Postgraduate Diploma

Information Security Breach Management

tech technological university

tech technological university

Postgraduate Diploma

Information Security Breach 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-information-security-breach-management**

Index

01

Introduction

Companies know that they are exposed to a large number of cyber-attacks, which is why the implementation of security policies is, nowadays, essential to ensure the protection of sensitive data. In this scenario, IT professionals must respond to foreseeable incidents suffered by the entity and adopt preventive measures to avoid new attacks. This 100% online program provides students with all the necessary tools to deal with IT security. The expert teaching team in this field and the extensive library with multimedia resources will favor the learning and specialization of professionals in a field that requires a high qualification.

You will be prepared to deal with any IT security incident that a company may suffer. Enroll in this Postgraduate Diploma"

IT security is becoming increasingly necessary given the large volume of sensitive data held by companies and institutions. However, in many cases, bad practices on the part of the personnel or the lack of knowledge in this technological field cause cracks and incidents to occur. These can sometimes generate losses or seriously affect the image of an entity.

This Postgraduate Diploma provides a specialized education that allows to analyze and manage incidents, from their detection through IDS/IPS systems and their subsequent treatment in SIEM, to the process of notification and escalation to the corresponding department. A whole process that requires expert IT professionals with knowledge of useful tools for monitoring information systems.

This program with an eminently practical approach will put the students in a situation before a Ransomware attack, to perfect their knowledge in the adoption of action measures and recovery protocols.

The 100% online mode of this program allows IT professionals to access quality multimedia content from day one without fixed schedules and from any device with internet access. TECH thus facilitates the learning of students who wish to combine their work and personal life with an education available to all.

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

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

Master to perfection with this Postgraduate Diploma, network monitoring programs such as Nagios, Zabbix or Pandora and keep an eye on your equipment"

Take a leap in your professional career. Specialize and provide answers to the IT security failures of companies and institutions. Enroll now"

Learn more about ISO 27035 standards and avoid security breaches that could threaten companies. Enroll in this qualification.

Manage SNM protocols and tools to perfection with this Postgraduate Diploma.

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

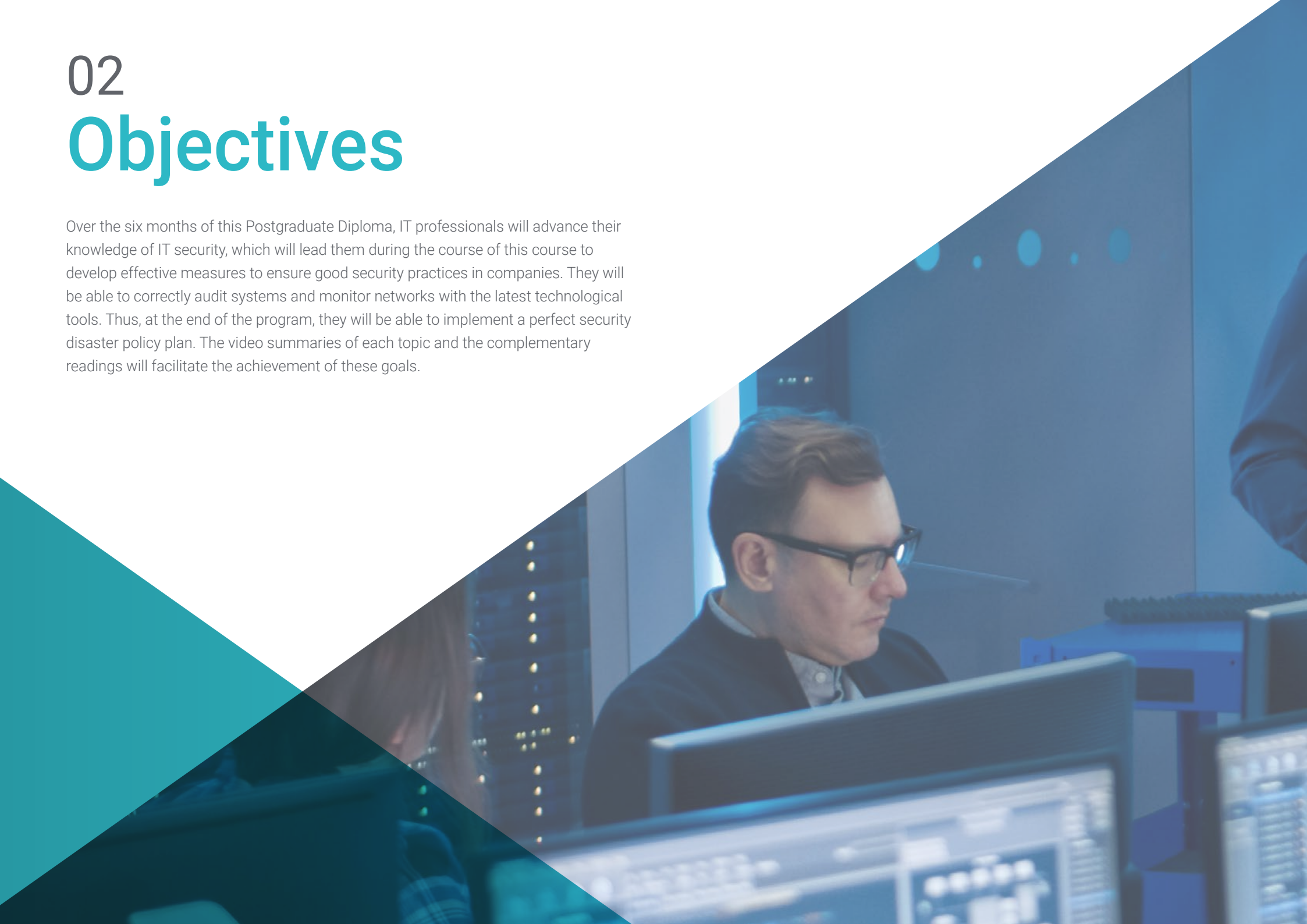
The multimedia content, developed with the latest educational technology, will provide the professional with situated and contextual learning, i.e., a simulated environment that will provide immersive education programmed to learn in real situations.

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

02

Objectives

Over the six months of this Postgraduate Diploma, IT professionals will advance their knowledge of IT security, which will lead them during the course of this course to develop effective measures to ensure good security practices in companies. They will be able to correctly audit systems and monitor networks with the latest technological tools. Thus, at the end of the program, they will be able to implement a perfect security disaster policy plan. The video summaries of each topic and the complementary readings will facilitate the achievement of these goals.

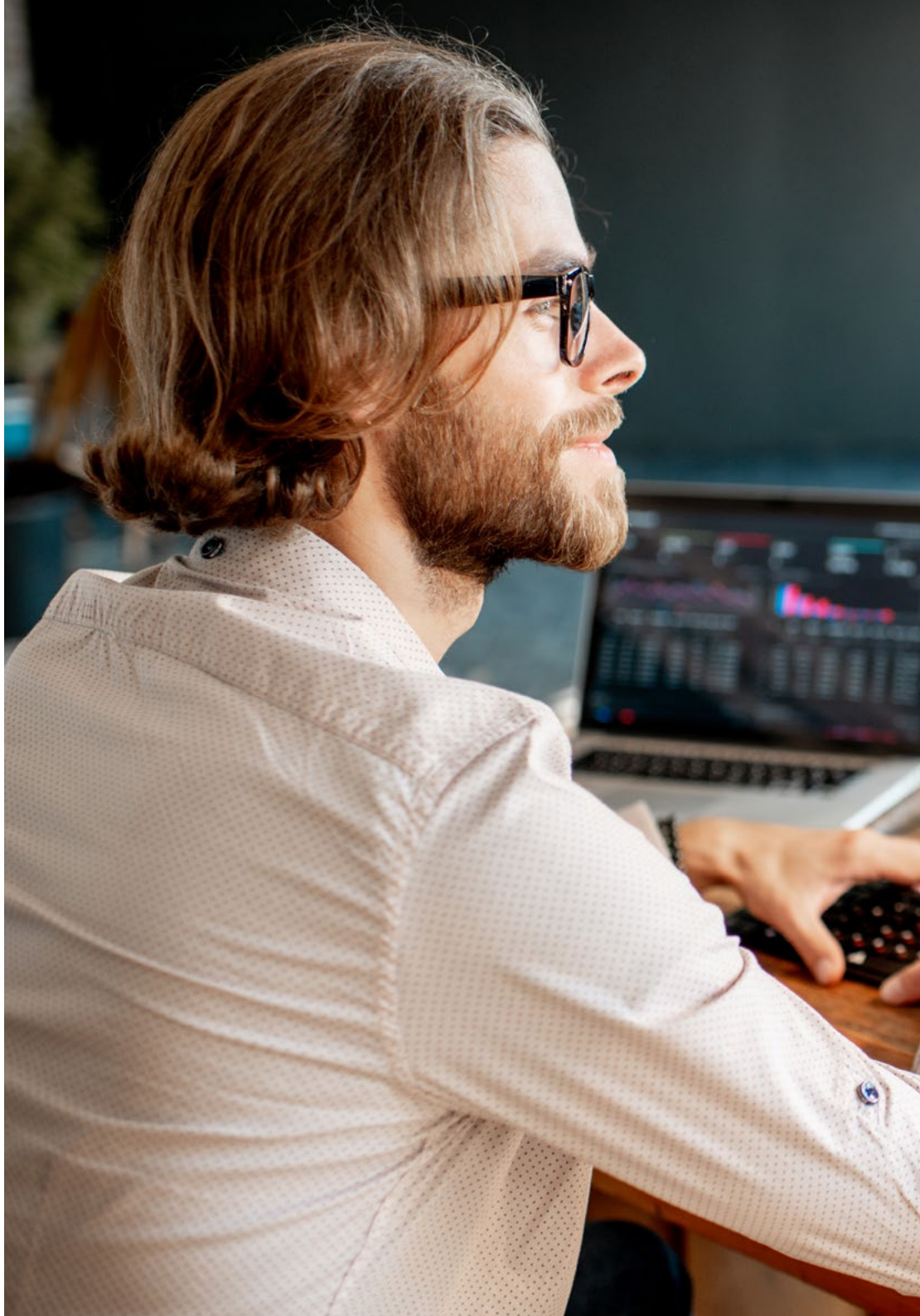


Develop the best IT security plan and become the expert that companies need to protect themselves"

General Objectives

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

TECH's pedagogical methodology will allow you to reach your most ambitious goals even sooner than you expect"



Specific Objectives

Module 1. Security Breach Management Policies

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

Module 2. Information System Security Policy Monitoring Tools

- Develop the concept of monitoring and implementation of metrics
- Configure Audit Trails on Systems and Monitor Networks
- Compile the best system monitoring tools currently available on the market

Module 3. Practical Security Disaster Recovery Policy

- Generate specialized knowledge on the concept of information security continuity
- Develop a business continuity plan
- Analyze an ICT continuity plan
- Design a disaster recovery plan

03

Course Management

TECH provides students with quality education and adjusted to the latest developments in the sector, in this case of Computer Security. In this Postgraduate Diploma, the IT professional will have access to extensive knowledge, thanks to the knowledge of a teaching team with extensive experience in cybersecurity and who are currently active in this field. For this reason, students will have at their disposal a teaching that is close to the reality that professionals live daily in the face of cyber-attacks.

Experts in security in public and private companies will give you the keys to boost your professional career in this field"

Management

Ms. Fernández Sapena, Sonia

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

Professors

Mr. Oropesiano Carrizosa, Francisco

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

Mr. Ortega López, Florencio

- Security Consultant (Identity Management) at SIA Group
- ICT and Security Consultant as an independent professional
- Teacher trainer in the IT sector
- Graduate in Technical Industrial Engineering at the University of Alcalá de Henares
- Master's Degree for Teachers by UNIR
- MBA in Business Administration and Management by IDE-CESEM
- Master's Degree in Information Technology Direction and Management by IDE-CESEM
- Certified Information Security Management (CISM) from ISACA

04

Structure and Content

The syllabus of this Postgraduate Diploma has been planned to address in its three modules the key points for the management of computer security incidents. In this way, students will learn about management policies, detection systems and prevention of instructions, to deepen throughout this program in the tools, protocols and security audits. Likewise, practical security disaster recovery will play an important role in this qualification. The practical cases and the Relearning system, based on the reiteration of content, will make it easier and faster for students to build all the knowledge of this qualification.

The wide range of multimedia resources enriches this syllabus prepared by experts in the field of computer security"

Module 1. Security Breach Management Policies

1.1. Information Security Incident Management Policies and Enhancements
- 1.1.1. Incident Management
- 1.1.2. Responsibilities and Procedures
- 1.1.3. Event Notification

1.2. Intrusion Detection and Prevention Systems (IDS/IPS)
- 1.2.1. System Operating Data
- 1.2.2. Types of Intrusion Detection Systems
- 1.2.3. Criteria for IDS/IPS Placement

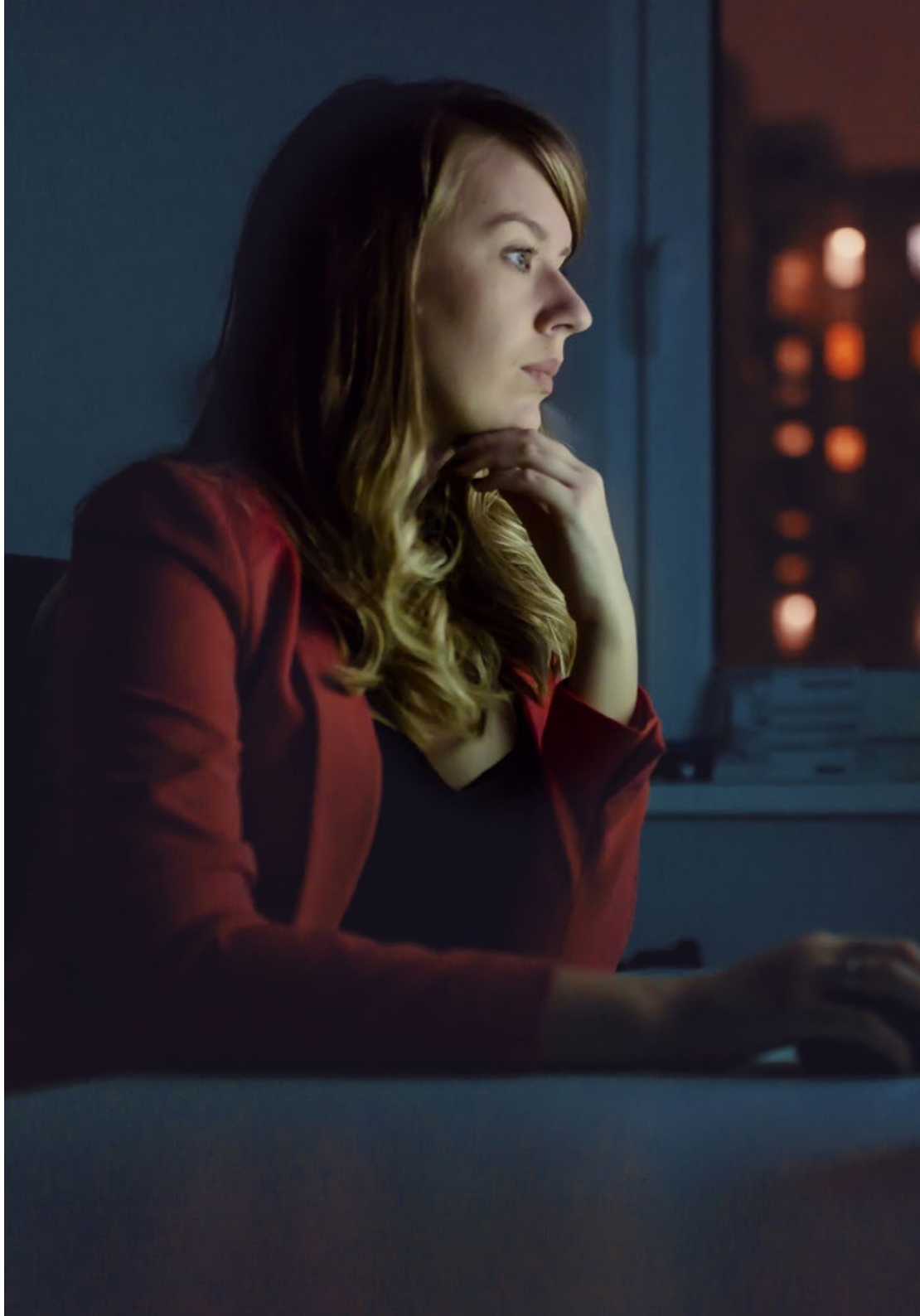
1.3. Security Incident Response
- 1.3.1. Data Collection Procedure
- 1.3.2. Intrusion Verification Process
- 1.3.3. CERT Organizations

1.4. Intrusion Attempt Notification and Management Process
- 1.4.1. Responsibilities in the Notification Process
- 1.4.2. Classification of Incidents
- 1.4.3. Resolution and Recovery Process

1.5. Forensic Analysis as a Security Policy
- 1.5.1. Volatile and Non-Volatile Evidence
- 1.5.2. Analysis and Collection of Electronic Evidence
  - 1.5.2.1. Analysis of Electronic Evidence
  - 1.5.2.2. Collection of Electronic Evidence

1.6. Intrusion Detection and Prevention Systems (IDS/IPS) Tools
- 1.6.1. Snort
- 1.6.2. Suricata
- 1.6.3. SolarWinds

1.7. Event Centralizing Tools
- 1.7.1. SIM
- 1.7.2. SEM
- 1.7.3. SIEM



1.8. CCN-STIC Security Guide 817
- 1.8.1. Cyber Incident Management
- 1.8.2. Metrics and Indicators

1.9. NIST SP800-61
- 1.9.1. Computer Security Incident Response Capability
- 1.9.2. Handling an Incident
- 1.9.3. Coordination and Information Sharing

1.10. ISO 27035
- 1.10.1. ISO 27035 Standard. Incident Management Principles
- 1.10.2. Incident Management Plan Preparation Guidelines
- 1.10.3. Incident Response Operations Guides

Module 2. Information Systems Security Policy Monitoring Tools

2.1. Information Systems Monitoring Policies
- 2.1.1. System Monitoring
- 2.1.2. Metrics
- 2.1.3. Types of Metrics

2.2. System Audit and Logging
- 2.2.1. System Audit and Logging
- 2.2.2. Windows Audit and Logging
- 2.2.3. Linux Audit and Logging

2.3. SNMP Protocol. Simple Network Management Protocol
- 2.3.1. SNMP Protocol
- 2.3.2. SNMP Functions
- 2.3.3. SNMP Tools

2.4. Network Monitoring
- 2.4.1. Network Monitoring in Control Systems
- 2.4.2. Monitoring Tools for Control Systems

2.5. Nagios. Network Monitoring System
- 2.5.1. Nagios
- 2.5.2. Operation of Nagios
- 2.5.3. Nagios Installation

2.6. Zabbix. Network Monitoring System
- 2.6.1. Zabbix
- 2.6.2. How Zabbix Works
- 2.6.3. Zabbix Installation

2.7. Cacti. Network Monitoring System
- 2.7.1. Cacti
- 2.7.2. How Cacti Works
- 2.7.3. Installation of Cacti

2.8. Pandora. Network Monitoring System
- 2.8.1. Pandora
- 2.8.2. Operation of Pandora
- 2.8.3. Pandora Installation

2.9. SolarWinds. Network Monitoring System
- 2.9.1. SolarWinds
- 2.9.2. Operation of SolarWinds
- 2.9.3. Installation of SolarWinds

2.10. Monitoring Regulations
- 2.10.1. CIS Controls Over Auditing and Record Keeping
- 2.10.2. NIST 800-123 (U.S.) USA

Module 3. Practical Security Disaster Recovery Policy

3.1. DRP. Disaster Recovery Plan
- 3.1.1. Objective of a DRP
- 3.1.2. Benefits of a DRP
- 3.1.3. Consequences of a Missing and Not Up-To-Date DRP

3.2. Guidance for Defining a DRP (Disaster Recovery Plan)
- 3.2.1. Scope and Objectives
- 3.2.2. Recuperation Strategy Design
- 3.2.3. Assignment of Roles and Responsibilities
- 3.2.4. Inventory of Hardware, Software and Services
- 3.2.5. Tolerance for Downtime and Data Loss
- 3.2.6. Establishment of the Specific Types of DRP Required
- 3.2.7. Implementation of a Training, Awareness and Communication Plan

3.3. Scope and Objectives of a DRP (Disaster Recovery Plan)
- 3.3.1. Response Guarantee
- 3.3.2. Technological Components
- 3.3.3. Scope of the Continuity Policy

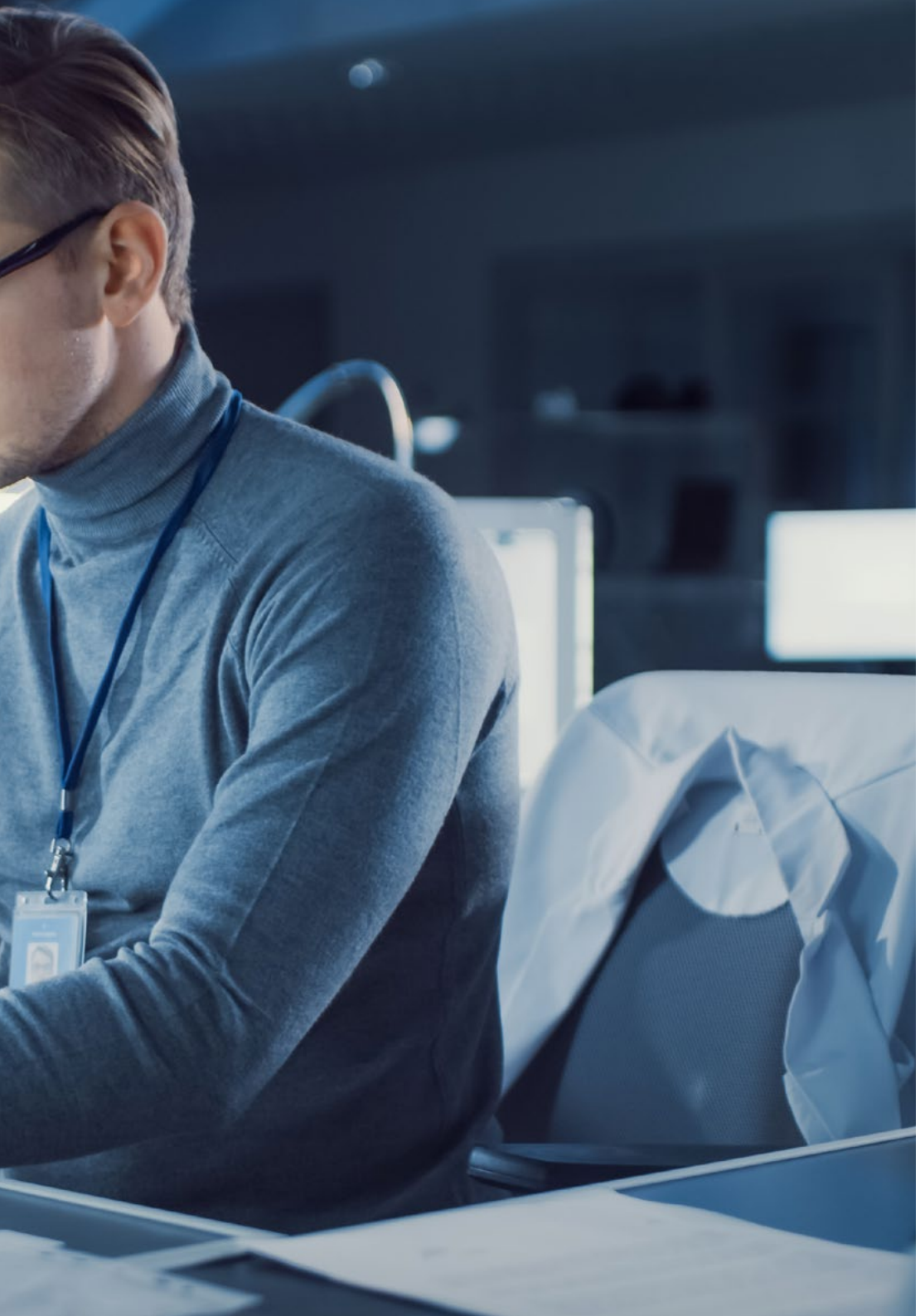
3.4. Designing a DRP (Disaster Recovery Plan) Strategy
- 3.4.1. Disaster Recovery Strategy
- 3.4.2. Budget
- 3.4.3. Human and Physical Resources
- 3.4.4. Management Positions at Risk
- 3.4.5. Technology
- 3.4.6. Date:

3.5. Continuity of Information Processes
- 3.5.1. Continuity Planning
- 3.5.2. Continuity Implementation
- 3.5.3. Verification of Continuity Assessment

3.6. Scope of a BCP (Business Continuity Plan)
- 3.6.1. Determination of the Most Critical Processes
- 3.6.2. Asset-Based Approach
- 3.6.3. Process Approach

3.7. Implementation of Guaranteed Business Processes
- 3.7.1. Priority Activities (PA)
- 3.7.2. Ideal Recovery Times (IRT)
- 3.7.3. Survival Strategies

3.8. Organizational Analysis
- 3.8.1. Acquisition of information
- 3.8.2. Business Impact Analysis (BIA)
- 3.8.3. Risk Analysis in the Organization



3.9. Response to Contingency
- 3.9.1. Crisis Plan
- 3.9.2. Operational Environment Recovery Plans
- 3.9.3. Technical Work or Incident Procedures

3.10. International Standard ISO 27031 BCP
- 3.10.1. Objectives
- 3.10.2. Terms and Definitions
- 3.10.3. Operation

The Relearning system and the 100% online format will be your allies to achieve a very useful learning in your professional field"

06

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

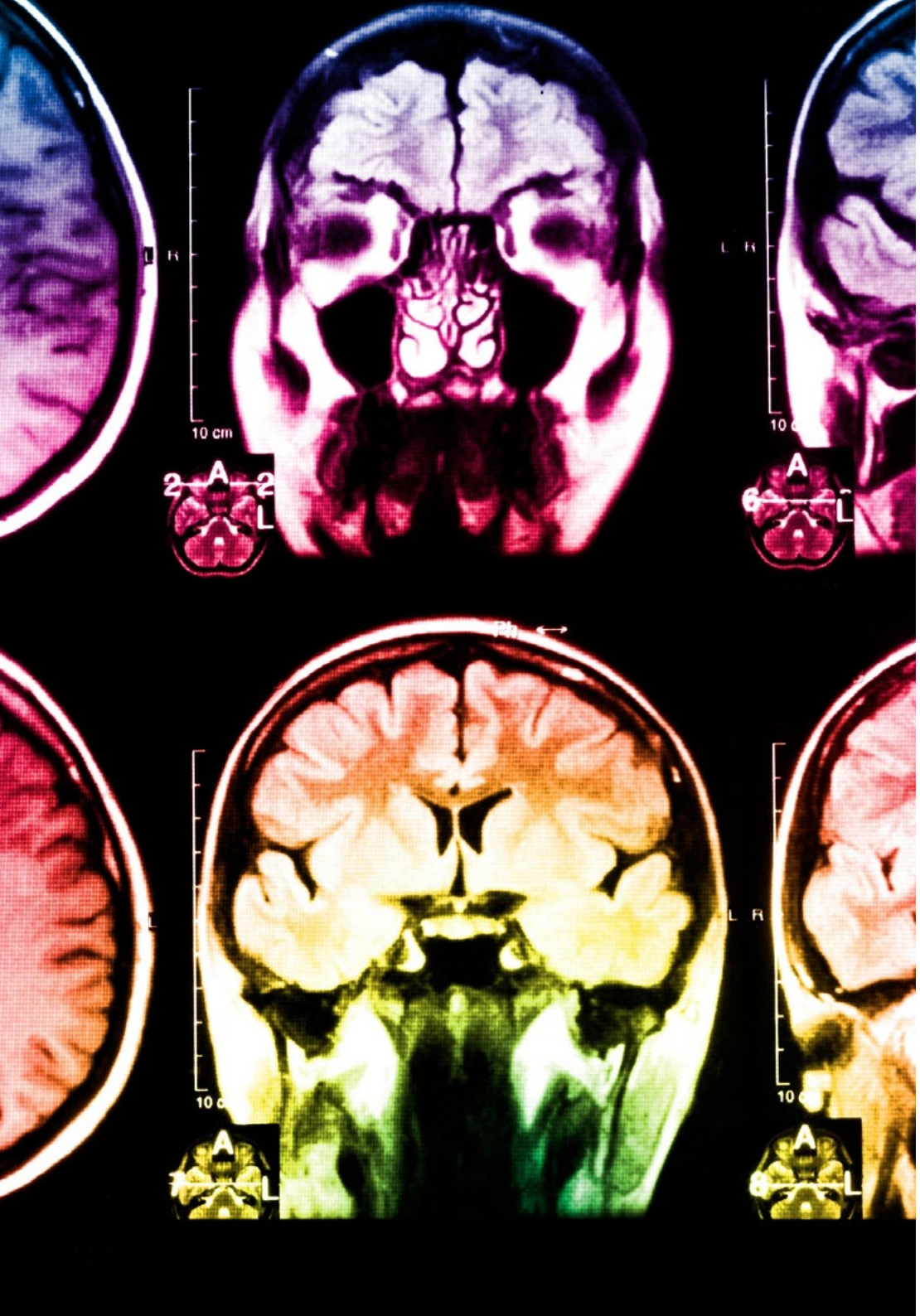
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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.

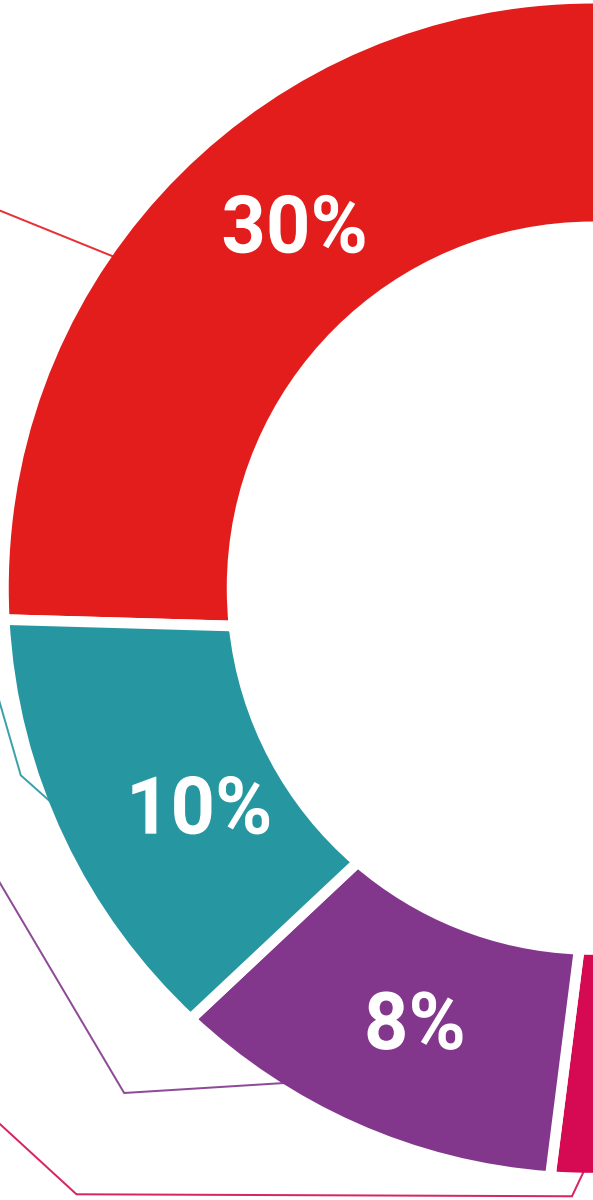
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

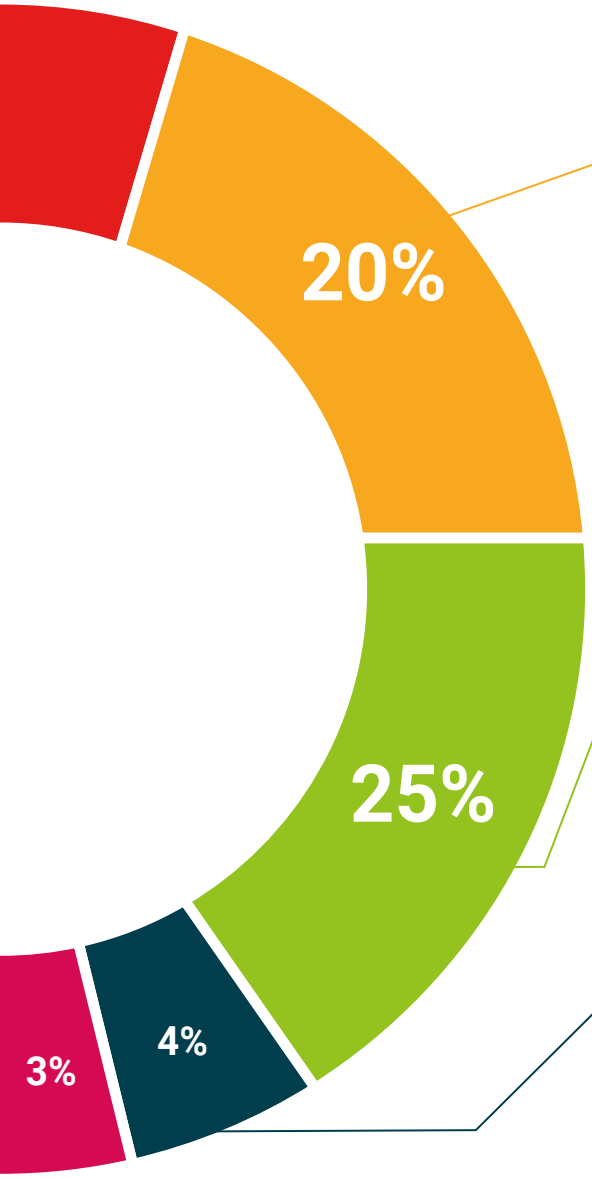
Practising Skills and Abilities

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 Information Security Breach 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 Information Security Breach 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 Information Security Breach Management**

Official Nº 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

Information Security Breach 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

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
Information Security Breach Management

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

Postgraduate Diploma

Information Security Breach Management

tech technological university