# Postgraduate Certificate

## Forensic Fundamentals and DFIR

tech technological university

tech technological university

# Postgraduate Certificate
## Forensic Fundamentals and DFIR

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

Website: www.techtitute.com/pk/information-technology/postgraduate-certificate/forensic-fundamentals-dfir

# Index

01

# Introduction

With the advance of new technologies such as information systems, institutions are increasingly present on the Internet. However, with the increase in cyber-attacks, companies are exposed to various setbacks. In this sense, if hackers gain access to your networks, they could delete sensitive data and even ask for ransom money in exchange for releasing the blocked systems. Therefore, it is important for companies to have experts in Forensic Fundamentals to detect security breaches and reduce their impact as much as possible. In response to this need, TECH launches an innovative program to implement advanced techniques for the analysis of digital evidence. In addition, it is taught in a 100% online modality, guaranteeing the convenience of the students.

*Do you want to analyze firewall logs and thus detect network intrusions? Achieve it in 150 hours thanks to this training"*

Companies are increasingly realizing the importance of having cybersecurity IT specialists in their organization. The benefits of this include protection of your digital assets and forensic investigation to determine both the causes and scope of potential incidents. In turn, these professionals also collect information that can be used as legal evidence and to prosecute cybercriminals. In this regard, they even help organizations comply with data security regulations and security breach notification requirements.

Faced with this situation, TECH is developing cutting-edge training so that students can prevent hacker attacks by implementing the most appropriate strategies. The academic itinerary will delve into the processes of evidence acquisition, based on the chain of custody. In this way, students will act as computer forensic laboratories and resolve incidents affecting organizations. The program will also address network packet analysis and students will perform firewall logs. Malware will also be provided, in order to perform disassembly techniques.
Graduates will apply DFIR methodologies and unleash their creativity to offer the most innovative business solutions.

In addition, in order to strengthen the mastery of the contents, this curriculum applies the Relearning system. It should be noted that TECH is a pioneer in the use of this teaching model, which promotes the assimilation of complex concepts through the natural and progressive reiteration of them. Along these lines, the program also includes materials in various formats, such as interactive summaries and explanatory videos.
All this in a convenient 100% online modality, which allows students to adjust their schedules according to their responsibilities.

This **Postgraduate Certificate in Forensic Fundamentals and DFIR** contains the most complete and up-to-date program on the market. The most important features include:

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

*You will create incident response plans at the world's best digital university according to Forbes”*

*You will achieve your objectives thanks to TECH's didactic tools, including explanatory videos and interactive summaries"*

*Need to recover data from damaged media? TECH provides you with the best tools to achieve it.*

*You will prepare forensic reports with which you will be able to appear as an expert witness in important trials.*

The program's teaching staff includes professionals from the field 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 during the academic year For this purpose, the students will be assisted by an innovative interactive video system created by renowned and experienced experts.

02

# Objectives

The design of this program will explore advanced techniques for the collection and analysis of digital evidence, addressing cases of security breaches. In this way, students will deepen their knowledge of archival analysis as well as the preservation of the chain of custody. In addition, students will examine the most beneficial tactics to minimize the impact of potential cyber incidents that may arise.

*Forget about memorizing! With the Relearning system you will integrate the concepts in a natural and progressive way"*

## General Objectives

- Acquire advanced skills in penetration testing and Red Team simulations, addressing the identification and exploitation of vulnerabilities in systems and networks
- Develop leadership skills to coordinate teams specialized in offensive cybersecurity, optimizing the execution of Pentesting and Red Team projects
- Develop skills in the analysis and development of malware, understanding its functionality and applying defensive and educational strategies
- Refine communication skills by preparing detailed technical and executive reports, presenting findings effectively to technical and executive audiences
- Promote an ethical and responsible practice in the field of cybersecurity, considering ethical and legal principles in all activities
- Keep students up-to-date with emerging trends and technologies in cybersecurity

*You will be supported by a faculty of distinguished professionals in Industrial Cybersecurity"*



## Specific Objectives

### Module 1. Forensic Fundamentals and DFIR

- Acquire a solid understanding of the fundamental principles of digital forensic investigation (DFIR) and their application in the resolution of cyber incidents
- Develop skills in the secure and forensic acquisition of digital evidence, ensuring the preservation of the chain of custody
- Learn how to perform forensic analysis of file systems
- Familiarize the student with advanced techniques for log and log analysis, allowing the reconstruction of events in digital environments
- Learn how to apply digital forensic investigation methodologies in case resolution, from identification to documentation of findings
- Familiarize the student with the analysis of digital evidence and the application of forensic techniques in Pentesting environments
- Develop skills in the preparation of detailed and clear forensic reports, presenting findings and conclusions in an understandable manner
- Foster effective collaboration with incident response (IR) teams, optimizing coordination in threat investigation and mitigation
- Promote ethical and legal practices in digital forensics, ensuring adherence to cybersecurity regulations and standards of conduct

03

# Course Management

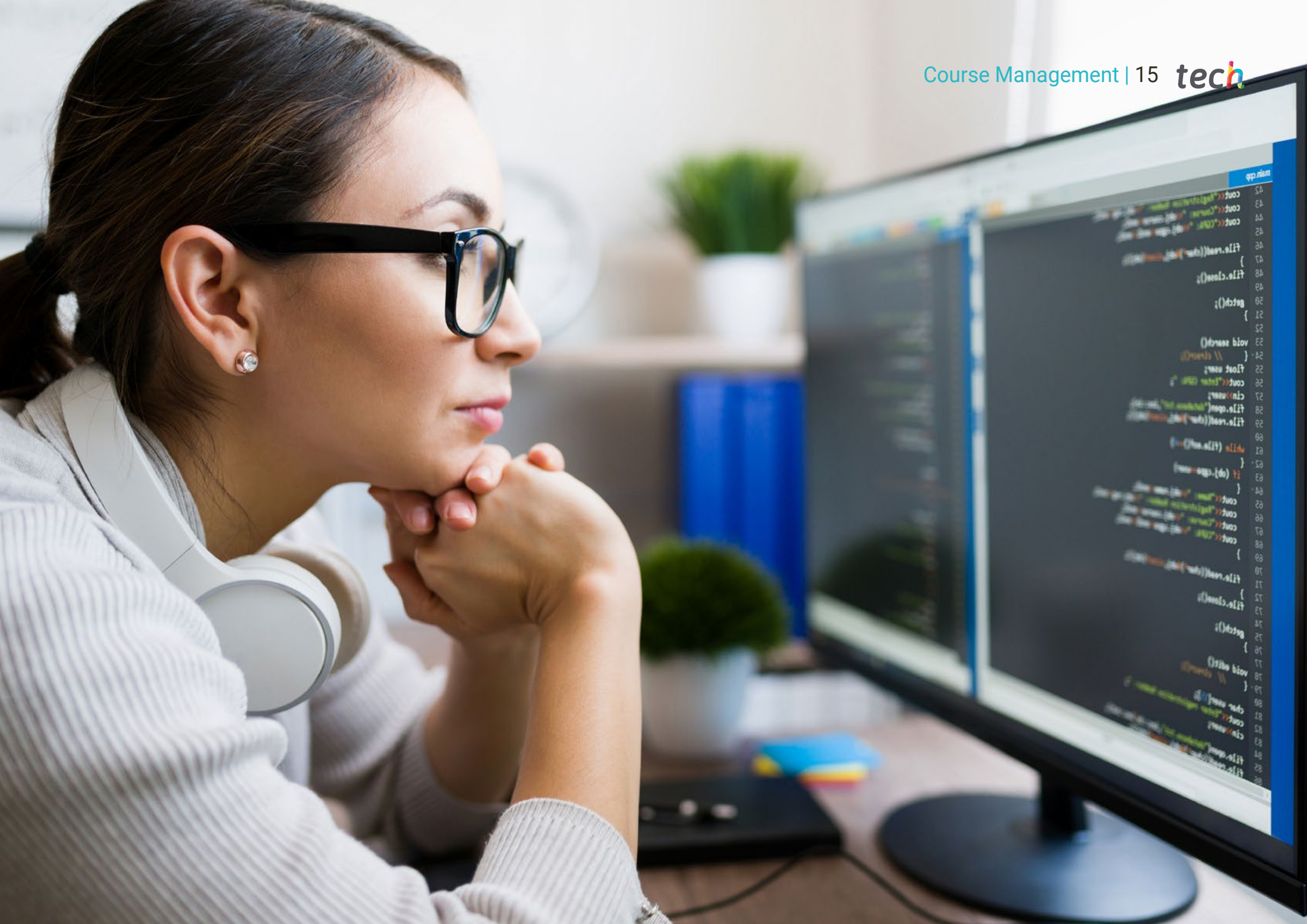
In its commitment to offer an education based on excellence, TECH counts on professionals of international prestige. These cybersecurity professionals have extensive work backgrounds, so through this training they offer the most effective tools for trainees to acquire essential digital forensics skills and respond to incidents. In this way, students have the guarantees they need to specialize in a digital sector that offers numerous job opportunities.

*Library full of multimedia resources in different audiovisual formats"*

## Management

### Mr. Carlos Gómez Pintado

- Manager of Cybersecurity and Network Team Cipherbit in Oesía Group
- Manager Advisor & Investor at Wesson App
- Graduate in Software Engineering and Information Society Technologies, Universidad Politécnica de Madrid
- Collaboration with educational institutions for the development of Higher Level Training Cycles in cybersecurity



04

# Structure and Content

The agenda will include simulations aimed at responding immediately to cyber incidents, reducing their effects and restoring operational normality. In addition, the academic itinerary goes deeper into the analysis of the most important operating systems (Windows, Linux and maCos) in order to enable students to recover data from damaged media. Malware analysis to identify malicious code and thus prevent organizations from suffering from viruses such as worms or Trojans will also be discussed in depth. In this way, students will acquire solid knowledge about digital forensics.

*Library full of multimedia resources in different audiovisual formats"*

## **Module 1.** Forensic Fundamentals and DFIR

1.1. Digital Forensics
- 1.1.1. History and Evolution of Computer Forensics
- 1.1.2. Importance of Computer Forensics in Cybersecurity
- 1.1.3. History and Evolution of Computer Forensics

1.2. Fundamentals of Computer Forensics
- 1.2.1. Chain of Custody and Its Application
- 1.2.2. Types of Digital Evidence
- 1.2.3. Evidence Acquisition Processes

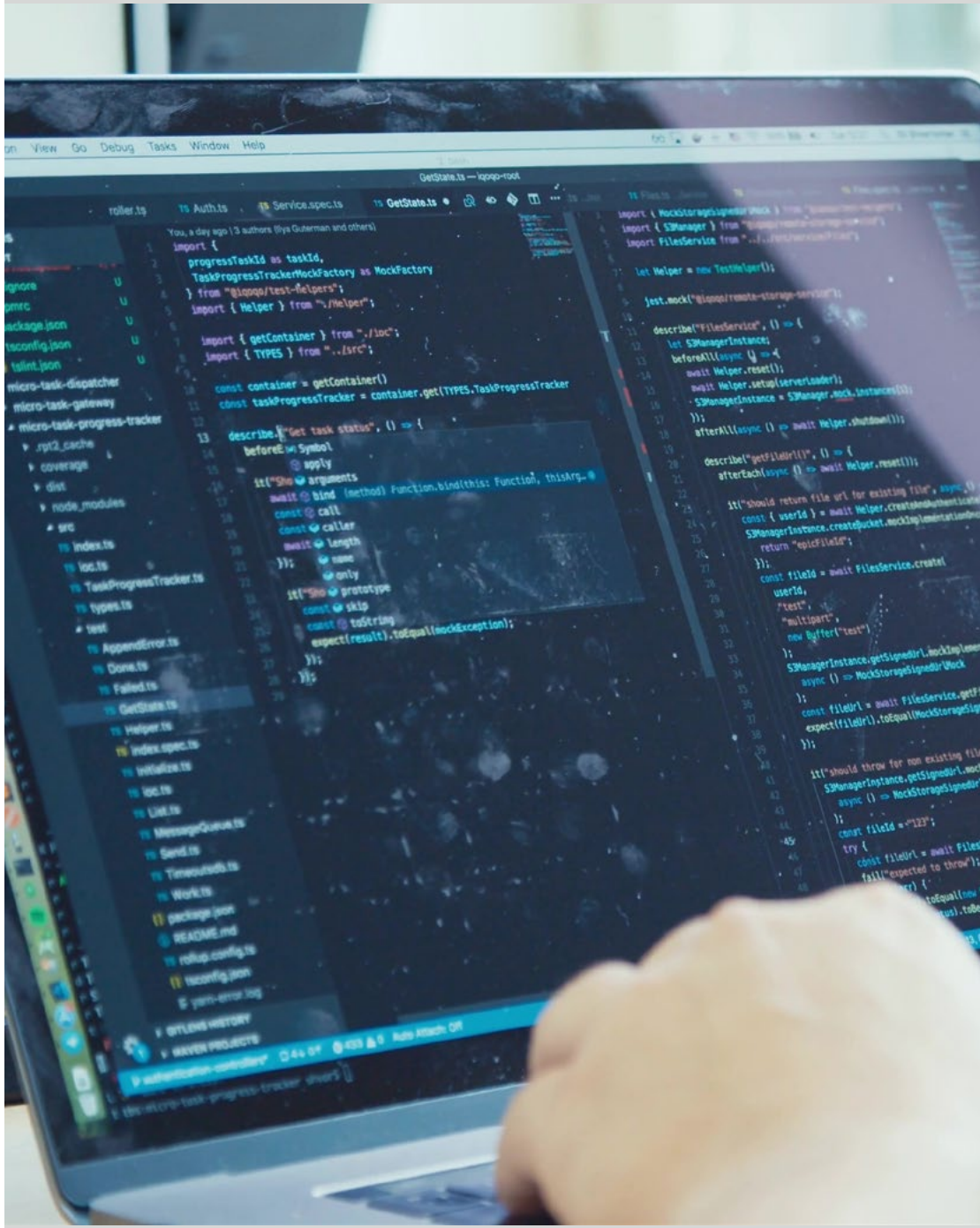
1.3. File Systems and Data Structure
- 1.3.1. Main File Systems
- 1.3.2. Data Hiding Methods
- 1.3.3. Analysis of File Metadata and Attributes

1.4. Operating Systems Analysis
- 1.4.1. Forensic Analysis of Windows Systems
- 1.4.2. Forensic Analysis of Linux Systems
- 1.4.3. Forensic Analysis of macOS Systems

1.5. Data Recovery and Disk Analysis
- 1.5.1. Data Recovery from Damaged Media
- 1.5.2. Disk Analysis Tools
- 1.5.3. Interpretation of File Allocation Tables

1.6. Network and Traffic Analysis
- 1.6.1. Network Packet Capture and Analysis
- 1.6.2. Firewall Log Analysis
- 1.6.3. Network Intrusion Detection

1.7. Malware and Malicious Code Analysis
- 1.7.1. Classification of Malware and Its Characteristics
- 1.7.2. Static and Dynamic Malware Analysis
- 1.7.3. Disassembly and Debugging Techniques



1.8. Log and Event Analysis
- 1.8.1. Types of Logs in Systems and Applications
- 1.8.2. Interpretation of Relevant Events
- 1.8.3. Log Analysis Tools

1.9. Respond to Security Incidents
- 1.9.1. Incident Response Process
- 1.9.2. Creating an Incident Response Plan
- 1.9.3. Coordination with Security Teams

1.10. Evidence and Legal Presentation
- 1.10.1. Rules of Digital Evidence in the Legal Field
- 1.10.2. Preparation of Forensic Reports
- 1.10.3. Appearance at Trial as an Expert Witness

*Library full of multimedia resources in different audiovisual formats"*

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

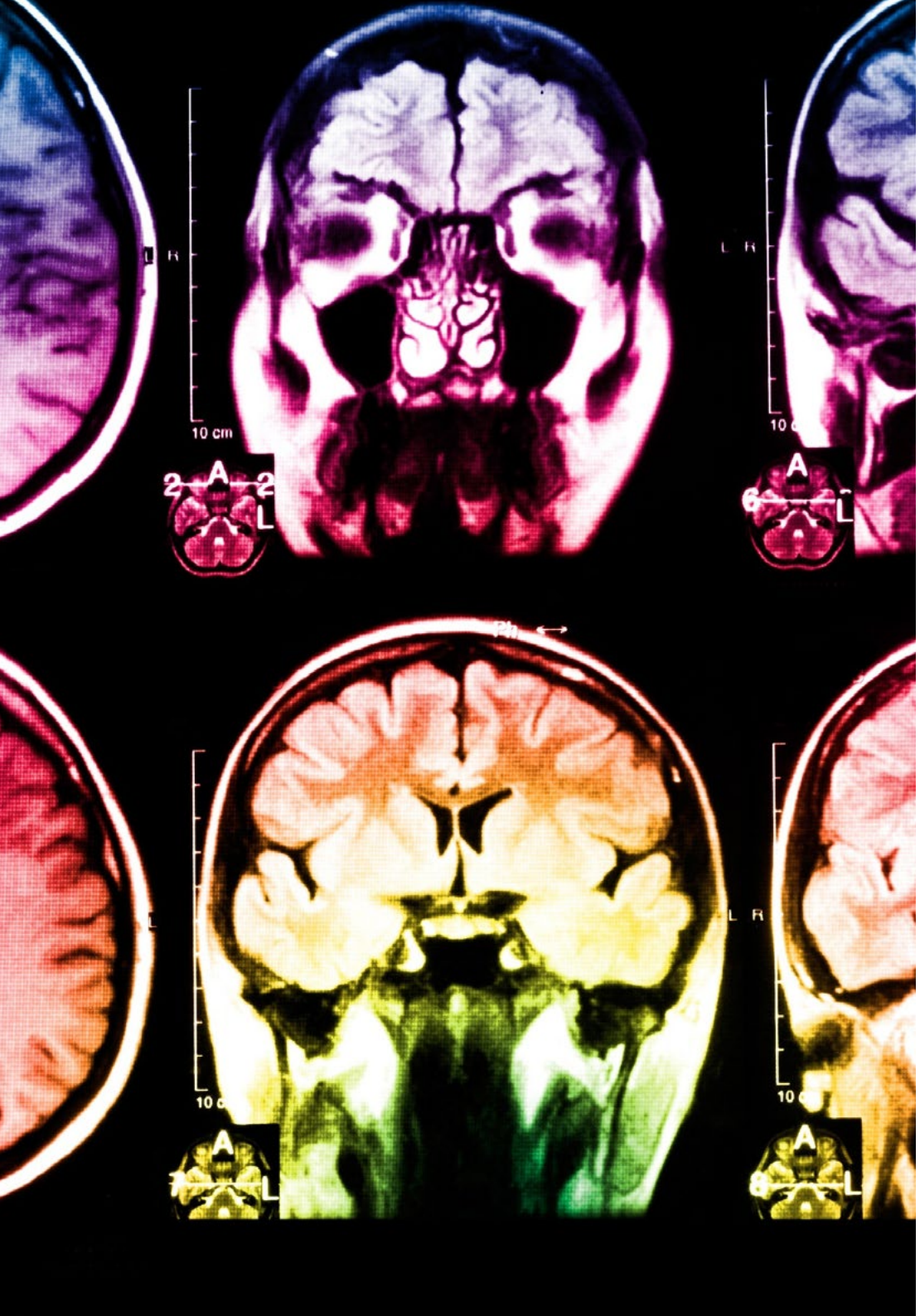
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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.

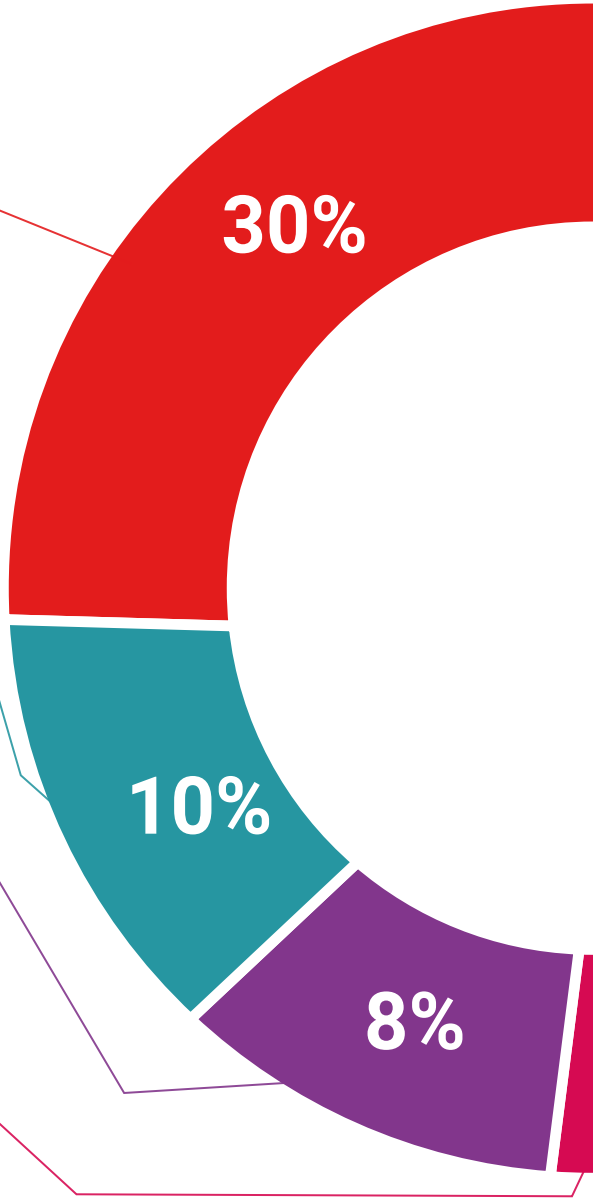
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

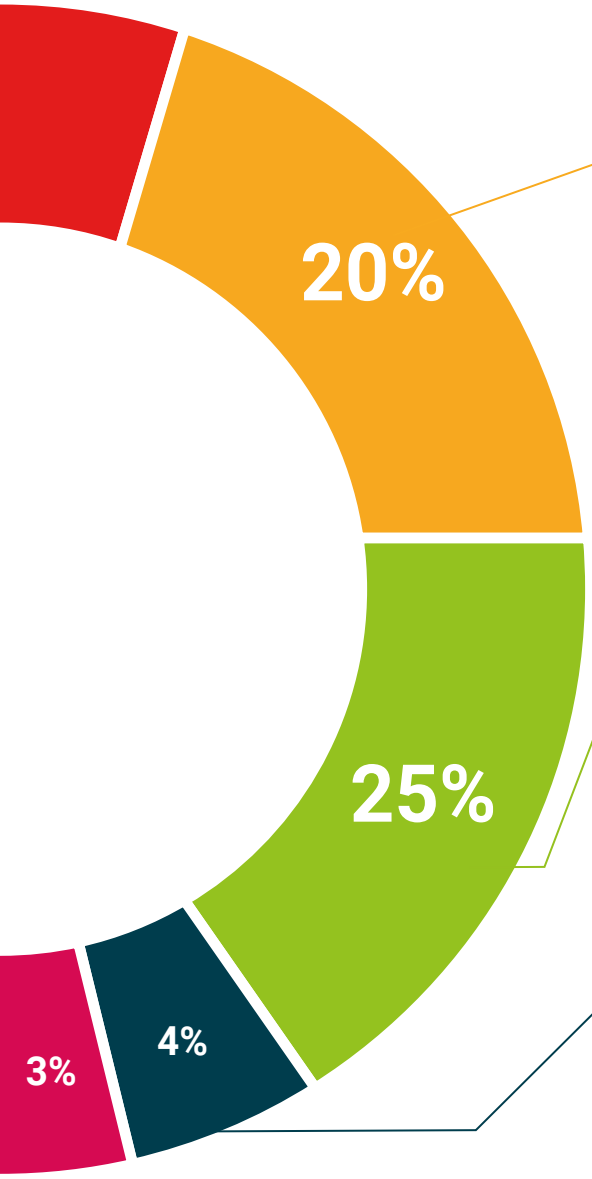
### Practising Skills and Abilities

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 Certificate in Forensic Fundamentals and DFIR guarantees, in addition to the most rigorous and up-to-date education, access to a Postgraduate Certificate 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 Certificate in Forensic Fundamentals and DFIR** 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 Certificate** issued by **TECH Technological University** via tracked delivery*.

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

Title: **Postgraduate Certificate in Forensic Fundamentals and DFIR**

Official Nº of Hours: **150 h.**


tech technological university

Awards the following

CERTIFICATE

to

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

For having passed and accredited the following program

POSTGRADUATE CERTIFICATE

in

Forensic Fundamentals and DFIR

This is a qualification awarded by this University, equivalent to 150 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 Certificate

## Forensic Fundamentals and DFIR

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

# Postgraduate Certificate

## Forensic Fundamentals and DFIR

tech technological university