Postgraduate Diploma
Security in Software Engineering

tech technological university

tech technological university

Postgraduate Diploma
Security in Software Engineering

- 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-security-software-engineering

Index

01
Introduction

This high-quality program will allow the student to learn about the information security process, its implications in confidentiality, integrity, availability and economic costs, as well as to understand the problems related to software security, its vulnerabilities and their classification.

With this highly scientifically rigorous program, the professional will acquire the knowledge required for internal IT control and for assessing and detecting vulnerabilities in online applications.

Specialize in computer systems with the help of professionals with extensive experience in the sector”

This comprehensive program in Security in *Software* Engineering will allow professionals in the IT industry to deepen their understanding and learn about the processes of management and monitoring of quality and secure software that meets the predefined requirements.

This Postgraduate Diploma specializes students in security in *software* engineering, with the aim of providing them with the knowledge and tools required for the design and control of complex systems, which reliably provide the answer to established problems.

The main objective of this training is that the student gains the ability to incorporate substantial qualitative improvements, providing new solutions to specific problems that arise. It also aims to educate professionals to be capable of using a systematic and quantifiable approach to software development and maintenance, so that they also obtain in-depth knowledge of computer programming and the implementation and planning of computer systems, from a practical perspective and adapted to the current reality.

With this program the student will have access to the most advanced teaching resources and will have the opportunity to study a program that brings together the most in-depth knowledge in the field. A group of highly scientifically qualified professors with extensive international experience will provide students with the most complete and up-to-date information on the latest advances and techniques in *Software* and Computer Systems Engineering.

The syllabus covers the main current topics in Security in *Software* Engineering in such a way that whoever masters them will be prepared to work in this field. Therefore, it is not just another diploma in your backpack, but a real learning tool to approach the topics of the specialty in a modern, objective way and with the ability to make a judgment based on today's most cutting-edge information.

It should be noted that since it is a 100% online Postgraduate Diploma, the student is not conditioned by fixed schedules or the need to move to another physical location, but can access the contents at any time of the day, balancing their work or personal life with their academic life.

If they want to differentiate themselves from others and be capable of designing complex systems engineering projects, this is the program for them.

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

- Practical cases presented by experts in Security in *Software* Engineering
- The graphic, schematic, and practical contents with which they are created, provide scientific and practical information on the disciplines that are essential for professional development
- Practical exercises where self-assessment can be used to improve learning
- Its special emphasis on innovative methodologies in the field of *Software* Engineering
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- Content that is accessible from any fixed or portable device with an Internet connection

> “*The completion of this Postgraduate Diploma will place professionals in Security in Software Engineering at the forefront of the latest developments in the sector"*

This Postgraduate Diploma is the best investment you can make when selecting a refresher program in the field of Security in Software Engineering. We offer you quality and free access to content"

This program comes with the best educational material, providing you with a contextual approach that will facilitate your learning.

This 100% online Postgraduate Diploma will allow you to combine your studies with your professional work. You choose where and when to train.

Its teaching staff includes professionals belonging to the field of Security in *Software* Engineering, who contribute their work experience to this training, as well as renowned specialists from reference 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 learning 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, the professional will be assisted by an innovative interactive video system developed by renowned and experienced experts in Security in *Software* Engineering.

02

Objectives

The Postgraduate Diploma in Security in *Software* Engineering is aimed at facilitating the performance of the professional to acquire and know the main developments in this field, which will allow them to practice their profession with the highest quality and professionalism.

> Our goal is for you to become the best professional in your sector. And for this we have the best methodology and content"

General Objectives

- Acquire new knowledge in Security in *Software* Engineering
- Acquire new skills in terms of new technologies and the latest software developments
- Process the data generated in *Software* Engineering activities

> *Improving your skills in the field of Security in Software Engineering will allow you to be more competitive. Continue your studies and give your career a boost"*

Specific Objectives

Module 1. Safety Management

- Know the information security process, its implications on confidentiality, integrity, availability and economic costs
- Learn the use of good security practices in the management of information technology services
- Acquire the knowledge for the correct certification of security processes
- Understand authentication mechanisms and methods for access control, as well as the access audit process
- Understand security management programs, risk management and security policy design
- Learn about business continuity plans, their phases and maintenance process
- Know the procedures for the correct protection of the company through DMZ networks, the use of intrusion detection systems and other methodologies

Module 2. *Software* Security

- Understand software security issues, vulnerabilities and how they are classified
- Know the design principles, methodologies and standards in software security
- Understand the application of security in the different phases of the software life cycle
- Acquire the knowledge required for the safe coding of software and the evaluation techniques
- Understand the methodologies and processes to guarantee security during the development and delivery of cloud services
- Understand the basics of cryptology and the different encryption techniques currently available

Module 3. Security Audit

- Acquire the knowledge required for the correct execution of the audit process and internal computer control
- Understand the processes to carry out for the security audit in systems and networks
- Understand the different support tools, methodologies and subsequent analysis during internet and mobile device security auditing
- Learn the properties and influencing factors that condition business risks and determine the correct implementation of appropriate risk management
- Know the risk mitigation measures, as well as the methodologies for the implementation of an Information Security Management System and the norms and standards to be used
- Understand the procedures for conducting the security audit, its traceability and presentation of results

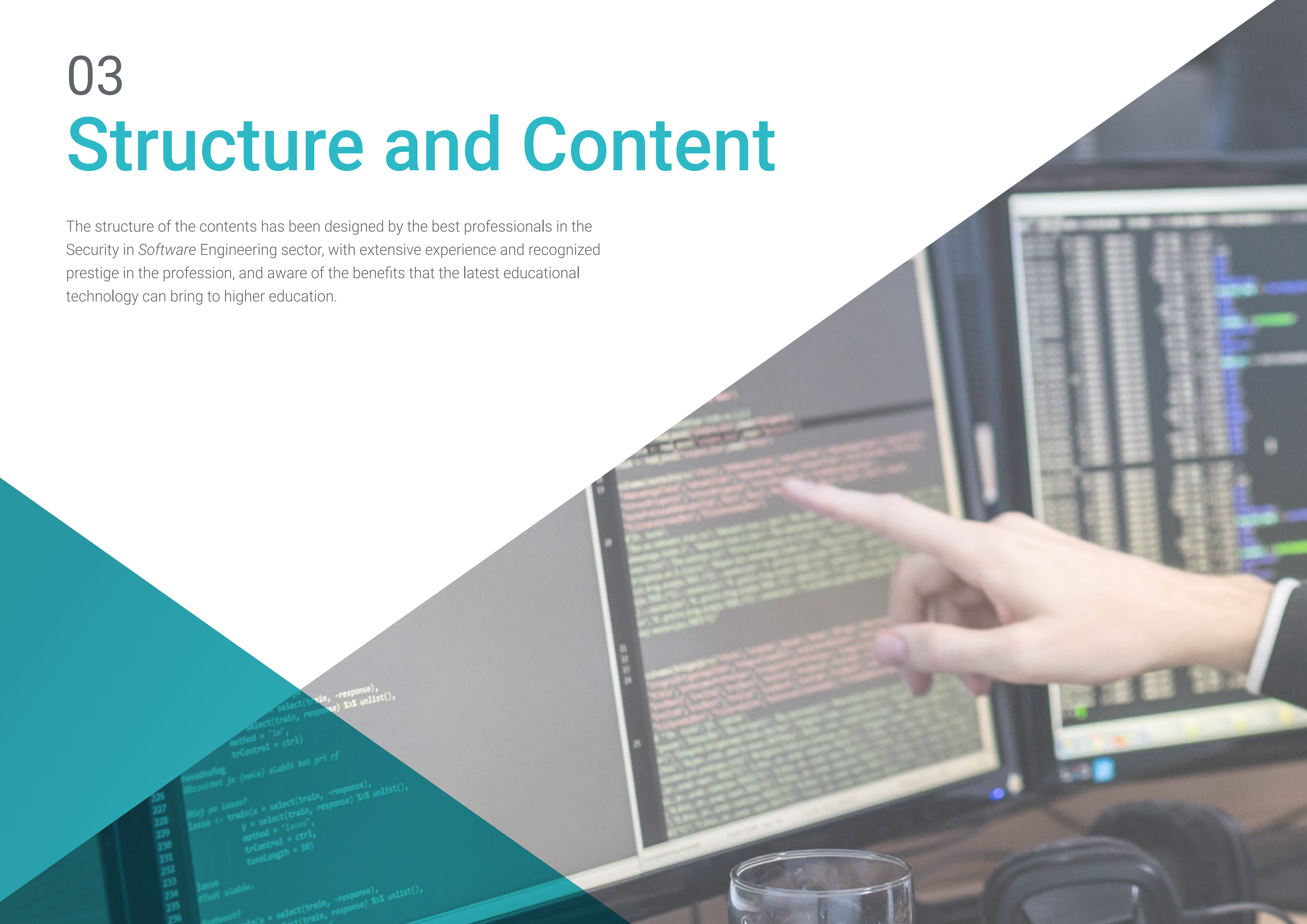
Module 4. Online Applications Security

- Acquire the knowledge required to evaluate and detect the vulnerabilities of online applications
- Understand the security policies and standards to be applied to online applications
- Know the procedures to use during the development of web applications and their subsequent evaluation through analysis and security tests
- Learn the security measures for the deployment and production of web applications
- Understand the concepts, functions and technologies to be applied in the security of web services, as well as security tests and protective measures
- Assimilate the procedures for ethical hacking, malware analysis and forensics
- Know the mitigation and containment measures for incidents on web services
- Acquire the knowledge to implement best practice techniques for the development and implementation of online applications as well as the most common errors

03

Structure and Content

The structure of the contents has been designed by the best professionals in the Security in *Software* Engineering sector, with extensive experience and recognized prestige in the profession, and aware of the benefits that the latest educational technology can bring to higher education.



We have the most complete and up-to-date scientific program on the market. We strive for excellence and for you to achieve it too”

Module 1. Safety Management

1.1. Information Security
- 1.1.1. Introduction
- 1.1.2. Information Security Involves Confidentiality, Integrity and Availability
- 1.1.3. Safety is an Economic Issue
- 1.1.4. Safety is a Process
- 1.1.5. Classification of Information
- 1.1.6. Information Security Involves Risk Management
- 1.1.7. Security is Articulated with Security Controls
- 1.1.8. Security is both Physical and Logical
- 1.1.9. Safety Involves People

1.2. The Information Security Professional
- 1.2.1. Introduction
- 1.2.2. Information Security as a Profession
- 1.2.3. Certifications (ISC)2
- 1.2.4. The ISO 27001 Standard
- 1.2.5. Best Security Practices in IT Service Management
- 1.2.6. Information Security Maturity Models
- 1.2.7. Other Certifications, Standards and Professional Resources

1.3. Access Control
- 1.3.1. Introduction
- 1.3.2. Access Control Requirements
- 1.3.3. Authentication Mechanisms
- 1.3.4. Authorization Methods
- 1.3.5. Access Accounting and Auditing
- 1.3.6. Triple A" Technologies

1.4. Information Security Programs, Processes and Policies
- 1.4.1. Introduction
- 1.4.2. Security Management Programs
- 1.4.3. Risk Management
- 1.4.4. Design of Security Policies

1.5. Business Continuity Plans
- 1.5.1. Introduction to BCPs
- 1.5.2. Phase I and II
- 1.5.3. Phase III and IV
- 1.5.4. Maintenance of the BCP

1.6. Procedures for the Correct Protection of the Company
- 1.6.1. DMZ Networks
- 1.6.2. Intrusion Detection Systems
- 1.6.3. Access Control Lists
- 1.6.4. Learning from the Attacker: *Honeypot*

1.7. Security Architecture Prevention
- 1.7.1. Overview. Activities and Layer Model
- 1.7.2. Perimeter Defence (*Firewalls, WAFs*, WAFs, IPS etc.)
- 1.7.3. Endpoint Defence (Equipment, Servers and Services)

1.8. Security Architecture Detection
- 1.8.1. Overview Detection and Monitoring
- 1.8.2. *Logs*, Encrypted Traffic Breaking, Recording and *Siems*
- 1.8.3. Alerts and Intelligence

1.9. Security Architecture Reaction
- 1.9.1. Reaction Products, Services and Resources
- 1.9.2. Incident Management
- 1.9.3. CERTS y CSIRTs

1.10. Security Architecture Recuperation
- 1.10.1. Resilience, Concepts, Business Requirements and Regulations
- 1.10.2. IT Resilience Solutions
- 1.10.3. Crisis Management and Governance

Module 2. *Software* Security

2.1. Problems of the Software Security
- 2.1.1. Introduction to the Problem of Software Security
- 2.1.2. Vulnerabilities and their Classification
- 2.1.3. Secure Software Properties
- 2.1.4. References

2.2. Software Security Design Principles
- 2.2.1. Introduction
- 2.2.2. Software Security Design Principles
- 2.2.3. Types of S-SDLC
- 2.2.4. Software Security in S-SDLC Phases
- 2.2.5. Methodologies and Standards
- 2.2.6. References

2.3. Software Lifecycle Safety in the Requirements and Design Phases
- 2.3.1. Introduction
- 2.3.2. Attack Modeling
- 2.3.3. Cases of Abuse
- 2.3.4. Safety Requirements Engineering
- 2.3.5. Risk Analysis Architectural
- 2.3.6. Design Patterns
- 2.3.7. References

2.4. Software Lifecycle Safety in the Coding, Testing and Operation Phases
- 2.4.1. Introduction
- 2.4.2. Risk-Based Safety Testing
- 2.4.3. Code Review
- 2.4.4. Penetration Test
- 2.4.5. Security Operations
- 2.4.6. External Review
- 2.4.7. References

2.5. Secure Coding Applications I
- 2.5.1. Introduction
- 2.5.2. Secure Coding Practices
- 2.5.3. Manipulation and Validation of Inputs
- 2.5.4. Memory Overflow
- 2.5.5. References

2.6. Secure Coding Applications II
- 2.6.1. Introduction
- 2.6.2. *Integers Overflows*, Truncation Errors and Problems with Type Conversions between Integers
- 2.6.3. Errors and Exceptions
- 2.6.4. Privacy and Confidentiality
- 2.6.5. Privileged Programs
- 2.6.6. References

2.7. Development and Cloud Security
- 2.7.1. Safety in Development; Methodology and Practice
- 2.7.2. PaaS, IaaS, CaaS and SaaS Models
- 2.7.3. Security in the Cloud and for Cloud Services

2.8. Encryption
- 2.8.1. Fundamentals of Cryptology
- 2.8.2. Symmetric and Asymmetric Encryption
- 2.8.3. Encryption at Rest and in Transit

2.9. Security Automation and Orchestration (SOAR)
- 2.9.1. Complexity of Manual Processing; Need to Automate Tasks
- 2.9.2. Products and Services
- 2.9.3. SOAR Architecture

2.10. Telework Safety
- 2.10.1. Need and Scenarios
- 2.10.2. Products and Services
- 2.10.3. Telework Safety

Module 3. Security Audit

3.1. Introduction to Information Systems in the Company
- 3.1.1. Introduction to Information Systems in the Company and the Role of IT Auditing
- 3.1.2. Definitions of "IT Audit" and "IT Internal Control"
- 3.1.3. Functions and Objectives of IT Auditing
- 3.1.4. Differences between Internal Control and IT Auditing

3.2. Internal Controls of Information Systems
- 3.2.1. Functional Flowchart of a Data Processing Center
- 3.2.2. Classification of Information Systems Controls
- 3.2.3. The Golden Rule

3.3. The Process and Phases of the Information Systems Audit
- 3.3.1. Risk Assessment and Other IT Auditing Methodologies
- 3.3.2. Execution of an Information Systems Audit. Phases of the Audit
- 3.3.3. Fundamental Skills of the Auditor of an IT System

3.4. Technical Audit of Security in Systems and Networks
- 3.4.1. Technical Security Audits. Intrusion Test. Previous Concepts
- 3.4.2. Security Audits in Systems. Support Tools
- 3.4.3. Security Audits in Networks. Support Tools

3.5. Technical Audit of Security on the Internet and in Mobile Devices
- 3.5.1. Internet Security Audit. Support Tools
- 3.5.2. Mobile Devices Security Audit. Support Tools
- 3.5.3. Annex 1. Structure of an Executive Report and Technical Report
- 3.5.4. Annex 2. Tools Inventory
- 3.5.5. Annex 3. Methods

3.6. Information Security Management System
- 3.6.1. Security of IS: Properties and Influential Factors
- 3.6.2. Business Risks and Risk Management: Implementing Controls
- 3.6.3. Information Security Management System (ISMS): Concept and Critical Success Factors
- 3.6.4. ISMS-PDCA Model
- 3.6.5. ISMS ISO-IEC 27001: Organizational Context
- 3.6.6. Annex 4. Context of the Organization
- 3.6.7. Annex 5. Leadership.
- 3.6.8. Annex 6. Planning
- 3.6.9. Annex 7. Support
- 3.6.10. Annex 8. Operation
- 3.6.11. Annex 9. Performance Evaluation
- 3.6.12. Annex 10. Improvement
- 3.6.13. Annex to ISO 27001/ISO-IEC 27002: Objectives and Controls
- 3.6.14. ISMS Audit

3.7. Carrying Out the Audit
- 3.7.1. Procedures
- 3.7.2. Techniques

3.8. Traceability
- 3.8.1. Methods
- 3.8.2. Analysis

3.9. Copyright
- 3.9.1. Techniques
- 3.9.2. Results

3.10. Reports and Presenting Proof
- 3.10.1. Types of Reports
- 3.10.2. Data Analysis
- 3.10.3. Presenting Proof

Module 4. Online Application Security

4.1. Vulnerabilities and Security Issues in Online Applications
- 4.1.1. Introduction to Online Application Security
- 4.1.2. Security Vulnerabilities in the Design of Web Applications
- 4.1.3. Security Vulnerabilities in the Implementation of Web Applications
- 4.1.4. Security Vulnerabilities in the Deployment of Web Applications
- 4.1.5. Official Lists of Security Vulnerabilities

4.2. Policies and Standards for Online Application Security
- 4.2.1. Pillars for the Security of Online Applications
- 4.2.2. Security Policy
- 4.2.3. Information Security Management System
- 4.2.4. Secure Software Development Life Cycle
- 4.2.5. Standards for Application Security

4.3. Security in the Design of Web Applications
- 4.3.1. Introduction to Web Application Security
- 4.3.2. Security in the Design of Web Applications

4.4. Testing the Security and Online Protection of Web Applications
- 4.4.1. Web Application Security Testing and Analysis
- 4.4.2. Web Application Deployment and Production Security

4.5. Web Services Security
- 4.5.1. Introduction to Web Services Security
- 4.5.2. Web Services Security Functions and Technologies

4.6. Testing the Security and Online Protection of Web Services
- 4.6.1. Evaluation of Web Services Security
- 4.6.2. Online Protection. *Firewalls and XML Gateways*

4.7. Ethical *Hacking*, *Malware and Forensics*
- 4.7.1. Ethical Hacking
- 4.7.2. *Malware* Analysis
- 4.7.3. Forensic Analysis

4.8. Incident Resolution on Web Services
- 4.8.1. Monitoring
- 4.8.2. Performance Measurement Tools
- 4.8.3. Containment Measures
- 4.8.4. Root Cause Analysis
- 4.8.5. Proactive Problem Management

4.9. Best Practices to ensure Application Security
- 4.9.1. Handbook of Best Practices in the Development of Online Applications
- 4.9.2. Handbook of Good Practices in the Implementation of Online Applications

4.10. Common Errors that Undermine Application Security
- 4.10.1. Common Errors in Development
- 4.10.2. Common Errors in Hosting
- 4.10.3. Common Production Errors

> *A comprehensive and multidisciplinary training program that will allow you to excel in your career, following the latest advances in the field of Security in Software Engineering"*

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.

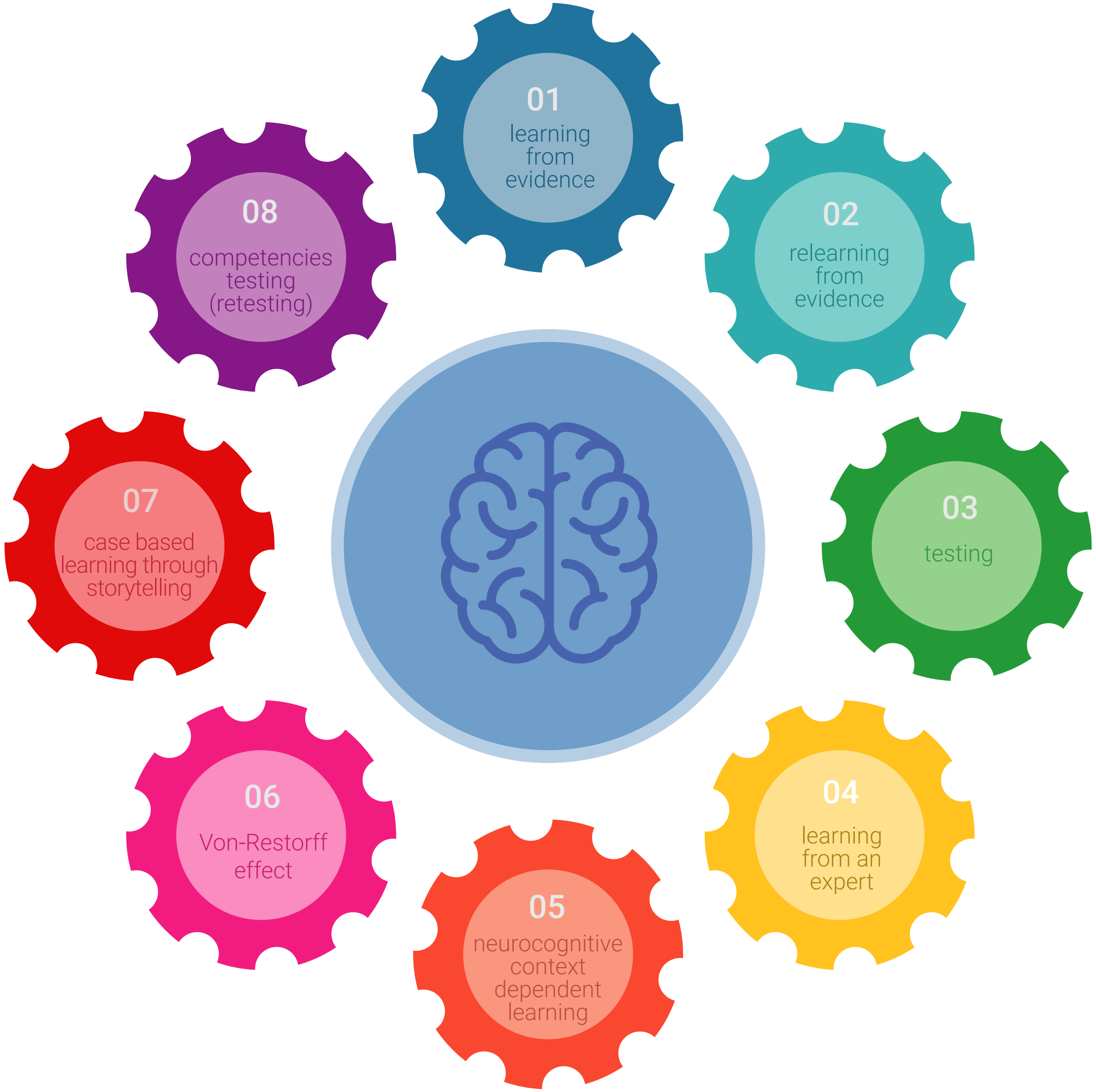
What should a professional do in a given situation? This is the question that you are presented with in the case method, an action-oriented learning method. Throughout the course, students will be presented with multiple real cases. They will have to combine all their knowledge and research, and argue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

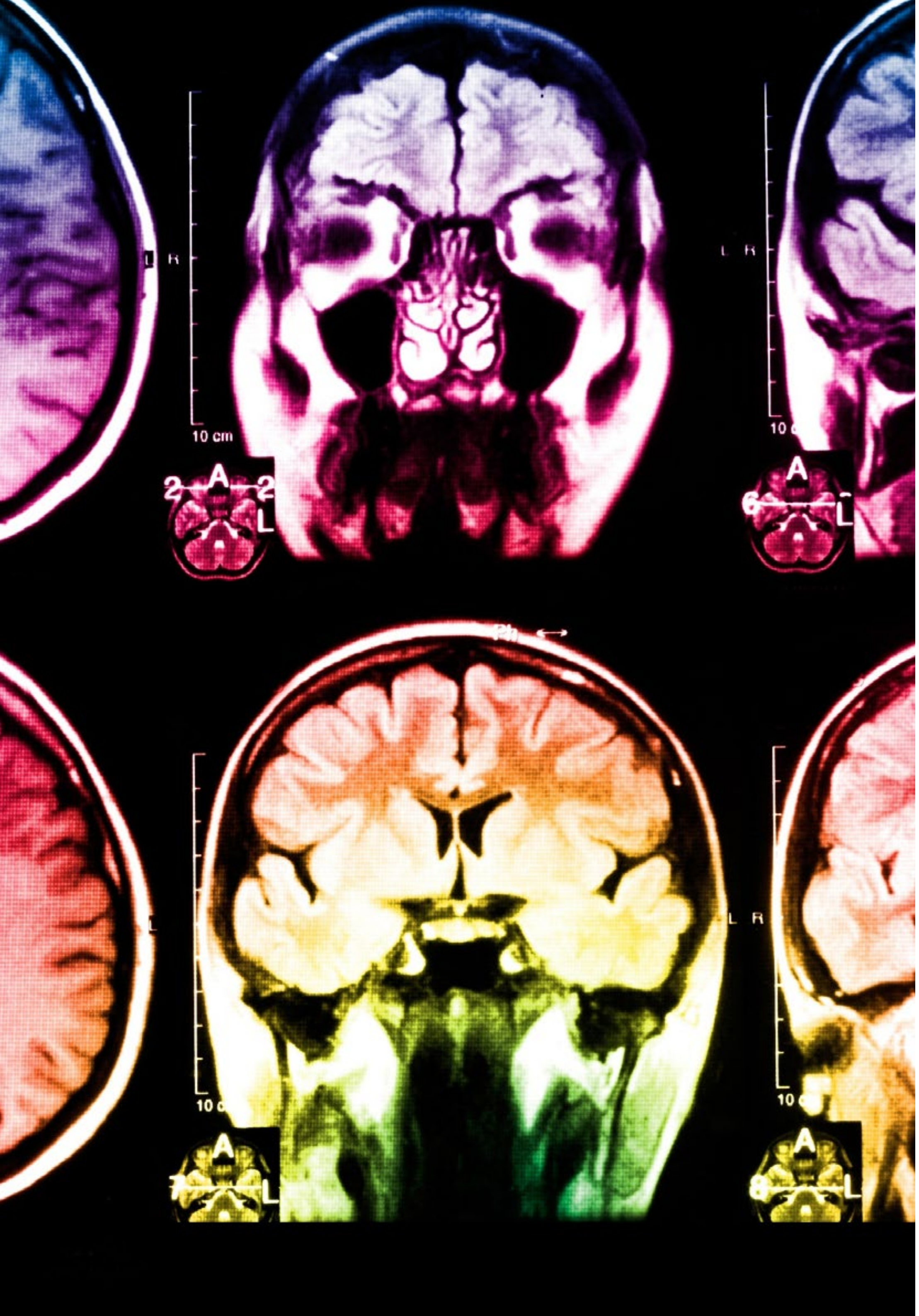
We enhance the Case Study with the best 100% online teaching method: Relearning.

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


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)

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.

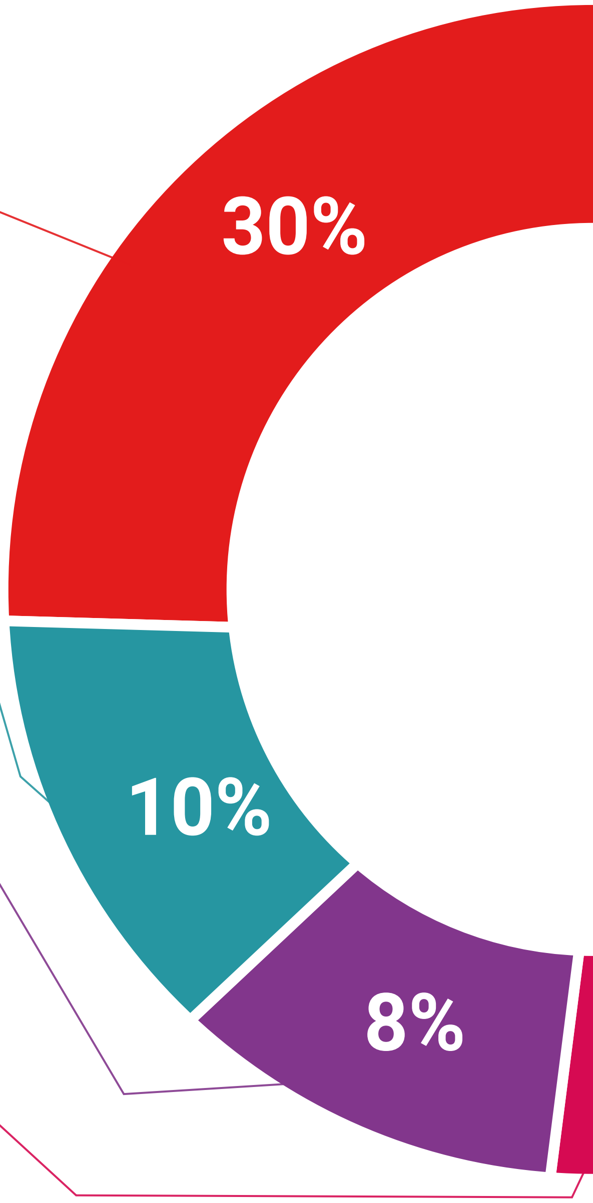
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

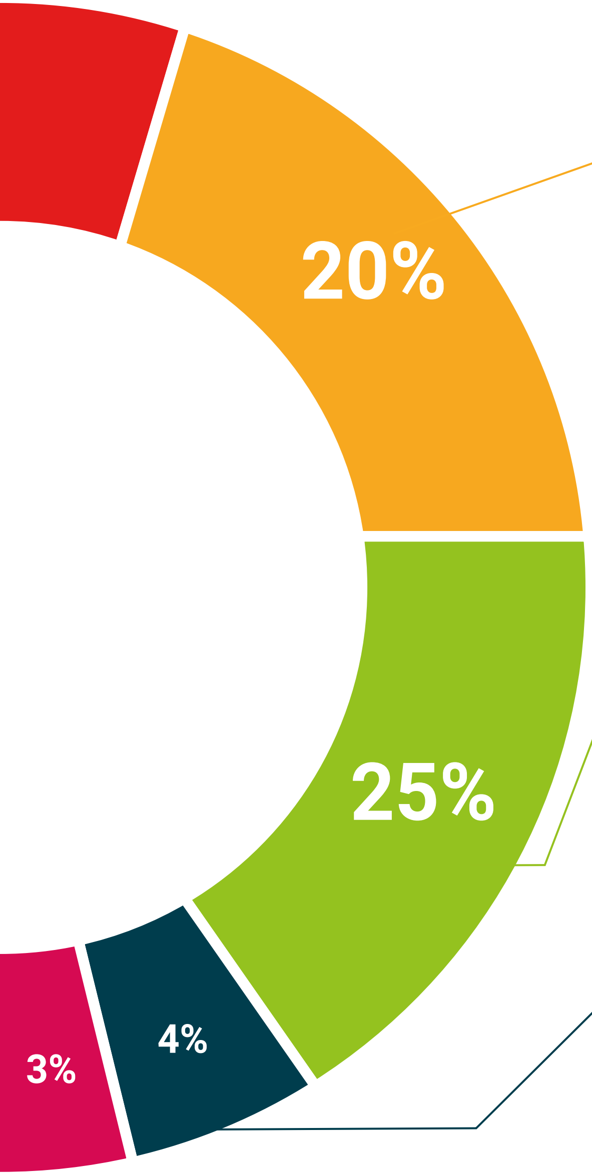
Practising Skills and Abilities

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.

05

Certificate

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

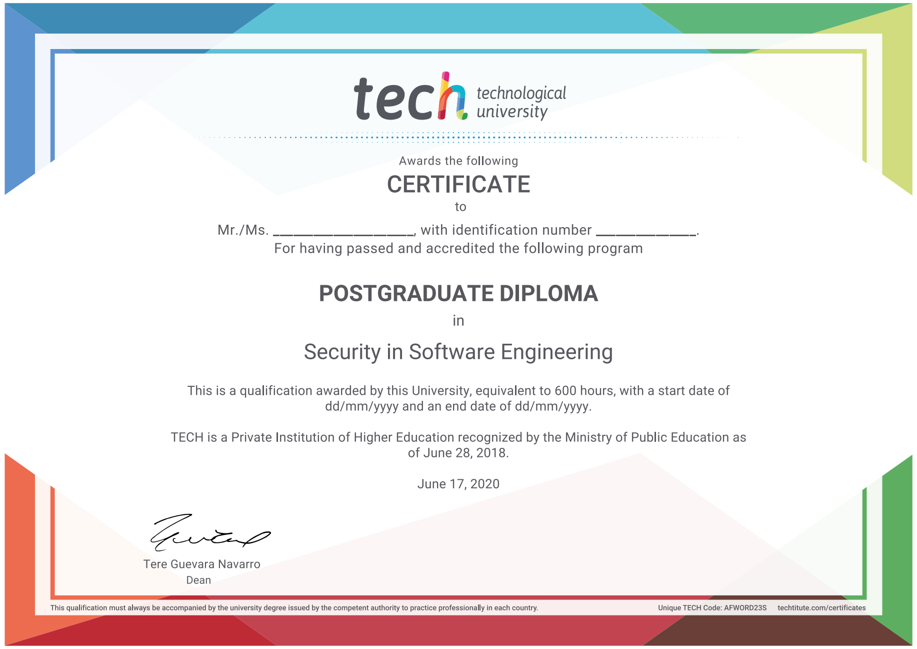
> *Successfully complete this program and receive your university qualification without having to travel or fill out laborious paperwork"*

This **Postgraduate Diploma in Security in Software Engineering** contains the most complete and up-to-date educational 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 Security in Software Engineering**
Official Nº of Hours: **600 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

Security in Software Engineering

This is a qualification awarded by this University, equivalent to 600 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
Security in Software Engineering

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

Postgraduate Diploma
Security in Software Engineering

tech technological university