Postgraduate Diploma

Security and Cryptography

tech global university

tech global university

Postgraduate Diploma
Security and Cryptography

- 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/postgraduate-diploma/postgraduate-diploma-security-cryptography

Index

01

Introduction

One of the most important areas in cybersecurity today is cryptography. This field makes it possible to protect all types of information through the encryption process, using tools such as algorithms. Companies of all types need to secure their data, so they look for professionals specialized in this field who can provide the security standards they need. This program, the most advanced in symmetric cryptography, block ciphers, quantum algorithms or *Blockchain* technology. All of this is based on a 100% online teaching system that allows professionals to combine their studies with their work, since it adjusts to their personal circumstances.

Thanks to this program, you will learn the best encryption methods to protect your clients' and employers' data"

Cryptography is a booming discipline for which professionals are increasingly in demand. This field makes it possible to protect all types of digital data and has applications in areas such as banking, online stores, databases of all kinds and is essential in the *Blockchain*. Thus, specializing in this area is a must for today's IT professional.

Many companies, not just technology companies, need cryptographic experts to make their information more secure, and this program responds to that demand. Throughout 3 modules, and in 450 hours of learning, the computer scientist will be able to delve into issues such as the mathematical foundations of cryptography, the methodology of analysis and risk management of information systems or the protection of algorithms against quantum computing.

The professional will be able to deepen in this discipline through a 100% online methodology, specially designed so that the student can combine their work with their studies. In addition, the program will be taught by a teaching staff of great prestige in the field of cryptography, who will teach this program using numerous multimedia resources.

The **Postgraduate Diploma in Security and Cryptography** is the most complete and up-to-date educational program on the market. Its most notable features are:

- The development of 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 work.
- Content that is accessible from any fixed or portable device with an Internet connection.

Cryptography is basic to companies like Facebook, Paypal or Amazon, and Blockchain technology has given it a huge boost, so specializing in this area can give access to numerous career opportunities"

From the best multimedia materials, and with a teaching staff composed of working professionals, you will learn all the keys to cryptography applied to computer security"

Cryptography is the big IT field of today: this program will allow you to specialize in it with the best online teaching on the market"

With this Postgraduate Diploma you will delve into aspects of cryptography such as the protection of algorithms against quantum computing"

The program includes, in its teaching staff, professionals from the sector who bring to this training the experience of their work, in addition to recognized specialists from prestigious reference societies and universities.

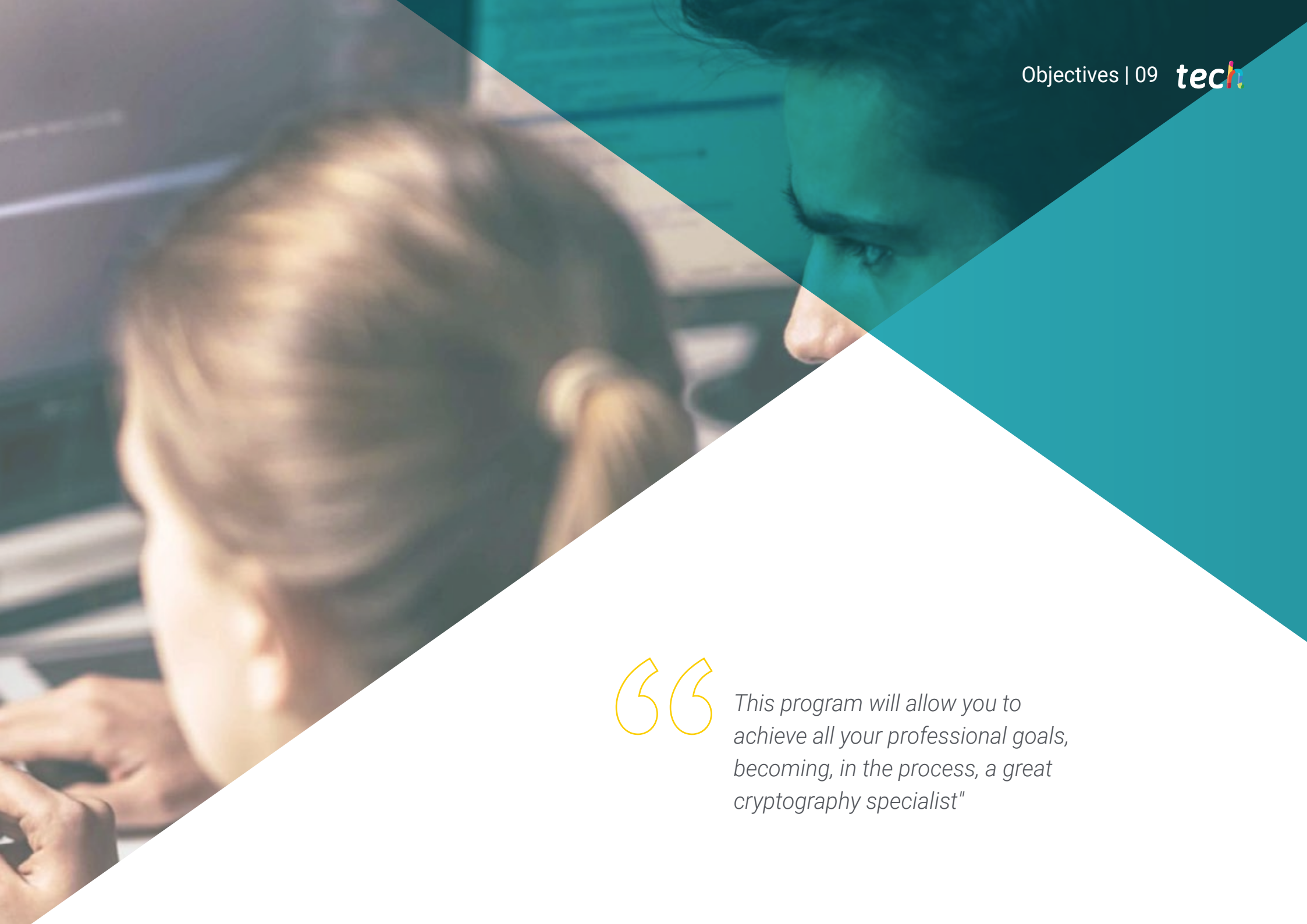
The multimedia content, developed with the latest educational technology, will provide the professional with situated and contextual learning, i.e., a simulated environment that will provide immersive training programmed to train in real situations.

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.

02

Objectives

The main objective of this Postgraduate Diploma in Security and Cryptography is to offer professionals the latest developments in this area of cybersecurity, so that upon completion they can work in any company that needs a specialist in this field. And for this, TECH offers you the most complete and up-to-date contents, the most flexible teaching system, and teachers of great prestige in the field of cryptography.



This program will allow you to achieve all your professional goals, becoming, in the process, a great cryptography specialist"

General Objectives

- Analyze and develop the concept of risk and uncertainty within the environment in which we live
- Examine the risk management model based on ISO 31.000
- Apply the MAGERIT methodology to evolve the model and take it a step further
- Design new risk management methodologies based on the *agile* risk management concept
- Identify, analyze, assess and treat the risks to be faced from a new business perspective based on a *risk-driven* model that not only allows us to survive in our environment, but also to contribute value
- Maximize the opportunities presented and eliminate exposure to all potential risks from the design itself
- Examine the science of cryptology and the relationship to its branches: cryptography, cryptanalysis, steganography and stegoanalysis
- Analyze the types of cryptography according to the type of algorithm and according to its use
- Compile key management systems
- Evaluate the different practical applications
- Examine digital certificates
- Examine the Public Key Infrastructure (PKI)
- Analyze the latest trends and challenges
- Determine the basic elements of a Business Continuity Plan (BCP) using the ISO-22301 guidelines as a basis
- Examine the risks arising from the non-existence of a Business Continuity Plan (BCP)
- Analyze the success criteria of a BCP and its integration into a company's overall risk management
- Specify the implementation phases of a Business Continuity Plan

Don't wait any longer: the professional progress you were looking for can be found in this Postgraduate Diploma"

Specific Objectives

Module 1. Risk Analysis and IT Security Environment

- Examine, with a holistic vision, the environment in which we move
- Identify the main risks and opportunities that may affect the achievement of our objectives
- Analyze risks based on the best practices available to us
- Assessing the potential impact of these risks and opportunities
- Develop techniques to deal with risks and opportunities in a way that maximizes value contribution
- Examine in depth the different risk and value transfer techniques
- Generate value from the design of proprietary models for agile risk management
- Examine results to propose continuous improvements in project and process management based on *risk-driven* management models
- Innovate and transform general data into relevant information for risk-based decision making

Module 2. Cryptography in IT

- Compile the fundamental operations (XOR, large numbers, substitution and transposition) and the various components (One-Way functions, Hash, random number generators)
- Analyze cryptographic techniques
- Develop the different cryptographic algorithms
- Demonstrate the use of digital signatures and their application in digital certificates
- Assess key management systems and the importance of cryptographic key lengths
- Examine key derivation algorithms
- Analyze key life cycle
- Evaluate block cipher and stream cipher modes
- Determine pseudorandom number generators
- Develop real-world cryptography application cases, such as Kerberos, PGP or smart cards
- Examine related associations and organizations, such as ISO, NIST or NCSC
- Determine the challenges in quantum computing cryptography

Module 3. Business Continuity Plan Associated with Security

- Present the key elements of each phase and analyze the characteristics of the Business Continuity Plan (BCP)
- Substantiate the need for a Business Continuity Plan
- Determine the success and risk maps for each phase of the Business Continuity Plan
- Specify how to establish an Action Plan for implementation
- Assess the completeness of a Business Continuity Plan (BCP)
- Develop a plan for the successful implementation of a Business Continuity Plan

03

Course Management

This program has great specialists who are professionally developed in the area of cryptography to teach its 3 modules. Thus, the teaching staff of this Postgraduate Diploma is one of its great strengths, since it includes specialists of great prestige in this field, and will transmit to the student all the keys to be able to work using the best encryption techniques and tools.

A teaching staff composed of active professionals in the field of cryptography will guide you through the entire learning process"

Management

Mr. Olalla Bonal, Martín

- *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 to companies
- Teacher Business-oriented companies *Blockchain* training

Professors

Mr. Gonzalo Alonso, Félix

- CEO and Founder of Smart REM Solutions
- Founding Partner and Head of Risk Engineering and Innovation Dynargy
- Manager and Founding Partner Risknova (Specialized Expert Technology Office)
- Degree in Industrial Organization Engineering from Comillas Pontifical University ICAI
- Graduate in Industrial Technical Engineering, specializing in Industrial Electronics, Comillas Pontifical University ICAI
- Master's Degree in Insurance Management from ICEA (Institute for the Collaboration between Insurance Companies)

Mr. Sevillano Izquierdo, Javier

- Global Cyber Security Architect Vodafone Spain
- Chief Technology Security Office (CTSO) Vodafone Spain
- Responsible for Technological Security Bankia
- Responsible for Technological Security Caja Madrid
- Security Manager 4B System
- SEINCA - Senior Analyst
- Superior Technician in Business Computing by Instituto Cibernos

Mr. Gozalo Fernández, Juan Luis

- Computer Engineer
- Associate Professor in DevOps and Blockchain at UNIR
- Exdirector Blockchain DevOps in Alastria
- Tinkerlink Mobile Application Development Manager at Cronos Telecom
- IT Manager at Banco Santander
- IT Service Management Technology Director at Barclays Bank Spain
- Degree in Computer Engineering from the National Distance Education University (UNED)

04

Structure and Content

This Postgraduate Diploma in Security and Cryptography is developed over 6 months, in 450 hours of learning. In addition, it has been structured in 3 modules, with which the computer scientist will delve into issues such as the methodology of analysis and risk management of information systems, the development of IT risk maps based on agile methodologies, artificial intelligence applied to risk management or cryptography applied to the *Blockchain*.

With this program you will have access to the latest content in steganography"

Module 1. Risk Analysis and IT Security Environment

1.1. Analysis of the environment
- 1.1.1. Analysis of the Economic Situation
  - 1.1.1.1. VUCA Environment
    - 1.1.1.1.1. Volatile
    - 1.1.1.1.2. Unsure
    - 1.1.1.1.3. Complex
    - 1.1.1.1.4. Ambiguous
  - 1.1.1.2. BANI Environment
    - 1.1.1.2.1. Broken
    - 1.1.1.2.2. Anxious
    - 1.1.1.2.3. Non-Linear
    - 1.1.1.2.4. Incomprehensible
- 1.1.2. General Environment Analysis PESTLE
  - 1.1.2.1. Politics
  - 1.1.2.2. Economics
  - 1.1.2.3. Social
  - 1.1.2.4. Technological
  - 1.1.2.5. Ecological/Environmental
  - 1.1.2.6. Legal
- 1.1.3. Analysis of the Internal Situation SWOT Analysis
  - 1.1.3.1. Objectives
  - 1.1.3.2. Threats
  - 1.1.3.3. Opportunities
  - 1.1.3.4. Strengths

1.2. Risk and Uncertainty
- 1.2.1. Risk
- 1.2.2. Risk Management
- 1.2.3. Risk Management Standards

1.3. ISO 31.000:2018 Risk Management Guidelines
- 1.3.1. Object
- 1.3.2. Principles
- 1.3.3. Frame of Reference
- 1.3.4. Process

1.4. Methodology for Analysis and Management of Information Systems Risks (MAGERIT)
- 1.4.1. MAGERIT Methodology
  - 1.4.1.1 Objectives
  - 1.4.1.2 Method
  - 1.4.1.3 Elements
  - 1.4.1.4 Techniques
  - 1.4.1.5 Available Tools (PILAR)

1.5. Cyber Risk Transfer
- 1.5.1. Risk Transfer
- 1.5.2. Cyber Risks Types
- 1.5.3. Cyber Risk Insurance

1.6. Agile Methodologies for Risk Management
- 1.6.1. Agile Methodologies
- 1.6.2. Scrum for Risk Management
- 1.6.3. *Agile Risk Management*

1.7. Technologies for Risk Management
- 1.7.1. Artificial Intelligence Applied to Risk Management
- 1.7.2. *Blockchain* and Cryptography Value Preservation Methods
- 1.7.3. Quantum Computing Opportunity or Risk

1.8. IT Risk Mapping Based on Agile Methodologies
- 1.8.1. Representation of Probability and Impact in Agile Environments
- 1.8.2. Risk as a Threat to Value
- 1.8.3. Re-Evolution in Project Management and Agile Processes Based on KRIs

1.9. *Risk-Driven* in Risk Management
- 1.9.1. *Risk Driven*
- 1.9.2. *Risk-Driven* in Risk Management
- 1.9.3. Development of a Risk-Driven Business Management Model

1.10. Innovation and Digital Transformation in IT Risk Management
- 1.10.1. Agile Risk Management as a Source of Business Innovation
- 1.10.2. Transforming Data into Useful Information for Decision Making
- 1.10.3. Holistic View of the Company through Risk

Module 2. Cryptography in IT

2.1. Cryptography
- 2.1.1. Cryptography
- 2.1.2. Fundamentals of Mathematics

2.2. Cryptology
- 2.2.1. Cryptology
- 2.2.2. Cryptanalysis
- 2.2.3. Steganography and Stegoanalysis

2.3. Cryptographic Protocols
- 2.3.1. Basic Blocks
- 2.3.2. Basic Protocols
- 2.3.3. Intermediate Protocols
- 2.3.4. Advanced Protocols
- 2.3.5. Exoteric Protocols

2.4. Cryptographic Techniques
- 2.4.1. Length of Passwords
- 2.4.2. Password Management
- 2.4.3. Types of Algorithms
- 2.4.4. Summary of Functions *Hash*
- 2.4.5. Pseudo-Random Number Generators
- 2.4.6. Use of Algorithms

2.5. Symmetric Cryptography
- 2.5.1. Block Ciphers
- 2.5.2. DES (*Data Encryption Standard*)
- 2.5.3. RC4 Algorithm
- 2.5.4. AES (*Advanced Encryption Standard*)
- 2.5.5. Combination of Block Ciphers
- 2.5.6. Password Derivation

2.6. Asymmetric Cryptography
- 2.6.1. Diffie-Hellman
- 2.6.2. DSA (*Digital Signature Algorithm*)
- 2.6.3. RSA (Rivest, Shamir and Adleman)
- 2.6.4. Elliptic Curve
- 2.6.5. Asymmetric Cryptography Types

2.7. Digital Certificates
- 2.7.1. Digital Signature
- 2.7.2. X509 Certificates
- 2.7.3. Public Key Infrastructure (PKI)

2.8. Implementations
- 2.8.1. Kerberos
- 2.8.2. IBM CCA
- 2.8.3. *Pretty Good Privacy* (PGP)
- 2.8.4. ISO *Authentication Framework*
- 2.8.5. SSL and TLS
- 2.8.6. Europay, MasterCard, and Visa (EMV)
- 2.8.7. Mobile Telephony Protocols
- 2.8.8. *Blockchain.*

2.9. Steganography
- 2.9.1. Steganography
- 2.9.2. Stegoanalysis
- 2.9.3. Applications and Uses

2.10. Quantum Cryptography
- 2.10.1. Quantum Algorithms
- 2.10.2. Algorithm Protection Against Quantum Computing
- 2.10.3. Quantum Key Distribution

Module 3. Business Continuity Plan Associated with Security

3.1. Business Continuity Plans
- 3.1.1. Business Continuity Plans (BCP)
- 3.1.2. Business Continuity Plans (BCP) Key Aspects
- 3.1.3. Business Continuity Plan (BCP) for Company Valuation

3.2. Metrics in Business Continuity Plans (BCP)
- 3.2.1. *Recovery Time Objective* (RTO) and *Recovery Point Objective* (RPO)
- 3.2.2. Maximum Tolerable Downtime (MTD)
- 3.2.3. Minimum Recovery Levels (ROL)
- 3.2.4. Recovery Point Objective (RPO)

3.3. Continuity Projects Types
- 3.3.1. Business Continuity Plans (BCP)
- 3.3.2. ICT Continuity Plan (ICTCP)
- 3.3.3. Disaster Recovery Plan (DRP)

3.4. Risk Management Associated with the BCP
- 3.4.1. Business Impact Analysis
- 3.4.2. Benefits of Implementing a BCP
- 3.4.3. Risk-Based Mentality

3.5. Life Cycle of a Business Continuity Plan
- 3.5.1. Phase 1: Analysis of the Organization
- 3.5.2. Phase 2: Determining the Continuity Strategy
- 3.5.3. Phase 3: Response to Contingency
- 3.5.4. Phase 4: Tests, Maintenance and Review

3.6. Organizational Analysis Phase of a BCP
- 3.6.1. Identification of Processes in the Scope of the BCP
- 3.6.2. Identification of Critical Business Areas
- 3.6.3. Identification of Dependencies between Areas and Processes
- 3.6.4. Determination of Appropriate BAT
- 3.6.5. Deliverables Creating a Plan

3.7. Phase of Determination of the Continuity Strategy in a BCP
- 3.7.1. Roles in the Strategy Determination Phase
- 3.7.2. Tasks of the Strategy Determination Phase
- 3.7.3. Deliverables

3.8. Contingency Response Phase in a BCP
- 3.8.1. Roles in the Response Phase
- 3.8.2. Tasks in this Phase
- 3.8.3. Deliverables

3.9. Testing, Maintenance and Revision Phase of a BCP
- 3.9.1. Roles in the Testing, Maintenance and Revision Phase
- 3.9.2. Tasks in the Testing, Maintenance and Revision Phase
- 3.9.3. Deliverables

3.10. ISO Standards Associated with Business Continuity Plans (BCP)
- 3.10.1. ISO 22301:2019
- 3.10.2. ISO 22313:2020
- 3.10.3. Other Related ISO and International Standards

"Companies in all industries will want to count on you to protect their most valuable data"

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

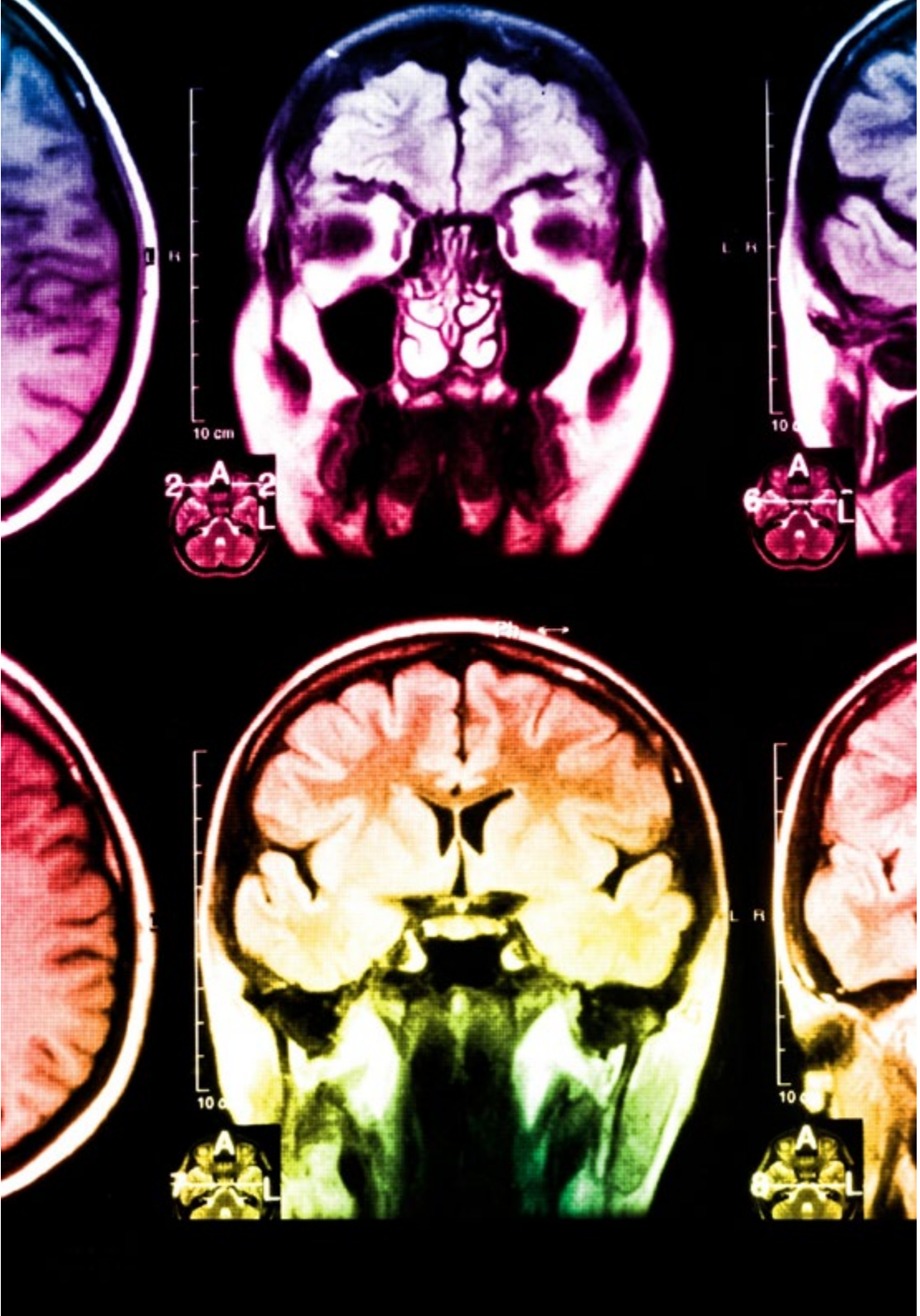
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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.

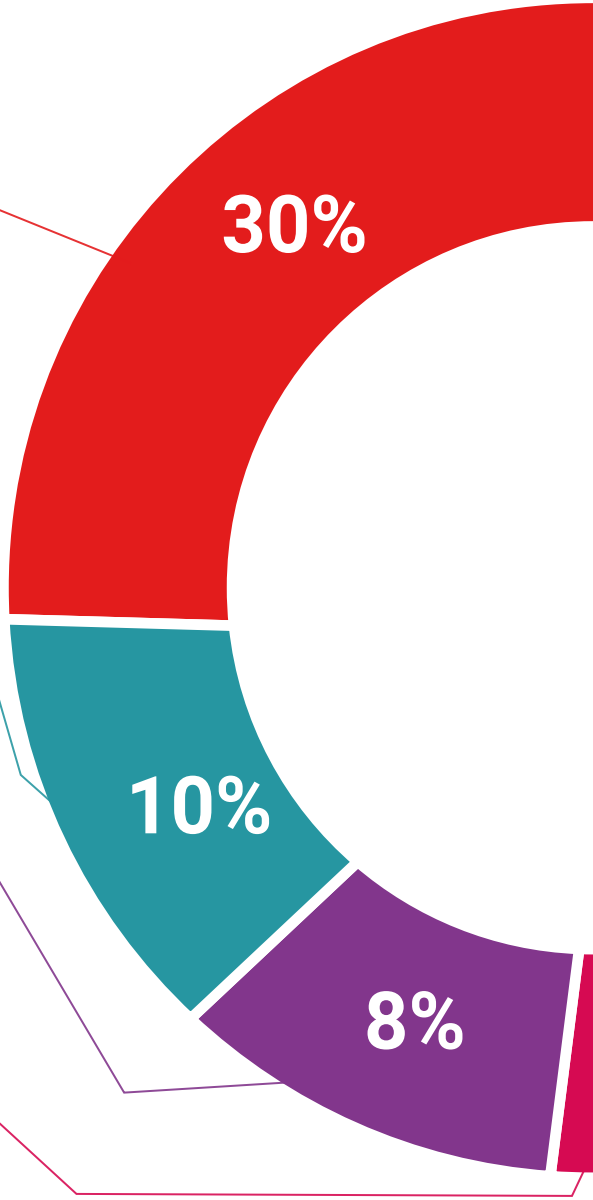
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

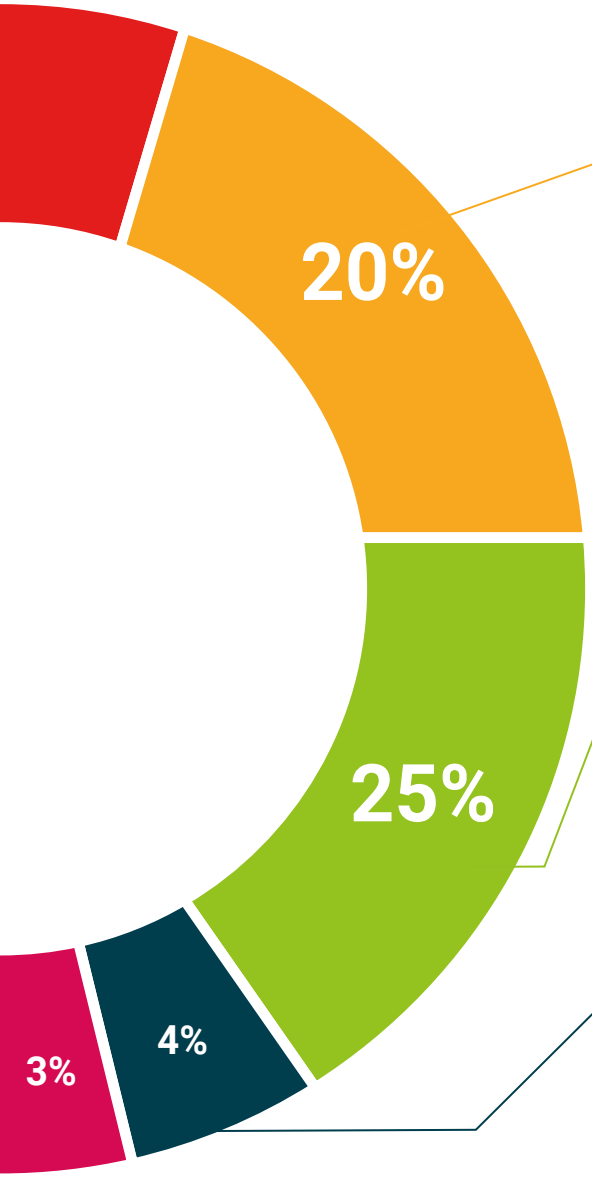
Practising Skills and Abilities

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 Security and Cryptography 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 Security and Cryptography** 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.

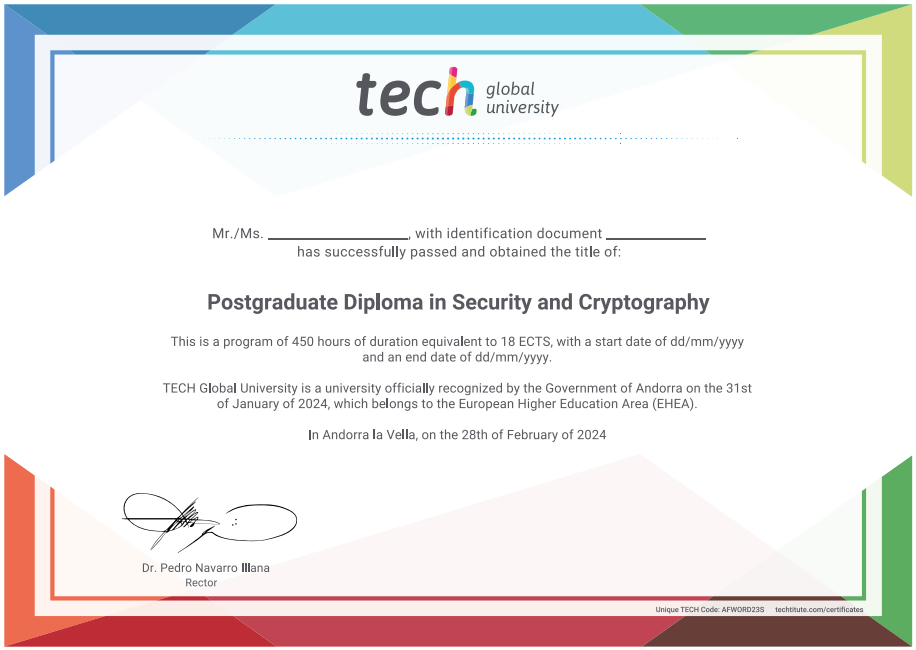
This **TECH Global University** title is a European program of continuing education and professional updating that guarantees the acquisition of competencies in its area of knowledge, providing a high curricular value to the student who completes the program.

Title: **Postgraduate Diploma in Security and Cryptography**

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 Security and Cryptography

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 additional cost.

tech global university

Postgraduate Diploma
Security and Cryptography

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

Postgraduate Diploma
Security and Cryptography

tech global university