

Postgraduate Diploma IT Security



Postgraduate Diploma IT Security

Course Modality: **Online**

Duration: **6 months.**

Certificate: **TECH Technological University**

Official N° of Hours: **450 h.**

Website: www.techtute.com/information-technology/postgraduate-diploma/postgraduate-diploma-it-security

Index

01

Introduction

p. 4

02

Objectives

p. 8

03

Course Management

p. 12

04

Structure and Content

p. 16

05

Methodology

p. 22

06

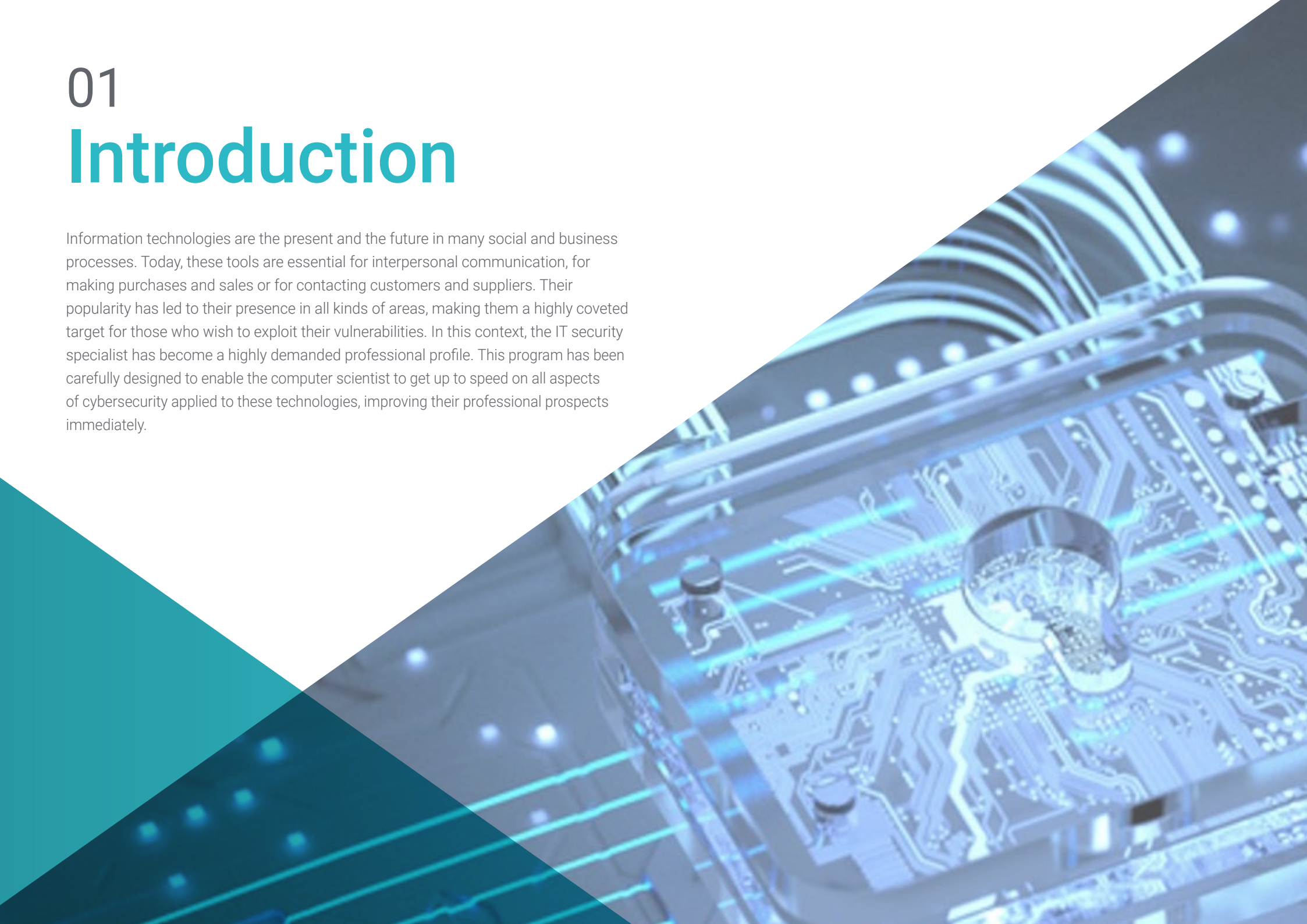
Certificate

p. 30

01

Introduction

Information technologies are the present and the future in many social and business processes. Today, these tools are essential for interpersonal communication, for making purchases and sales or for contacting customers and suppliers. Their popularity has led to their presence in all kinds of areas, making them a highly coveted target for those who wish to exploit their vulnerabilities. In this context, the IT security specialist has become a highly demanded professional profile. This program has been carefully designed to enable the computer scientist to get up to speed on all aspects of cybersecurity applied to these technologies, improving their professional prospects immediately.



“

This program will allow you to specialize in IT Security, which will give you access to great career opportunities in an area of IT that is increasingly in demand"

The new technological context demands from the professional a deepening to adapt to the existing transformations in IT Security. Thus, these information technologies are omnipresent and are used in all types of business and social processes. As a result, there are numerous aspects that are at risk of being exposed to exploitable vulnerabilities.

This situation is of great concern to companies, which see how inadequate security can jeopardize their business. The solution, then, is the hiring of professionals specialized in this field, which is why the IT Security specialist is currently one of the most sought-after and highly valued profiles by corporations in different areas and sectors.

In response to this demand, this Postgraduate Diploma is presented, which is developed through a 100% online format, and has a teaching staff of enormous international prestige in this field of cybersecurity. In addition, this program presents its contents in a variety of multimedia formats: interactive summaries, videos, case studies, master classes, practical activities, etc. All to achieve the objective of providing the professional with the latest developments in security applied to information technologies.

This **Postgraduate Diploma in IT Security** contains the most complete and up-to-date program on the market. Its most notable features are:

- ◆ Case studies presented by IT and cybersecurity experts
- ◆ The graphic, schematic, and practical contents with which they are created, provide scientific and practical information on the disciplines that are essential for professional practice
- ◆ Practical exercises where the self-assessment process can be carried out to improve learning
- ◆ Its special emphasis on innovative methodologies
- ◆ Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- ◆ Access to content from any fixed or portable device with an Internet connection



With this program you will be able to deepen in relevant aspects of IT Security such as secure development in communications and software operation"

“

TECH's 100% online teaching system will allow you to combine your work with your studies, as it adapts to all your personal and professional circumstances"

The program's teaching staff includes professionals from 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 training programmed to train 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, the student will be assisted by an innovative interactive video system created by renowned and experienced experts.

The faculty of this program is composed of working professionals who are familiar with all the latest developments in this area of cybersecurity.

Your professional profile will improve once you complete this Postgraduate Diploma, which is taught using numerous multimedia resources.



02 Objectives

The main objective of this Postgraduate Diploma in IT Security is to provide professionals with the best tools to adapt to the new IT context, transformed by the digitalization process that has spread to all areas of society. Thus, you will be in the best position to work as a cybersecurity specialist in any company that wants to protect its business from new IT threats.



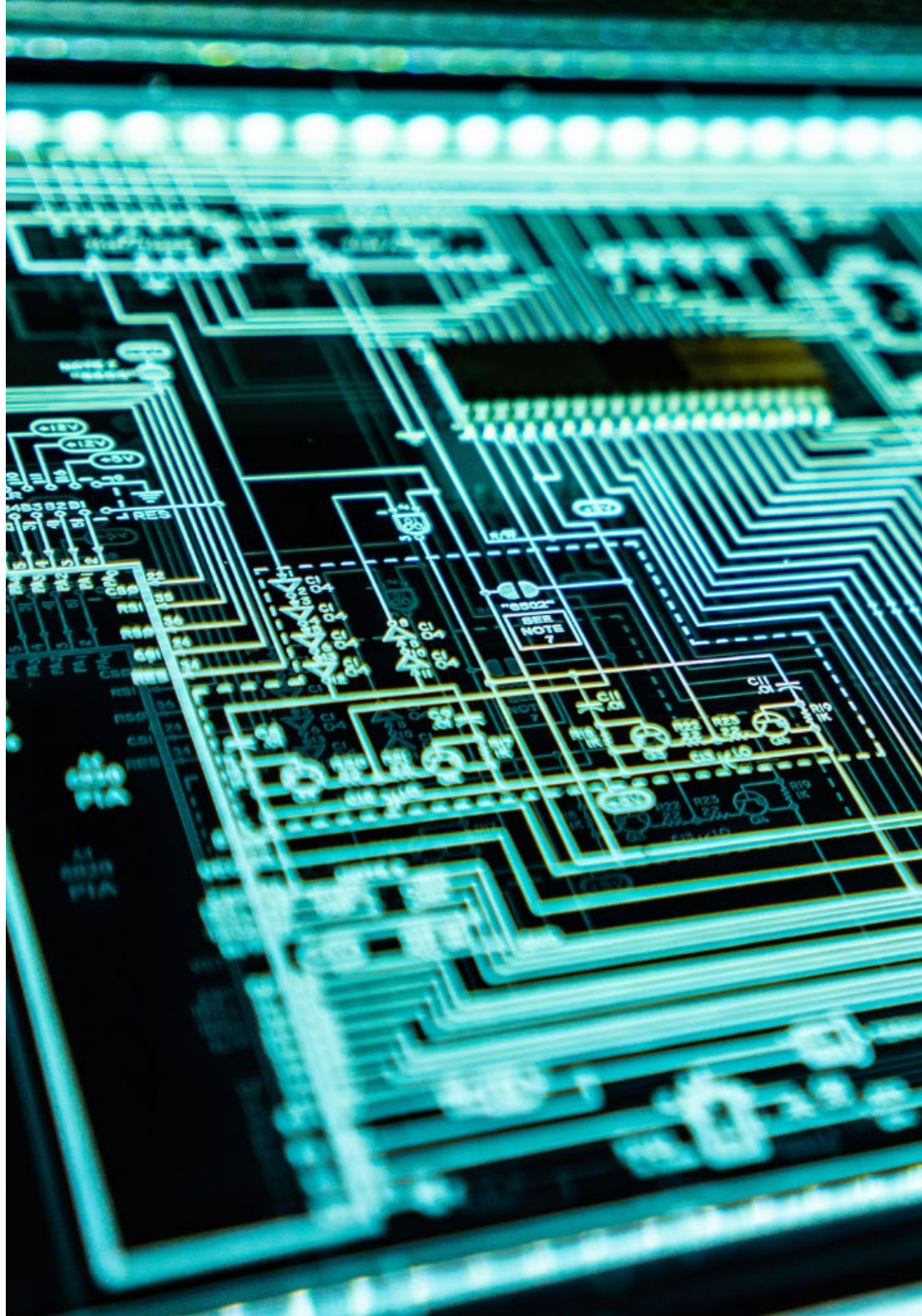
“

TECH's objective is to provide you with the most up-to-date knowledge so that you can develop your work with the maximum guarantees, making you a reference professional in the sector"



General Objectives

- ◆ Generate specialized knowledge about an information system, types and security aspects that must be taken into account
- ◆ Identify the vulnerabilities of an information system
- ◆ Apply the most appropriate security measures depending on the threats
- ◆ Develop legal regulations and criminalization of crime attacking an information system
- ◆ Determine the security policy and plan for a company's information system, completing the design and implementation of the Contingency Plan
- ◆ Generate specialized knowledge about the IT security ecosystem
- ◆ Assessing knowledge in terms of cybersecurity
- ◆ Develop best practices in secure development
- ◆ Present the risks for companies of not having an IT security environment
- ◆ Examine the process of designing a security strategy when deploying corporate *cloudservices*
- ◆ Identify the areas of *Cloudsecurity*
- ◆ Analyze the services and tools in each of the security areas
- ◆ Assess the differences in the concrete implementations of different public *cloud* vendors





Specific Objectives

Module 1. Security in System Design and Development

- ◆ Assess the security of an information system in all its components and layers
- ◆ Identify current security threat types and trends
- ◆ Establish security guidelines by defining security and contingency policies and plans
- ◆ Analyze strategies and tools to ensure the integrity and security of information systems
- ◆ Apply specific techniques and tools for each type of attack or security vulnerability
- ◆ Protect sensitive information stored in the information system
- ◆ Have the legal framework and typification of the crime, completing the vision with the typification of the offender and his victim

Module 2. Security in Communications and Software Operation

- ◆ Develop specialized physical and logical security knowledge
- ◆ Demonstrate knowledge of communications and networks
- ◆ Identify major malicious attacks
- ◆ Establish a secure development framework
- ◆ Demonstrate knowledge of the main information security management system regulations
- ◆ Support the operation of a cybersecurity operations center
- ◆ Demonstrate the importance of having cybersecurity practices for organizational disasters

Module 3. Security in *Cloud* Environments

- ◆ Identifying risks of a public *cloud* infrastructure deployment
- ◆ Define security requirements
- ◆ Developing a security plan for a *cloud* deployment
- ◆ Identify the cloud services to be deployed for the execution of a security plan
- ◆ Determine the operations necessary for the prevention mechanisms
- ◆ Establish guidelines for a *logging* and monitoring system
- ◆ Propose incident response actions



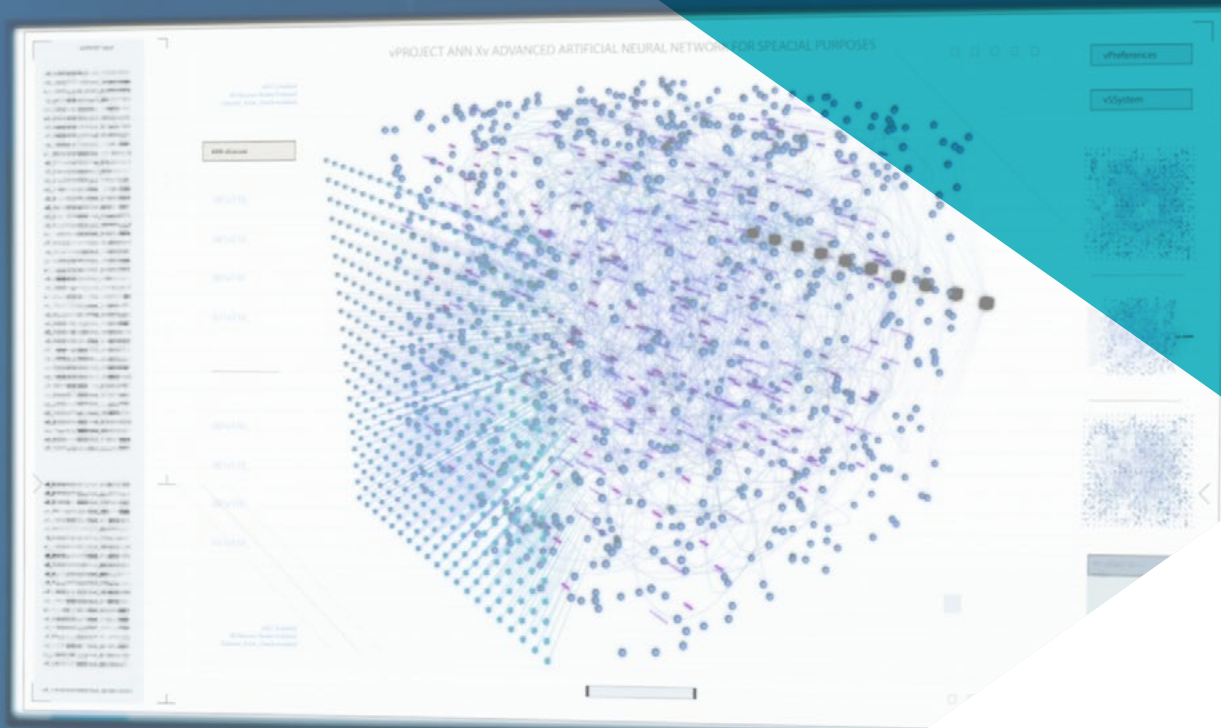
You will be able to progress quickly in your career, as your new knowledge will position you as a highly sought-after specialist"

03

Course Management

IT security is an area that is constantly evolving, requiring the most advanced knowledge that only a working professional can provide. For this reason, TECH has put its efforts in having prestigious specialists in this field in charge of the teaching this program, providing the student with the best skills to effectively develop in designing company protection.





“

This program is what you need: you will have at your fingertips the greatest specialists in IT Security at an international level”

Management



Mr. Olalla Bonal, Martín

- ◆ Director de Información en ePETID - Global Animal Health
- ◆ Blockchain Technical Specialist at IBM SPGI
- ◆ *Blockchain* Architect
- ◆ Infrastructure Architect in Banking
- ◆ Project management and implementation of solutions
- ◆ Digital Electronics Technician
- ◆ Teacher Hyperledger Fabric Training for companies
- ◆ Teacher Business-oriented companies *Blockchain* training



Professors

Mr. Nogales Ávila, Javier

- ◆ Enterprise Cloud and sourcing senior consultant. Quint
- ◆ Cloud and Technology Consultant. Indra
- ◆ Associate Technology Consultant. Accenture
- ◆ Graduate by Jaen University y University of Technology and Economics of Budapest (BME)
- ◆ Degree in Industrial Organization Engineering

Mr. Gómez Rodríguez, Antonio

- ◆ Cloud Solutions Engineer at Oracle
- ◆ Project Manager at Sopra Group
- ◆ Project Manager at Everis
- ◆ Project Manager at Empresa pública de Gestion de Programas Culturales. Department of Culture of Andalusia
- ◆ Information Systems Analyst. Sopra Group
- ◆ Degree in Telecommunications Engineering from the Polytechnic University of Catalonia
- ◆ Postgraduate Degree in Information Technologies and Systems, Catalan Institute of Technology
- ◆ E-Business Master, La Salle School of Business

Ms. Jurado Jabonero, Lorena

- ◆ Head of Information Security (CISO) at Grupo Pascual
- ◆ Graduate in Computer Engineering from Alfonso X El Sabio University
- ◆ Technical Computer Engineer from Polytechnical University of Madrid
- ◆ Knowledge: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, etc.

04

Structure and Content

In order to achieve the proposed objectives, this Postgraduate Diploma in IT Security has been divided into 3 specialized modules, which can be completed over 450 hours of learning. Thus, throughout this program, the computer scientist will learn about the latest advances in computer security in communications and software operation, security in *Cloud Computing* environments, the security of storage systems or authorization systems, among many other relevant aspects in this area.



“

*This program will allow you to
apply the best forensic analysis
techniques applied to IT Security”*

Module 1. Security in System Design and Development

- 1.1. Information Systems
 - 1.1.1. Information System Domains
 - 1.1.2. Information System Components
 - 1.1.3. Information System Activities
 - 1.1.4. Life Cycle of an Information System
 - 1.1.5. Information System Resources
- 1.2. IT Systems Types
 - 1.2.1. Types of Information Systems
 - 1.2.1.1. Corporate
 - 1.2.1.2. Strategic
 - 1.2.1.3. According to the Area of Application
 - 1.2.1.4. Specific
 - 1.2.2. Information Systems Real Examples
 - 1.2.3. Evolution of Information Systems: Stages
 - 1.2.4. Methods of Information Systems
- 1.3. Information System Security Legal Implications
 - 1.3.1. Access to Data
 - 1.3.2. Security Threats: Vulnerabilities
 - 1.3.3. Legal Implications: Criminal Offenses
 - 1.3.4. Maintenance Procedures of an Information System
- 1.4. Information System Security Security Protocol
 - 1.4.1. Information System Security
 - 1.4.1.1. Integrity
 - 1.4.1.2. Confidentiality
 - 1.4.1.3. Availability
 - 1.4.1.4. Authentication
 - 1.4.2. Security Services
 - 1.4.3. Information Security Protocols Types
 - 1.4.4. Information System Sensitivity
- 1.5. Information System Security Access Control Measures and Systems
 - 1.5.1. Security Measures
 - 1.5.2. Type of Security Measures
 - 1.5.2.1. Prevention
 - 1.5.2.2. Detection
 - 1.5.2.3. Correction
 - 1.5.3. Access Control Systems Types
 - 1.5.4. Cryptography
- 1.6. Network and Internet Security
 - 1.6.1. *Firewalls*
 - 1.6.2. Digital Identification
 - 1.6.3. Viruses and Worms
 - 1.6.4. *Hacking*
 - 1.6.5. Examples and Real Cases
- 1.7. Computer Crimes
 - 1.7.1. Computer Crimes
 - 1.7.2. Computer Crimes Types
 - 1.7.3. Computer Crimes Attack Types
 - 1.7.4. The Case for Virtual Reality
 - 1.7.5. Profiles of Offenders and Victims Criminalization of the Crime
 - 1.7.6. Computer Crimes Examples and Real Cases
- 1.8. Security Plans in Information Systems
 - 1.8.1. Security Plan Objectives
 - 1.8.2. Security Plan Plan
 - 1.8.3. Risk Plan Analysis
 - 1.8.4. Security Policy Implementation in the Organization
 - 1.8.5. Security Plan Implementation in the Organization
 - 1.8.6. Security Procedures Types
 - 1.8.7. Security Plan Examples:

- 1.9. Contingency Plan
 - 1.9.1. Contingency Plan Functions
 - 1.9.2. Emergency Plan: Elements and Objectives
 - 1.9.3. Contingency Plan in the Organization Implementation
 - 1.9.4. Contingency Plans Examples:
- 1.10. Information Systems Security Governance
 - 1.10.1. Legal Regulations
 - 1.10.2. Standards
 - 1.10.3. Certifications
 - 1.10.4. Technologies

Module 2. Security in Communications and Software Operation

- 2.1. Computer Security in Communications and Software Operation
 - 2.1.1. IT Security
 - 2.1.2. Cybersecurity
 - 2.1.3. Cloud Security
- 2.2. IT Security in Communications and Software Operation Types
 - 2.2.1. Physical Security
 - 2.2.2. Logical Security
- 2.3. Communications Security
 - 2.3.1. Main Elements
 - 2.3.2. Network Security
 - 2.3.3. Best Practices
- 2.4. Cyberintelligence
 - 2.4.1. Social Engineering
 - 2.4.2. *Deep Web*
 - 2.4.3. *Phishing*
 - 2.4.4. *Malware*
- 2.5. Secure Development in Communications and Software Operation
 - 2.5.1. Secure Development HTTP Protocol
 - 2.5.2. Secure Development Life Cycle
 - 2.5.3. Secure Development PHP Security
 - 2.5.4. Secure Development NET Security
 - 2.5.5. Secure Development Best Practices

- 2.6. Information Security Management Systems in Communications and Software Operation
 - 2.6.1. GDPR
 - 2.6.2. ISO 27021
 - 2.6.3. ISO 27017/18
- 2.7. SIEM Technologies
 - 2.7.1. SIEM Technologies
 - 2.7.2. SOC Operations
 - 2.7.3. SIEM *Vendors*
- 2.8. The Role of Security in Organizations
 - 2.8.1. Roles in Organizations
 - 2.8.2. Role of IoT Specialists in Companies
 - 2.8.3. Recognized Certifications in the Market
- 2.9. Forensic Analysis
 - 2.9.1. Forensic Analysis
 - 2.9.2. Forensic Analysis Methodology
 - 2.9.3. Forensic Analysis Tools and Implementation
- 2.10. Cybersecurity Today
 - 2.10.1. Main Cyber Attacks
 - 2.10.2. Employability Forecasts
 - 2.10.3. Challenges

Module 3. Security in *Cloud* Environments

- 3.1. Security in *Cloud Computing* Environments
 - 3.1.1. Security in *Cloud Computing* Environments
 - 3.1.2. Security in *Cloud Computing* Environments. Security Threats and Risks
 - 3.1.3. Security in *Cloud Computing* Environments. Key Security Aspects
- 3.2. Types of *Cloud* Infrastructure
 - 3.2.1. Public
 - 3.2.2. Private
 - 3.2.3. Hybrid

- 3.3. Shared Management Model
 - 3.3.1. Security Elements Managed by Supplier
 - 3.3.2. Elements Managed by the Client
 - 3.3.3. Definition of the Security Strategy
- 3.4. Prevention Mechanisms
 - 3.4.1. Authentication Management Systems
 - 3.4.2. Authorization Management System: Access Policies
 - 3.4.3. Key Management Systems
- 3.5. Securing Systems
 - 3.5.1. Securing Storage Systems
 - 3.5.2. Protection of Database Systems
 - 3.5.3. Securing Data in Transit
- 3.6. Infrastructure Protection
 - 3.6.1. Secure Network Design and Implementation
 - 3.6.2. Security in Computing Resources
 - 3.6.3. Tools and Resources to Protect the Infrastructure
- 3.7. Detection of Threats and Attacks
 - 3.7.1. Auditing, *Logging* and Monitoring Systems
 - 3.7.2. Event and Alarm Systems
 - 3.7.3. SIEM Systems
- 3.8. Incident Response
 - 3.8.1. Incident Response Plan
 - 3.8.2. Business Continuity
 - 3.8.3. Forensic Analysis and Remediation of Incidents of the Same Nature



- 3.9. Security in Public Clouds
 - 3.9.1. AWS(Amazon Web Services)
 - 3.9.2. Microsoft Azure
 - 3.9.3. Google GCP
 - 3.9.4. Oracle Cloud
- 3.10. Regulations and Compliance
 - 3.10.1. Compliance with Safety Regulations
 - 3.10.2. Risk Management
 - 3.10.3. People and Process in the Organizations

“

The most complete and up-to-date syllabus on the market is now within your reach. Matriculate, you won't regret it"

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.



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

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 IT Security 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 Certificate in IT Security** 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 IT Security**

Official N° of Hours: **450 h.**



*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.

future
health confidence people
education information tutors
guarantee accreditation teaching
institutions technology learning
community commitment
personalized service innovation
knowledge present
online training
development language
virtual classroom



Postgraduate Diploma IT Security

Course Modality: **Online**

Duration: **6 months.**

Certificate: **TECH Technological University**

Official N° of Hours: **450 h.**

Postgraduate Diploma IT Security