Postgraduate Diploma
Offensive Cybersecurity

tech technological university

tech technological university

Postgraduate Diploma
Offensive Cybersecurity

- 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-offensive-cybersecurity

Index

01

Introduction

Cybersecurity is an essential aspect for institutions to protect their digital assets, maintain their social reputation and safeguard themselves against espionage by competitors. As a result, more and more companies are requesting the incorporation of IT experts in their organization charts, in order to avoid consequences that could even affect their financial capabilities. In this context, these specialists need to constantly update their knowledge and skills to keep abreast of cybercrime techniques. For this reason, TECH has developed an innovative Postgraduate Diploma, in which threats will be identified and mitigated. It should be noted that the entire program will be taught in a 100% online modality, to ensure that students have greater convenience and flexibility.

entComponentBooster
VehicleBlueprintLibrary.h
VehicleGameMode.h
VehicleGameState.h
VehicleGameUserSettings.h
VehicleGameViewportClient.h
VehicleTypes.h

```
GENERATED_UCLASS_BODY()

// Begin Actor overrides
virtual void PostInitializeComponents()
virtual void Tick(float DeltaSeconds)
virtual void ReceiveHit(class UPrimitiveComponent
virtual void FellOutOfWorld(const class UDamageType
// End Actor overrides

// Begin Pawn overrides
virtual void SetupPlayerInputComponent(class UInputComponent
virtual float TakeDamage(float Damage, struct FDamage
virtual void TornOff() override;
// End Pawn overrides

/** Identifies if pawn is in its dying
UPROPERTY(VisibleAnywhere, Blueprint
uint32 bIsDying:1;

/** replicating death on
UFUNCTION()
void OnRep_Dying(

/** Return
virtual
```

You will deepen your knowledge of the Kerberos protocol and protect information in network environments”

Every day the media report cases involving hackers who damage institutions by accessing their databases. The consequences of these attacks are severe, disrupting operations and preventing businesses from functioning effectively. In fact, it can directly impact your economy by incurring fines for non-compliance with regulations and limiting revenue.

In this regard, TECH has created a cutting-edge program to detect the most commonly used intrusion techniques, as well as the best strategies to deal with them. Under the guidance of experienced faculty, the curriculum will lay the essential groundwork for understanding how hackers think. It will also provide various solutions aimed at providing secure infrastructures for the management of digital certificates in an enterprise network.

Professionals will also learn how to optimize the preparation of online environments, thanks to the configuration of virtual machines or snapshots. In addition, malware will be analyzed, probing calls with API Monitor and observing network requests with TCPView. Graduates will learn theoretical concepts in simulated environments, preparing them for real-world challenges in Offensive Cybersecurity. Finally, emphasis will be placed on the ethics and social responsibility that should characterize experts in this field.

To consolidate the mastery of all these contents, the Postgraduate Diploma applies the innovative Relearning system. 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. The program is also supported by materials in various formats, such as explanatory videos, interactive summaries and infographics. All this in a convenient 100% online modality, which allows each person to adjust their the schedules of each person according to their responsibilities and availability.

This **Postgraduate Diploma in Offensive Cybersecurity** 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 Offensive Cybersecurity
- The graphic, schematic and eminently practical content of the system provides complete 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

> *Develop your skills as an offensive auditor and embark on a new professional challenge in the most prestigious digital companies”*

Do you want to become a Big Bounty Hunter? You will catch any vulnerability on the Internet thanks to this program.

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

In just 6 months you will master identity management in Azure AD. Enroll now!.

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 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 offers a unique educational experience, which stands out for its practical and innovative approach to cybersecurity. In this way, students will learn from vulnerability analysis to advanced intrusion techniques. In this line, optimal measures will be offered to evaluate and strengthen the different cybernetic systems. In addition, emphasis will be placed on both the legal and ethical responsibilities that experts in this field must adopt.

> *Reduce malware threats with the world's best digital university, according to Forbes”*

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

Specific Objectives

Module 1. Offensive Security

- Familiarize the graduate with penetration testing methodologies, including key phases such as information gathering, vulnerability analysis, exploitation and documentation
- Develop practical skills in the use of specialized Pentesting tools to identify and assess vulnerabilities in systems and networks
- Study and understand the tactics, techniques and procedures used by malicious actors, enabling the identification and simulation of threats
- Apply theoretical knowledge in practical scenarios and simulations, facing real challenges to strengthen Pentesting skills
- Develop effective documentation skills, creating detailed reports reflecting findings, methodologies used, and recommendations for safety improvement
- Practice effective collaboration in offensive security teams, optimizing the coordination and execution of Pentesting activities

Module 2. Network and Windows System Attacks

- Develop skills to identify and assess specific vulnerabilities in Windows operating systems
- Learn advanced tactics used by attackers to infiltrate and persist in networks based on Windows environments
- Acquire skills in strategies and tools to mitigate specific threats targeting Windows operating systems
- Familiarize the graduate with forensic analysis techniques applied to Windows systems, facilitating the identification and response to incidents
- Apply theoretical knowledge in simulated environments, participating in practical exercises to understand and counteract specific attacks on Windows systems
- Learn specific strategies for securing enterprise environments using Windows operating systems, considering the complexities of enterprise infrastructures

- Develop competencies to evaluate and improve security configurations in Windows systems, ensuring the implementation of effective measures
- Promote ethical and legal practices in the execution of attacks and tests on Windows systems, considering the ethical principles of cybersecurity
- Keep the student up-to-date with the latest trends and threats in Windows system attacks, ensuring the continued relevance and effectiveness of the skills acquired

Module 3. *Malware* Analysis and Development

- Acquire advanced knowledge of the nature, functionality and behavior of malware, understanding its various forms and targets
- Develop skills in forensic analysis applied to malware, enabling the identification of indicators of compromise (IoC) and attack patterns
- Learn strategies for effective *malware* detection and prevention, including the deployment of advanced security solutions
- Familiarize the student with the development of malware for educational and defensive purposes, allowing a deep understanding of the tactics used by attackers
- Promote ethical and legal practices in malware analysis and development, ensuring integrity and accountability in all activities
- Apply theoretical knowledge in simulated environments, participate in hands-on exercises to understand and counter malicious attacks
- Develop skills to evaluate and select anti-malware security tools, considering their effectiveness and adaptability to specific environments
- Learn how to implement effective mitigation against malicious threats, reducing the impact and spread of malware on systems and networks
- Foster effective collaboration with security teams, integrating strategies and efforts to protect against malware threats
- Keep the graduate up to date with the latest trends and techniques used in malware analysis and development, ensuring the continued relevance and effectiveness of the skills acquired

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

03
Course Management

In its commitment to offer educational excellence, TECH has a prestigious teaching staff. It should be noted that these specialists have an extensive professional background, having been part of recognized companies dedicated to Offensive Cybersecurity. For this reason, the academic itinerary will include the most advanced resources and technologies in this field. In addition, a comprehensive approach will be offered to meet the expectations demanded by the graduate to specialize in a field that will provide many opportunities.

> You will be supported by a faculty of distinguished professionals in Offensive Cybersecurity”

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

Professors

Mr. Yuba González Parrilla

- Offensive Security Line and Network Team Coordinator
- Predictive Project Management Specialist at the Project Management Institute
- SmartDefense Specialist
- Web Application Penetration Tester Expert at eLearnSecurity
- Junior Penetration Tester in eLearnSecurity
- Graduated in Computer Engineering at the Polytechnic University of Madrid

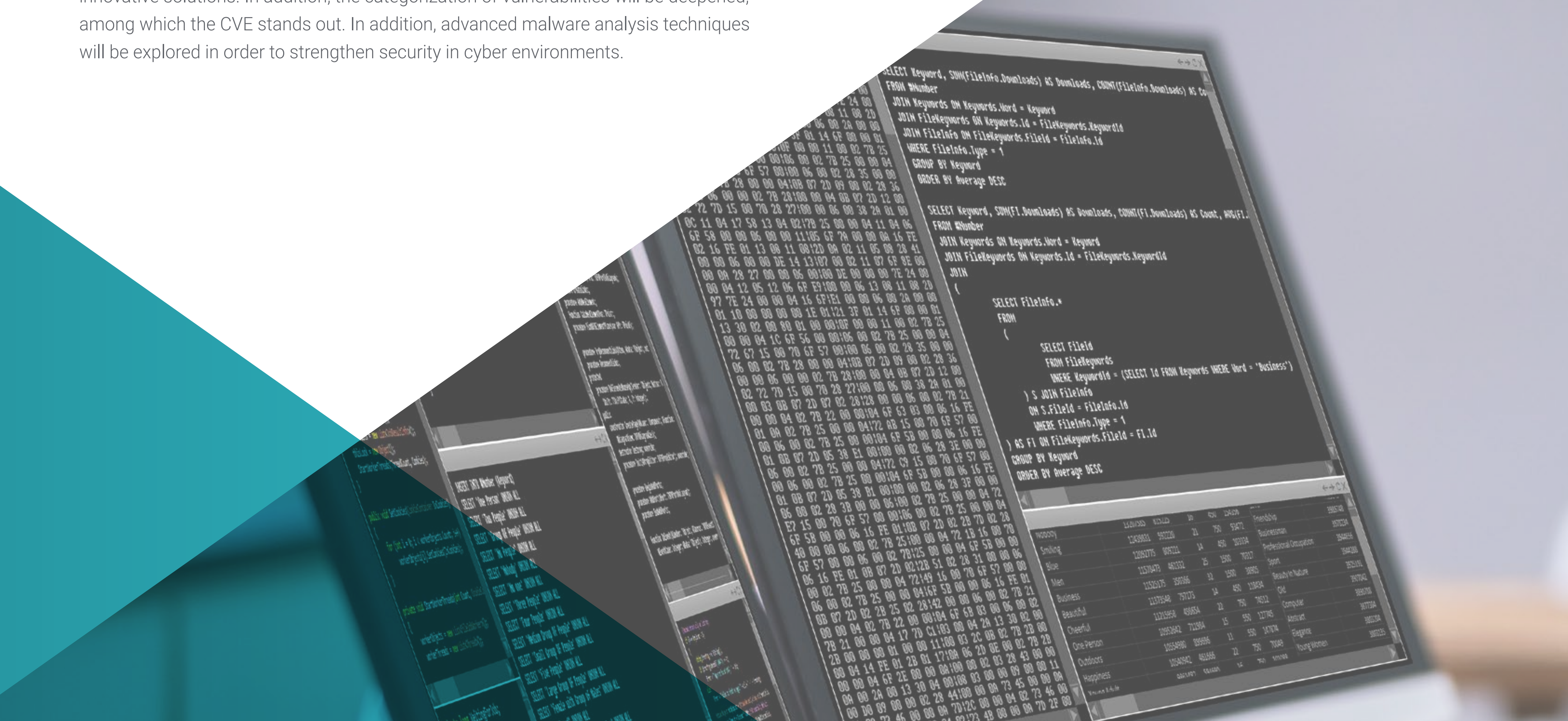
Mr. Alejandro Gallego Sánchez

- Pentester in Oesia Group
- Cybersecurity Consultant in Integrated Technology Business, S.L
- Audiovisual Technician in Audiovisual Engineering S.A
- Graduate in Cybersecurity Engineering from the Rey Juan Carlos University

04

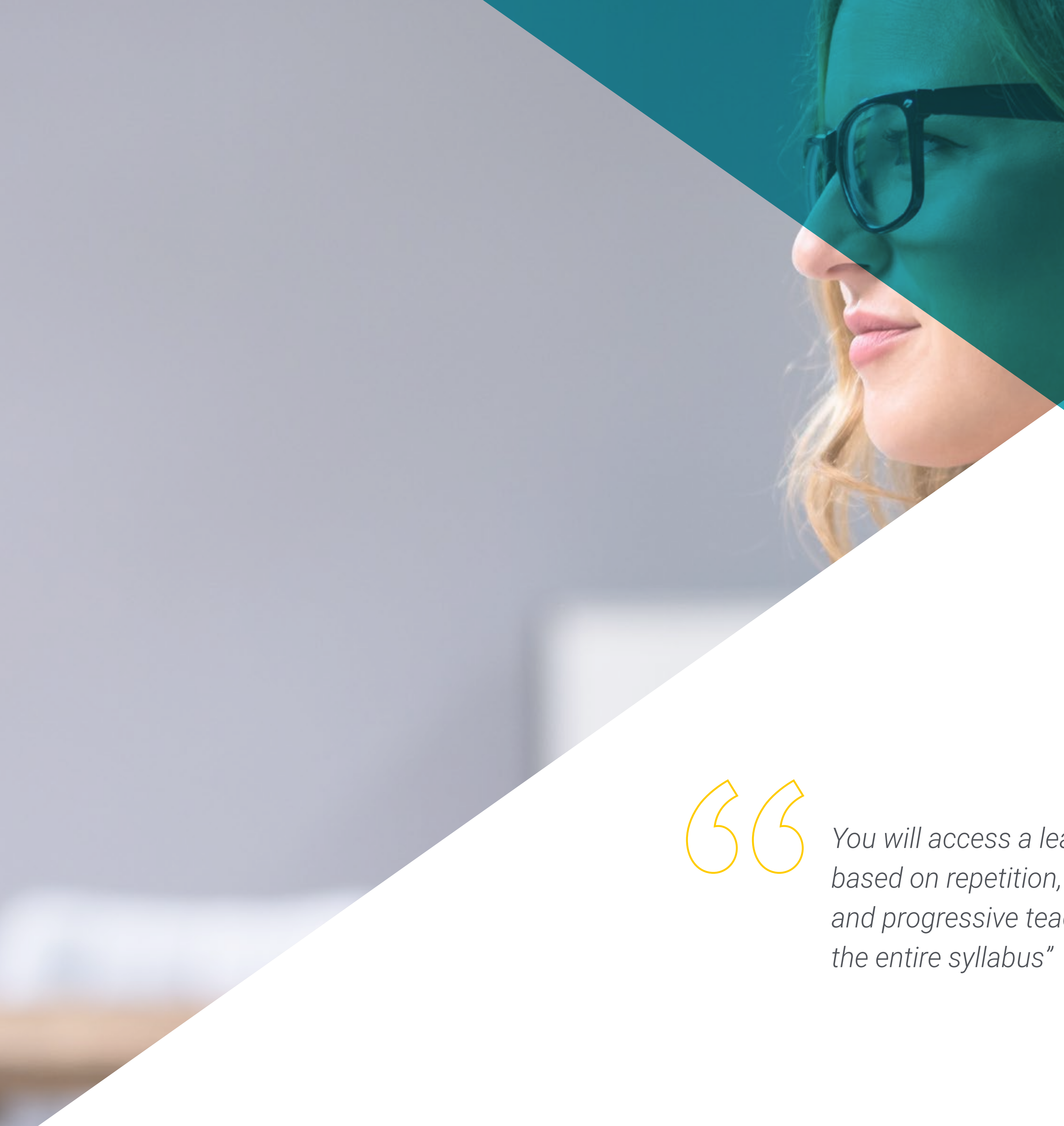
Structure and Content

This program is structured in 3 modules: Offensive Security, Network or Windows Systems Attack, and Malware Analysis and Development. Throughout the curriculum, a practical perspective oriented to the detection of early threats will be provided. In this sense, students' creativity will be encouraged to overcome challenges through innovative solutions. In addition, the categorization of vulnerabilities will be deepened, among which the CVE stands out. In addition, advanced malware analysis techniques will be explored in order to strengthen security in cyber environments.



```
SELECT Keyword, SUM(FileInfo.Downloads) AS Downloads, COUNT(FileInfo.Downloads) AS Co
FROM #Number
 JOIN Keywords ON Keywords.Word = Keyword
 JOIN FileKeywords ON Keywords.Id = FileKeywords.KeywordId
 JOIN FileInfo ON FileKeywords.FileId = FileInfo.Id
 WHERE FileInfo.Type = 1
 GROUP BY Keyword
 ORDER BY Average DESC

SELECT Keyword, SUM(FI.Downloads) AS Downloads, COUNT(FI.Downloads) AS Count, AVG(FI.
FROM #Number
 JOIN Keywords ON Keywords.Word = Keyword
 JOIN FileKeywords ON Keywords.Id = FileKeywords.KeywordId
 JOIN
 (
        SELECT FileInfo.*
        FROM
        (
              SELECT FileId
              FROM FileKeywords
              WHERE KeywordId = (SELECT Id FROM Keywords WHERE Word = 'Business')
        ) S JOIN FileInfo
        ON S.FileId = FileInfo.Id
        WHERE FileInfo.Type = 1
 ) AS FI ON FileKeywords.FileId = FI.Id
 GROUP BY Keyword
 ORDER BY Average DESC
```



You will access a learning system based on repetition, with a natural and progressive teaching throughout the entire syllabus"

Module 1. Offensive Security

1.1. Definition and Context
- 1.1.1. Fundamental Concepts of Offensive Security
- 1.1.2. Importance of Cybersecurity Today
- 1.1.3. Offensive Security Challenges and Opportunities

1.2. Basis of Cybersecurity
- 1.2.1. Early Challenges and Evolving Threats
- 1.2.2. Technological Milestones and Their Impact on Cybersecurity
- 1.2.3. Cybersecurity in the Modern Era

1.3. Basis of Offensive Security
- 1.3.1. Key Concepts and Terminology
- 1.3.2. Think Outside the Box
- 1.3.3. Differences between Offensive and Defensive Hacking

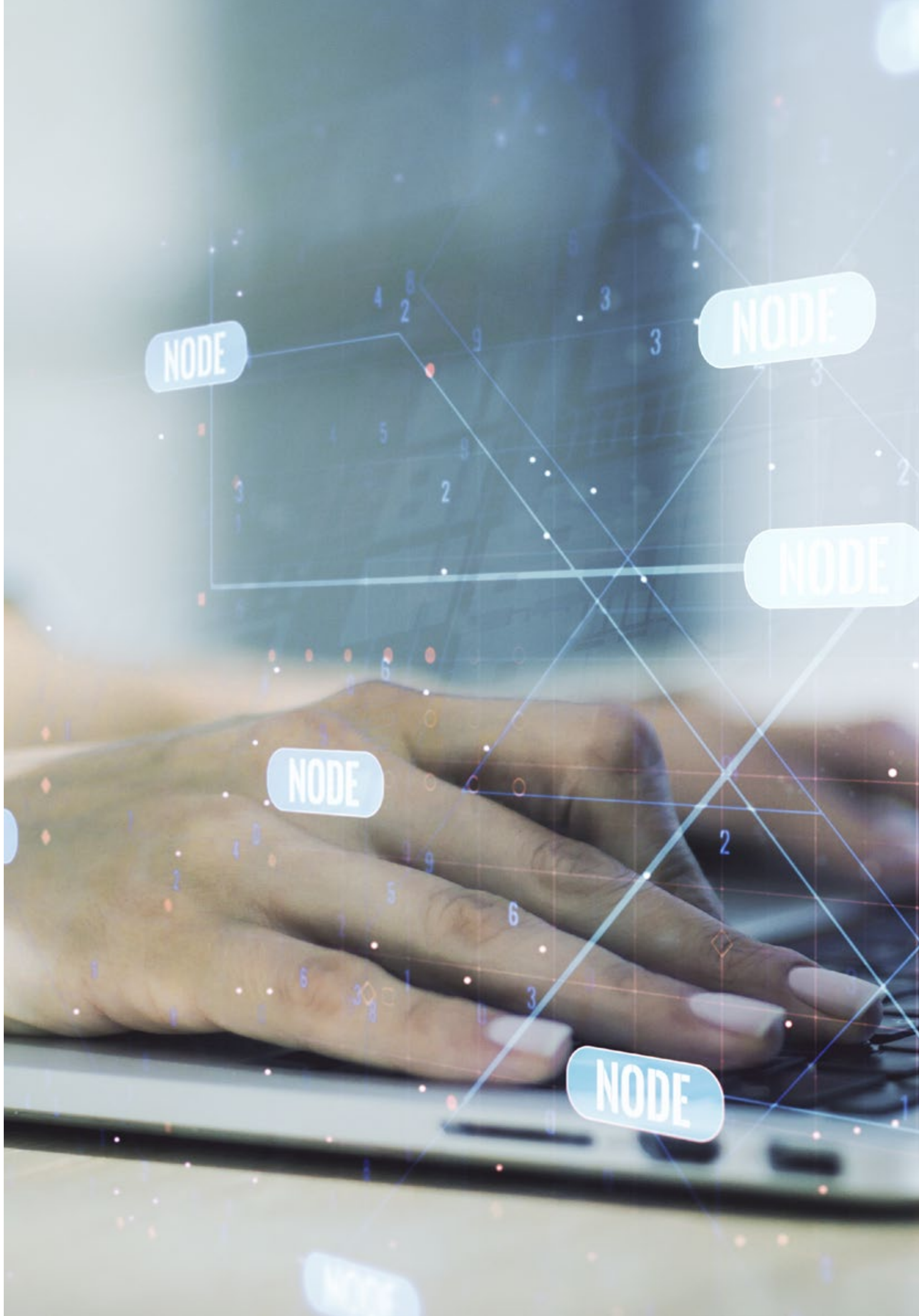
1.4. Offensive Security Methodologies
- 1.4.1. PTES (Penetration Testing Execution Standard)
- 1.4.2. OWASP (Open Web Application Security Project)
- 1.4.3. Cyber Security Kill Chain

1.5. Offensive Security Roles and Responsibilities
- 1.5.1. Main Profiles
- 1.5.2. Bug Bounty Hunters
- 1.5.3. Researching: The Art of Research

1.6. Offensive Auditor's Arsenal
- 1.6.1. Operating Systems for Hacking
- 1.6.2. Introduction to C2
- 1.6.3. Metasploit: Fundamentals and Use
- 1.6.4. Useful Resources

1.7. OSINT: Open Source Intelligence
- 1.7.1. OSINT Fundamentals
- 1.7.2. OSINT Tools and Techniques
- 1.7.3. OSINT Applications in Offensive Security

1.8. Scripting Introduction to Automation
- 1.8.1. Scripting Fundamentals
- 1.8.2. Scripting in Bash
- 1.8.3. Scripting in Python



1.9. Vulnerability Categorization
 1.9.1. CVE (Common Vulnerabilities and Exposure)
 1.9.2. CWE (Common Weakness Enumeration)
 1.9.3. CAPEC (Common Attack Pattern Enumeration and Classification)
 1.9.4. CVSS (Common Vulnerability Scoring System)
 1.9.5. MITRE ATT & CK

1.10. Ethics and Hacking
 1.10.1. Principles of Hacker Ethics
 1.10.2. The Line between Ethical Hacking and Malicious Hacking
 1.10.3. Legal Implications and Consequences
 1.10.4. Case Studies: Ethical Situations in Cybersecurity

Module 2. Network and Windows System Attacks

2.1. Windows and Active Directory
 2.1.1. History and Evolution of Windows
 2.1.2. Active Directory Basics
 2.1.3. Active Directory Functions and Services
 2.1.4. General Architecture of the Active Directory

2.2. Networking in Active Directory Environments
 2.2.1. Network Protocols in Windows
 2.2.2. DNS and its Operation in the Active Directory
 2.2.3. Network Diagnostic Tools
 2.2.4. Implementation of Networks in Active Directory

2.3. Authentication and Authorization in Active Directory
 2.3.1. Authentication Process and Flow
 2.3.2. Credential Types
 2.3.3. Credentials Storage and Management
 2.3.4. Authentication Security

2.4. Permissions and Policies in Active Directory
 2.4.1. GPOs
 2.4.2. Application and Management of GPOs
 2.4.3. Active Directory Permissions Management
 2.4.4. Vulnerabilities and Mitigations in Permits

2.5. Kerberos Basics
- 2.5.1. What Is Kerberos?
- 2.5.2. Components and Operation
- 2.5.3. Kerberos Tickets
- 2.5.4. Kerberos in the Context of Active Directory

2.6. Advanced Kerberos Techniques
- 2.6.1. Common Kerberos Attacks
- 2.6.2. Mitigations and Protections
- 2.6.3. Kerberos Traffic Monitoring
- 2.6.4. Advanced Kerberos Attacks

2.7. Active Directory Certificate Services (ADCS)
- 2.7.1. PKI Basics
- 2.7.2. ADCS Roles and Components
- 2.7.3. ADCS Configuration and Deployment
- 2.7.4. Safety at ADCS

2.8. Attacks and Defenses in Active Directory Certificate Services (ADCS)
- 2.8.1. Common ADCS Vulnerabilities
- 2.8.2. Attacks and Exploitation Techniques
- 2.8.3. Defenses and Mitigations
- 2.8.4. ADCS Monitoring and Auditing

2.9. Active Directory Audit
- 2.9.1. Importance of Auditing in the Active Directory
- 2.9.2. Audit Tools
- 2.9.3. Detection of Anomalies and Suspicious Behaviors
- 2.9.4. Incident Response and Recovery

2.10. Azure AD
- 2.10.1. Azure AD Basics
- 2.10.2. Synchronization with Local Active Directory
- 2.10.3. Identity Management in Azure AD
- 2.10.4. Integration with Applications and Services

Module 3. Malware Analysis and Development

- 3.1. Malware Analysis and Development
  - 3.1.1. History and Evolution of Malware
  - 3.1.2. Classification and Types of Malware
  - 3.1.3. Malware Analysis
  - 3.1.4. Malware Development
- 3.2. Preparing the Environment
  - 3.2.1. Configuration of Virtual Machines and Snapshots
  - 3.2.2. Malware Analysis Tools
  - 3.2.3. Malware Development Tools
- 3.3. Windows Basics
  - 3.3.1. PE file format (Portable Executable)
  - 3.3.2. Processes and Threads
  - 3.3.3. File System and Registry
  - 3.3.4. Windows Defender
- 3.4. Basic Malware Techniques
  - 3.4.1. Shellcode Generation
  - 3.4.2. Execution of Shellcode on Disk
  - 3.4.3. Disk vs Memory
  - 3.4.4. Execution of Shellcode in Memory
- 3.5. Intermediate Malware Techniques
  - 3.5.1. Persistence in Windows
  - 3.5.2. Home Folder
  - 3.5.3. Registration Keys
  - 3.5.4. Screensaver
- 3.6. Advanced Malware Techniques
  - 3.6.1. Shellcode Encryption (XOR)
  - 3.6.2. Shellcode Encryption (RSA)
  - 3.6.3. String Obfuscation
  - 3.6.4. Process Injection
- 3.7. Static Malware Analysis
  - 3.7.1. Analyzing Packers with DIE (Detect It Easy)
  - 3.7.2. Analyzing Sections with PE-Bear
  - 3.7.3. Decompilation with Ghidra
- 3.8. Dynamic Malware Analysis
  - 3.8.1. Observing Behavior with Process Hacker
  - 3.8.2. Analyzing Calls with API Monitor
  - 3.8.3. Analyzing Registry Changes with Regshot
  - 3.8.4. Observing Network Requests with TCPView
- 3.9. Analysis in .NET
  - 3.9.1. Introduction to .NET
  - 3.9.2. Decompiling with dnSpy
  - 3.9.3. Debugging with dnSpy
  - 3.10. Analyzing Real Malware
- 3.10.1.Preparing the Environment
  - 3.10.2. Static Malware Analysis
  - 3.10.3. Dynamic Malware Analysis
  - 3.10.4. YARA Rule Creation

> *No preset evaluation schedules or timetables. That's what this TECH program is like!”*

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.

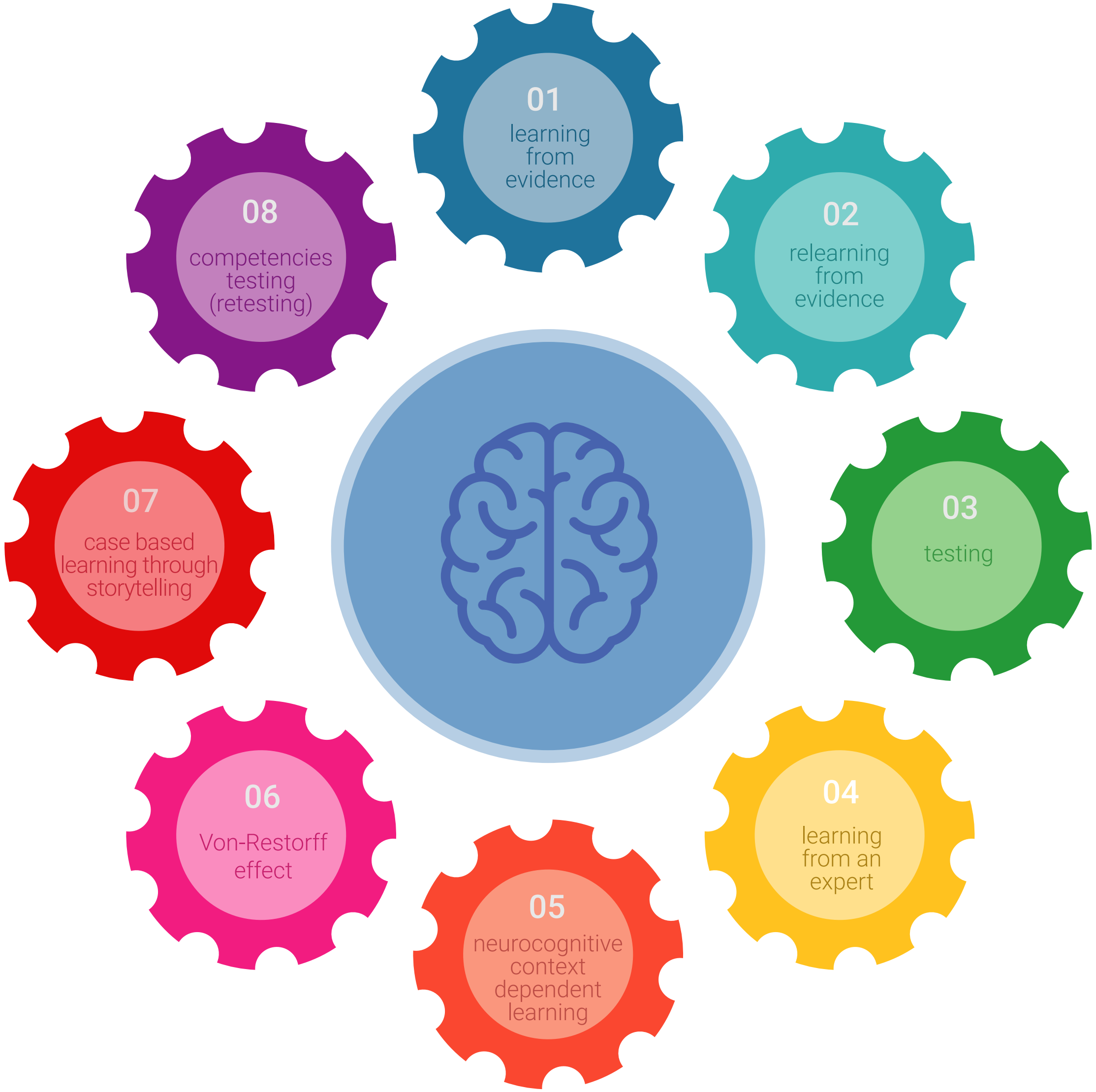
What should a professional do in a given situation? This is the question that you are presented with in the case method, an action-oriented learning method. Throughout the course, students will be presented with multiple real cases. They will have to combine all their knowledge and research, and argue 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.

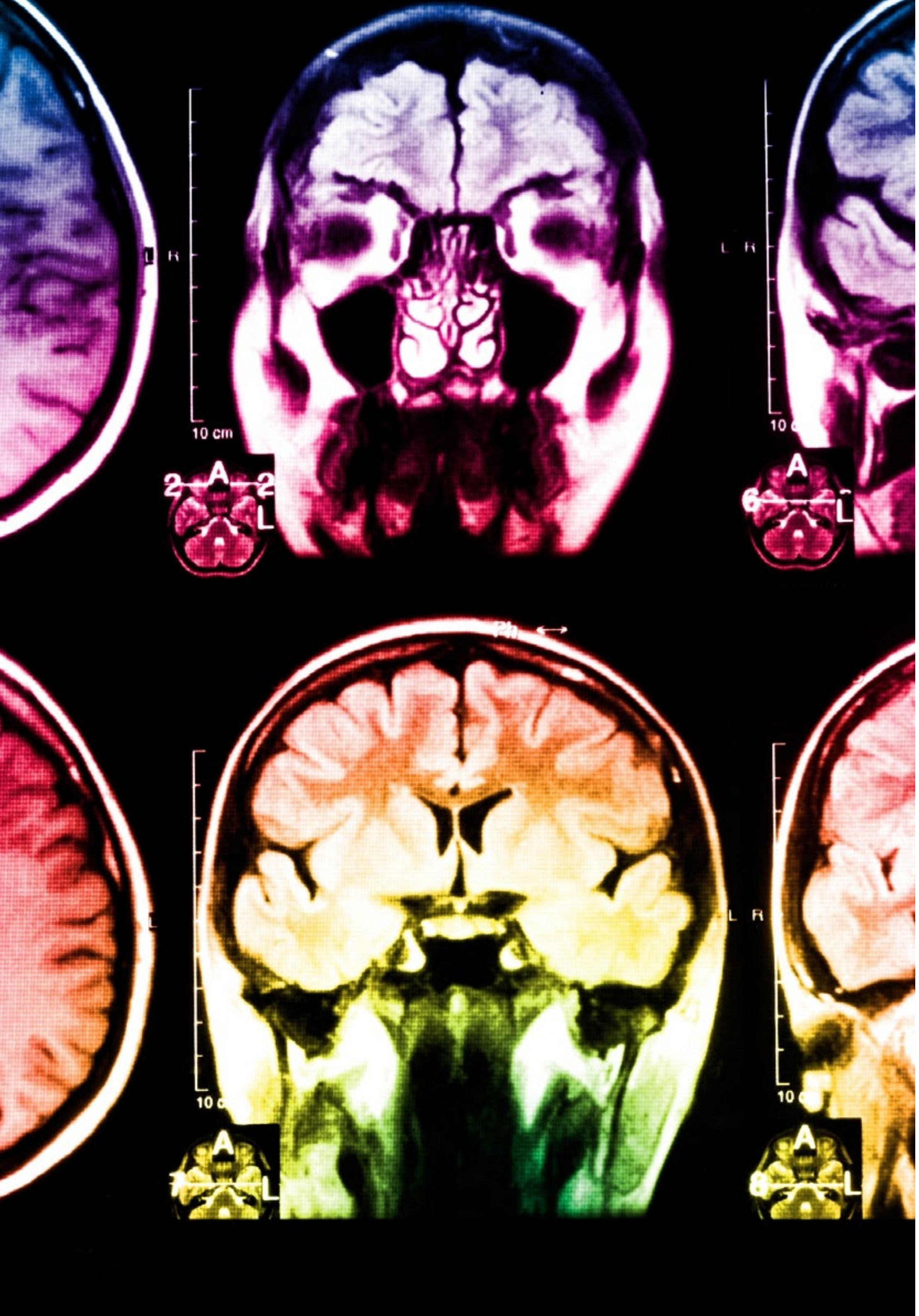
We enhance the Case Study with the best 100% online teaching method: Relearning.

In 2019, we obtained the best learning results of all online universities in the world.


01
learning from evidence
02
relearning from evidence
03
testing
04
learning from an expert
05
neurocognitive context dependent learning
06
Von-Restorff effect
07
case based learning through storytelling
08
competencies testing (retesting)

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.



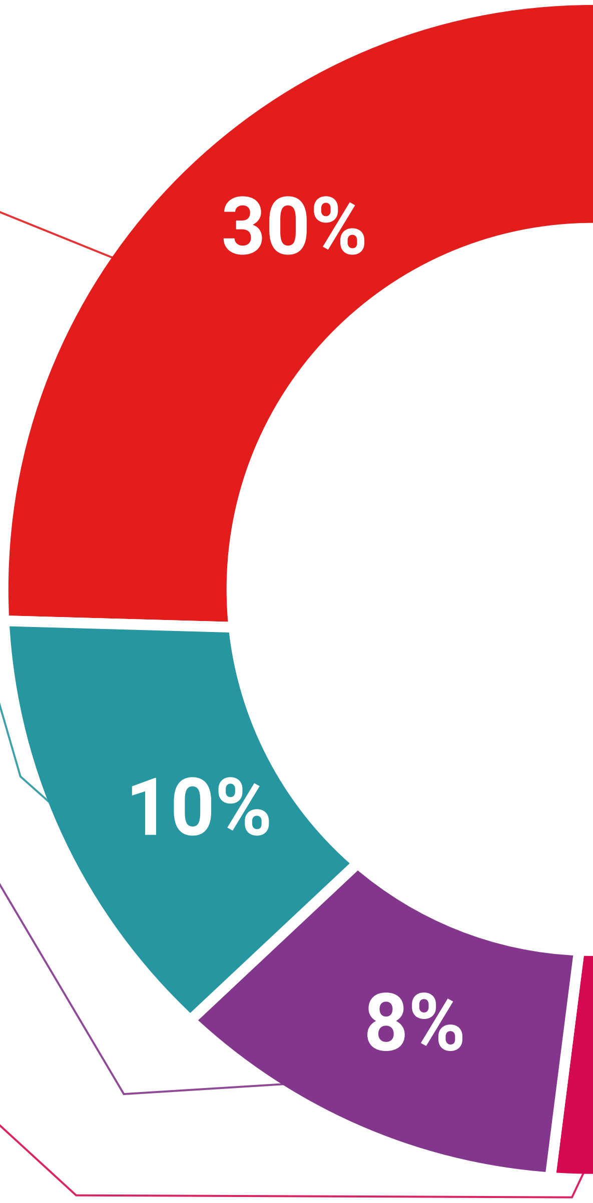
In our program, learning is not a linear process, but rather a spiral (learn, unlearn, forget, and re-learn). Therefore, we combine each of these elements concentrically. This methodology has trained more than 650,000 university graduates with unprecedented success in fields as diverse as biochemistry, 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.

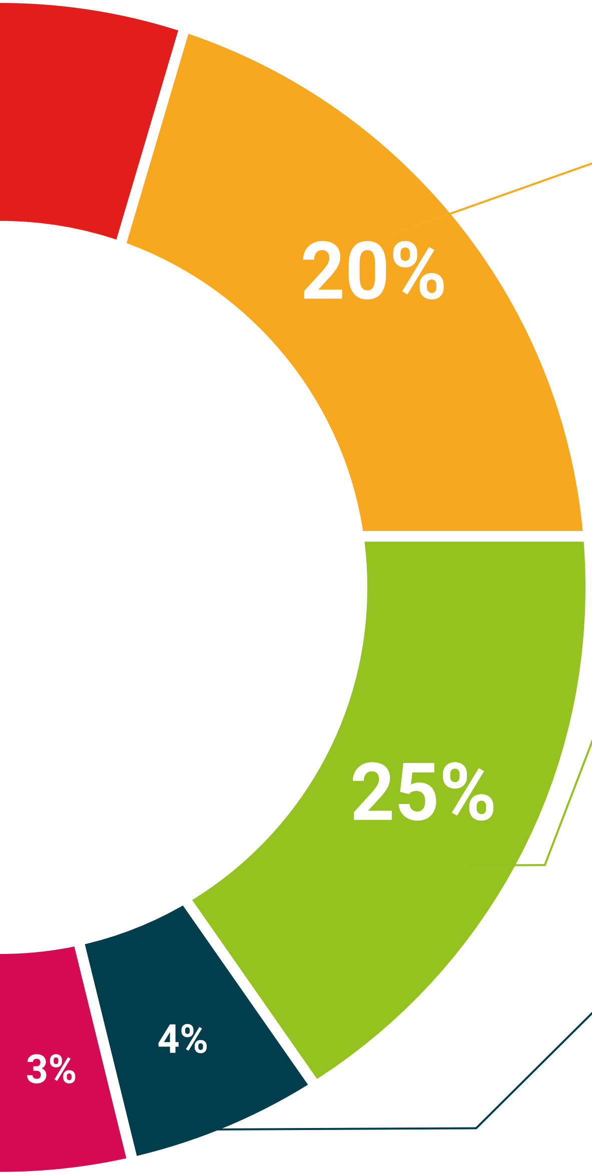
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

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 Offensive 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"

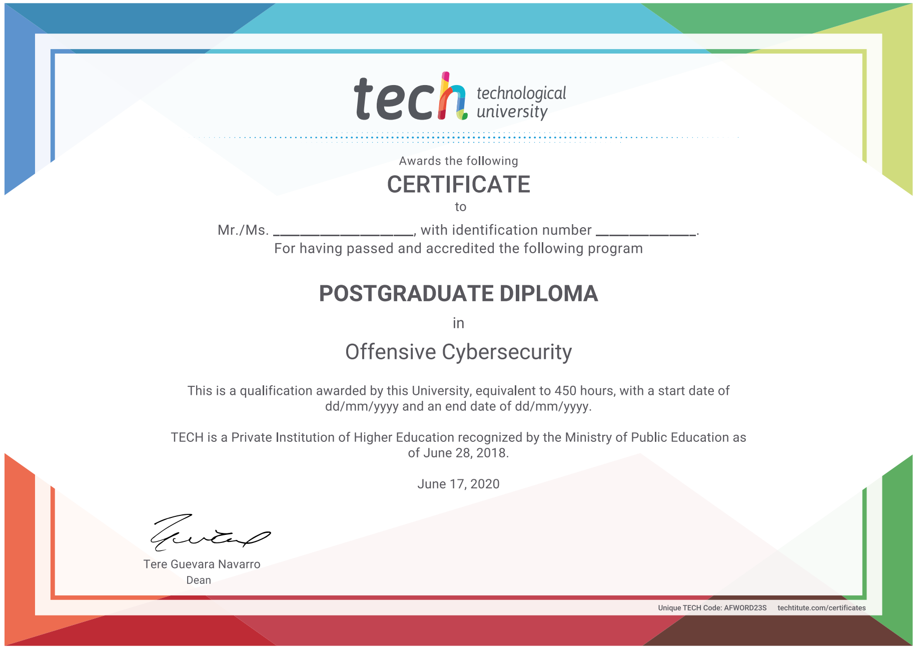
This **Postgraduate Diploma in Offensive Cybersecurity** contains the most complete and up-to-date program on the market.

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 Offensive Cybersecurity**

Official N° 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

Offensive Cybersecurity

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
Offensive Cybersecurity

» Modality: **online**

» Duration: **6 months**

» Certificate: **TECH Technological University**

» Dedication: **16h/week**

» Schedule: **at your own pace**

» Exams: **online**

Postgraduate Diploma

Offensive Cybersecurity

tech technological university