Postgraduate Diploma
IT Security Management

tech technological university

tech technological university

Postgraduate Diploma
IT Security Management

- Modality: **online**
- Duration: **6 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

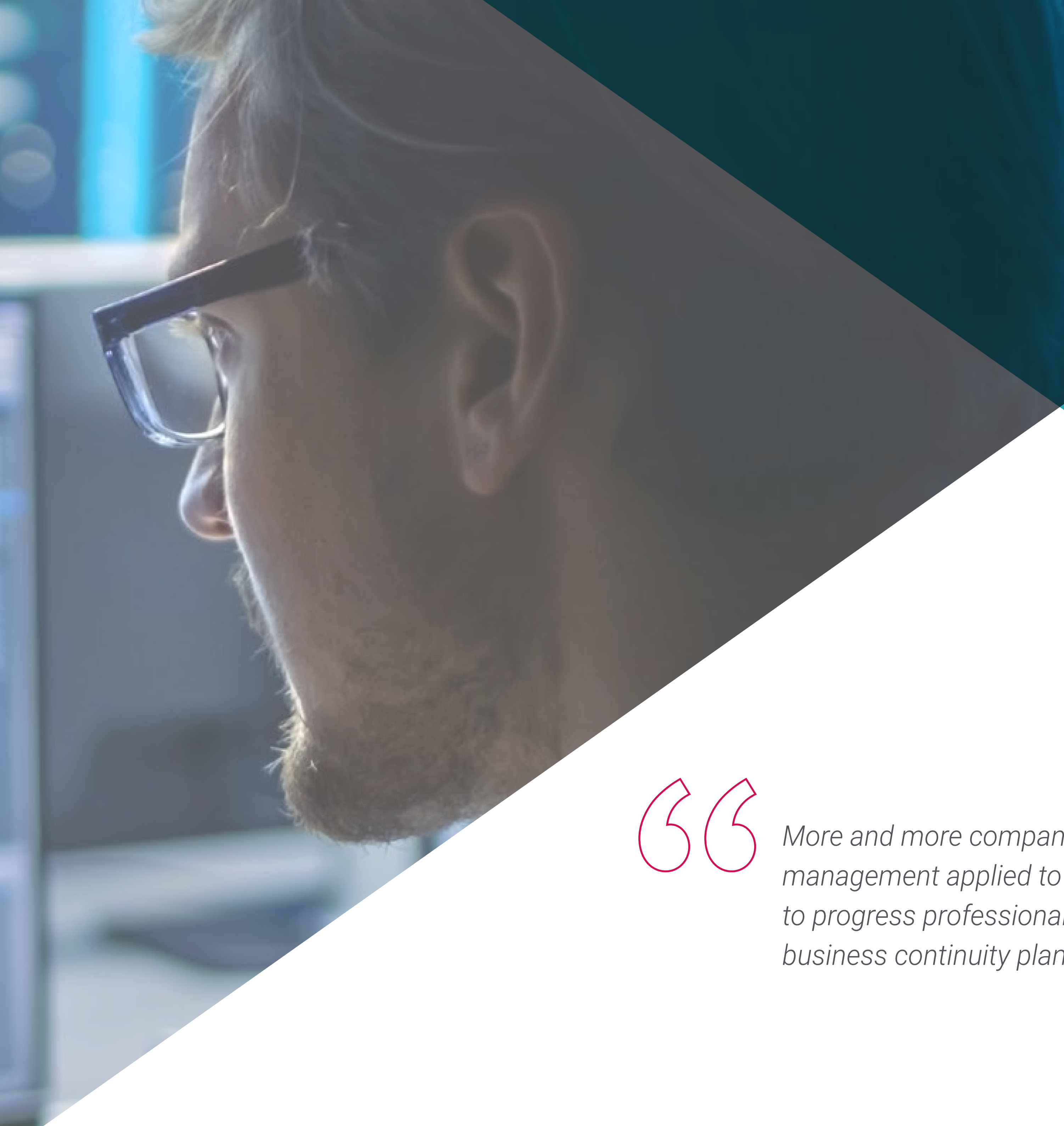
Website: **www.techtitute.com/in/information-technology/postgraduate-diploma/postgraduate-diploma-it-security-management**

Index

01

Introduction

The integration of IT in many companies has had a collateral effect: IT security risks have increased. Now, companies need to be aware of various attacks and vulnerabilities that can affect their proper functioning and services. For this reason, it is essential to have a specialist in the company in charge of managing security around these technologies. And this program offers the professional the opportunity to learn about the most advanced IT protection methods in this field, since it will delve into aspects such as risk assessment based on business parameters, identity and access management or intrusion testing.



More and more companies need specialists in security management applied to IT. This program will allow you to progress professionally, delving into issues such as business continuity planning associated with security"

It is a fact: there are hardly any companies that do not use digital and IT tools in their internal processes. Activities and operations such as employee identification, logistics systems or contact with suppliers and customers are now mainly carried out using information technology. But these technologies must be subject to proper design and monitoring, as they can be exploited to obtain data or to gain access to sensitive aspects of the company.

For this reason, the security management specialist is an increasingly in-demand position, and cannot be filled by just any IT specialist. Highly up-to-date knowledge that takes into account the latest developments in cybersecurity is required. Thus, this Postgraduate Diploma has been designed to offer the professional the latest advances in this area, delving into issues such as security audits, terminal equipment security, or the most effective response to different incidents.

This program is also developed in a 100% online format that adapts to the circumstances of the professional, allowing them to study when, where and however they want. It will also have a teaching staff of great prestige in the field of cybersecurity that will be supported by numerous multimedia resources to make the learning process comfortable, fast and effective.

This **Postgraduate Diploma in IT Security Management** contains the most complete and up-to-date educational 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

> *This program will allow you to go deeper into aspects such as the life cycle of a business continuity plan or vulnerability management"*

TECH provides you with the best multimedia resources: case studies, theoretical and practical activities, videos, interactive summaries... Everything so that the learning process is agile and you can take advantage of every minute invested"

You will be able to respond appropriately to all types of cybersecurity threats. Enroll and become a leading specialist.

Study at your own pace, without interruptions or rigid schedules: TECH's teaching method is that convenient.

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.

02

Objectives

Taking into account the growing complexity of the cybersecurity field, the main goal of this Postgraduate Diploma in IT Security Management is to bring the professional closer to the most important developments in this field. In this way, you will be able to become a leading specialist in the field, being able to work managing and directing cybersecurity of companies in all types of sectors.

> *TECH helps you to achieve your goals thanks to this program, with which you can apply for important professional positions in the most important national and international companies"*

General Objectives

- Develop an Information Security Management System (ISMS)
- Identify the key elements that make up an ISMS
- Evaluate the different security architecture models to establish the most appropriate model for the organization
- Identify the regulatory frameworks of application and their regulatory bases
- Analyze the organizational and functional structure of an information security area (the CISO's office)
- Establish an audit program that meets the organization's cybersecurity self-assessment needs
- Develop a vulnerability scanning and monitoring program and a cybersecurity incident response plan
- 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

Specific Objectives

Module 1. Information Security Architectures and Models

- Align the Safety Management Plan with the strategic objectives of the organization
- Establish an ongoing risk management framework as an integral part of the Security Management Plan
- Determine appropriate indicators for monitoring the implementation of the ISMS
- Establish a policy-based security strategy
- Analyze the objectives and procedures associated with the employee, supplier and partner awareness plan
- Identify, within the regulatory framework, the regulations, certifications and laws applicable in each organization
- Develop the fundamental elements required by the ISO 27001:2013 standard
- Implement a privacy management model in line with the European GDPR/RGPD regulation

Module 2. IT Security Management

- Identify the different structures that an information security area can have
- Develop a security model based on three lines of defense
- Present the different periodic and extraordinary committees in which the cybersecurity area is involved
- Specify the technological tools that support the main functions of the security operations team (SOC)
- Evaluate vulnerability control measures appropriate to each scenario
- Develop the security operations framework based on the NIST CSF
- Specify the scope of the different types of audits (Red Team, Pentesting, Bug Bounty, etc.)
- Propose the activities to be carried out after a security incident
- Set up an information security command center that encompasses all relevant stakeholders (authorities, customers, suppliers, etc.)

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 successful Business Continuity Plan Implementation for our Business

> *You will be the leading IT security specialist in your environment. Don't wait any longer: enroll now"*

03

Course Management

Having at your disposal the greatest international specialists in security management in the field of IT is a great opportunity for professionals. And that is exactly what this University Expert offers, which has a teaching staff made up of prestigious engineers and computer scientists who will provide the student with the most advanced techniques and procedures to guarantee the internal security of a company.

You will be in contact with the leading specialists in cybersecurity, who will give you all the keys to work at the highest level in this area"

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 for companies
- Teacher Blockchain Training for Businesses

Professors

Mr. Tobal Redondo, Javier

- HUAWEI Application Innovation Program Manager
- Information Security Manager of the Payment Division Amadeus IT Group
- Chief Information Security Officer FINTONIC, Financial Services
- Services Engineer and Architect in the Services and Security Planning and Architecture Area at Amena / Orange Spain
- Degree in Computer Science from the University of Deusto (Bilbao, Spain)
- Postgraduate degree in Industrial Computing Industrial Engineering School Bilbao

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

The syllabus of this Postgraduate Diploma in IT Security Management has been structured into 3 modules that will be developed throughout 450 hours of learning. During this period, the professional will delve into relevant aspects of this sector such as forensic analysis, information security models, the regulatory framework applicable in this area or the configuration of network security rules, among many other issues.

> *You will have at your disposal the most comprehensive syllabus, presented through didactic resources that you can access 24 hours a day”*

Module 1. Information Security Architectures and Models

1.1. Information Security Architecture
- 1.1.1. ISMSI / PDS
- 1.1.2. Strategic Alignment
- 1.1.3. Risk Management
- 1.1.4. Performance Measurement

1.2. Information Security Models
- 1.2.1. Based on Security Policies
- 1.2.2. Based on Protection Tools
- 1.2.3. Bases on Teamwork

1.3. Security Model Key Components
- 1.3.1. Risk Identification
- 1.3.2. Definition of Controls
- 1.3.3. Continuous Assessment of Risk Levels
- 1.3.4. Awareness Plan for Employees, Suppliers, Partners, etc.

1.4. Risk Management Process
- 1.4.1. Asset Identification
- 1.4.2. Threat Identification
- 1.4.3. Risk Assessment
- 1.4.4. Prioritization of Controls
- 1.4.5. Reassessment and Residual Risk

1.5. Business Processes and Information Security
- 1.5.1. Business Processes
- 1.5.2. Risk Assessment Based on Business Parameters
- 1.5.3. Business Impact Analysis
- 1.5.4. Business Operations and Information Security

1.6. Continuous Improvement Process
- 1.6.1. Deming's Cycle
  - 1.6.1.1. Planning
  - 1.6.1.2. Do
  - 1.6.1.3. Verify
  - 1.6.1.4. Act

1.7. Security Architectures
- 1.7.1. Selection and Homogenization of Technologies
- 1.7.2. Identity Management Authentication
- 1.7.3. Access Management Authorization
- 1.7.4. Network Infrastructure Security
- 1.7.5. Encryption Technologies and Solutions
- 1.7.6. Endpoint Detection and Response (EDR)

1.8. Regulatory Framework
- 1.8.1. Sectoral Regulations
- 1.8.2. Certifications
- 1.8.3. Legislations

1.9. The ISO 27001 Standard
- 1.9.1. Implementation
- 1.9.2. Certification
- 1.9.3. Audits and Penetration Tests
- 1.9.4. Continuous Risk Management
- 1.9.5. Classification of Information

1.10. Privacy Legislation GDPR
- 1.10.1. Scope of General Data Protection Regulation (GDPR)
- 1.10.2. Personal Data
- 1.10.3. Roles in the Processing of Personal Data
- 1.10.4. ARCO Rights
- 1.10.5. DPO Functions

Module 2. IT Security Management

- 2.1. Safety Management
  - 2.1.1. Security Operations
  - 2.1.2. Legal and Regulatory Appearance
  - 2.1.3. Business Authorization
  - 2.1.4. Risk Management
  - 2.1.5. Identity and Access Management
- 2.2. Structure of the Security Area The CISO's office
  - 2.2.1. Organisational Structure. Position of the CISO in the Structure
  - 2.2.2. Lines of Defence
  - 2.2.3. CISO Office Organization Chart
  - 2.2.4. Budget Management
- 2.3. Government Security
  - 2.3.1. Security Committee
  - 2.3.2. Risk Monitoring Committee
  - 2.3.3. Audit Committee
  - 2.3.4. Crisis Committee
- 2.4. Government Security Functions
  - 2.4.1. Policies and Standards
  - 2.4.2. Security Management Plan
  - 2.4.3. Control Panels
  - 2.4.4. Awareness and Training
  - 2.4.5. Supply Chain Security
- 2.5. Security Operations
  - 2.5.1. Identity and Access Management
  - 2.5.2. Configuration of Network Security Rules Firewalls
  - 2.5.3. IDS/IPS Platform Management
  - 2.5.4. Vulnerability Analysis
- 2.6. Cybersecurity Framework NIST CSF
  - 2.6.1. NIST Methodology
    - 2.6.1.1. Log In
    - 2.6.1.2. Protect
    - 2.6.1.3. Detect
    - 2.6.1.4. Respond
    - 2.6.1.5. Recover
- 2.7. Security Operations Center (SOC) Functions
  - 2.7.1. Protection *Red Team, Pentesting, Threat Intelligence*
  - 2.7.2. Detection SIEM, *User Behavior Analytics, Fraud Prevention*
  - 2.7.3. Response
- 2.8. Security Audits
  - 2.8.1. Intrusion Test
  - 2.8.2. *Red Team* Exercises
  - 2.8.3. Source Code Audits Secure Development
  - 2.8.4. Component Safety (*Software Supply Chain*))
  - 2.8.5. Forensic Analysis
- 2.9. Incident Response
  - 2.9.1. Preparation
  - 2.9.2. Detection, Analysis and Reporting
  - 2.9.3. Containment, Eradication and Recovery
  - 2.9.4. Post-Incident Activity
    - 2.9.4.1. Retention of Evidence
    - 2.9.4.2. Forensic Analysis
    - 2.9.4.3. Gap Management
  - 2.9.5. Official Cyber Incident Management Guides
- 2.10. Vulnerability Management
  - 2.10.1. Vulnerability Analysis
  - 2.10.2. Vulnerability Assessment
  - 2.10.3. System Basing
  - 2.10.4. Day 0 Vulnerabilities Zero-Day

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

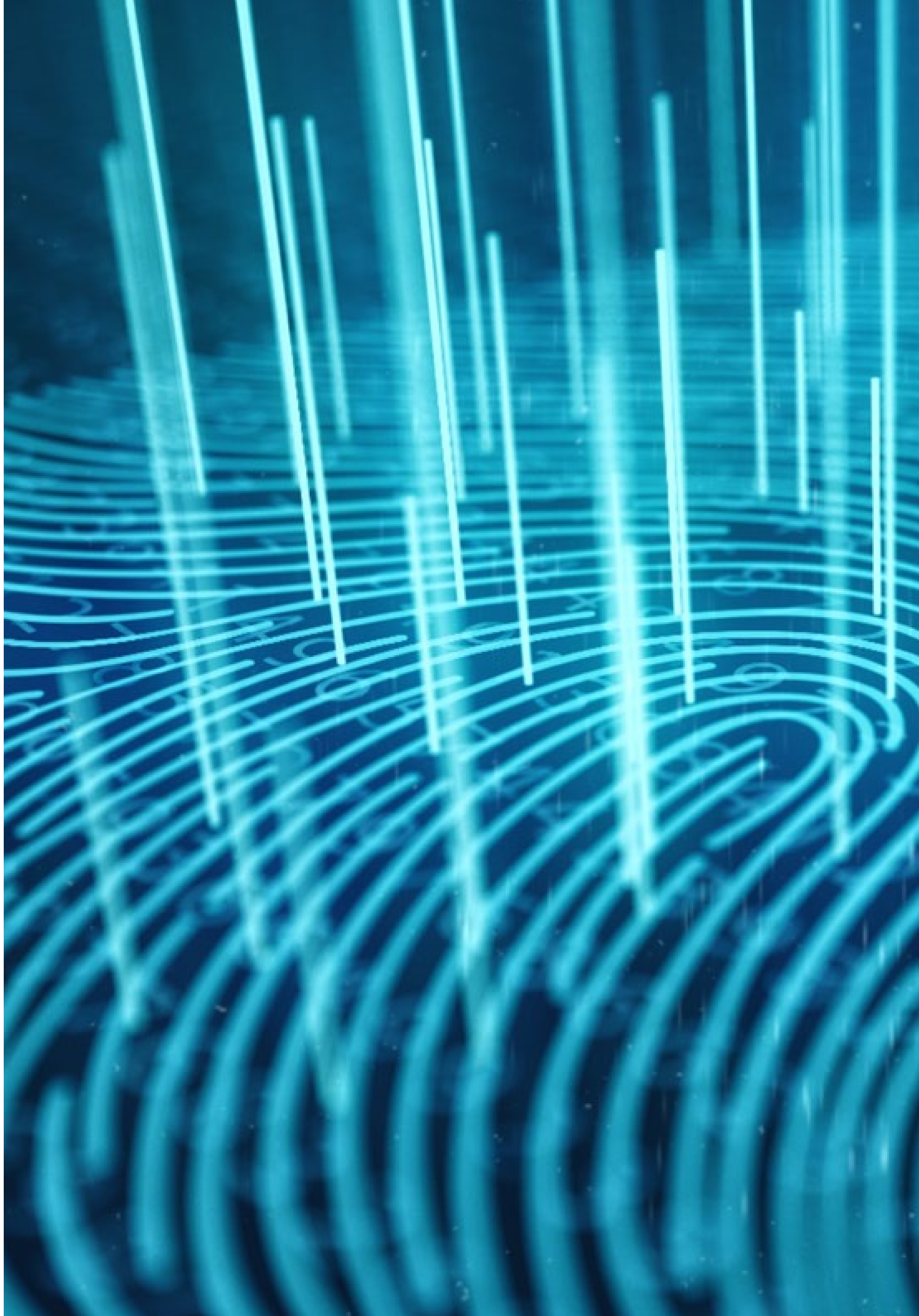
3.2. Metrics in Business Continuity Plans (BCP)
- 3.2.1. *Recovery Time Objective* (RTO) and *Recovery Point Objective* (RPO)
- 3.2.2. Maximum Tolerable Downtime (MTD)
- 3.2.3. Minimum Recovery Levels (ROL)
- 3.2.4. Recovery Point Objective (RPO)

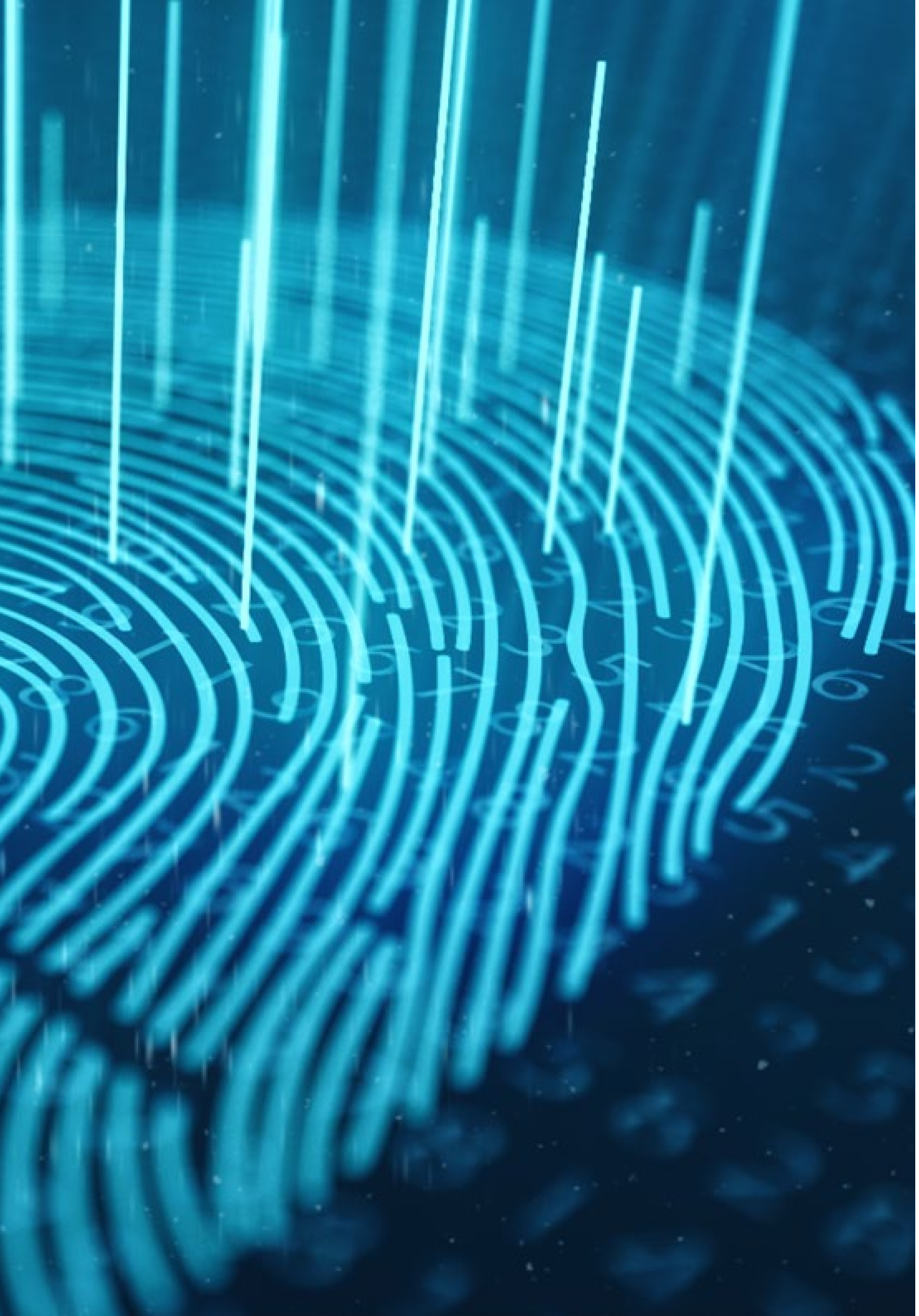
3.3. Continuity Projects Types
- 3.3.1. Business Continuity Plans (BCP)
- 3.3.2. ICT Continuity Plan (ICTCP)
- 3.3.3. Disaster Recovery Plan (DRP)

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: Organization Analysis
- 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

> *This program will allow you to delve into issues such as identifying dependencies between areas and processes, a fundamental aspect to establish correct cybersecurity"*

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

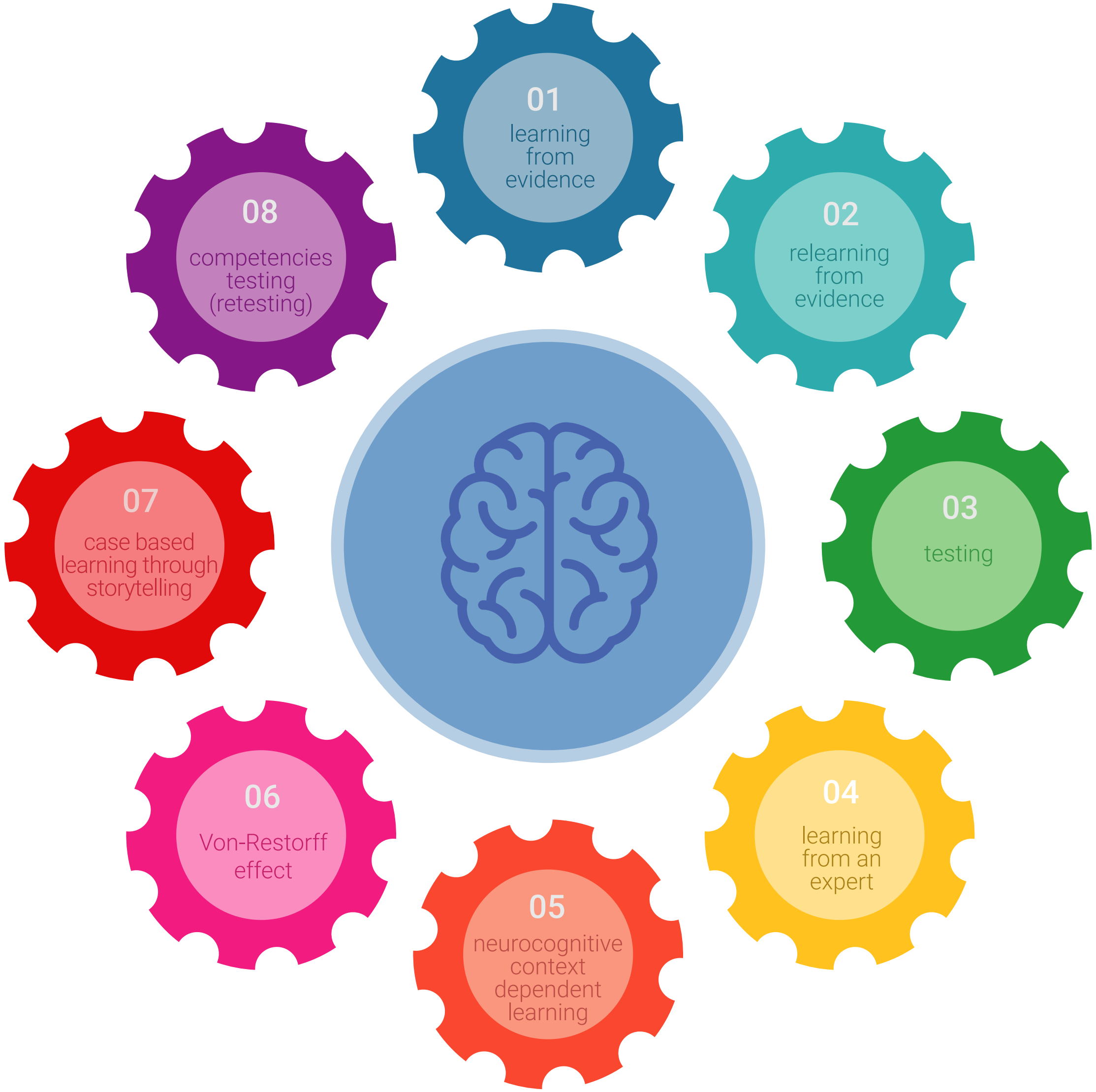
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

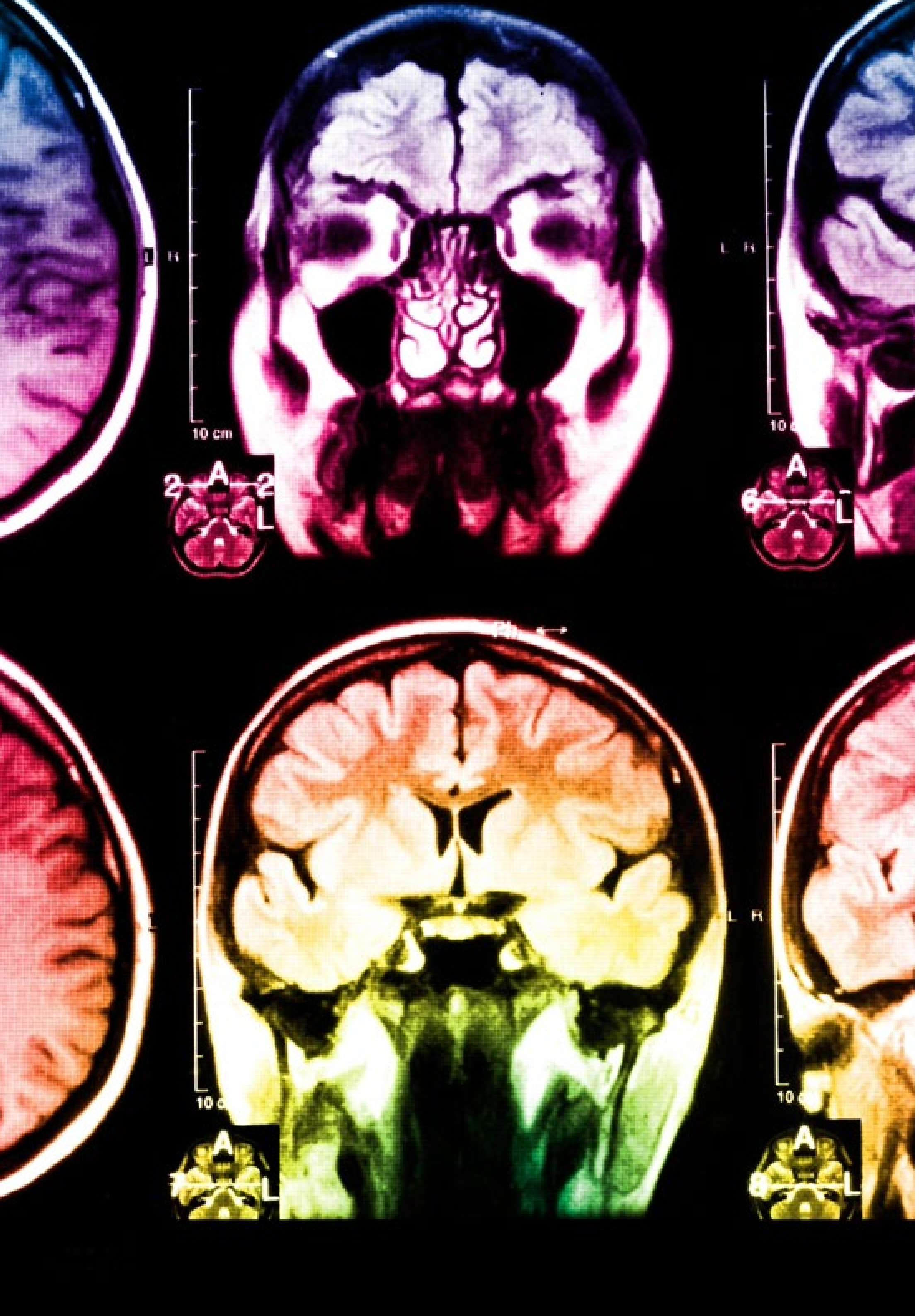
We enhance the Case Study with the best 100% online teaching method: Relearning.

> *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.

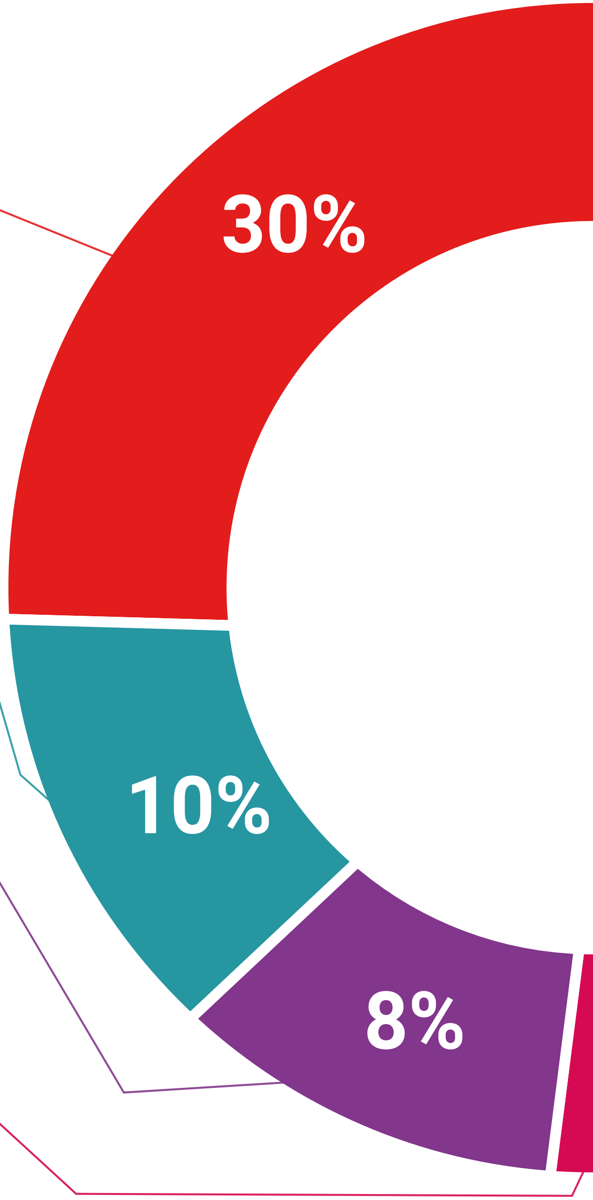
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

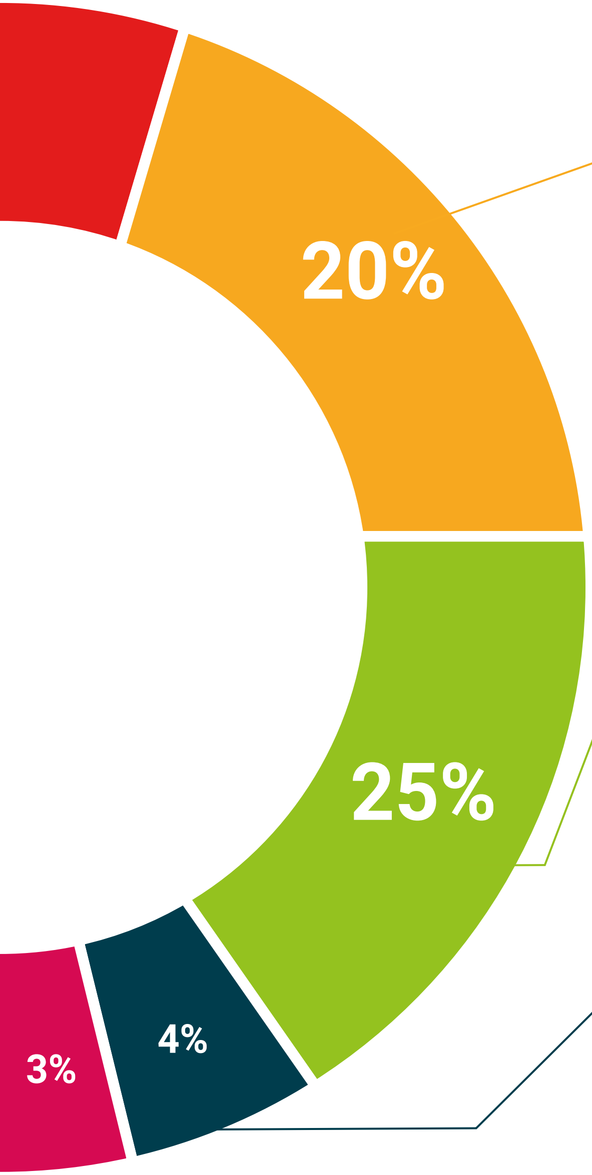
Practising Skills and Abilities

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 IT Security Management guarantees students, in addition to the most rigorous and up-to-date education, access to a Postgraduate Diploma issued by TECH Technological University.

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

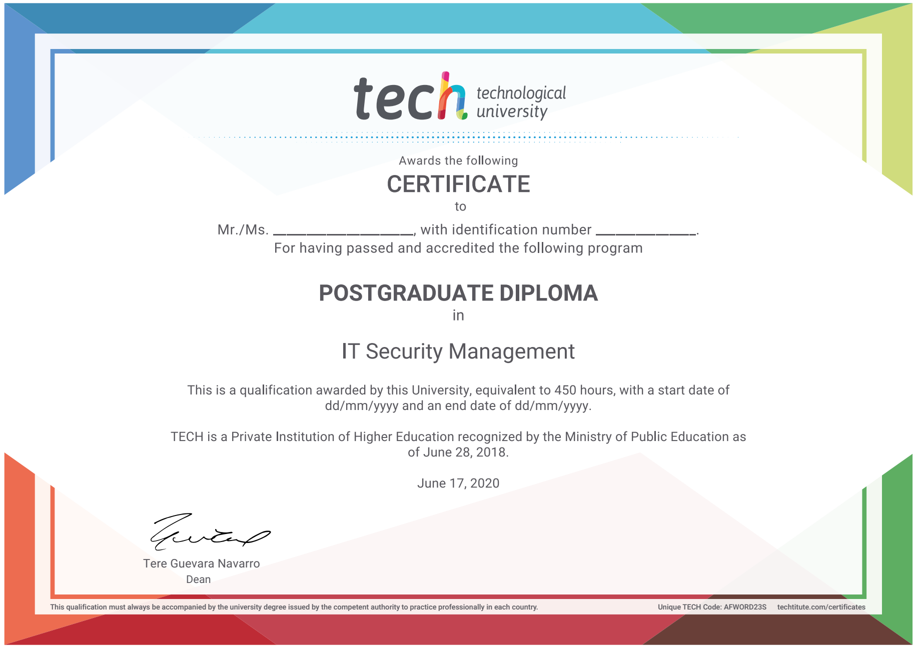
This **Postgraduate Diploma in IT Security Management** contains the most complete and up-to-date program on the market.

After the student has passed the assessments, they will receive their corresponding **Postgraduate Diploma** issued by **TECH Technological University** via tracked delivery*.

The certificate issued by **TECH Technological University** will reflect the qualification obtained in the Postgraduate Diploma, and meets the requirements commonly demanded by labor exchanges, competitive examinations, and professional career evaluation committees.

Title: **Postgraduate Diploma in IT Security Management**

Official N° of Hours: **450 h.**



tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. _______________, with identification number ___________.

For having passed and accredited the following program

POSTGRADUATE DIPLOMA

in

IT Security Management

This is a qualification awarded by this University, equivalent to 450 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH is a Private Institution of Higher Education recognized by the Ministry of Public Education as of June 28, 2018.

June 17, 2020

Tere Guevara Navarro
Dean

This qualification must always be accompanied by the university degree issued by the competent authority to practice professionally in each country.

Unique TECH Code: AFWORD23S techtitute.com/certificates

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

tech technological university

Postgraduate Diploma
IT Security Management

- Modality: **online**
- Duration: **6 months**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Postgraduate Diploma
IT Security Management

tech technological university