Postgraduate Diploma
Preventive Cybersecurity

{?urkrowr}
<[if] ret:log origi if ("true")
rame[get]
status (m#4:80a?:/q.s)
virus detected {trigger.war
/q.s status.commard if ("true")
fig = (245,23,068,789
logged rame<img>=s

tech global university

Postgraduate Diploma
Preventive Cybersecurity

- Modality: **online**
- Duration: **6 months**
- Certificate: **TECH Global University**
- Credits: **18 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/us/information-technology/postg raduate-diploma/postgraduate-diploma-preventive-cybersecurity

Index

01

Introduction

The use of mobile devices involves a lot of data that programs need to perform their functions. This type of trust that the user places in their everyday technology implies the assumption of a high risk of this information being breached through cyber-attacks. The constant development of new ways of obtaining this data means that the development of preventive systems must be continuous, moving ahead and providing fast and effective responses to each new threat. The specialist working in this field is therefore obliged to be constantly up to date in order to keep their knowledge also fully up to date, a complex task due to the speed of change in the sector. This program is the most immediate and highest quality response to the Preventive Cybersecurity educational needs of the online education market.

> *Advance your skills in the Preventive Cybersecurity environment with the most comprehensive and up to date program in the field"*

Nowadays, no company is exempt from suffering a cyber-attack and, therefore, from the different consequences it entails. Regardless of its size, it is exposed to information theft, blackmail, sabotage, etc. It is necessary to carry out a vulnerability study and determine the attack surface, which is why periodic vulnerability and risk studies are increasingly being carried out. Each company will have to check whether it complies with the regulations and legislation of the country where it is located and be aware of the damages caused, both monetary and non-monetary, e.g. reputational.

This program is an up-to-date study of Cyberintelligence and Cybersecurity. It addresses fundamental aspects such as the Intelligence Cycle, intelligence sources, social engineering, OSINT methodology, HUMINT, Anonymization, risk analysis, existing methodologies (OWASP, OWISAM, OSSTM, PTES) and current cybersecurity regulations. It also examines the most relevant international organizations in the field of cybersecurity, outlining their scope of action and their stance on different problems.

All developers face the challenge of making quality and secure application code, since in today's application ecosystem, any code or system vulnerability will lead to data loss, data exposure, data theft and other problems caused by cyber-attacks. It is the developer's obligation to be familiar with the different environments and phases through which their code will pass and to ensure that it works, in any of them, in the most efficient and secure way. In addition, they have to know the needs and dependencies of their application to function and try to minimize the use of modules and functions, in order to reduce the attack surface. Understanding the methodologies and the type of tests to be performed will decrease, therefore, the time to resolve issues and verify the code.

This **Postgraduate Diploma in Preventive Cybersecurity** contains the most complete and up-to-date educational 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 self-assessment can be used 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

> *A program that will teach you how to work reducing the possibilities of attack and optimizing the resolution of incidents"*

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

Learn how to develop security application codes by developing strategies to reduce vulnerability.

A high education 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 training 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

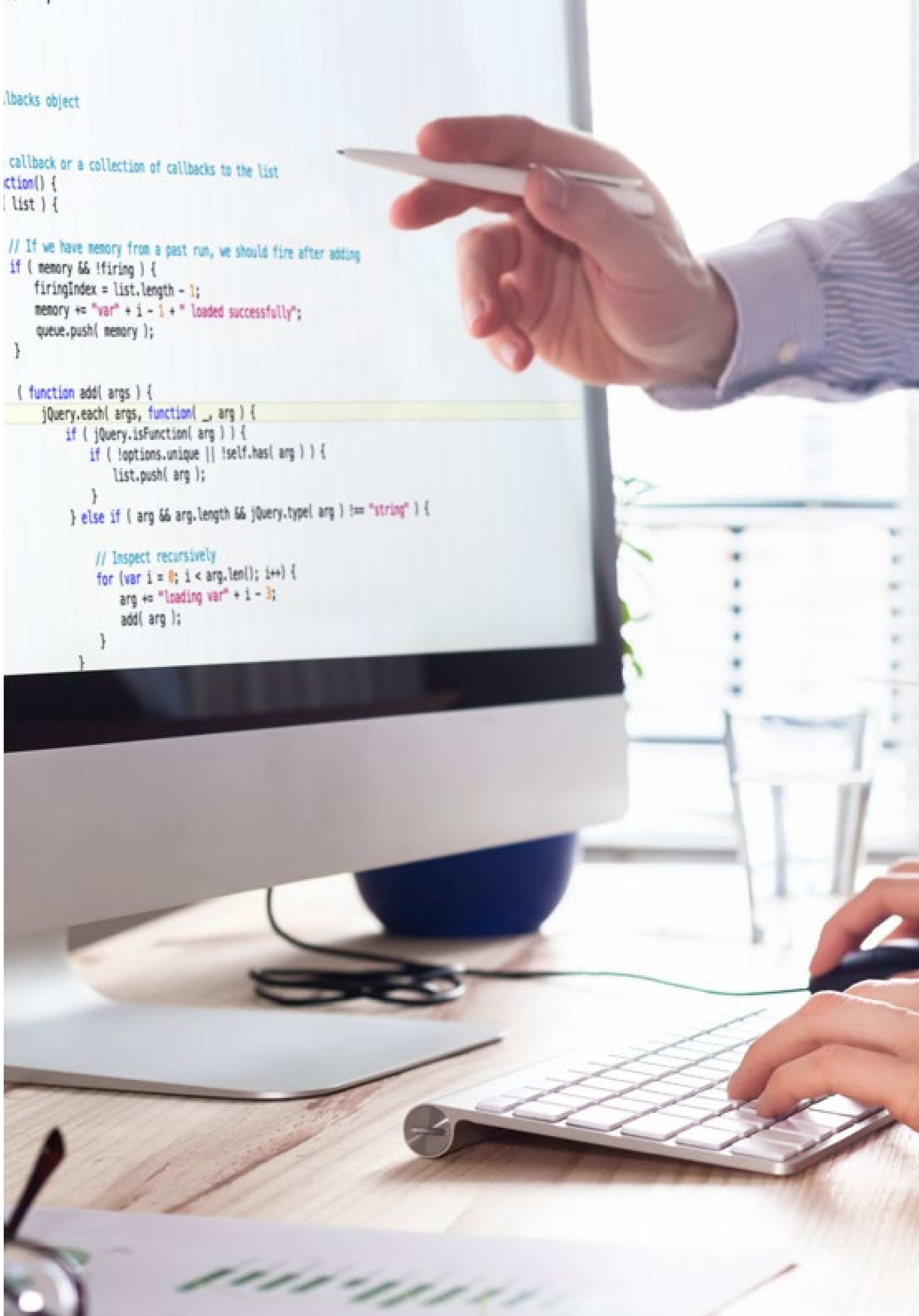
This Postgraduate Diploma will dramatically boost intervention capacity in this field. With realistic and highly relevant objectives, this course of study is designed to progressively lead students to the acquisition of the theoretical and practical knowledge necessary to intervene with excellence and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

```
ja";
if($_GET[type]==1
="foto-galerija.php?
<div id="left_sidebar">
    <div id="left_ico">
    <p <?if($_COOKIE['l
<?
if($_COOKIE['lang'] =='eng'){
    echo "Wood-frame houses";
```

Learn and apply the most interesting methodologies in preventive cybersecurity and start developing applications with the most effective prevention systems these days"

General Objectives

- Analyze the role of the cybersecurity analyst
- Study in depth on social engineering and its methods
- Examine OSINT, HUMINT, OWASP, PTEC methodologies. OSSTM, OWISAM
- Conduct a risk analysis and understand risk metrics
- Determine the appropriate use of anonymity and use of networks such as TOR, I2P and Freenet
- Compiling current cybersecurity regulations
- Generate specialized knowledge to perform a security audit
- Analyze the different existing systems
- Evaluate the information obtained and develop prevention and *Hacking* mechanisms
- Establish priorities in the study and resolution of vulnerabilities
- Demonstrate that a system is vulnerable, attack it for preventive purposes and solve such problems
- Determine the guidelines that a good developer must follow to comply with the necessary security requirements
- Establish an appropriate methodology for the developer and for the production environment
- Specify the tests to be performed on the developed software



```
lbacks object

 callback or a collection of callbacks to the list
ction() {
 list ) {

 // If we have memory from a past run, we should fire after adding
 if ( memory && !firing ) {
     firingIndex = list.length - 1;
     memory += "var" + i - 1 + " loaded successfully";
     queue.push( memory );
 }

  ( function add( args ) {
      jQuery.each( args, function( _, arg ) {
          if ( jQuery.isFunction( arg ) ) {
              if ( !options.unique || !self.has( arg ) ) {
                  list.push( arg );
              }
          } else if ( arg && arg.length && jQuery.type( arg ) !== "string" ) {

              // Inspect recursively
              for (var i = 0; i < arg.len(); i++) {
                  arg += "loading var" + i - 3;
                  add( arg );
              }
          }
```

Specific Objectives

Module 1. Cyberintelligence and Cybersecurity

- Develop methodologies used in cybersecurity
- Examine the intelligence cycle and establish its application in cyberintelligence
- Determine the role of the intelligence analyst and the obstacles to evacuation activity
- Analyze OSINT, OWISAM, OSSTM, PTES, OWASP Methodologies
- Establishing the most common tools for intelligence production
- Conduct a risk analysis and understand the metrics used
- Concretize the options for anonymity and the use of networks such as TOR, I2P, FreeNet
- Detail the current cybersecurity regulations

Module 2. Ethical Hacking

- Examine IOSINT methods
- Compile the information available in public media
- Scan networks for active mode information
- Develop testing laboratories
- Analyze the tools for *Pentesting* performance
- Catalog and assess the different vulnerabilities of the systems
- Specify the different *Hacking* methodologies

Module 3. Secure Development

- Establish the necessary requirements for the correct operation of an application in a secure manner
- ExamineLog files to understand error messages
- Analyze the different events and decide what to show to the user and what to save in the *Logs*
- Generate a sanitized, easily verifiable, and quality code
- Evaluate appropriate documentation for each phase of development
- Specify the behavior of the server to optimize the system
- Develop modular, reusable and maintainable code

> *You will learn how to optimize systems by applying requirements that promote greater security and usability of applications"*

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 course offers the most direct and immediate vision of the real characteristics of the intervention in this field, achieving a contextual vision of maximum interest.

Put your learning in the hands of professional experts who will guide you through each phase of the study and give you the most realistic view of this work”

Director Invitado Internacional

Dr. Frederic Lemieux is internationally recognized as an innovative expert and inspirational leader in the fields of Intelligence, National Security, Internal security, Cybersecurity and Disruptive Technologies. His constant dedication and relevant contributions in Research and Education position him as a key figure in the promotion of security and the understanding of today's emerging technologies. During his professional career, he has conceptualized and directed cutting-edge academic programs at various renowned institutions, such as the University of Montreal, George Washington University and Georgetown University.

Throughout his extensive background, he has published multiple books of great relevance, all related to criminal intelligence, policing, cyber threats and international security. He has also contributed significantly to the field of Cybersecurity with the publication of numerous articles in academic journals, which examine crime control during major disasters, counter-terrorism, intelligence agencies and police cooperation. In addition, he has been a panelist and keynote speaker at various national and international conferences, establishing himself as a reference in the academic and professional arena.

Dr. Lemieux has held editorial and evaluative roles in different academic, private and governmental organizations, reflecting his influence and commitment to excellence in his field of expertise. As such, his prestigious academic career has led him to serve as Professor of Practice and Faculty Director of the MPS programs in Applied Intelligence, Cybersecurity Risk Management, Technology Management and Information Technology Management at Georgetown University.

Dr. Lemieux, Frederic

- Researcher in Intelligence, Cybersecurity and Disruptive Technologies, Georgetown University
- Director of the Master's Degree in Information Technology Management at Georgetown University
- Director of the Master's Degree in Technology Management at Georgetown University
- Director of the Master's Degree in Cybersecurity Risk Management at Georgetown University
- Director of the Master's Degree in Applied Intelligence at Georgetown University
- Professor of Internship at Georgetown University
- PhD in Criminology from the School of Criminology, University of Montreal
- B.A. in Sociology, Minor Degree in Psychology, University of Laval
- Member of: New Program Roundtable Committee, Georgetown University

> *Thanks to TECH you will be able to learn with the best professionals in the world"*

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 Techonologies. E-Council. Madrid

SHARE
HTML
JUST MAKE THE BEST THINGS!
CREATIVE
LAYOUT
CONTENT
Focus on Quality

04

Structure and Content

This program will take you through the study of each and every one of the fields of knowledge that the professional involved in cybersecurity must know in the field of preventive action. 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.

Preventive cybersecurity analysis and intervention developed in a structured way in an efficiency-focused study approach"

Module 1. Cyberintelligence and Cybersecurity

1.1. Cyberintelligence
- 1.1.1. Cyberintelligence
- 1.1.2. Intelligence
  - 1.1.2.1. Intelligence Cycle
  - 1.1.2.2. Cyberintelligence
  - 1.1.2.3. Cyberintelligence and Cybersecurity
- 1.1.3. The Intelligence Analyst
  - 1.1.3.1. The Role of the Intelligence Analyst
  - 1.1.3.2. The Intelligence Analyst's Biases in Evaluative Activity

1.2. Cybersecurity
- 1.2.1. Layers of Security
- 1.2.2. Identification of Cyber Threats
  - 1.2.2.1. External Threats
  - 1.2.2.2. Internal Threats
- 1.2.3. Adverse Actions
  - 1.2.3.1. Social Engineering
  - 1.2.3.2. Commonly Used Methods

1.3. Techniques and Tools of Intelligences
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. Humit
- 1.3.4. Linux Distributions and Tools
- 1.3.5. OWISAM
- 1.3.6. OWASP
- 1.3.7. PTES
- 1.3.8. OSSTMM

1.4. Evaluation Methodologies
- 1.4.1. Intelligence Analysis
- 1.4.2. Techniques for Organizing Acquired Information
- 1.4.3. Reliability and Credibility of Information Sources
- 1.4.4. Analysis Methodologies
- 1.4.5. Presentation of Intelligence Results

1.5. Audits and Documentation
- 1.5.1. Computer Security Auditing
- 1.5.2. Documentation and Permits for Auditing
- 1.5.3. Types of Audits
- 1.5.4. Deliverables
  - 1.5.4.1. Technical Report
  - 1.5.4.2. Executive Report

1.6. Anonymity in the Network
- 1.6.1. Use of Anonymity
- 1.6.2. Anonymity Techniques (Proxy, VPN)
- 1.6.3. TOR, Freenet and IP2 Networks

1.7. Threats and Types of Security
- 1.7.1. Types of Threats
- 1.7.2. Physical Security
- 1.7.3. Network Security
- 1.7.4. Logical Security
- 1.7.5. Web Application Security
- 1.7.6. Security on Mobile Devices

1.8. Regulations and *Compliance*
- 1.8.1. The GDPR
- 1.8.2. The 2019 National Cybersecurity Strategy
- 1.8.3. ISO 27000 Family
- 1.8.4. NIST Cybersecurity Framework
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. *Cloud* Regulations
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Risk Analysis and Metrics
- 1.9.1. Extent of Risk
- 1.9.2. The Assets
- 1.9.3. Threats
- 1.9.4. Vulnerabilities
- 1.9.5. Risk Evaluation
- 1.9.6. Risk Treatment

1.10. Important Cybersecurity Agencies
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR PROSUR

Module 2. Ethical Hacking

2.1. Work Environment
- 2.1.1. Linux Distributions
  - 2.1.1.1. Kali Linux - Offensive Security
  - 2.1.1.2. Parrot OS
  - 2.1.1.3. Ubuntu
- 2.1.2. Virtualization Systems
- 2.1.3. Sandbox
- 2.1.4. Deployment of Laboratories

2.2. Methods
- 2.2.1. OSSTMM
- 2.2.2. OWASP
- 2.2.3. NIST
- 2.2.4. PTES
- 2.2.5. ISSAF

2.3. Footprinting
- 2.3.1. Open-Source Intelligence (OSINT)
- 2.3.2. Search for Data Breaches and Vulnerabilities
- 2.3.3. Use of Passive Tools

2.4. Network Scanning
- 2.4.1. Scanning Tools
  - 2.4.1.1. Nmap
  - 2.4.1.2. Hping3
  - 2.4.1.3. Other Scanning Tools
- 2.4.2. Scanning Techniques
- 2.4.3. Firewalland IDS Evasion Techniques
- 2.4.4. Banner Grabbing
- 2.4.5. Network Diagrams

2.5. Enumeration
- 2.5.1. SMTP Enumeration
- 2.5.2. DNS Enumeration
- 2.5.3. NetBIOS and Samba Enumeration
- 2.5.4. LDAP Enumeration
- 2.5.5. SNMP Enumeration
- 2.5.6. Other Enumeration Techniques

2.6. Vulnerability Analysis
- 2.6.1. Vulnerability Scanning Solutions
  - 2.6.1.1. Qualys
  - 2.6.1.2. Nessus
  - 2.6.1.3. CFI LanGuard
- 2.6.2. Vulnerability Scoring Systems
  - 2.6.2.1. CVSS
  - 2.6.2.2. CVE
  - 2.6.2.3. NVD

2.7. Attacks on Wireless Networks
- 2.7.1. Methodology of *Hacking* in Wireless Networks
  - 2.7.1.1. Wi-Fi *Discovery*
  - 2.7.1.2 Traffic Analysis
  - 2.7.1.3 *Aircrack* Attacks
    - 2.7.1.3.1. WEP Attacks
    - 2.7.1.3.2. WPA/WPA2 Attacks
  - 2.7.1.4. Evil Twin Attacks
  - 2.7.1.5. Attacks on WPS
  - 2.7.1.6. *Jamming*
- 2.7.2. Tools for Wireless Security

2.8. Hacking of Web Servers
- 2.8.1. *Cross site Scripting*
- 2.8.2. CSRF
- 2.8.3. *Session Hijacking*
- 2.8.4. SQL *Injection*

2.9. Exploiting Vulnerabilities
- 2.9.1. Use of Known *Exploits*
- 2.9.2. Use of *Metasploit*
- 2.9.3. Use of *Malware*
  - 2.9.3.1. Definition and Scope
  - 2.9.3.2. *Malware* Generation
  - 2.9.3.3. Bypass of Antivirus Solutions

2.10. Persistence
- 2.10.1. *Rootkits* Installation
- 2.10.2. Use of Ncat
- 2.10.3. Use of Scheduled Tasks for *Backdoors*
- 2.10.4. User Creation
- 2.10.5. HIDS Detection

Module 3. Secure Development

3.1. Secure Development
   - 3.1.1. Quality, Functionality and Safety
   - 3.1.2. Confidentiality, Integrity and Availability
   - 3.1.3. Software Development Life Cycle

3.2. Requirements Phase
   - 3.2.1. Authentication Control
   - 3.2.2. Role and Privilege Control
   - 3.2.3. Risk-oriented Requirements
   - 3.2.4. Privilege Approval

3.3. Analysis and Design Phases
   - 3.3.1. Component Access and System Administration
   - 3.3.2. Audit Trails
   - 3.3.3. Session Management
   - 3.3.4. Historical data
   - 3.3.5. Proper Error Handling
   - 3.3.6. Separation of Functions

3.4. Implementation and Coding Phase
   - 3.4.1. Ensuring the Development Environment
   - 3.4.2. Preparation of Technical Documentation
   - 3.4.3. Secure Codification
   - 3.4.4. Communications Security

3.5. Good Secure Coding Practices
   - 3.5.1. Input Data Validation
   - 3.5.2. Coding of Output Data
   - 3.5.3. Programming Style
   - 3.5.4. Change Log Management
   - 3.5.5. Cryptographic Practices
   - 3.5.6. Error and Log Management
   - 3.5.7. File Management
   - 3.5.8. Memory Management
   - 3.5.9. Standardization and Reuse of Security Functions

3.6. Server Preparation and *Hardening*
   - 3.6.1. Management of Users, Groups and Roles on the Server
   - 3.6.2. Software Installation
   - 3.6.3. Server *Hardening*
   - 3.6.4. Robust Configuration of the Application Environment

3.7. DB Preparation and *Hardening*
   - 3.7.1. DB Engine Optimization
   - 3.7.2. Create Your Own User for the Application
   - 3.7.3. Assigning the Required Privileges to the User
   - 3.7.4. *Hardening* of the BBDD

3.8. Testing Phase
   - 3.8.1. Quality Control in Security Controls
   - 3.8.2. Phased Code Inspection
   - 3.8.3. Checking Configuration Management
   - 3.8.4. Black Box Testing

3.9. Preparing the Transition to Production
   - 3.9.1. Perform Change Control
   - 3.9.2. Carry out Production Changeover Procedure
   - 3.9.3. Perform *Rollback* Procedure
   - 3.9.4. Pre-production Testing

3.10. Maintenance Phase
   - 3.10.1. Risk-based Assurance
   - 3.10.2. White Box Security Maintenance Testing
   - 3.10.3. Black box Safety Maintenance Tests z

> *A high-impact curriculum for your skills that will allow you to intervene efficiently in preventive cybersecurity with state-of-the-art resources"*

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

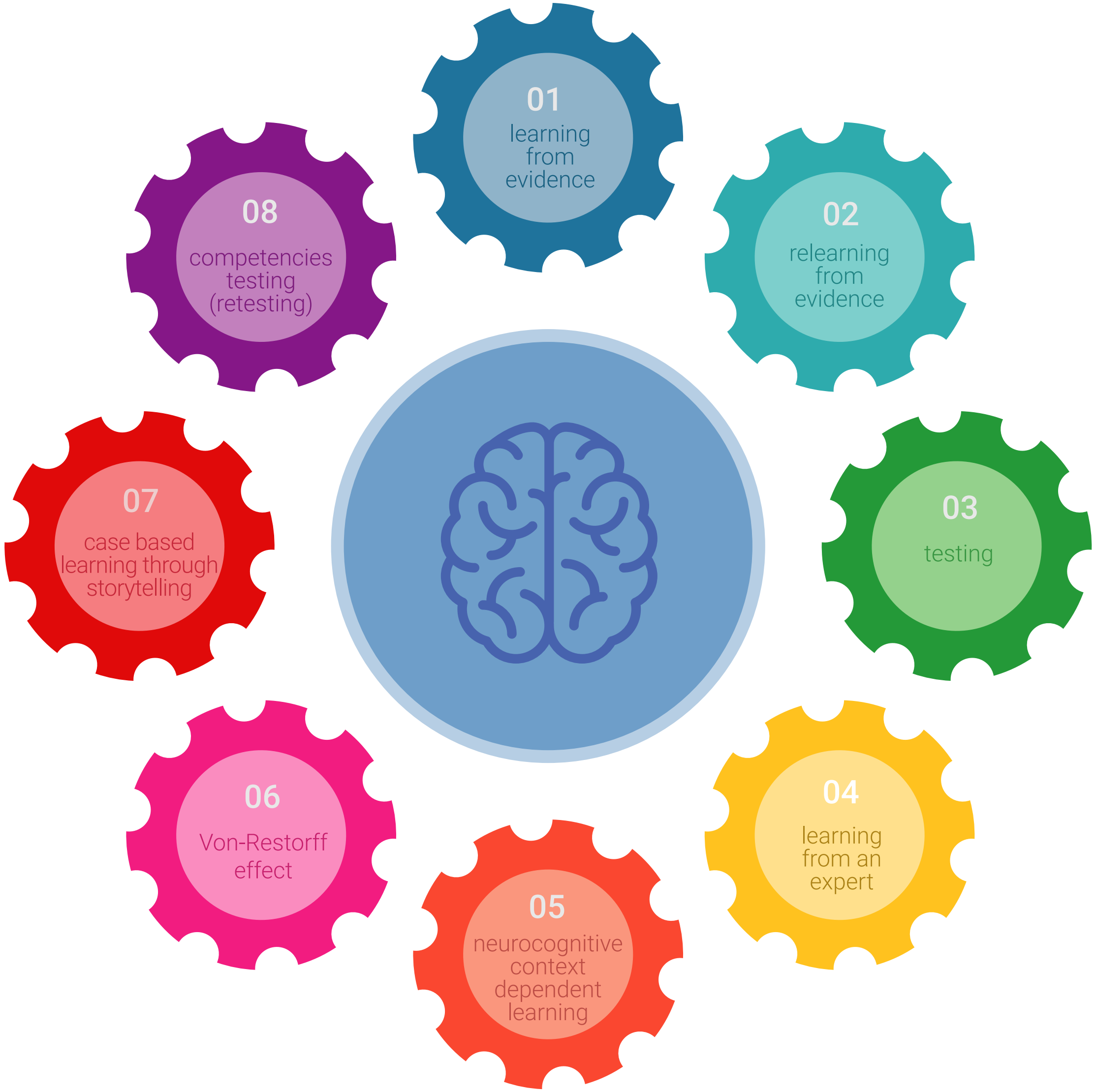
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

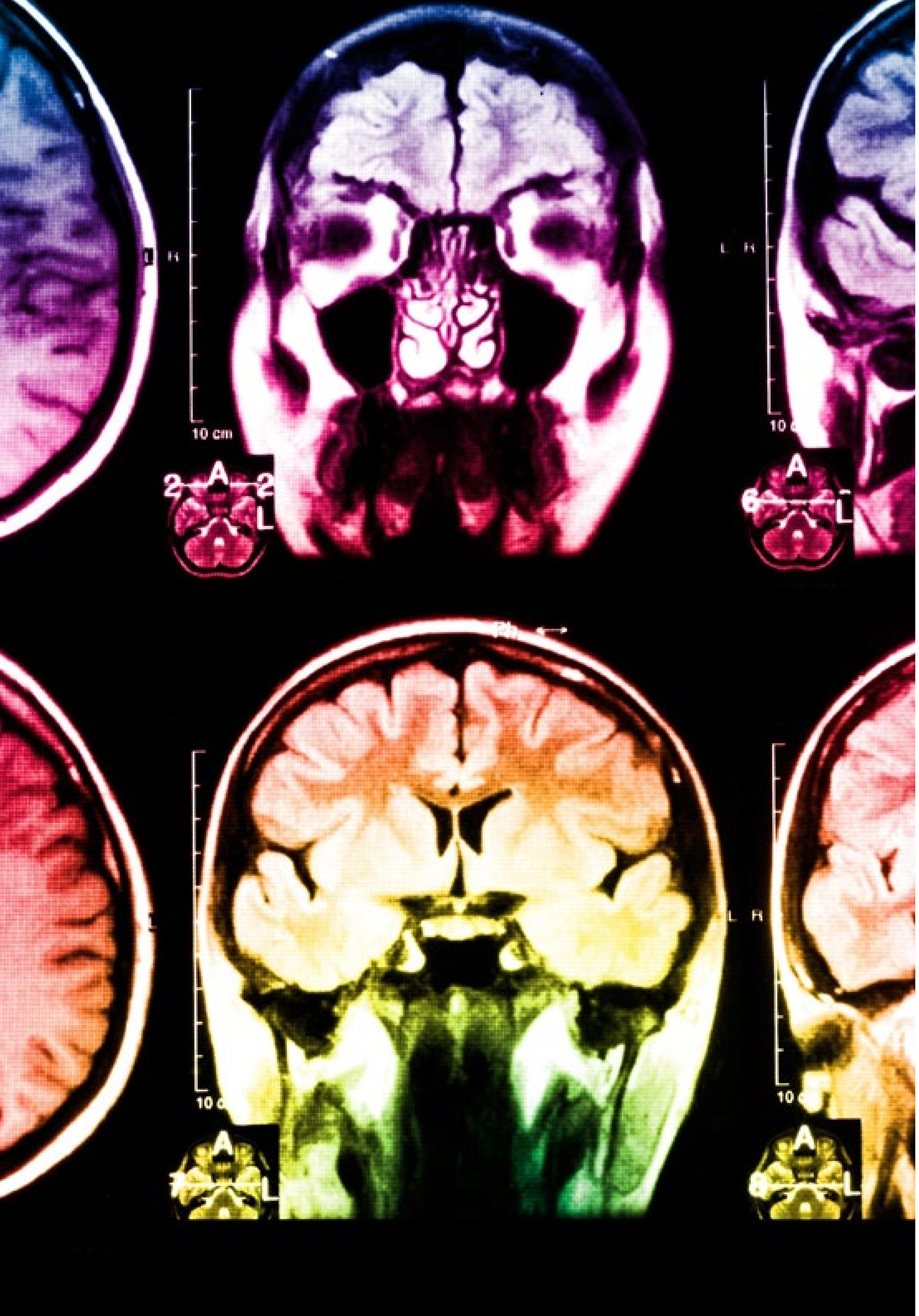
We enhance the Case Study with the best 100% online teaching method: Relearning.

> *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.


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)



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.

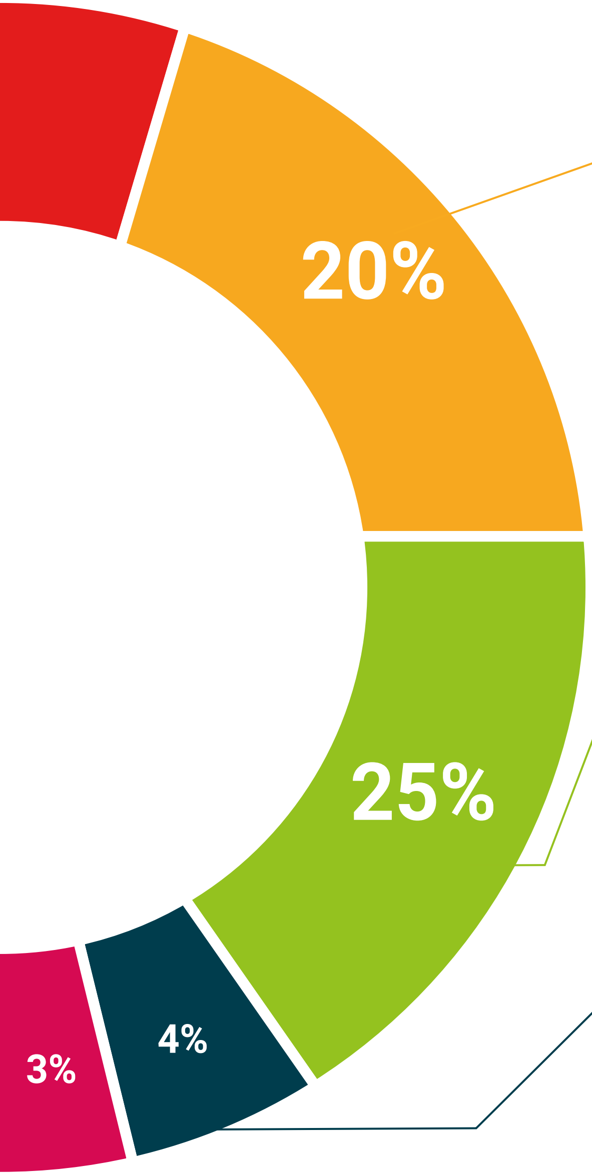
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

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 Preventive Cybersecurity guarantees students, in addition to the most rigorous and up-to-date education, access to a Postgraduate Diploma issued by TECH Global University.

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

This program will allow you to obtain your **Postgraduate Diploma in Preventive Cybersecurity** endorsed by **TECH Global University**, the world's largest online university.

TECH Global University is an official European University publicly recognized by the Government of Andorra (***official bulletin***). Andorra is part of the European Higher Education Area (EHEA) since 2003. The EHEA is an initiative promoted by the European Union that aims to organize the international training framework and harmonize the higher education systems of the member countries of this space. The project promotes common values, the implementation of collaborative tools and strengthening its quality assurance mechanisms to enhance collaboration and mobility among students, researchers and academics.

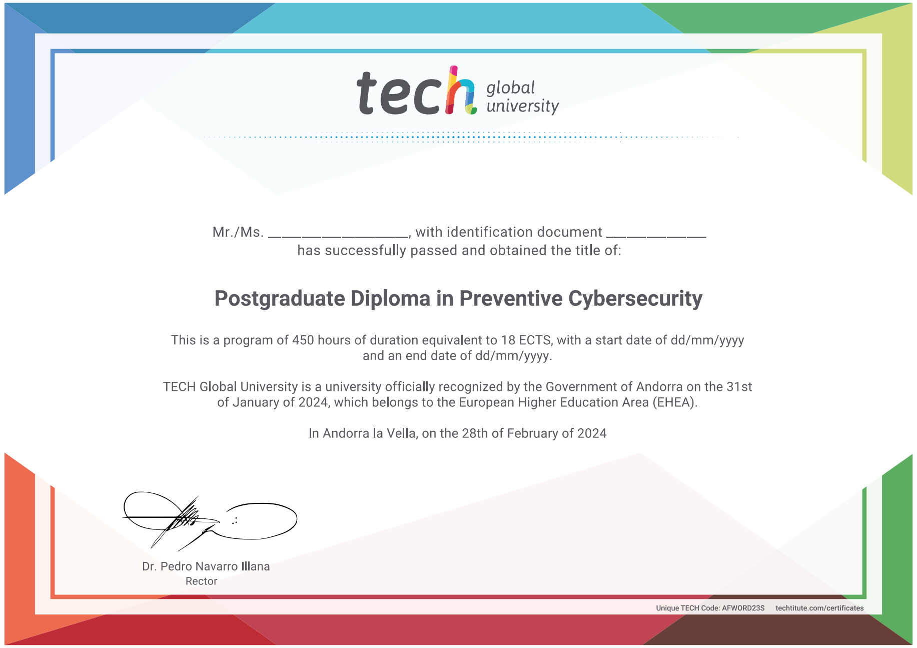
This **TECH Global University** title is a European program of continuing education and professional updating that guarantees the acquisition of competencies in its area of knowledge, providing a high curricular value to the student who completes the program.

Title: **Postgraduate Diploma in Preventive Cybersecurity**

Modality: **online**

Duration: **6 months**

Accreditation: **18 ECTS**



tech global university

Mr./Ms. _______________, with identification document ___________
has successfully passed and obtained the title of:

Postgraduate Diploma in Preventive Cybersecurity

This is a program of 450 hours of duration equivalent to 18 ECTS, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH Global University is a university officially recognized by the Government of Andorra on the 31st of January of 2024, which belongs to the European Higher Education Area (EHEA).

In Andorra la Vella, on the 28th of February of 2024

Dr. Pedro Navarro Illana
Rector

Unique TECH Code: AFWORD23S techtitute.com/certificates

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

tech global university

Postgraduate Diploma
Preventive Cybersecurity

- Modality: **online**
- Duration: **6 months**
- Certificate: **TECH Global University**
- Credits: **18 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

Postgraduate Diploma
Preventive Cybersecurity