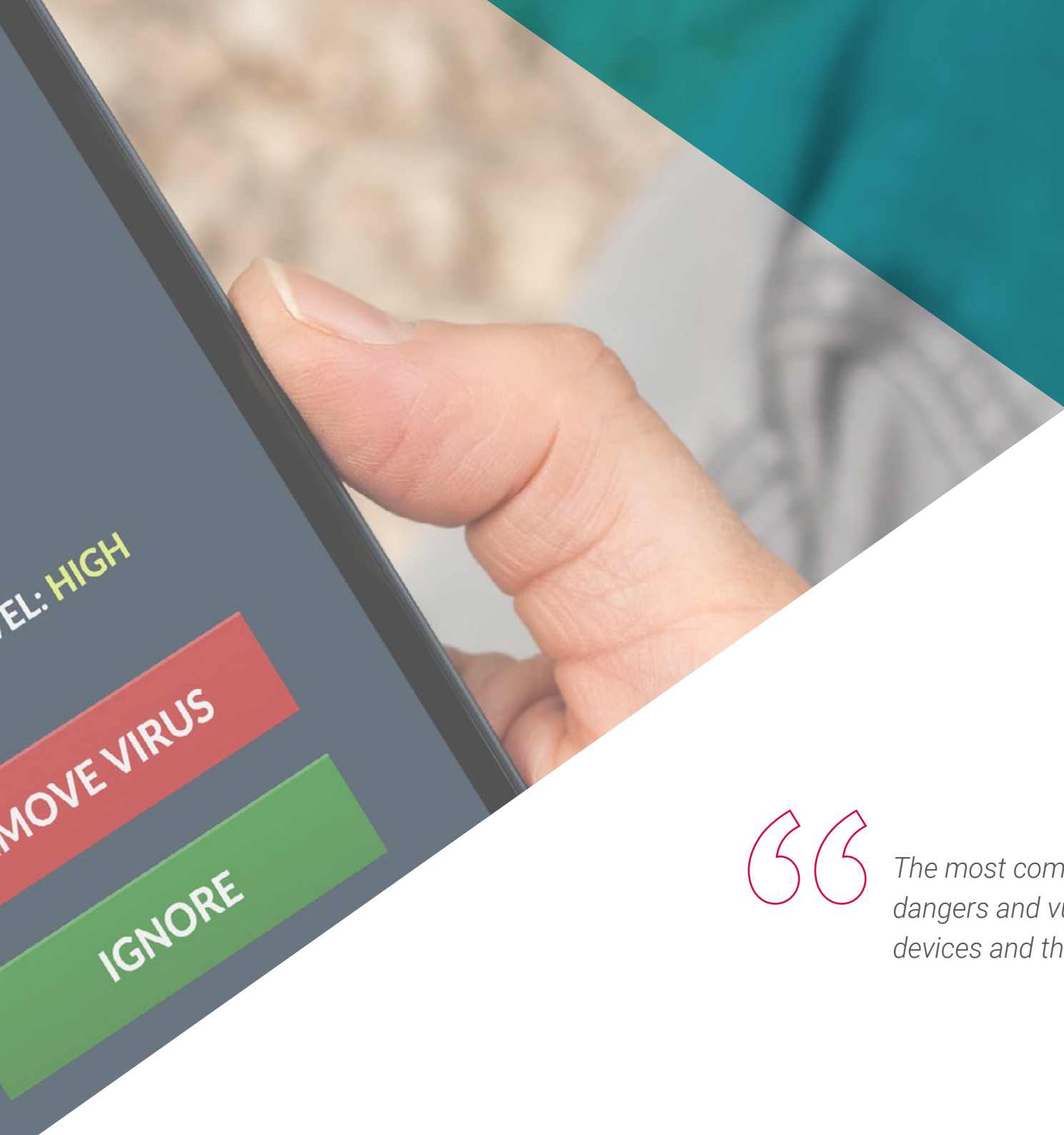
Course Modality: **Online**
Duration: **6 months.**
Certificate: **TECH Technological University**
Official Nº of Hours: **600 h.**
Website: www.techtitute.com/pk/information-technology/postgraduate-diploma/postgraduate-diploma-defensive-cybersecurity

Index

01

Introduction

At the present time, in which daily life is directly linked to the use of mobile devices, knowing the possible forms of vulnerability that accompany their use is an absolute necessity for professionals in the field of technology. With the sophistication of the various models, an unusual work capacity has been achieved, which has turned them into highly sophisticated tools that even access sensitive personal and corporate data. This Postgraduate Diploma will deeply study all aspects in which cyber-attacks can occur by developing the most innovative and effective defensive cybersecurity strategies of the moment. A highly educational course that will allow you to act as a specialist in this field.



The most complete tour through the dangers and vulnerabilities of mobile devices and their cyber protection"

Home and business security needs to be structured in layers, it is like a chain and will only be as strong as the weakest link in the chain. This Postgraduate Diploma presents the main threats to users' computers and servers so that we are able to take the appropriate measures and be alert to any situation.

The more new functionalities there are and the more we communicate with each other, the more our attack surface increases. In other words, the possibilities and ways for cybercriminals to achieve their goals are growing. That is why security defense and monitoring systems must evolve as well. Because in a world where teleworking and Cloud services are becoming more and more common, a traditional perimeter firewall is not enough. For this reason, this Postgraduate Diploma will also address the importance of designing a multi-layer defence, also known as "Defence in depth" covering all aspects of a corporate network where some of the concepts and systems that will be discussed can also be used and applied in a domestic environment.

There is no such thing as 100% security, but if you know the types of attacks you face, the risks you are exposed to and have the information you need to deal with them, you have taken an important step and added another layer of security to your information.

This **Postgraduate Diploma in Defensive Cybersecurity** contains the most complete and up-to-date program on the market. The most important features include:

- Practical case studies presented by experts
- The graphic, schematic, and practical contents with which they are created, provide scientific and practical information on the disciplines that are essential for professional practice
- Practical exercises where the self-assessment process can be carried out to improve learning
- Its special emphasis on innovative methodologies in Advanced Practice Nursing
- 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.

Start acting with the broadest knowledge of the types of risks currently existing and the means of defence applicable in each case"

A complete tour that will allow you to know what they are and how current cyber threats work as a basis for developing defensive strategies"

With a totally practice-focused approach, this Postgraduate Diploma will boost your skills to the level of a specialist.

A highly educational process, created to be affordable and flexible, with the most interesting methodology of online teaching.

The program's teaching staff includes professionals from the sector who contribute their work experience to this 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 specialization 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. This will be done with the help of an innovative system of interactive videos made by renowned experts.

02

Objectives

This Postgraduate Diploma will allow you to advance exponentially in your capacity to intervene in this field. With realistic and highly relevant objectives, this course of study is designed to progressively lead students to the acquisition of the theoretical and practical knowledge necessary to intervene with excellence and to develop transversal competencies that will allow them to face complex situations by developing appropriate and precise responses.

A complete update on all aspects in which defensive cybersecurity has developed in recent times"

General Objectives

- Assessing the security of user equipment and servers
- Examine potential threats based on the usage environment
- Analyze solutions for each threat
- Develop appropriate usage policies
- Analyze the general framework, the importance of multilayer defense and monitoring systems
- Examine the most important threat detection and prevention systems.
- Develop firewall solutions on hotst Linux and Cloud providers
- Evaluate new threat detection systems, as well as their evolution with respect to more traditional solutions
- Generate complete intelligent solutions to automate incident behaviors
- Analyze the main current mobile platforms, their characteristics and use
- Examine existing vulnerabilities and threats, as well as the main attack vectors
- Assess the risks associated with vulnerabilities both outside and inside the company
- Determine tools and best practice guidelines for securing mobile devices
- Analyze the IoT in different areas today
- Examining the evolution and impact of IoT
- Determine the parts of an IoT project
- Identify, analyze and assess security risks of the IoT project parts

Specific Objectives

Module 1. Host Security

- Specify the Backup policies for personal and professional data
- Assess the different tools to provide solutions to specific security problems
- Establish mechanisms to have an up-to-date system
- Scan equipment for Intruders
- Determine system access rules
- Screen and classify mails to avoid frauds
- Generate lists of permitted software

Module 2. Network Security (Perimeter)

- Analyze current network architectures to identify the perimeter to protect
- Develop specific firewall and Linux configurations to mitigate the most common attacks
- Compile the most commonly used solutions such as Snort and Suricata, as well as their configuration
- Examine the different additional layers provided by next-generation firewalls and networking capabilities in Cloud environments
- Determine the tools for network protection and demonstrate why they are fundamental to a multilayer defence

Module 3. Smartphone Security

- Examine the various attack vectors to avoid becoming an easy target
- Determine the main attacks and types of Malware to which mobile device users are exposed
- Analyze the most current devices to establish greater security in the configuration
- Specify the main steps to perform a penetration test on both iOS and Android platforms
- Develop specialized knowledge about the different protection and security tools
- Establish best practices in programming for mobile devices

Module 4. IoT Security

- Analyze the main IoT architectures
- Examine connectivity technologies
- Develop the main application protocols
- Specify the different types of existing devices
- Assessing risk levels and known vulnerabilities
- Develop safe use policies
- Establishing appropriate conditions of use for these devices

03

Course Management

The teachers who teach this program have been selected for their exceptional competence in this field. They combine technical and practical experience with teaching experience, offering students first-class support in achieving their goals. Through them, the program offers the most direct and immediate vision of the real characteristics of the intervention in this field, achieving a contextual vision of maximum interest.

The direct vision of a profession in constant movement, through expert professionals who will give you the most realistic view of this job"

Management

Ms. Fernández Sapena, Sonia

- Computer Security and Ethical Hacking Trainer. Getafe National Reference Center for Informatics and Telecommunications. Madrid
- Certified E-Council instructor. Madrid
- Trainer in the following certifications: EXIN Ethical Hacking Foundation y 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)
- Colaboradora externa CSO/SSA (Chief Security Officer/Senior Security Architect). University of the Balearic Islands
- Computer Engineer. Alcalá de Henares University. Madrid
- Master in DevOps: Docker and Kubernetes. Cas Training. Madrid
- Microsoft Azure Security Technologies. E-Council. Madrid

Professors

Mr. Catalá Barba, José Francisco

- Intermediate Command in MINISDEF. Different tasks and responsibilities within GOE III, such as administration and incident management of the internal network, development of customized programs for different areas, training courses for network users and group personnel in general
- Electronic technician in Ford Factory located in Almusafes, Valencia, robot programming, PLC's, repair and maintenance
- Electronic Technician
- Developer of applications for mobile devices

Mr. Jiménez Ramos, Álvaro

- Senior Security Analyst at The Workshop
- Cybersecurity Analyst L1 at Axians
- Cybersecurity Analyst L2 at Axians
- Cybersecurity analyst at SACYR S.A
- Degree in Telematics Engineering from the Polytechnic University of Madrid
- Professional Master's Degree in Cybersecurity and Ethical Hacking by CICE
- Advanced Course in Cybersecurity by Deusto Training

Ms. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applications Developer at B60. UK
- Analyst Programmer for the management, coordination and documentation of virtualized environment of security alarms at client's site
- Analyst Programmer of Java applications for ATMs at client's site
- Software Development Professional for signature validation and document management application at customer's site
- Systems Technician for the migration of equipment and for the management, maintenance and training of PDA mobile devices at the customer's site
- Technical Engineering from Computer Systems. Open University of Catalonia
- Professional Master's Degree in Computer Security and Ethical Hacking Official EC-Council and CompTIA by the Professional School of New Technologies CICE

Mr. Peralta Alonso, Jon

- Attorney / DPO Altia Consultores S.A
- Lecturer in Professional Master's Degree in Personal Data Protection, Cybersecurity and ICT Law. Public University of the Basque Country (UPV-EHU)
- Lawyer / Legal advisor. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L
- Legal Advisor / Intern. Professional office: Oscar Padura
- Law Degree. Public University of the Basque Country
- Professional Master's Degree in Data Protection Officer. Escuela innovadora EIS
- Professional Master's Degree in Law. Public University of the Basque Country
- Professional Master's Degree in Civil Litigation Practice. International University Isabel I of Castile

04

Structure and Content

The agenda of this program covers each and every one of the areas of knowledge that the professional involved in cybersecurity must know in the context of defensive measures. To this end, it has been structured with a view to the efficient acquisition of summative knowledge, which will favor the absorption of learning and consolidate what has been studied, providing students with the capacity to intervene as quickly as possible. A high-intensity, high-quality course created to educate the best in the industry.

All aspects that defensive cybersecurity analysis and intervention requires, developed in a structured way in an efficiency-focused study approach"

Module 1. Host Security

1.1. Backup Copies
- 1.1.1. Backup Strategies
- 1.1.2. Tools for Windows
- 1.1.3. Tools for Linux
- 1.1.4. Tools for MacOS

1.2. User Antivirus
- 1.2.1. Types of Antivirus
- 1.2.2. Antivirus for Windows
- 1.2.3. Antivirus for Linux
- 1.2.4. Antivirus for MacOS
- 1.2.5. Antivirus for Smartphones

1.3. Intrusion Detectors - HIDS
- 1.3.1. Intrusion Detection Methods
- 1.3.2. Sagan
- 1.3.3. Aide
- 1.3.4. Rkhunter

1.4. Local Firewall
- 1.4.1. Firewalls for Windows
- 1.4.2. Firewalls for Linux
- 1.4.3. Firewalls for MacOS

1.5. Password Managers
- 1.5.1. Password
- 1.5.2. LastPass
- 1.5.3. KeePass
- 1.5.4. Sticky Password
- 1.5.5. RoboForm

1.6. Phishing Detectors
- 1.6.1. Manual Detection of Phishing
- 1.6.2. AntiphishingTools

1.7. Spyware
- 1.7.1. Avoidance Mechanisms
- 1.7.2. Antispyware Tools

1.8. Trackers
- 1.8.1. Measures to Protect the System
- 1.8.2. Anti-tracking Tools

1.9. EDR - End point Detection and Response
- 1.9.1. EDR System Behavior
- 1.9.2. Differences between EDR and Antivirus
- 1.9.3. The Future of EDR Systems

1.10. Control Over Software Installation
- 1.10.1. Repositories and Software Stores
- 1.10.2. Lists of Permitted or Prohibited Software
- 1.10.3. Update Criteria
- 1.10.4. Software Installation Privileges

Module 2. Network Security (Perimeter)

2.1. Threat Detection and Prevention Systems
- 2.1.1. General Framework for Security Incidents
- 2.1.2. Current Defence Systems: Defence in Depth and SOC
- 2.1.3. Current Network Architectures
- 2.1.4. Types of Tools for Incident Detection and Prevention
  - 2.1.4.1. Network-based Systems
  - 2.1.4.2. Host-Based Systems
  - 2.1.4.3. Centralized Systems
- 2.1.5. Instance/Hosts, Container and Serverless Communication and Detection

2.2. Firewall
- 2.2.1. Types of Firewalls
- 2.2.2. Attacks and Mitigation
- 2.2.3. Common Firewalls in Linux Kernel
  - 2.2.3.1. UFW
  - 2.2.3.2. Nftables and Iptables
  - 2.2.3.3. Firewalls
- 2.2.4. Detection Systems Based on System Logs
  - 2.2.4.1. TCP Wrappers
  - 2.2.4.2. BlockHosts and DenyHosts
  - 2.2.4.3. Fail2Ban

2.3. Intrusion Detection and Prevention Systems (IDS/IPS)
- 2.3.1. Attacks on IDS/IPS
- 2.3.2. IDS/IPS Systems
  - 2.3.2.1. Snort
  - 2.3.2.2. Suricata

2.4. Next Generation Firewalls (NGFW)
- 2.4.1. Differences between NGFW and Traditional Firewalls
- 2.4.2. Main Capabilities
- 2.4.3. Commercial Solutions
- 2.4.4. Firewalls for Cloud Services
  - 2.4.4.1. Architecture Cloud VPC
  - 2.4.4.2. Cloud ACLs
  - 2.4.4.3. Security Group

2.5. Proxy
- 2.5.1. Types of Proxy
- 2.5.2. Uses of Proxies. Advantages and Disadvantages

2.6. Antivirus Engines
- 2.6.1. General Context of Malware and IOCs
- 2.6.2. Antivirus Engine Problems

2.7. Email Protection Systems
- 2.7.1. Antispam
  - 2.7.1.1. Black and White Lists
  - 2.7.1.2. Bayesian Filters
- 2.7.2. Mail Gateway (MGW)

2.8. SIEM
- 2.8.1. Components and Architecture
- 2.8.2. Correlation Rules and Use Cases
- 2.8.3. Current Challenges of SIEM Systems

2.9. SOAR
- 2.9.1. SOAR and SIEM: Enemies or Allies
- 2.9.2. The Future of SOAR Systems

2.10. Others Network-based Systems
- 2.10.1. WAF
- 2.10.2. NAC
- 2.10.3. HoneyPots and HoneyNets
- 2.10.4. CASB

Module 3. Smartphone Security

3.1. The World of Mobile Devices
- 3.1.1. Types of Mobile Platforms
- 3.1.2. IOS Devices
- 3.1.3. Android DevicesDispositivos android

3.2. Mobile Security Management
- 3.2.1. OWASP Mobile Security Project
  - 3.2.1.1. Top 10 Vulnerabilities
- 3.2.2. Communications, Networks and Connection Modes

3.3. The Mobile Device in the Enterprise Environment
- 3.3.1. Risk
- 3.3.2. Security Policies
- 3.3.3. Device Monitoring
- 3.3.4. Mobile Device Management (MDM)

3.4. User Privacy and Data Security
- 3.4.1. Statements of Information
- 3.4.2. Data Protection and Confidentiality
  - 3.4.2.1. Licences
  - 3.4.2.2. Encryption
- 3.4.3. Secure Data Storage
  - 3.4.3.1. Secure Storage on iOS
  - 3.4.3.2. Secure Storage on Android
- 3.4.4. Best Practices in Application Development

3.5. Vulnerabilities and Attack Vectors
- 3.5.1. Vulnerabilities
- 3.5.2. Attack Vectors
  - 3.5.2.1. Malware
  - 3.5.2.2. Data Exfiltration
  - 3.5.2.3. Data Manipulation

3.6. Main Threats
- 3.6.1. Unforced User
- 3.6.2. Malware
  - 3.6.2.1. Types of Malware
- 3.6.3. Social Engineering
- 3.6.4. Data Leakage
- 3.6.5. Information Theft
- 3.6.6. Unsecured Wi-Fi Networks
- 3.6.7. Outdated Software
- 3.6.8. Malicious Applications
- 3.6.9. Insecure Passwords
- 3.6.10. Weak or No Security Configuration
- 3.6.11. Physical Access
- 3.6.12. Loss or Theft of the Device
- 3.6.13. Identity Theft (Integrity)
- 3.6.14. Weak or Broken Cryptography
- 3.6.15. Denial of Service (DoS)

3.7. Main Attacks
- 3.7.1. Phishing Attacks
- 3.7.2. Attacks Related to Communication Modes
- 3.7.3. Smishing Attacks
- 3.7.4. Cryptojacking Attacks
- 3.7.5. Man in The Middle

3.8. Hacking
- 3.8.1. Rooting and Jailbreaking
- 3.8.2. Anatomy of a Mobile Attack
  - 3.8.2.1. Threat Propagation
  - 3.8.2.2. Malware Installation on the Device
  - 3.8.2.3. Persistence
  - 3.8.2.4. Payload Execution and Information Extraction
- 3.8.3. Hacking on IOS Devices: Mechanisms and Tools
- 3.8.4. Hacking on Android Devices: Mechanisms and Tools

3.9. Penetration Testing
- 3.9.1. iOS Pentesting
- 3.9.2. Android Pentesting
- 3.9.3. Tools

3.10. Safety and Security
- 3.10.1. Security Configuration
  - 3.10.1.1. On iOS Devices
  - 3.10.1.2. On Android Devices
- 3.10.2. Safety Measures
- 3.10.3. Protection Tools

Module 4. IoT Security

4.1. Devices
- 4.1.1. Types of Devices
- 4.1.2. Standardized Architectures
  - 4.1.2.1. OneM2M
  - 4.1.2.2. IoTWF
- 4.1.3. Application Protocols
- 4.1.4. Connectivity Technologies

4.2. IoT Devices. Areas of Application
- 4.2.1. SmartHome
- 4.2.2. SmartCity
- 4.2.3. Transportation
- 4.2.4. *Wearables*
- 4.2.5. Health Sector
- 4.2.6. IioT

4.3. Communication Protocols
- 4.3.1. MQTT
- 4.3.2. LWM2M
- 4.3.3. OMA-DM
- 4.3.4. TR-069

4.4. SmartHome
- 4.4.1. Home Automation
- 4.4.2. Networks
- 4.4.3. Household Appliances
- 4.4.4. Surveillance and Security

4.5. SmartCity
- 4.5.1. Lighting
- 4.5.2. Meteorology
- 4.5.3. Security/Safety

4.6. Transportation
- 4.6.1. Localisation
- 4.6.2. Making Payments and Obtaining Services
- 4.6.3. Connectivity

4.7. Wearables
- 4.7.1. Smart Clothing
- 4.7.2. Smart Jewelry
- 4.7.3. Smart Watches

4.8. Health Sector
- 4.8.1. Exercise/Heart Rate Monitoring
- 4.8.2. Monitoring of Patients and Elderly People
- 4.8.3. Implantable
- 4.8.4. Surgical Robots

4.9. Connectivity
- 4.9.1. Wi-Fi
- 4.9.2. Bluetooth
- 4.9.3. Built-in Connectivity

4.10. Securitization
- 4.10.1. Dedicated Networks
- 4.10.2. Password Managers
- 4.10.3. Use of Encrypted Protocols
- 4.10.4. Tips for Use

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

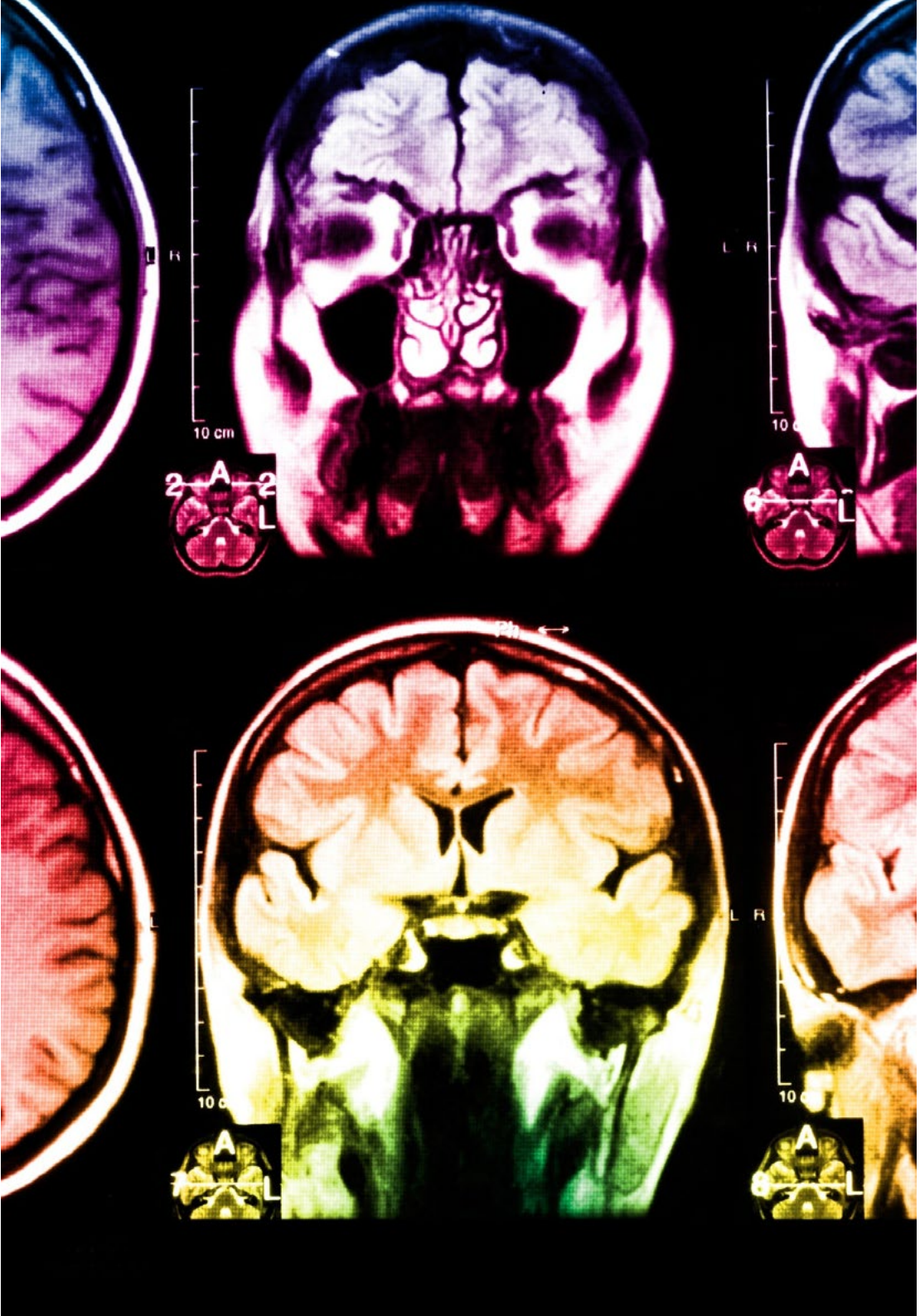
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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.

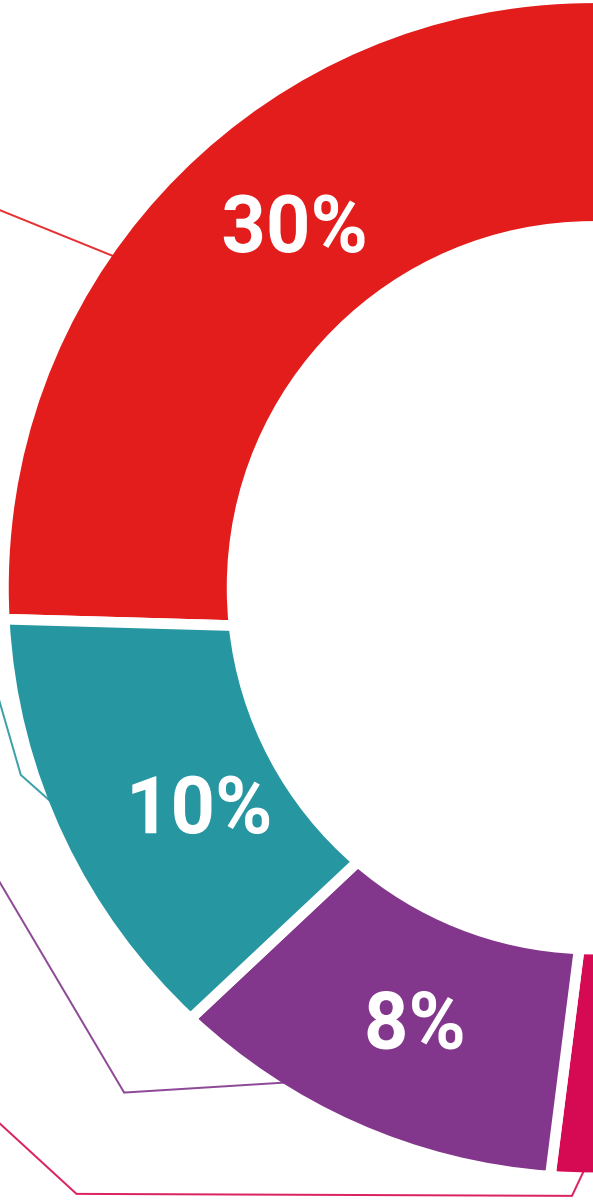
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

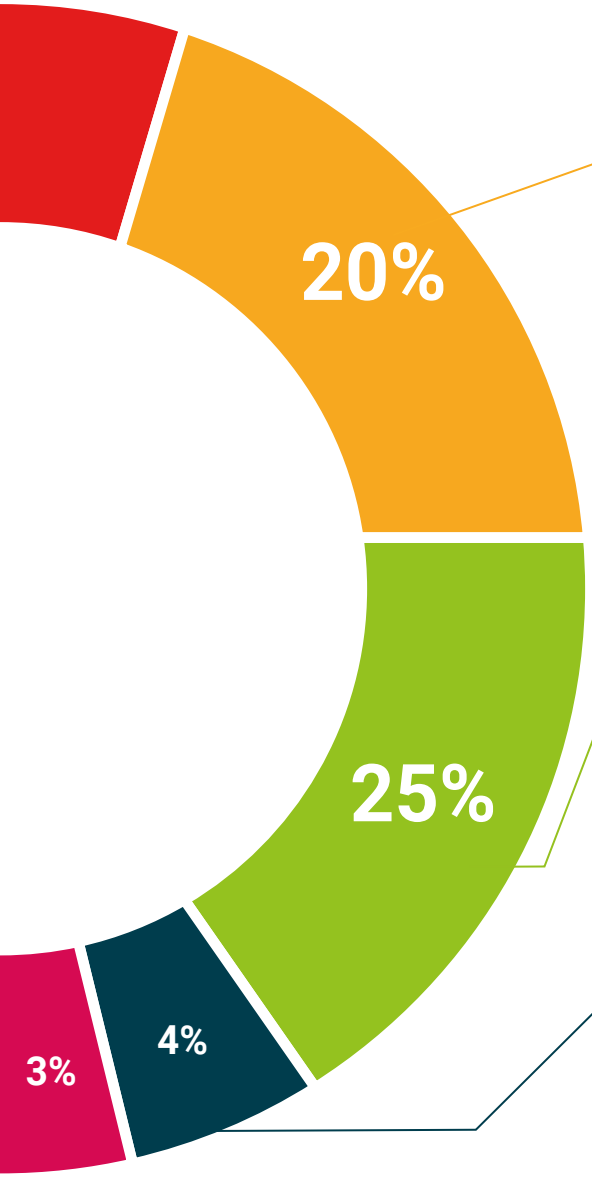
Practising Skills and Abilities

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.

06

Certificate

The Postgraduate Diploma in Defensive Cybersecurity 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 Defensive Cybersecurity** 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 Defensive Cybersecurity**

Official Number of Hours: **600 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

Defensive Cybersecurity

This is a qualification awarded by this University, equivalent to 600 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

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

June 17, 2020

Tere Guevara Navarro

Dean

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

Unique TECH Code: AFWORD23S techtitute.com/certificates

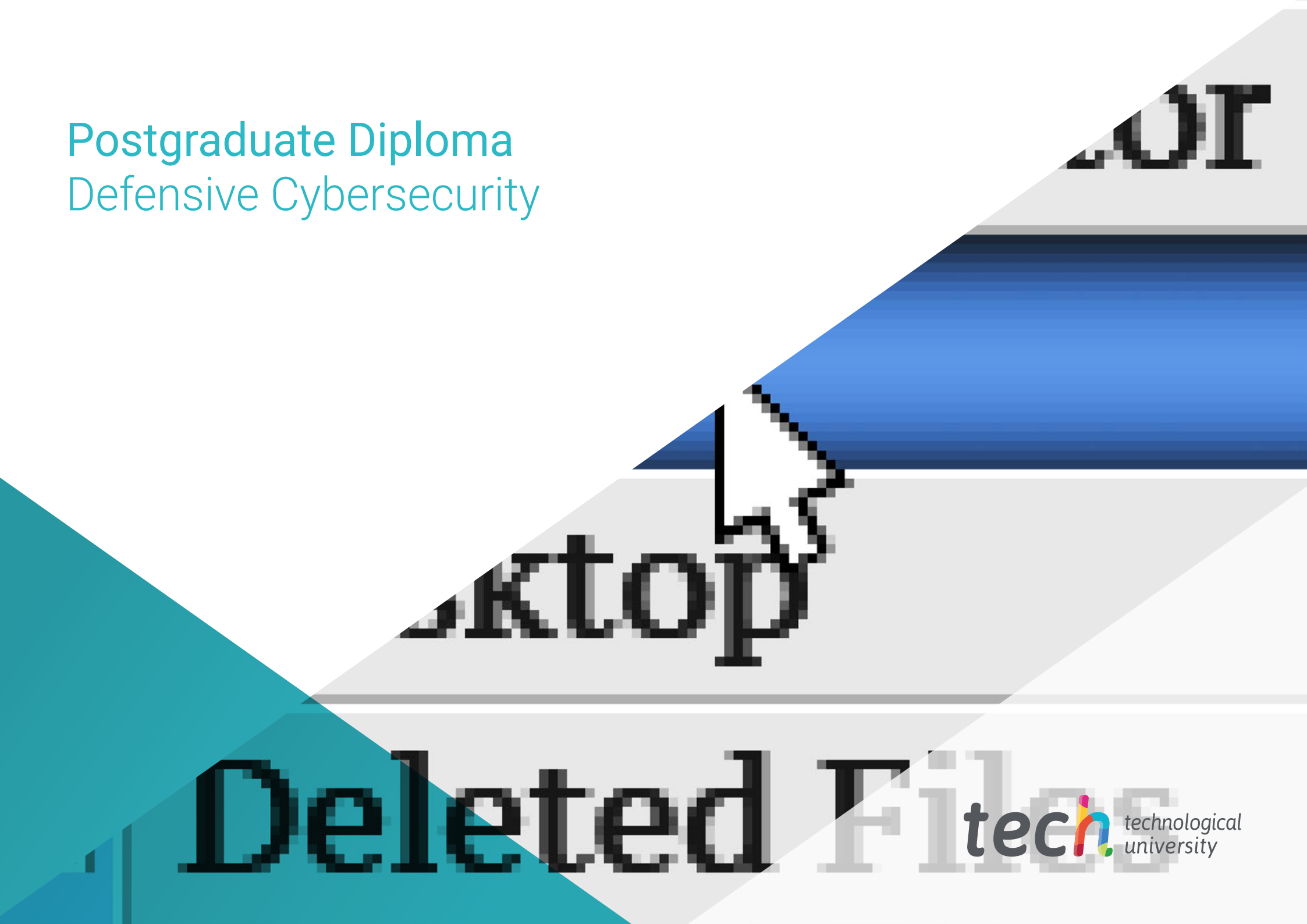
*Apostille Convention. In the event that the student wishes to have their paper certificate issued with an apostille, TECH EDUCATION will make the necessary arrangements to obtain it, at an additional cost.

tech technological university

Postgraduate Diploma
Defensive Cybersecurity

Course Modality: **Online**
Duration: **6 months.**
Certificate: **TECH Technological University**
Official Nº of Hours: **600 h.**

Postgraduate Diploma
Defensive Cybersecurity



tech technological university