Postgraduate Diploma

Computer Security
Defense Measures

tech global university

tech global university

Postgraduate Diploma

Computer Security Defense Measures

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

Website: www.techtitute.com/us/information-technology/postgraduate-diploma/postgraduate-diploma-computer-security-defense-measures

Index

01

Introduction

The financial, business and tourism sectors have suffered an increase in social engineering attacks that jeopardize sensitive and valuable information of the entities themselves and their customers. Cyber attacks continue to be a headache for companies, which is why the number of jobs created to ensure IT security has been increasing in recent years. In response to this need, this program provides IT professionals with a specialization in the field of adopting IT defense measures in the face of any attack. An expert teaching team in the area teaches this qualification in 100% online mode, allowing to acquire a current and comprehensive learning thanks to its extensive multimedia content.

Give the best answer in computer security and prevent companies from falling into social engineering with this Postgraduate Diploma"

Implementing IT security policies entails a cost for companies, but they are willing to bear it due to the high losses that hacking of their systems entails for them, compromising their correct operation and the provision of services to their customers. A key role in this scenario is played by IT professionals.

This Postgraduate Diploma provides students with in-depth learning in computer security defense measures, which start with an analysis of the threats and then classify them correctly in order to find out where a company is more or less vulnerable. Likewise, the teaching team specialized in this subject will provide the essential tools to carry out a computer forensic analysis. In this way, the detection of incidents through IDS/IPS systems and their treatment in SIEM up to the notification and escalation process will be shown.

In order to be at the forefront of security defense, IT professionals will develop, in this qualification, techniques to mitigate denial of service, *Session Hacking* and attacks on web applications. All this, in a 100% online teaching mode, which allows students to balance their professional work with a program that offers multimedia and innovative content. They only need a device with an Internet connection to access a study plan that can be taken at their own pace.

This **Postgraduate Diploma in Computer Security Defense Measures** contains the most complete and up-to-date program on the market. The most important features include:

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

Effectively implement security policies against Session Hijacking, Hacking Web Servers or Mobile Platforms thanks to this Postgraduate Diploma"

Controls the ISO 27035 standard and meets the requirements for a correct incident management. Enroll in this Postgraduate Diploma"

Grow in your professional career with a program that will allow you to deepen in the analysis and control of computer threats.

You are just one click away from enrolling in a Postgraduate Diploma that will open up more career opportunities.

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

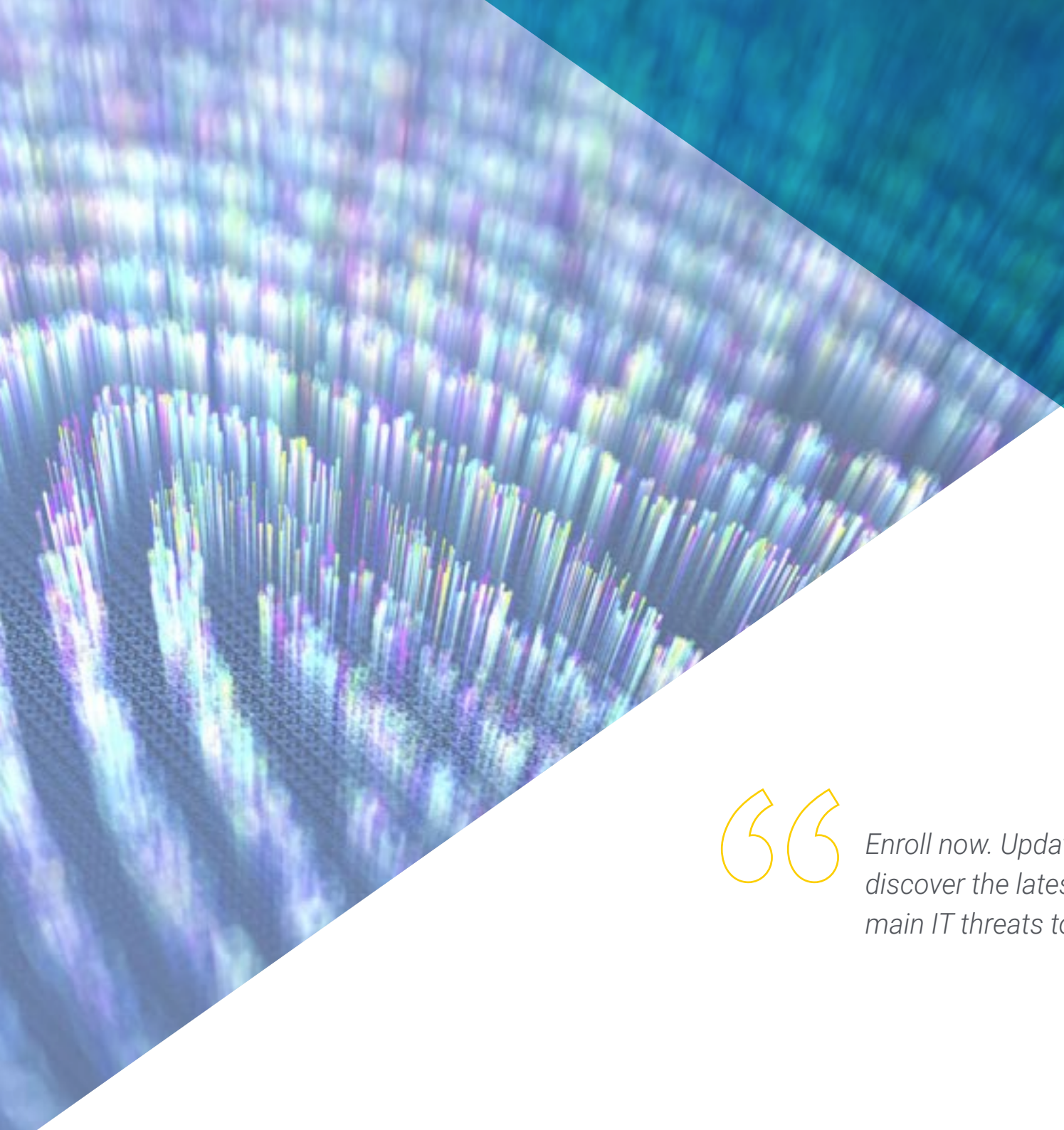
The multimedia content, developed with the latest educational technology, will provide the professional with situated and contextual learning, i.e., a simulated environment that will provide immersive education programmed to learn in real situations.

This program is designed around Problem-Based Learning, whereby the professional must try to solve the different professional practice situations that arise throughout the program. For this purpose, students will be assisted by an innovative interactive video system created by renowned and experienced experts.

02

Objectives

This Postgraduate Diploma proposes an education whose goal is to enable IT professionals to obtain a qualification specialized in the field of security. Thus, throughout this program they will improve their skills in threat analysis, comparing the different management methodologies that will allow them to select the one that best suits the incident. They will also be trained to technically implement measures to mitigate the main threats received by the company. In this way, IT professionals will obtain a qualification that will allow them to progress in the workplace.



Enroll now. Update your knowledge and discover the latest techniques to prevent the main IT threats to a company"

General Objectives

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

Access a university qualification that will provide you with the latest and most effective strategies to manage any IT attack"

Specific Objectives

Module 1. Security Policies for the Analysis of Threats in Computer Systems

- Analyze the meaning of threats
- Determine the phases of preventive threat management
- Compare different threat management methodologies

Module 2. Security Incident Management Policies

- Develop specialized knowledge on how to manage incidents caused by IT security events
- Determine the operation of a security incident handling team
- Analyze the different phases of an IT security event management
- Review standardized protocols for handling security incidents

Module 3. Practical Implementation of Security Policies against Attacks

- Determine the different real attacks to our information system
- Evaluate the various security policies to mitigate attacks
- Technically implement measures to mitigate major threats

03

Course Management

TECH carefully selects all the teaching staff who teach the programs. This Postgraduate Diploma has a highly qualified professional in the field of computer security. The experience as head of security in this area in public and private entities, guarantee students a close knowledge that brings great value to the professional who wants to know firsthand the main measures taken in this field to the main threats suffered. In this way, the practical cases presented are similar to real situations that the students must face in their work environment, and therefore will make them grow professionally.

A teaching staff specialized in computer security will put all their knowledge at your disposal to help you advance in your professional career"

Management

Ms. Fernández Sapena, Sonia

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

Professors

Ms. López García, Rosa María

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

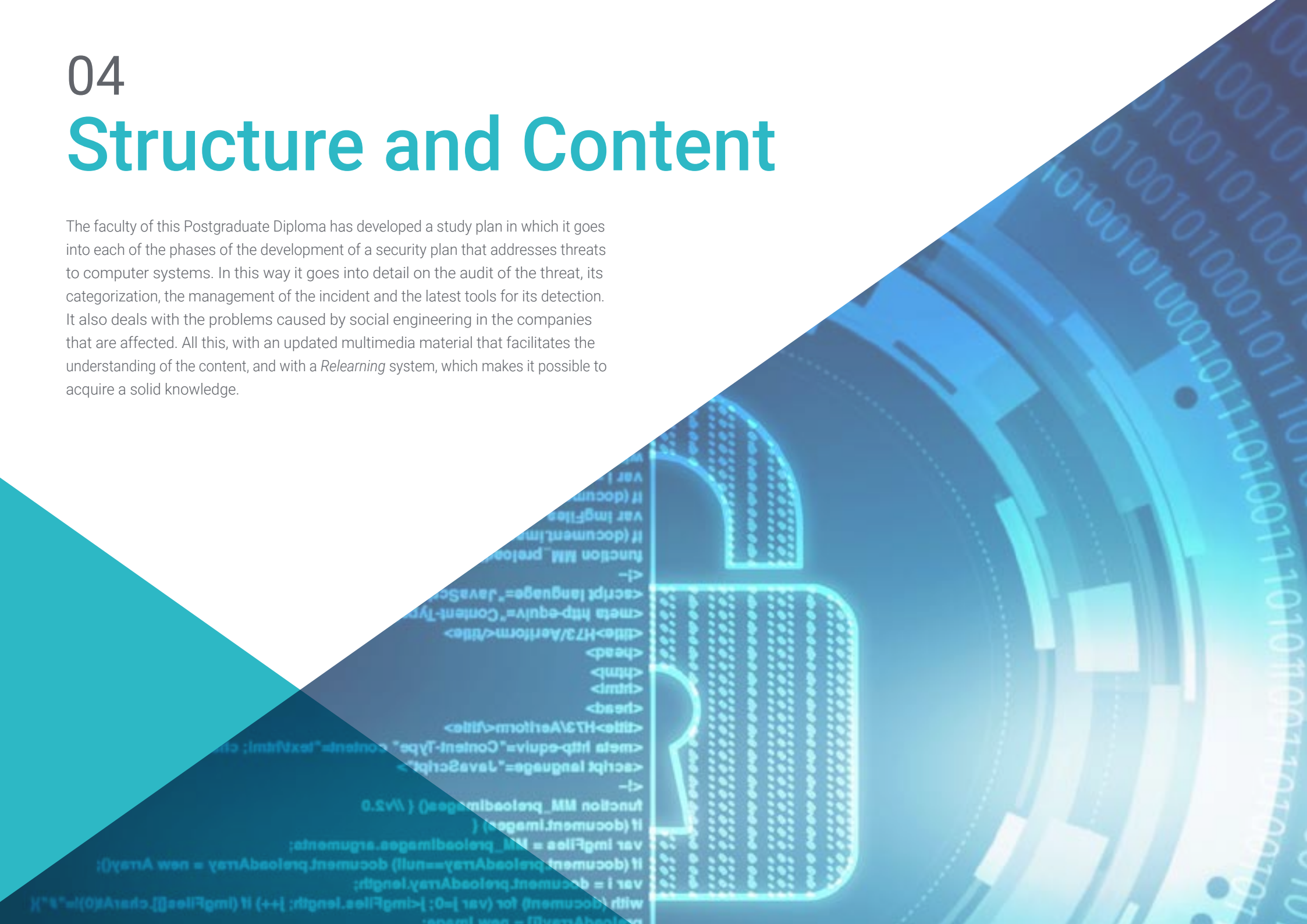
Mr. Oropesiano Carrizosa, Francisco

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

04

Structure and Content

The faculty of this Postgraduate Diploma has developed a study plan in which it goes into each of the phases of the development of a security plan that addresses threats to computer systems. In this way it goes into detail on the audit of the threat, its categorization, the management of the incident and the latest tools for its detection. It also deals with the problems caused by social engineering in the companies that are affected. All this, with an updated multimedia material that facilitates the understanding of the content, and with a *Relearning* system, which makes it possible to acquire a solid knowledge.



Access to a 100% online teaching, flexible, that allows you to go at your own pace. Balance your personal life with quality teaching. Sign up"

Module 1. Security Policies for the Analysis of Threats in Computer Systems

1.1. Threat Management in Security Policies
- 1.1.1. Risk Management
- 1.1.2. Security Risk
- 1.1.3. Threat Management Methodologies
- 1.1.4. Implementation of Methodologies

1.2. Phases of Threat Management
- 1.2.1. Identification
- 1.2.2. Analysis
- 1.2.3. Localization
- 1.2.4. Safeguard Measures

1.3. Audit Systems for Threat Localization
- 1.3.1. Classification and Information Flow
- 1.3.2. Analysis of Vulnerable Processes

1.4. Risk Classification
- 1.4.1. Types of Risk
- 1.4.2. Calculation of Threat Probability
- 1.4.3. Residual Risk

1.5. Risk Treatment
- 1.5.1. Implementation of Safeguard Measures
- 1.5.2. Transfer or Assume

1.6. Control Risks
- 1.6.1. Continuous Risk Management Process
- 1.6.2. Implementation of Security Metrics
- 1.6.3. Strategic Model of Information Security Metrics

1.7. Practical Methodologies for Threat Analysis and Control
- 1.7.1. Threat Catalog
- 1.7.2. Catalog of Control Measures
- 1.7.3. Safeguards Catalog

1.8. ISO 27005
- 1.8.1. Risk Identification
- 1.8.2. Risk Analysis
- 1.8.3. Risk Evaluation

1.9. Risk, Impact and Threat Matrix
- 1.9.1. Data, Systems and Personnel
- 1.9.2. Threat Probability
- 1.9.3. Magnitude of Damage

1.10. Design of Phases and Processes in Threat Analysis
- 1.10.1. Identification of Critical Organizational Elements
- 1.10.2. Determination of Threats and Impacts
- 1.10.3. Impact and Risk Analysis
- 1.10.4. Methods

Module 2. Security Incident Management Policies

2.1. Information Security Incident Management Policies and Enhancements
- 2.1.1. Incident Management
- 2.1.2. Responsibilities and Procedures
- 2.1.3. Event Notification

2.2. Intrusion Detection and Prevention Systems (IDS/IPS)
- 2.2.1. System Operating Data
- 2.2.2. Types of Intrusion Detection Systems
- 2.2.3. Criteria for IDS/IPS Placement

2.3. Security Incident Response
- 2.3.1. Data Collection Procedure
- 2.3.2. Intrusion Verification Process
- 2.3.3. CERT Organizations

2.4. Intrusion Attempt Notification and Management Process
- 2.4.1. Responsibilities in the Notification Process
- 2.4.2. Classification of Incidents
- 2.4.3. Resolution and Recovery Process

2.5. Forensic Analysis as a Security Policy
- 2.5.1. Volatile and Non-Volatile Evidence
- 2.5.2. Analysis and Collection of Electronic Evidence
  - 2.5.2.1. Analysis of Electronic Evidence
  - 2.5.2.2. Collection of Electronic Evidence

2.6. Intrusion Detection and Prevention Systems (IDS/IPS) Tools
- 2.6.1. Snort
- 2.6.2. Suricata
- 2.6.3. SolarWinds

2.7. Event Centralizing Tools
- 2.7.1. SIM
- 2.7.2. SEM
- 2.7.3. SIEM

2.8. CCN-STIC Security Guide 817
- 2.8.1. Cyber Incident Management
- 2.8.2. Metrics and Indicators

2.9. NIST SP800-61
- 2.9.1. Computer Security Incident Response Capability
- 2.9.2. Handling an Incident
- 2.9.3. Coordination and Information Sharing

2.10. ISO 27035
- 2.10.1. ISO 27035 Standard. Incident Management Principles
- 2.10.2. Incident Management Plan Preparation Guidelines
- 2.10.3. Incident Response Operations Guides

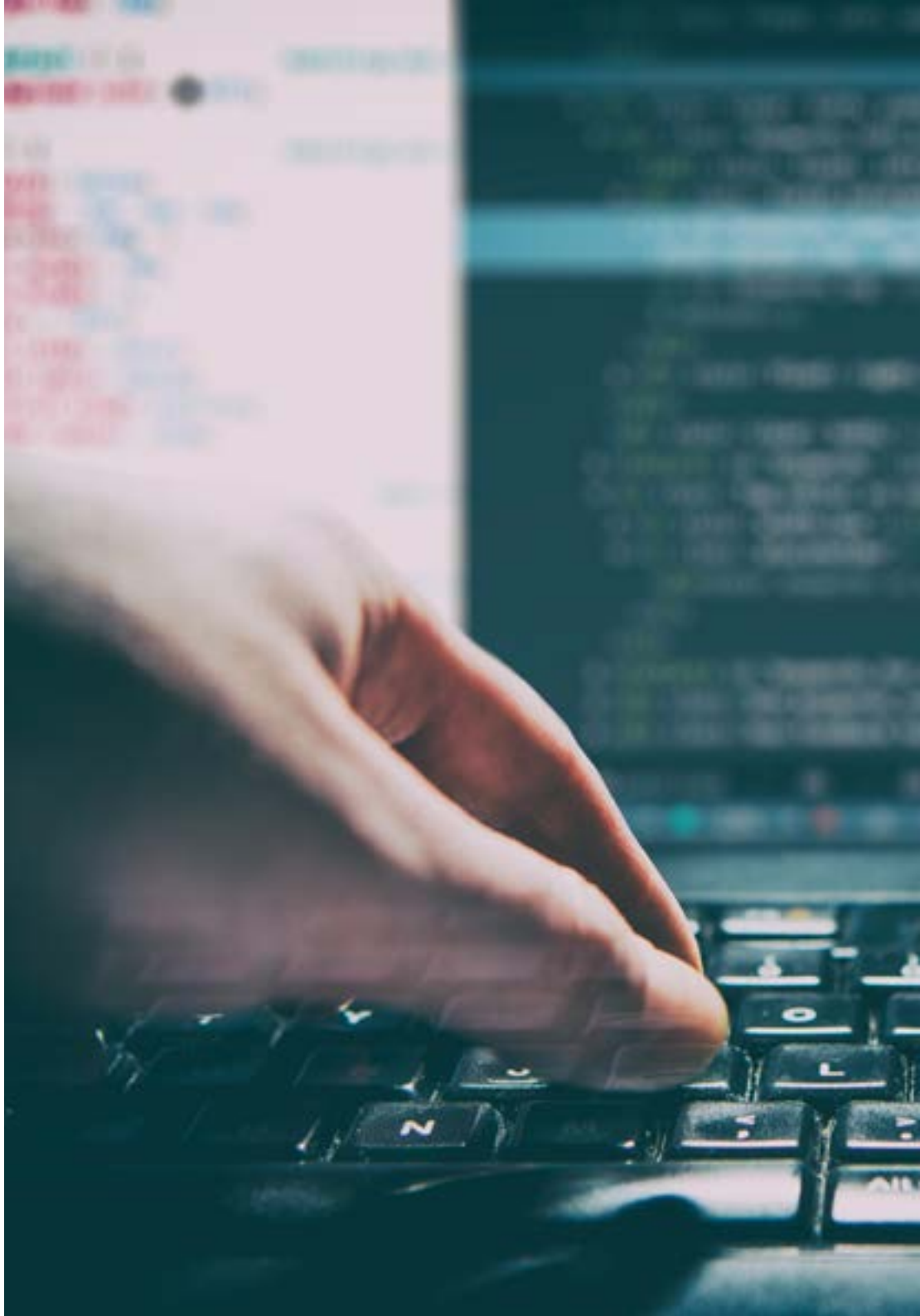
Module 3. Practical Implementation of Security Policies against Attacks

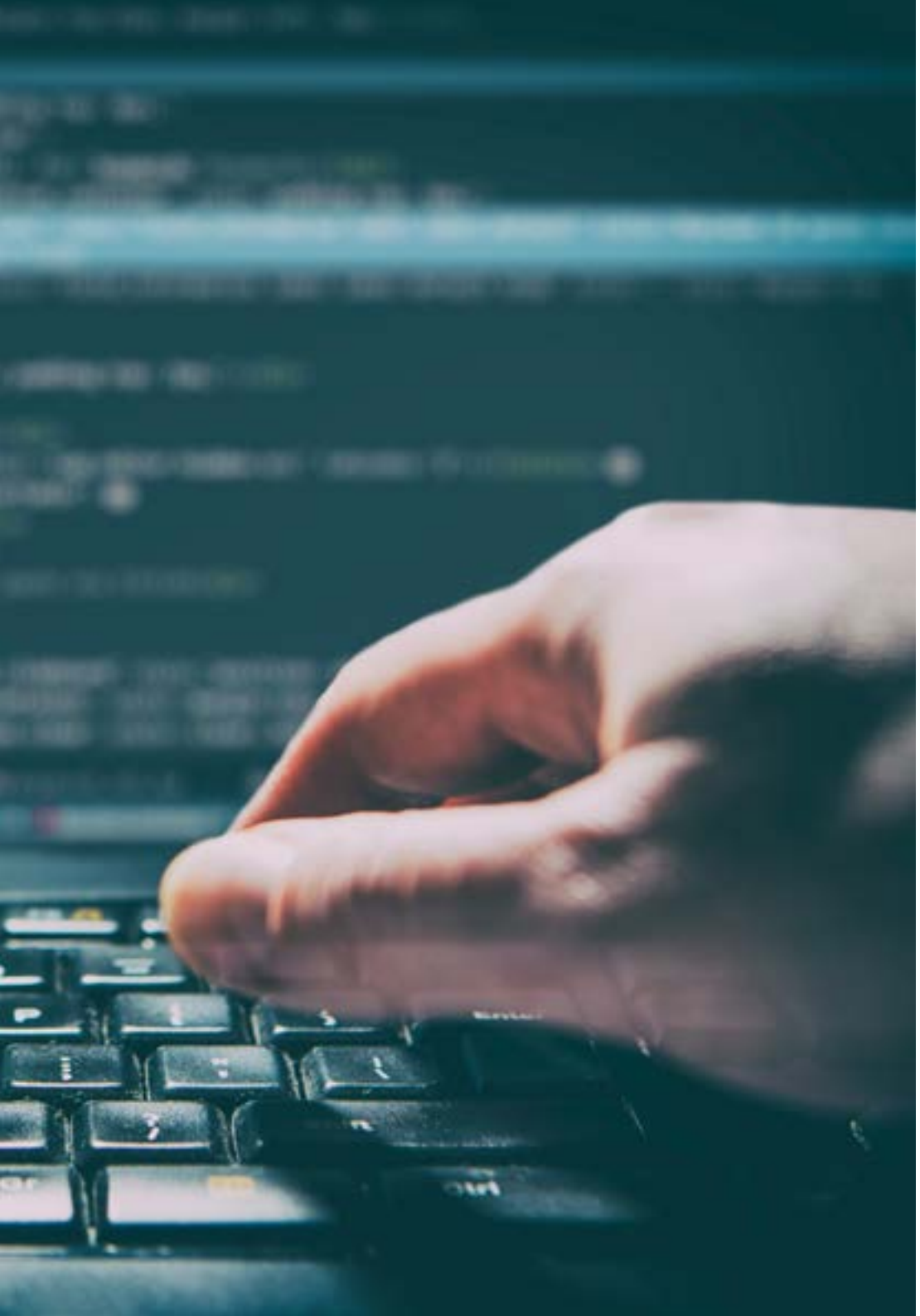
3.1. System Hacking
- 3.1.1. Risks and Vulnerabilities
- 3.1.2. Countermeasures

3.2. DoS Attack
- 3.2.1. Risks and Vulnerabilities
- 3.2.2. Countermeasures

3.3. Session Hijacking
- 3.3.1. The Process of Hijacking
- 3.3.2. Hijacking Countermeasures

3.4. Evading IDS, Firewalls and Honeypots
- 3.4.1. Avoidance Techniques
- 3.4.2. Implementation of Countermeasures





3.5. Hacking Web Servers
  3.5.1. Attacks on Web Servers
  3.5.2. Implementation of Defense Measures
3.6. Hacking Web Applications
  3.6.1. Attacks on Web Applications
  3.6.2. Implementation of Defense Measures
3.7. Hacking Wireless Networks
  3.7.1. Vulnerabilities in Wi-Fi Networks
  3.7.2. Implementation of Defense Measures
3.8. Hacking Mobile Platforms
  3.8.1. Vulnerabilities of Mobile Platforms
  3.8.2. Implementation of Countermeasures
3.9. Ramsonware
  3.9.1. Ramsonware Vulnerabilities
  3.9.2. Implementation of Countermeasures
3.10. Social Engineering
  3.10.1. Types of Social Engineering
  3.10.2. Countermeasures for Social Engineering

Case studies and multimedia content are the most powerful tools of this Postgraduate Diploma. Get trained in this field and advance your career"

05

Methodology

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

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

Discover Relearning, a system that abandons conventional linear learning, to take you through cyclical teaching systems: a way of learning that has proven to be extremely effective, especially in subjects that require memorization"

Case Study to contextualize all content

Our program offers a revolutionary approach to developing skills and knowledge. Our goal is to strengthen skills in a changing, competitive, and highly demanding environment.

At TECH, you will experience a learning methodology that is shaking the foundations of traditional universities around the world"

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

The student will learn to solve complex situations in real business environments through collaborative activities and real cases.

A learning method that is different and innovative

This TECH program is an intensive educational program, created from scratch, which presents the most demanding challenges and decisions in this field, both nationally and internationally. This methodology promotes personal and professional growth, representing a significant step towards success. The case method, a technique that lays the foundation for this content, ensures that the most current economic, social and professional reality is taken into account.

> *Our program prepares you to face new challenges in uncertain environments and achieve success in your career"*

The case method has been the most widely used learning system among the world's leading Information Technology schools for as long as they have existed. The case method was developed in 1912 so that law students would not only learn the law based on theoretical content. It consisted of presenting students with real-life, complex situations for them to make informed decisions and value judgments on how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

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

Relearning Methodology

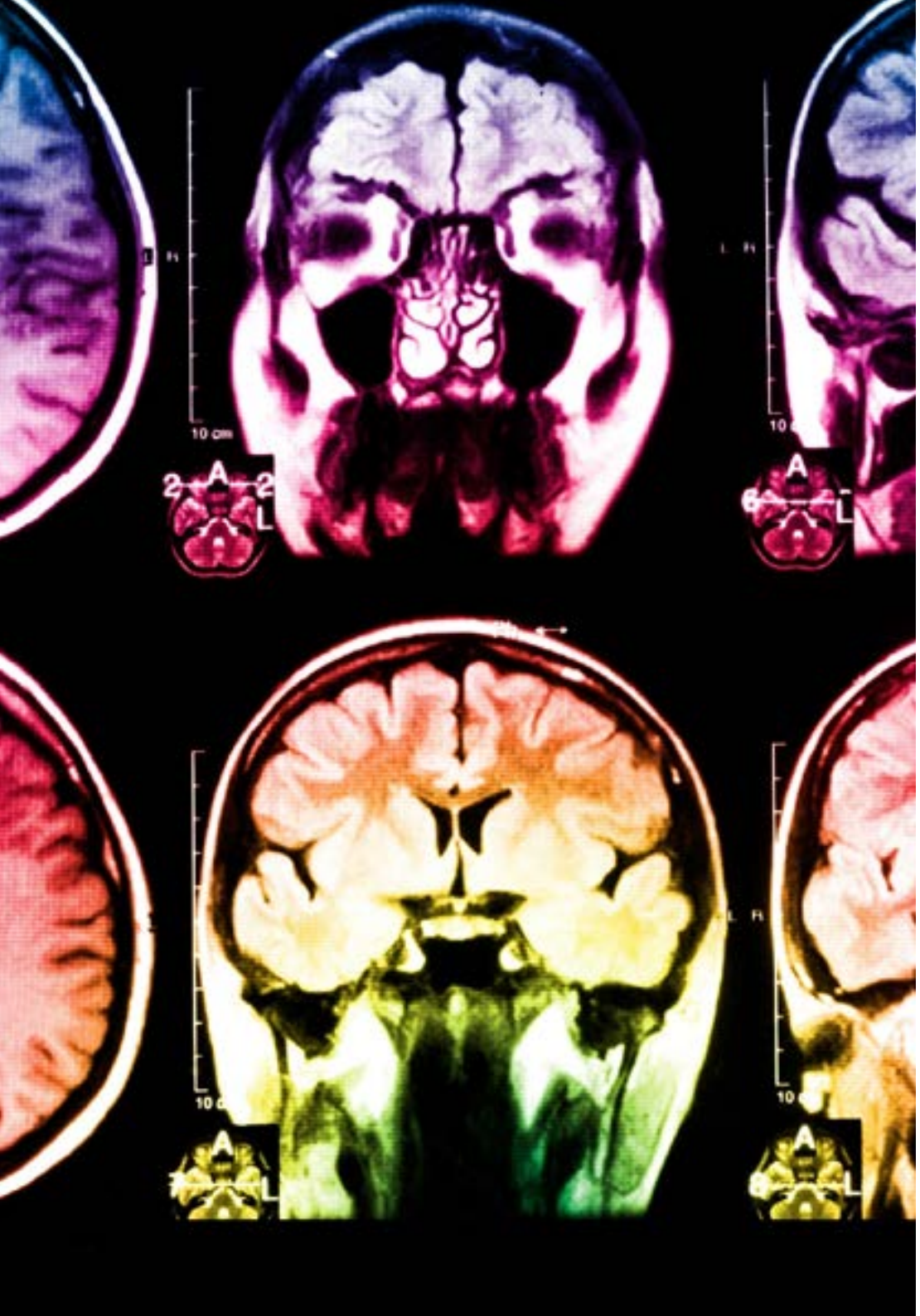
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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

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

At TECH you will learn using a cutting-edge methodology designed to train the executives of the future. This method, at the forefront of international teaching, is called Relearning.

Our university is the only one in the world authorized to employ this successful method. In 2019, we managed to improve our students' overall satisfaction levels (teaching quality, quality of materials, course structure, objectives...) based on the best online university indicators.



In our program, learning is not a linear process, but rather a spiral (learn, unlearn, forget, and re-learn). Therefore, we combine each of these elements concentrically. This methodology has trained more than 650,000 university graduates with unprecedented success in fields as diverse as biochemistry, genetics, surgery, international law, management skills, sports science, philosophy, law, engineering, journalism, history, and financial markets and instruments. All this in a highly demanding environment, where the students have a strong socio-economic profile and an average age of 43.5 years.

Relearning will allow you to learn with less effort and better performance, involving you more in your training, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation for success.

From the latest scientific evidence in the field of neuroscience, not only do we know how to organize information, ideas, images and memories, but we know that the place and context where we have learned something is fundamental for us to be able to remember it and store it in the hippocampus, to retain it in our long-term memory.

In this way, and in what is called neurocognitive context-dependent e-learning, the different elements in our program are connected to the context where the individual carries out their professional activity.

This program offers the best educational material, prepared with professionals in mind:

Study Material

All teaching material is produced by the specialists who teach the course, specifically for the course, so that the teaching content is highly specific and precise.

These contents are then applied to the audiovisual format, to create the TECH online working method. All this, with the latest techniques that offer high quality pieces in each and every one of the materials that are made available to the student.

Classes

There is scientific evidence suggesting that observing third-party experts can be useful.

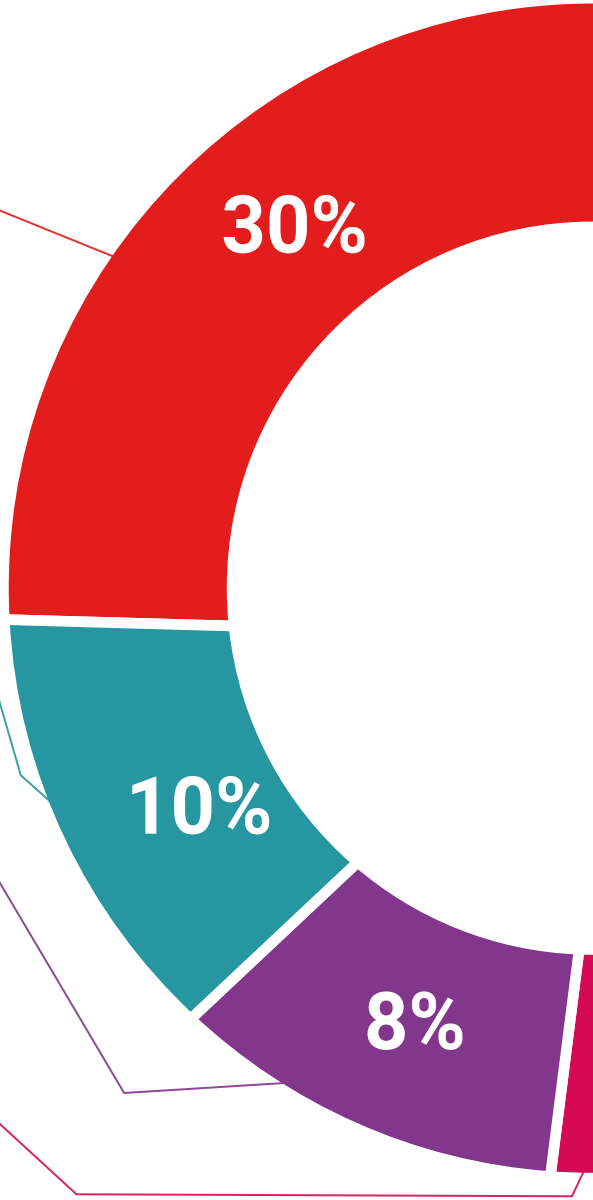
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

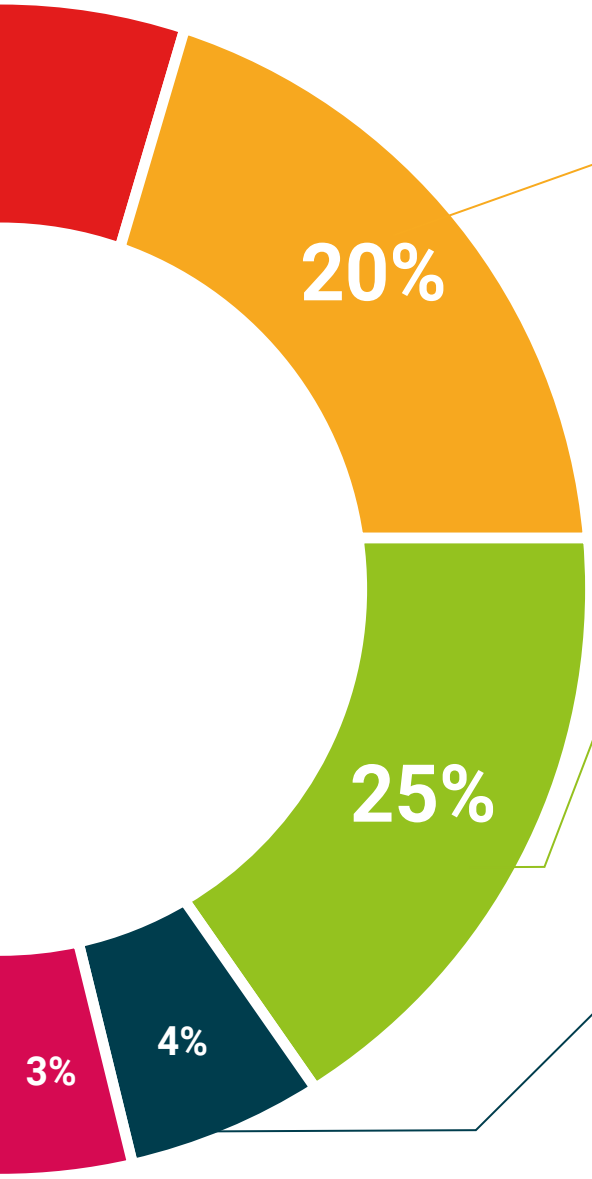
Practising Skills and Abilities

They will carry out activities to develop specific skills and abilities in each subject area. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop in the context of the globalization that we are experiencing.

Additional Reading

Recent articles, consensus documents and international guidelines, among others. In TECH's virtual library, students will have access to everything they need to complete their course.





Case Studies

Students will complete a selection of the best case studies chosen specifically for this program. Cases that are presented, analyzed, and supervised by the best specialists in the world.

Interactive Summaries

The TECH team presents the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

This exclusive educational system for presenting multimedia content was awarded by Microsoft as a "European Success Story".

Testing & Retesting

We periodically evaluate and re-evaluate students' knowledge throughout the program, through assessment and self-assessment activities and exercises, so that they can see how they are achieving their goals.

06

Certificate

The Postgraduate Diploma in Computer Security Defense Measures 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 private qualification will allow you to obtain a **Postgraduate Diploma in Computer Security Defense Measures** 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.

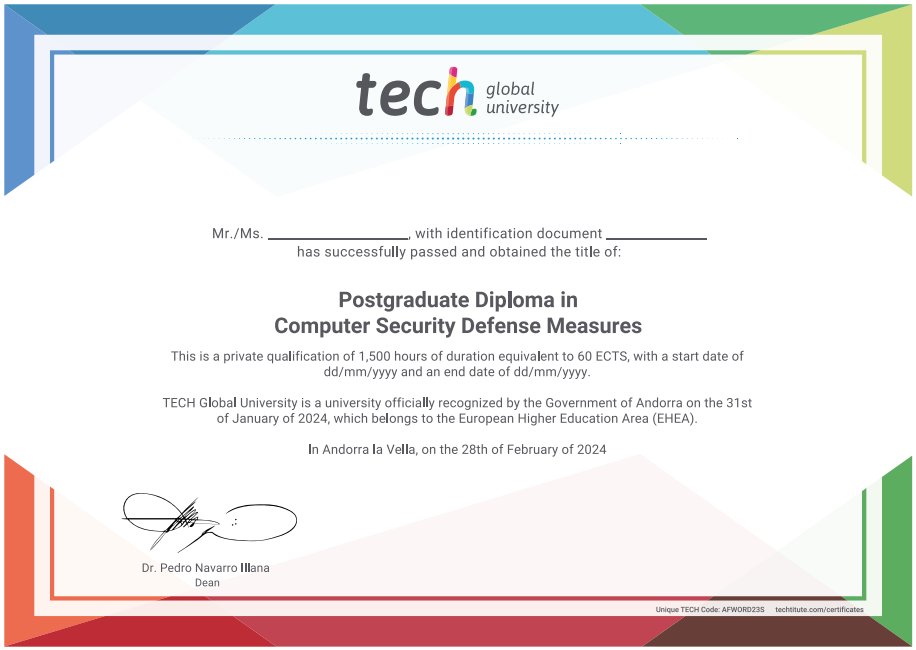
This **TECH Global University** private qualification is a European program of continuing education and professional updating that guarantees the acquisition of competencies in its area of knowledge, providing a high curricular value to the student who completes the program.

Title: **Postgraduate Diploma in Computer Security Defense Measures**

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 Computer Security Defense Measures

This is a private qualification of 1,500 hours of duration equivalent to 60 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
Dean

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 additional cost.

tech global university

Postgraduate Diploma

Computer Security Defense Measures

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

Postgraduate Diploma

Computer Security Defense Measures

tech global university