Advanced Master's Degree

Secure Information Management

Advanced Master's Degree

Secure Information Management

- Modality: **online**
- Duration: **2 years**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

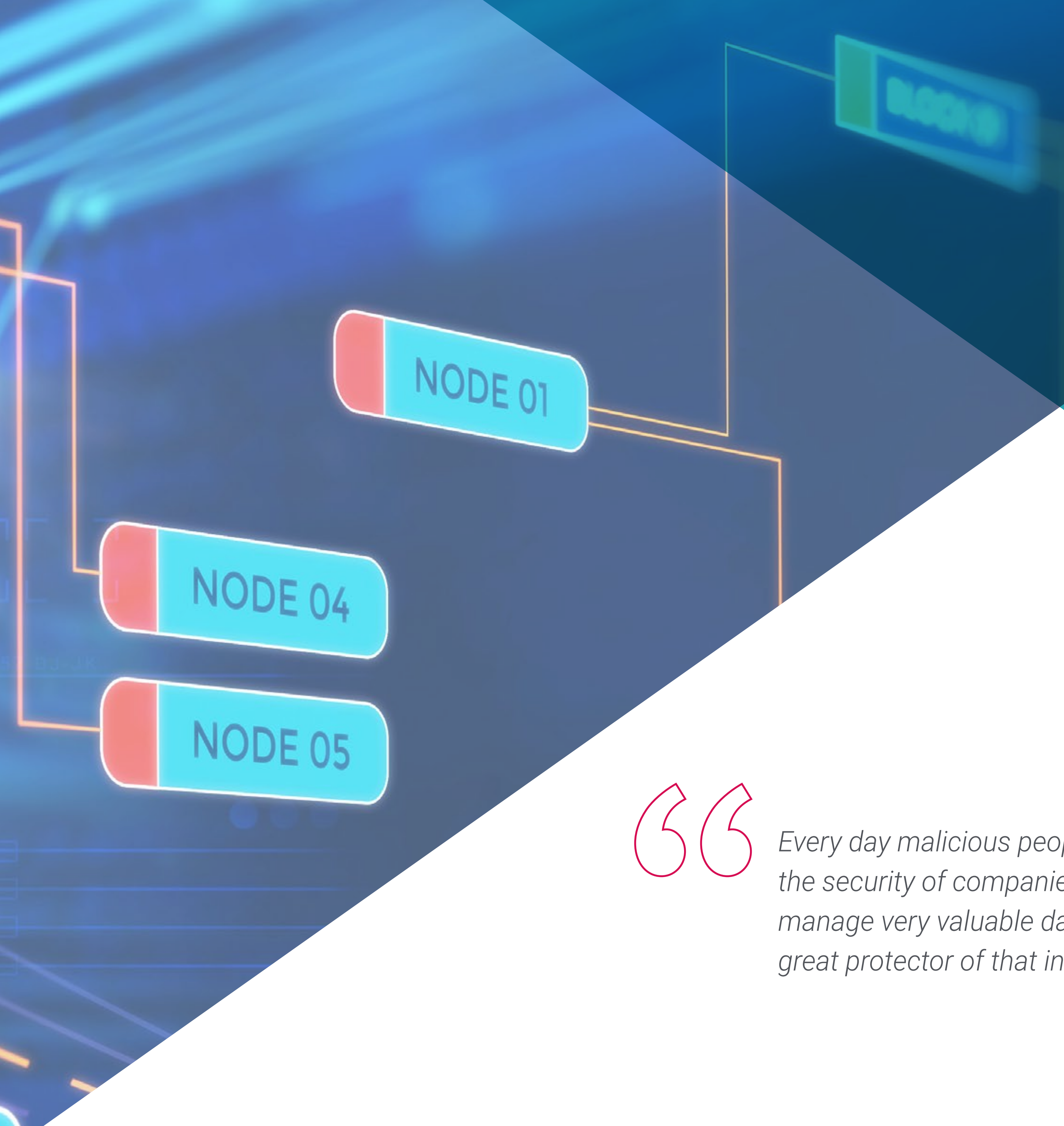
Website: www.techtitute.com/pk/information-technology/advanced-master-degree/advanced-master-degree-secure-information-management

Index

01

Introduction

Today's world is dominated by the digital environment. It manages a large number of activities in different fields. Therefore, leisure, work or contact with friends and family leisure, work or contact with friends and family are hard to imagine without the Internet and all the existing online tools. For this reason, huge amounts of information are transferred on a daily basis, from innocuous data in conversations through social networks and messaging applications, to highly sensitive personal and professional information hosted on banking or business websites. In this complex landscape, companies require specialists who can manage all types of information pertaining to these areas, while doing so with adequate attention to their security. Numerous companies are looking for personnel with this profile to protect their information.



> *Every day malicious people try to compromise the security of companies and institutions that manage very valuable data: you could be the great protector of that information”*

Every day, millions of people perform all kinds of activities on the Internet. They check the news, chat with friends and family, share opinions on social networks, carry out administrative tasks in different companies and institutions, share all kinds of files or do work-related tasks. Therefore, countless amounts of data are being created and transferred all over the world at every moment.

Managing them with adequate security is not a simple task, as it requires a range of specific knowledge from various fields that would not normally be in contact with each other. For that reason, this Advanced Master's Degree in Secure Information Management is an outstanding opportunity for all those engineers and IT professionals who want to integrate information management and cybersecurity to become top specialists in both areas.

Many companies and institutions handle highly sensitive and valuable data that requires proper administration, preservation and monitoring. There are still not many experts in both disciplines who can take charge and adequately manage all aspects. Therefore, students who complete this Advanced Master's Degree will be perfectly placed to reach top positions in companies who are seeking to secure their digital information

To this end, TECH has designed the best content and has brought together the best teachers, with extensive professional experience in these areas, so that students receive the most complete education possible and can progress in the workplace.

This **Advanced Master's Degree in Secure Information Management** contains the most complete and up-to-date educational program on the market. The most important features include:

- The development of case studies presented by computer science experts
- The graphic, schematic, and eminently practical contents with which they are created, provide scientific and practical information on the disciplines that are essential for professional practice
- Practical exercises where self-assessment can be used to improve learning
- Its special emphasis on innovative methodologies in digital data management and security
- 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

> *Everything we do in the digital realm is recorded. Make the Internet a safer place thanks to this Advanced Master's Degree"*

The best companies in the country will trust you with the management and security of their data when you complete this program"

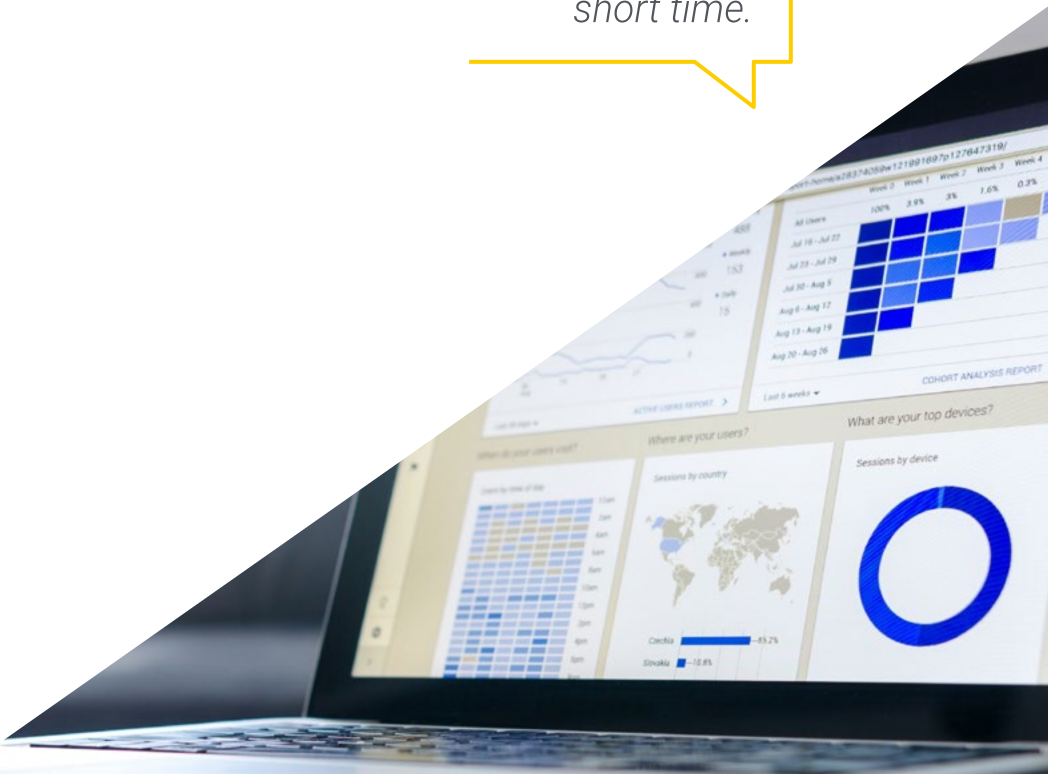
This Advanced Master's Degree combines two essential disciplines for the future of your career. Enroll now and achieve all your goals.

Learn all about data management and data security and see how you advance professionally in a very short time.

Its teaching staff includes professionals belonging to the field, who bring the experience of their work to this program, 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 an immersive learning experience designed to train for real-life situations.

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



02

Objectives

The main objective of this Advanced Master's Degree in Secure Information Management is to provide students with the best knowledge in two distinct but interrelated branches of computer science and engineering: data management in the digital environment and cybersecurity. By combining these two areas, computer scientists and professionals who take this program will be able to apply the best solutions in every situation that arises in their careers, offering the most appropriate tools to their companies in order to manage and protect all types of sensitive information.

Your goal is to be the best specialist in your company and TECH offers you the tools to achieve it"

General objectives

- Analyze the benefits of the application of data analytics techniques in each department of the company
- Develop the basis for understanding the needs and applications of each department
- Generate specialized knowledge to select the right tools
- Propose techniques and objectives to be as productive as possible according to the department
- Analyze the role of the cybersecurity analyst
- Delve into social engineering and its methods
- Examine OSINT, HUMINT, OWASP, PTEC, OSSTM and OWISAM methodologies
- Conduct a risk analysis and understand risk metrics
- Determine the appropriate use of anonymity and use of networks such as TOR, I2P and Freenet
- Compile current cybersecurity regulations
- Generate specialized knowledge to perform a security audit
- Develop appropriate usage policies
- Examine the most important threat detection and prevention systems
- Evaluate new threat detection systems, as well as their evolution with respect to more traditional solutions
- Analyze the main current mobile platforms, their characteristics and use
- Identify, analyze and assess security risks of the IoT project parts
- Evaluate the information obtained and develop prevention and hackingmechanisms
- Apply reverse engineering to the cybersecurity environment
- Specify the tests to be performed on the developed software
- Collect all existing evidence and data to conduct a forensic report
- Duly submit the forensic report
- Analyze the current and future state of computer security
- Examine the risks of new emerging technologies
- Compile the different technologies in relation to computer security

> *Cybersecurity and data management are fast-moving disciplines. Take this Advanced Master's Degree and get the most up-to-date knowledge"*

Specific objectives

Module 1. Data Analytics in the Business Organization

- Develop analytical skills to make quality decisions
- Examine effective marketing and communication campaigns
- Determine the creation of scorecards and KPIs according to the department
- Generate specialized knowledge to develop predictive analytics
- Propose business and loyalty plans based on market research
- Develop the ability to listen to the customer
- Apply statistical, quantitative and technical knowledge in real situations

Module 2. Data Management, Data Manipulation and Data Science Reporting

- Perform data analysis
- Unify diverse data: achieving consistency of information
- Produce relevant, effective information for decision making
- Determine the best practices for data management according to its typology and uses
- Establish data access and reuse policies
- Ensure security and availability: availability, integrity and confidentiality of information
- Examine tools for data management using programming languages

Module 3. IoT Devices and Platforms as a Foundation for Data Science

- Identify what IoT is (Internet of Things) and IIoT (Industrial Internet of Things)
- Examine the Industrial Internet Consortium
- Analyze what is the IoT reference architecture
- Address IoT sensors and devices and their classification
- Identify communications protocols and technologies used in IoT

- Examine the different Cloud platforms in IoT: general purpose, industrial and open source
- Develop data exchange mechanisms
- Establish security requirements and strategies
- Present the different IoT and IIoT application areas

Module 4. Graphical Representation for Data Analysis

- Generate specialized knowledge in data representation and analytics
- Examine the different types of grouped data
- Establish the most commonly used graphical representations in different fields
- Determine the principles of design in data visualization
- Present graphic narrative as a tool
- Analyze the different software tools for graphing and exploratory data analysis

Module 5. Science Data Tools

- Develop skills to convert data into information from which knowledge can be extracted
- Determine the main characteristics of a dataset, its structure, components and the implications of its distribution in modeling
- Support decision making by performing comprehensive data analysis in advance
- Develop skills to solve practical cases using data science techniques
- Establish the most appropriate general tools and methods for modeling each dataset based on the preprocessing performed
- Evaluate results analytically, understanding the impact of the chosen strategy on the different metrics
- Demonstrate critical capacity to the results obtained after applying preprocessing or modeling methods

Module 6. Data Mining Selection, Processing and Transformation

- Generate specialized knowledge about the statistical prerequisites for any data analysis and evaluation
- Develop the necessary skills for data identification, preparation and transformation
- Evaluate the different methodologies presented and identify advantages and disadvantages
- Examine problems in high dimensional data environments
- Develop the implementation of the algorithms used for data preprocessing
- Demonstrate the ability to interpret data visualization for descriptive analysis
- Develop advanced knowledge on the different existing data preparation techniques for data cleaning, normalization and transformation

Module 7. Predictability and Analysis of Stochastic Phenomena

- Analyze time series
- Develop the formulation and basic properties of univariate time series models
- Examine the methodology of modeling and prediction of real time series
- Determine the univariate models including outliers
- Apply dynamic regression models and apply the methodology for the construction of such models from observed series
- Address the spectral analysis of univariate time series, as well as the fundamental aspects related to periodogram-based inference and its interpretation
- Estimate the probability and trend of a time series for a given time horizon

Module 8. Design and Development of Intelligent Systems

- Analyze the transition from information to knowledge
- Develop the different types of machine learning techniques
- Examine metrics and scores to quantify the quality of the models
- Implement the different machine learning algorithms
- Identify probabilistic reasoning models
- Laying the foundation for deep learning
- Demonstrate the skills acquired to understand the different machine learning algorithms

Module 9. Data-intensive Systems and Architectures

- Determine the requirements of mass data usage systems
- Examine different data models and analyzing databases
- Analyze the key functionalities for distributed systems and their importance in different types of systems
- Evaluate which widely used applications use the fundamentals of distributed systems to design their systems
- Analyze the way in which databases store and retrieve information
- Specify the different replication models and the associated problems
- Develop ways of partitioning and distributed transactions
- Determine batch systems and (near) real-time systems

Module 10. Practical Application of Data Science in Business Sectors

- Analyze the state of the art of artificial intelligence (AI) and data analytics
- Develop specialized knowledge of the most widely used technologies
- Generate a better understanding of the technology through use cases
- Analyze the chosen strategies to select the best technologies to implement
- Determine the areas of application
- Examine the actual and potential risks of the applied technology
- Propose benefits derived from the use
- Identify future trends in specific sectors

Module 11. Cyberintelligence and Cybersecurity

- Develop methodologies used in cybersecurity.
- Examine the intelligence cycle and establish its application in cyberintelligence
- Determine the role of the intelligence analyst and the obstacles to evacuation activity
- Establish the most common tools for intelligence production
- Conduct a risk analysis and understand the metrics used
- Gain sound knowledge the anonymity options and the use of networks such as TOR, I2P, FreeNet
- Detail the current regulations in cybersecurity
- Specify backup policies for personal and professional data

Module 12. Host Security

- Assess the different tools to provide solutions to specific security problems
- Establish mechanisms to have an updated system
- Scan equipment for intruders
- Determine system access rules
- Screen and classify mails to avoid frauds
- Generate lists of allowed software
- Analyze current network architectures to identify the perimeter to protect

Module 13. Network Security (Perimeter)

- Develop specific firewall and Linux configurations to mitigate the most common attacks
- Compile the most commonly used solutions such as Snort and Suricata, as well as their configuration
- Examine the different additional layers provided by next-generation firewalls and network functionalities in cloud environments
- Determine the tools for network protection and demonstrate why they are fundamental to a multilayer defense
- Examine the different attack vectors to avoid becoming an easy target

Module 14. Smartphone Security

- Determine the main attacks and types of malware to which users of mobile devices are exposed
- Analyze the most current devices to establish greater security in the configuration
- Specify the main steps to perform a penetration test on both iOS and Android platforms
- Develop specialized knowledge about the different protection and security tools
- Establish best practices in mobile device-oriented programming
- Analyze the main IoT architectures

Module 15. IoT Security

- Examine connectivity technologies
- Develop the main application protocols
- Specify the different types of existing devices
- Assess risk levels and known vulnerabilities
- Develop safe use policies
- Establish appropriate conditions of use for these devices
- Examine IOSINT methods

Module 16. Ethical Hacking

- Compile the information available in public media
- Scan networks for active mode information
- Develop testing laboratories
- Analyze the tools for pentesting performance
- Catalog and assess the different vulnerabilities of the systems
- Specify the different hacking methodologies

Module 17. Reverse Engineering

- Analyze the phases of a compiler
- Examine x86 processor architecture and ARM processor architecture
- Determine the different types of analysis
- Apply sandboxing in different environments
- Develop different malware analysis techniques
- Establish malware analysis-oriented tools

Module 18. Secure Development

- Establish the necessary requirements for the correct operation of an application in a secure manner
- Examine log files to understand error messages
- Analyze the different events and decide what to show to the user and what to keep in the logs
- Generate a sanitized, easily verifiable, and quality code
- Evaluate appropriate documentation for each phase of development
- Specify the behavior of the server to optimize the system

- Develop modular, reusable and maintainable code

Module 19. Forensic Analysis

- Identify the different elements that evidence a crime
- Generate specialized knowledge to obtain data from different media before they are lost
- Recovery of intentionally deleted data
- Analyze system logs and records
- Determine how data is duplicated so as not to alter the originals
- Substantiate the evidence for consistency
- Generate a solid and seamless report
- Present conclusions in a coherent manner
- Establish how to defend the report before the competent authority
- Specify strategies for safe teleworking

Module 20. Current and Future Challenges in IT Security

- Examine the use of cryptocurrencies, the impact on the economy and security
- Analyze the situation of users and the degree of digital illiteracy
- Determine the scope of use of blockchain
- Present alternatives to IPv4 in network addressing
- Develop strategies to educate the population in the correct use of technologies
- Generate specialized knowledge to meet new security challenges and prevent identity theft
- Specify strategies for safe teleworking

03

Skills

Students who complete this Advanced Master's Degree in Secure Information Management will be able to perform a large number of highly specialized tasks in the fields of data management and cybersecurity. Therefore, this degree combines both branches to offer complementary knowledge that can be crossed and used in different situations and professional environments. In this way, students will undergo a comprehensive learning process that will guide them to become true specialists in the field.

> *Your new skills will make you the top specialist in your environment"*

General skills

- Develop a technical and business perspective of data analysis
- Understand the most current algorithms, platforms and tools for the exploration, visualization, manipulation, processing and analysis of data
- Implement a business vision necessary for value creation as a key element for decision making
- Be able to address problems specific to data analysis
- Know the methodologies used in cybersecurity
- Evaluate each type of threat in order to offer an optimal solution in each case
- Generate complete intelligent solutions to automate incident behaviors
- Know how to assess the risks associated with vulnerabilities both outside and inside the company
- Understand the evolution and impact of IoT over time
- Demonstrate that a system is vulnerable, attack it for preventive purposes and solve those problems
- Apply sandboxing in different environments
- Know the guidelines that a good developer must follow in order to comply with the necessary security requirements

Specific skills

- Specialize in data science from a technical and business perspective
- Visualize data in the most appropriate way to favor data sharing and understanding by different profiles
- Address the key functional areas of the organization where data science can deliver the most value
- Develop the data life cycle, its typology and the technologies and phases necessary for its management
- Process and manipulate data using specific languages and libraries
- Develop advanced knowledge in fundamental data mining techniques for data selection, preprocessing and transformation
- Specialize in the main machine learning algorithms for extracting hidden knowledge from data
- Generate specialized knowledge in the software architectures and systems required for intensive data use
- Determine how the IoT can be a source of data generation and key information on which to apply data science for knowledge extraction
- Analyze the different ways of applying data science in different sectors or verticals by learning from real examples
- Perform defensive security operations
- Have an in-depth and specialized perception of IT security
- Possess specialized knowledge in the field of cybersecurity and cyberintelligence
- Have in-depth knowledge of fundamental aspects such as the intelligence cycle, intelligence sources, social engineering, OSINT methodology, HUMINT, anonymization and risk analysis, existing methodologies (OWASP, OWISAM, OSSTM, PTES) and current cybersecurity regulations
- Understand the importance of devising a multi-layer defense, also known as defense in depth, covering all aspects of a corporate network where some of the concepts and systems we will see can also be used and applied in a home environment
- Know how to apply security processes for smartphones and portable devices
- Know the means to perform the so-called ethical hacking and protect a company from a cyberattack
- Investigate a cybersecurity incident
- Know the different attack and defense techniques available
- Analyze the role of the cybersecurity analyst and learn how social engineering works and its methods

> *Do you want to distinguish yourself from other specialists, but don't know how? This Advanced Master's Degree is what you are looking for"*

04

Course Management

This degree is taught by the best professors in the fields of cybersecurity and digital data management. Their experience guarantees that students will have access to the most complete and up-to-date content so that they can apply it directly to their professional careers. In this way, the teachers of this Advanced Master's Degree in Secure Information Management will transmit all their knowledge to the students, ensuring that they become highly qualified specialists who are highly-sought-after by large companies in their countries.

> *The best specialists teach you how to be an outstanding professional in the sector"*

International Guest Director

Frederic Lemieux, Ph.D. is internationally recognized as an innovative expert and inspirational leader in the fields of **Intelligence, Homeland Security, Homeland Security, Cybersecurity** and **Disruptive Technologies.** His constant dedication and relevant contributions in research and education position him as a key figure in the promotion of security and understanding of today's emerging technologies. During his professional career, he has conceptualized and directed cutting-edge academic programs at several renowned institutions, such as **the University of Montreal, George Washington University** and **Georgetown University**.

Throughout his extensive background, he has published multiple books of great relevance, all of them related to **criminal intelligence, policing, cyber threats, and cyber threats and international security.** He has also contributed significantly to the field of Cybersecurity with the publication of numerous articles in academic journals, which examine crime control during major disasters, the fight against terrorism, intelligence agencies and police cooperation. In addition, he has been a panelist and keynote speaker at various national and international conferences, establishing himself as a reference in the academic and professional arena.

Dr. Lemieux has held editorial and evaluative roles in different academic, private and governmental organizations, reflecting his influence and commitment to excellence in his field of expertise. In this way, his prestigious academic career has led him to serve as Professor of Practice and Faculty Director of the MPS programs in **Applied Intelligence, Cybersecurity Risk Management, Technology Management and Information Technology Management** at **Georgetown University.**

Dr. Lemieux, Frederic

- Researcher in Intelligence, Cybersecurity and Disruptive Technologies at Georgetown University.
- Director of the Master's Program in Information Technology Management at Georgetown University
- Director of the Master in Technology Management at Georgetown University.
- Director of the Master in Cybersecurity Risk Management at Georgetown University
- Director of the Master's Program in Applied Intelligence at Georgetown University.
- Professor of Internship at Georgetown University
- PhD in Criminology from the School of Criminology, University of Montreal.
- B.A. in Sociology, Minor Degree in Psychology, University of Laval, France
- Member of: New Program Roundtable Committee, by Georgetown University

> *Thanks to TECH you will be able to learn with the best professionals in the world"*

Management

Dr. Peralta Martín-Palomino, Arturo

- CEO and CTO at Prometeus Global Solutions
- CTO en Corporate Technologies in Corporate Technologies
- CTO in AI Shephers GmbH
- Doctorate in Psychology from the University of Castilla La Mancha
- PhD in Economics, Business and Finance from the Camilo José Cela University. Outstanding Award in her PhD
- Doctorate in Psychology from the University of Castilla la Mancha
- Master's Degree in Advanced Information Technologies from the University of Castilla la Mancha
- Master MBA+E (Master's Degree in Business Administration and Organizational Engineering) from the University of Castilla La Mancha
- Associate lecturer, teaching undergraduate and master's degrees in Computer Engineering at the University of Castilla la Mancha
- Professor of the Master's Degree in Big Data and Data Science at the International University of Valencia
- Lecturer of the Master's Degree in Industry 4.0 and the Master's Degree in Industrial Design and Product Development
- Member of the SMILe Research Group of the University of Castilla la Mancha

Ms. Fernández Sapena, Sonia

- Computer Security and Ethical Hacking Trainer, Getafe National Reference Center for Informatics and Telecommunications Madrid
- Certified e-Council instructor, Madrid
- Trainer in the following certifications: EXIN Ethical Hacking Foundation y 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*). University of the Balearic Islands
- Computer Engineer Alcalá de Henares University, Madrid
- Master's Degree in DevOps: Docker and Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Techonologies. e-Council. Madrid

Professors

Mr. Armero Fernández, Rafael

- Business Intelligence Consultant at SDG Group
- Digital Engineer at Mi-GSO
- Logistic Engineer at Torrecid S.A
- Quality Intern at INDRA
- Graduate in Aerospace Engineering from the Polytechnic University of Valencia
- Master's Degree in Professional Development 4.0 from the University of Alcalá de Henares

Mr. Peris Morillo, Luis Javier

- Technical Lead in Capitole Consulting
- Senior Technical Lead & Delivery Lead Support en HCL
- Agile Coach and Director of Operations at Mirai Advisory
- Developer, Team Lead, Scrum Master, Agile Coach, Product Manager in DocPath
- Higher Engineering in Computer Science from the ESI of Ciudad Real (UCLM)
- Postgraduate in Project Management by CEOE - Confederación Española de Organizaciones Empresariales (Spanish Confederation of Business Organizations)
- 50+ MOOCs taken, taught by renowned universities such as Stanford University, Michigan University, Yonsei University, Polytechnic University of Madrid, etc.

Mr. Montoro Montarroso, Andrés

- Researcher in the SMILe Group at the University of Castilla-La Mancha
- Data Scientist at Prometeus Global Solutions
- Degree in Computer Engineering from the University of Castilla-La Mancha. in Computer Science
- Master's Degree in Data Science and Computer Engineering from the University of Granada

Ms. Fernández Meléndez, Galina

- Data Analyst at ADN Mobile Solution
- ETL processes, data mining, data analysis and visualization, establishment of KPI's, Dashboard design and implementation, management control
- ADN Mobile Solution-Gijón-Spain R development, SQL management, among others
- Pattern determination, predictive modelling, machine learning
- Bachelor's degree in Business Administration. Bicentennial University of Aragua- Caracas
- Diploma in Planning and Public Finance. Venezuelan School School of Planning-School of Finance
- Professional Master's Degree in Data Analysis and Business Intelligence, University of Oviedo
- MBA in Business Administration and Management (European Business School, Barcelona)
- Master in Big Data and Business Intelligence (European Business School, Barcelona)

Ms. Pedrajas Parabás, Elena

- Business Analyst at Management Solutions in Madrid
- Researcher in the Department of Computer Science and Numerical Analysis at the University of Córdoba
- Researcher at the Singular Center for Research in Intelligent Technologies in Santiago de Compostela
- Degree in Computer Engineering Master's Degree in Data Science and Computer Engineering Intelligence (European Business School, Barcelona)

Ms. Martínez Cerrato, Yésica

- Electronic Security Product Technician at Securitas Security Spain
- Business Intelligence Analyst at Ricopia Technologies (Alcalá de Henares)
- Degree in Electronic Communications Engineering at the Polytechnic School, University of Alcalá
- Responsible for training new recruits on commercial management software (CRM, ERP, INTRANET), product and procedures in Ricopia Technologies (Alcalá de Henares)
- Responsible for training new scholarship holders incorporated to the Computer Classrooms at the University of Alcalá
- Project Manager in the area of Key Accounts Integration at Correos and Telégrafos (Madrid)
- Computer Technician-Responsible for computer classrooms OTEC, University of Alcalá (Alcalá de Henares)
- Computer classes teacher at ASALUMA Association (Alcalá de Henares)
- Scholarship for Training as a Computer Technician in OTEC, University of Alcala (Alcalá de Henares)

Mr. Fondón Alcalde, Rubén

- Customer Value Management Business Analyst at Vodafone Spain
- Head of Service Integration at Entelgy for Telefónica Global Solutions
- Online account manager for clone servers at EDM Electronics
- Business Analyst for Southern Europe at Vodafone Global Enterprise
- Telecommunications Engineer from the European University of Madrid
- Master's Degree in Big Data and Analytics from the International University of Valencia

Mr. Díaz Díaz-Chirón, Tobías

- Researcher at the ArCO laboratory of the University of Castilla-La Mancha, a group dedicated to projects related to computer architectures and networks
- Consultant at Blue Telecom, a company dedicated to the telecommunications sector
- Degree in Computer Engineering from the University of Castilla-La Mancha

Mr. Tato Sánchez, Rafael

- Project management at INDRA SISTEMAS S.A. Management of the maintenance contract for intelligent transport systems installations dependent on the Traffic Control and Management Center of the Traffic General Directorate in Madrid
- Technical Director at INDRA SISTEMAS S.A. responsible for the Traffic Control and Management Center of the Traffic General Directorate in Madrid
- Systems Engineer ENA TRÁFICO Sau
- Industrial Technical Engineer in Electricity from the Polytechnic University of Madrid
- Degree in Industrial Electronics and Automation Engineering in from the European University of Madrid
- Professional certification. SSCE0110. Teaching for vocational training for employment
- Master's Degree in Industry 4.0 from the International University of La Rioja (UNIR)

Mr. Catalá Barba, José Francisco

- Middle Management in MINISDEF. Different tasks and responsibilities within GOE III, such as administration and incident management of the internal network, development of customized programs for different areas, training courses for network users and group personnel in general
- Electronic technician at Ford Factory located in Almusafes, Valencia, robot programming, PLC's, repair and maintenance
- Electronic Technician
- Developer of applications for mobile devices

Mr. Jiménez Ramos, Álvaro

- Security Analyst at Capgemini
- Cybersecurity Analyst L1 at Axians
- Cybersecurity Analyst L2 at Axians
- Cybersecurity Analyst at SACYR S.A.
- Degree in Telematic Engineering from the Polytechnic University of Madrid
- Master's Degree in Cybersecurity and Ethical Hacking from CICE
- Advanced Course in Cybersecurity by Deusto Training

Ms. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Application Developer at B60 UK
- Analyst Programmer for the management, coordination and documentation of virtualized environment of security alarms at client's site
- Analyst Programmer of Java applications for ATMs at client's site
- Software Development Professional for signature validation and document management application at customer's site
- Systems Technician for the migration of equipment and for the management, maintenance and training of PDA mobile devices at the customer's site
- Technical Engineering of Computer Systems from Universitat Oberta de Catalunya (UOC)
- Master's Degree in Computer Security and Ethical Hacking Official EC- Council and CompTIA from the Professional School of New Technologies CICE

Mr. Peralta Alonso, Jon

- Lawyer / DPO Altia Consultores S.A.
- Lecturer in Master in Personal Data Protection, Cybersecurity and ICT Law, University of the Basque Country (UPV-EHU)
- Lawyer/Legal Advisor, Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Legal Advisor/Intern Professional office: Oscar Padura
- Degree in Law, Public University of the Basque Country
- Master's Degree in Data Protection Commission, EIS Innovative School
- Master's Degree in Law, Public University of the Basque Country
- Master's Degree in Civil Litigation Practice, International University Isabel I de Castilla

Mr. Redondo, Jesús Serrano

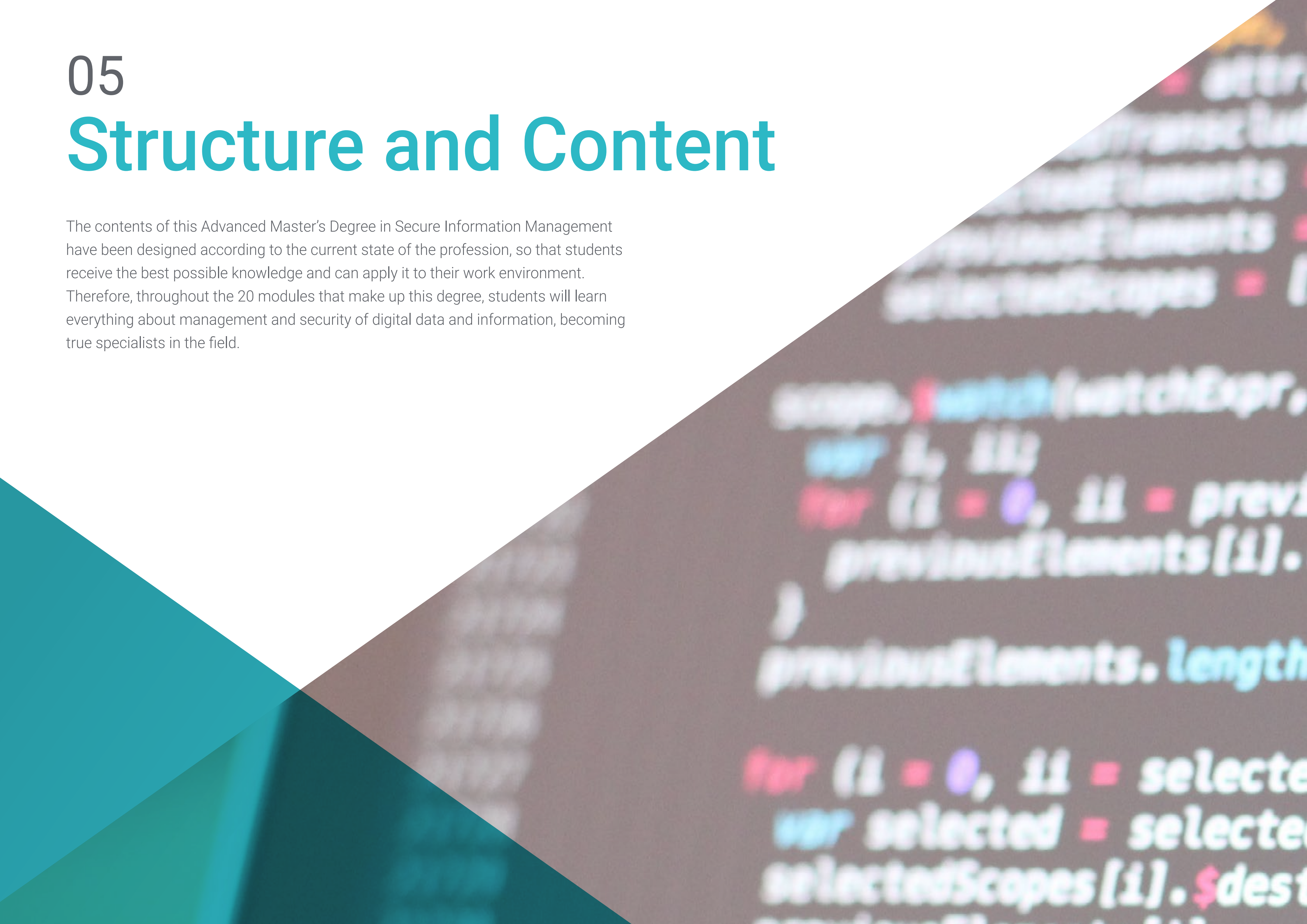
- Junior FrontEnd Developer & Junior Cybersecurity Technician
- FrontEnd Developer at Telefónica, Madrid
- Developer of FrontEnd. Best Pro Consulting SL, Madrid
- Telecommunications equipment and services installer Grupo Zener, Castilla y León
- Telecommunications equipment and services installer Lican Comunicaciones SL, Castilla y León
- Certificate in Computer Security CFTIC Getafe, Madrid
- Superior Technician Telecommunications and Computer Systems IES Trinidad Arroyo, Palencia
- Senior Technician MV and LV Electrotechnical Installations IES Trinidad Arroyo, Palencia
- Training in reverse engineering, stenography, encryption Academia Hacker Incibe (Talentos Incibe)

> *The leading professionals in the field have come together to offer you the most comprehensive knowledge in this field, so that you can develop with total guarantees of success"*

05

Structure and Content

The contents of this Advanced Master’s Degree in Secure Information Management have been designed according to the current state of the profession, so that students receive the best possible knowledge and can apply it to their work environment. Therefore, throughout the 20 modules that make up this degree, students will learn everything about management and security of digital data and information, becoming true specialists in the field.



```
element, attr, ngSwitch
.ngSwitch || attr.on,
ches = [],
= [],
= [],
[];

, function ngSwitchWatchAction(va

iousElements.length; i < i
remove();

= 0;

edScopes.le
dElemen
troy
```

> *There is no better program. This Advanced Master’s Degree offers you everything you need to be the top expert in these areas”*

Module 1. Data Analytics in the Business Organization

1.1. Business Analysis
- 1.1.1. Business Analysis
- 1.1.2. Data Structure
- 1.1.3. Phases and Elements

1.2. Data Analytics in the Enterprise
- 1.2.1. Scorecards and KPIs by Departments
- 1.2.2. Operational, Tactical and Strategic Reporting
- 1.2.3. Data Analytics Applied to Each Department
  - 1.2.3.1. Marketing and Communication
  - 1.2.3.2. Commercial
  - 1.2.3.3. Customer Service
  - 1.2.3.4. Purchasing
  - 1.2.3.5. Administration.
  - 1.2.3.6. HR
  - 1.2.3.7. Production
  - 1.2.3.8. IT

1.3. Marketing and Communication
- 1.3.1. KPIs to Measure, Applications and Benefits
- 1.3.2. Marketing Systems and Data Warehouse
- 1.3.3. Implementation of a Data Analytics Framework in Marketing
- 1.3.4. Marketing and Communication Plan
- 1.3.5. Strategies, Forecasting and Campaign Management

1.4. Commercial and Sales
- 1.4.1. Contributions of Data Analytics in the Commercial Area
- 1.4.2. Needs of the Sales Department
- 1.4.3. Market Research

1.5. Customer Service
- 1.5.1. Loyalty
- 1.5.2. Personal Quality and Emotional Intelligence
- 1.5.3. Customer Satisfaction

1.6. Purchasing
- 1.6.1. Data Analytics for Market Research
- 1.6.2. Data Analytics for Competitive Studies
- 1.6.3. Other Applications

1.7. Administration.
- 1.7.1. Needs of the Administration Department
- 1.7.2. Data Warehouse and Financial Risk Analysis
- 1.7.3. Data Warehouse and of Credit Risk Analysis

1.8. Human Resources
- 1.8.1. HR and Benefits of Data Analysis
- 1.8.2. Data Analytics Tools in the HR Department
- 1.8.3. Application of Data Analytics in HR

1.9. Production
- 1.9.1. Data Analysis in a Production Department
- 1.9.2. Applications
- 1.9.3. Benefits

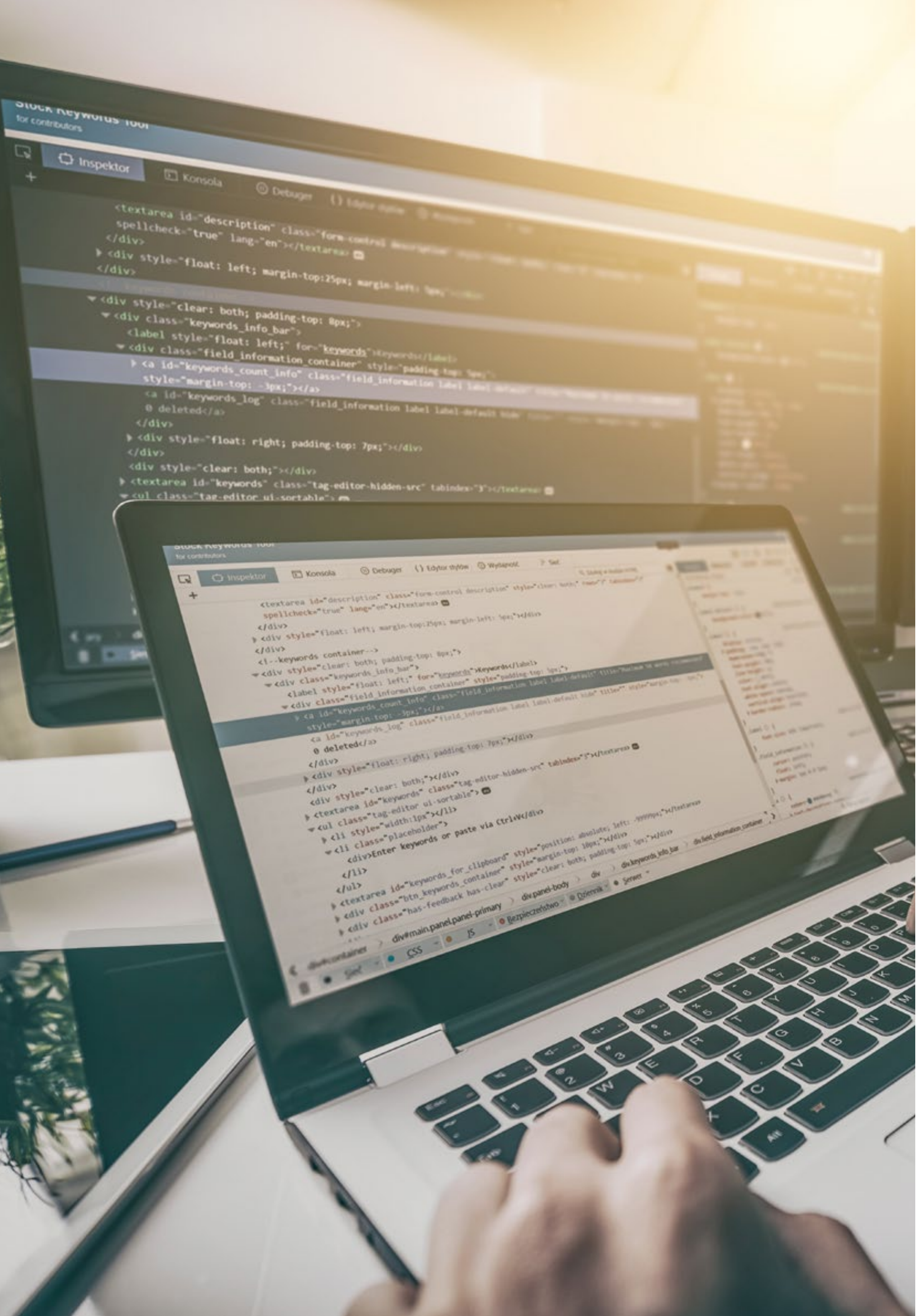
1.10. IT
- 1.10.1. IT Department
- 1.10.2. Data Analytics and Digital Transformation
- 1.10.3. Innovation and Productivity

Module 2. Data Management, Data Manipulation and Data Science Reporting

2.1. Statistics. Variables, Indexes and Ratios
- 2.1.1. Statistics
- 2.1.2. Statistical Dimensions
- 2.1.3. Variables, Indexes and Ratios

2.2. Data Typology
- 2.2.1. Qualitative
- 2.2.2. Quantitative
- 2.2.3. Characterization and Categories

2.3. Knowledge of Data from Measurement
- 2.3.1. Centralization Measures
- 2.3.2. Measures of Dispersion
- 2.3.3. Correlation



2.4. Knowledge of Data from Graphs
- 2.4.1. Display by Data Type
- 2.4.2. Interpretation of Graphic Information
- 2.4.3. Customization of Graphics with R

2.5. Probability
- 2.5.1. Probability
- 2.5.2. Probability Function
- 2.5.3. Distributions

2.6. Data Collection
- 2.6.1. Methodology of Data Collection
- 2.6.2. Data Collection Tools
- 2.6.3. Data Collection Channels

2.7. Data Cleaning
- 2.7.1. Phases of Data Cleansing
- 2.7.2. Data Quality
- 2.7.3. Data Manipulation (with R)

2.8. Data Analysis, Interpretation and Evaluation of Results
- 2.8.1. Statistical Measures
- 2.8.2. Relationship Indices
- 2.8.3. Data Mining

2.9. Data Warehouse
- 2.9.1. Components
- 2.9.2. Design

2.10. Data Availability
- 2.10.1. Access
- 2.10.2. Uses
- 2.10.3. Security/Safety

Module 3. IoT Devices and Platforms as a Foundation for Data Science

3.1. Internet of Things
- 3.1.1. Internet of the Future Internet of Things
- 3.1.2. The Industrial Internet Consortium

3.2. Architecture of Reference
- 3.2.1. The Architecture of Reference
- 3.2.2. Layers
- 3.2.3. Components

3.3. Sensors and IoT Devices
- 3.3.1. Principal Components
- 3.3.2. Sensors and Actuators

3.4. Communications and Protocols
- 3.4.1. Protocols. OSI Model
- 3.4.2. Communication Technologies

3.5. Cloud Platforms for IoT and IIoT
- 3.5.1. General Purpose Platforms
- 3.5.2. Industrial Platforms
- 3.5.3. Open Code Platforms

3.6. Data Management on IoT Platforms
- 3.6.1. Data Management Mechanisms Open Data
- 3.6.2. Data and Visualization Exchange

3.7. IoT Security
- 3.7.1. Requirements and Security Areas
- 3.7.2. Strategies of IIoT Security

3.8. Applications of IoT
- 3.8.1. Intelligent Cities
- 3.8.2. Health and Fitness
- 3.8.3. Smart Home
- 3.8.4. Other Applications

3.9. Applications of IIoT
- 3.9.1. Fabrication
- 3.9.2. Transport
- 3.9.3. Energy
- 3.9.4. Agriculture and Livestock
- 3.9.5. Other Sectors

3.10. Industry 4.0
- 3.10.1. IoRT (Internet of Robotics Things)
- 3.10.2. 3D Additive Manufacturing
- 3.10.3. Big Data Analytics

Module 4. Graphical Representation for Data Analysis

4.1. Exploratory Analysis
- 4.1.1. Representation for Information Analysis
- 4.1.2. The Value of Graphical Representation
- 4.1.3. New Paradigms of Graphic Representation

4.2. Optimization for Data Science
- 4.2.1. Color Range and Design
- 4.2.2. Gestalt in Graphic Representation
- 4.2.3. Mistakes to Avoid and Tips

4.3. Basic Data Sources
- 4.3.1. For Quality Representation
- 4.3.2. For Quantity Representation
- 4.3.3. For Time Representation

4.4. Complex Data Sources
- 4.4.1. Files, Lists and Databases
- 4.4.2. Open Data
- 4.4.3. Continuous Generation Data

4.5. Types of Graphs
- 4.5.1. Basic Representation
- 4.5.2. Representation in Blocks
- 4.5.3. Representation for Dispersion Analysis
- 4.5.4. Circular Representations
- 4.5.5. Bubble Representations
- 4.5.6. Geographic Representations

- 4.6. Types of Visualization
  - 4.6.1. Comparative and Relational
  - 4.6.2. Distribution
  - 4.6.3. Hierarchical
- 4.7. Report Design with Graphical Representation
  - 4.7.1. Application of Graphs in Marketing Reports
  - 4.7.2. Application of Graphs in Scorecards and KPIs
  - 4.7.3. Application of Graphs in Strategic Plans
  - 4.7.4. Other Uses: Science, Health, Business
- 4.8. Graphic Narration
  - 4.8.1. Graphic Narration
  - 4.8.2. Evolution
  - 4.8.3. Uses
- 4.9. Orientated Tools to Visualization
  - 4.9.1. Advanced Tools
  - 4.9.2. Online Software
  - 4.9.3. Open Source
- 4.10. New Technologies in Data Visualization
  - 4.10.1. Reality Visualization Systems
  - 4.10.2. Reality Enhancement and Improvement Systems
  - 4.10.3. Intelligent Systems

Module 5. Science Data Tools

- 5.1. Data Science
  - 5.1.1. Data Science
  - 5.1.2. Advanced Tools for the Data Scientist
- 5.2. Data, Information and Knowledge
  - 5.2.1. Data, Information and Knowledge
  - 5.2.2. Types of Data
  - 5.2.3. Data Sources
- 5.3. From Data to Information
  - 5.3.1. Data Analysis
  - 5.3.2. Types of Analysis
  - 5.3.3. Extracting Information from a Dataset
- 5.4. Extraction of Information by Visualization
  - 5.4.1. Visualization as an Analysis Tool
  - 5.4.2. Visualization Methods
  - 5.4.3. Visualization of a Dataset
- 5.5. Data Quality
  - 5.5.1. Quality Data
  - 5.5.2. Data Cleansing
  - 5.5.3. Basic Data Processing
- 5.6. Dataset
  - 5.6.1. Dataset Enrichment
  - 5.6.2. The Curse of Dimensionality
  - 5.6.3. Modification of Our Dataset
- 5.7. Unbalance
  - 5.7.1. Class Imbalance
  - 5.7.2. Unbalance Mitigation Techniques
  - 5.7.3. Balancing a Dataset
- 5.8. Unsupervised Models
  - 5.8.1. Unsupervised Learning
  - 5.8.2. Methods
  - 5.8.3. Classification with Unsupervised Models
- 5.9. Supervised Models
  - 5.9.1. Supervised Model
  - 5.9.2. Methods
  - 5.9.3. Classification with Supervised Models
- 5.10. Tools and Good Practices
  - 5.10.1. Good Practices for the Data Scientist
  - 5.10.2. The Best Model
  - 5.10.3. Useful Tools

Module 6. Data Mining Selection, Processing and Transformation

6.1. Statistical Inference
- 6.1.1. Descriptive Statistics vs. Statistical Inference
- 6.1.2. Parametric Procedures
- 6.1.3. Non-Parametric Procedures

6.2. Exploratory Analysis
- 6.2.1. Descriptive Analysis
- 6.2.2. Visualization
- 6.2.3. Data Preparation

6.3. Data Preparation
- 6.3.1. Integration and Data Cleansing
- 6.3.2. Data Normalization
- 6.3.3. Transforming Attributes

6.4. Missing Values
- 6.4.1. Treatment of Missing Values
- 6.4.2. Maximum Likelihood Imputation Methods
- 6.4.3. Missing Value Imputation Using Machine Learning

6.5. Data Noise
- 6.5.1. Noise Classes and Attributes
- 6.5.2. Noise Filtering
- 6.5.3. The Effect of Noise

6.6. The Curse of Dimensionality
- 6.6.1. Oversampling
- 6.6.2. Undersampling
- 6.6.3. Multidimensional Data Reduction

6.7. From Continuous to Discrete Attributes
- 6.7.1. Continuous vs. Discrete Data
- 6.7.2. Discretization Process

6.8. The Data
- 6.8.1. Data Selection
- 6.8.2. Prospects and Selection Criteria
- 6.8.3. Selection Methods

6.9. Instance Selection
- 6.9.1. Methods for Instance Selection
- 6.9.2. Prototype Selection
- 6.9.3. Advanced Methods for Instance Selection

6.10. Data Processing in Big Data Environments
- 6.10.1. Big Data
- 6.10.2. Classic Preprocessing vs. Massive
- 6.10.3. Smart Data

Module 7. Predictability and Analysis of Stochastic Phenomena

7.1. Time Series
- 7.1.1. Time Series
- 7.1.2. Use and Applicability
- 7.1.3. Related Case Studies

7.2. The Time Series
- 7.2.1. Trend Seasonality of ST
- 7.2.2. Typical Variations
- 7.2.3. Residue Analysis

7.3. Typologies
- 7.3.1. Stationary
- 7.3.2. Non-Stationary
- 7.3.3. Transformations and Adjustments

7.4. Schemes for Time Series
- 7.4.1. Additive Scheme (Model)
- 7.4.2. Multiplying Scheme (Model)
- 7.4.3. Procedures to Determine the Type of Model

7.5. Basic Forecast Methods
- 7.5.1. Media
- 7.5.2. Naïve
- 7.5.3. Seasonal Naïve
- 7.5.4. Comparison of Methods

- 7.6. Residue Analysis
  - 7.6.1. Autocorrelation
  - 7.6.2. Residue ACF
  - 7.6.3. Correlation Test
- 7.7. Regression in the Context of Time Series
  - 7.7.1. ANOVA
  - 7.7.2. Fundamentals
  - 7.7.3. Practical Application
- 7.8. Predictive Time Series Models
  - 7.8.1. ARIMA
  - 7.8.2. Exponential Smoothing
- 7.9. Time Series Manipulation and Analysis with R
  - 7.9.1. Data Preparation
  - 7.9.2. Pattern Identification
  - 7.9.3. Model Analysis
  - 7.9.4. Prediction
- 7.10. Combined Graphical Analysis with R
  - 7.10.1. Typical Situations
  - 7.10.2. Practical Application for Solving Simple Problems
  - 7.10.3. Practical Application for Solving Advanced Problems

Module 8. Design and Development of Intelligent Systems

- 8.1. Data Pre-Processing
  - 8.1.1. Data Pre-Processing
  - 8.1.2. Data Transformation
  - 8.1.3. Data Mining
- 8.2. Automatic Learning
  - 8.2.1. Supervised and Unsupervised Learning
  - 8.2.2. Reinforcement Learning
  - 8.2.3. Other Learning paradigms
- 8.3. Classification Algorithms
  - 8.3.1. Inductive Automatic Learning
  - 8.3.2. SVM and KNN
  - 8.3.3. Metrics and Scores for Ranking
- 8.4. Regression Algorithms
  - 8.4.1. Linear Regression, Logistic Regression and Nonlinear Models
  - 8.4.2. Temporary Series
  - 8.4.3. Metrics and Scores for Regression
- 8.5. Clustering Algorithms
  - 8.5.1. Hierarchical Grouping Techniques
  - 8.5.2. Partitional Grouping Techniques
  - 8.5.3. Metrics and Scores for Clustering
- 8.6. Association Rules Techniques
  - 8.6.1. Methods for Rules Extraction
  - 8.6.2. Metrics and scores for Association Rule Algorithms
- 8.7. Advanced Classification Techniques Multiclassifiers
  - 8.7.1. Bagging Algorithms
  - 8.7.2. “Random Forests” Classifier
  - 8.7.3. “Boosting” for Decision Trees
- 8.8. Probabilistic Graphical Models
  - 8.8.1. Probabilistic Models
  - 8.8.2. Bayesian Networks Properties, Representation and Parameterization
  - 8.8.3. Others Probabilistic Graphical Models
- 8.9. Neural Networks
  - 8.9.1. Machine Learning with Artificial Neural Networks
  - 8.9.2. Feedforward Networks
- 8.10. Deep Learning
  - 8.10.1. Deep Feedforward Networks
  - 8.10.2. Convolutional Neural Networks and Sequence Models
  - 8.10.3. Tools to Implement Deep Neural Networks

Module 9. Data-intensive Systems and Architectures

9.1. Non-Functional Requirements Pillars of Big Data Applications
- 9.1.1. Reliability
- 9.1.2. Adaptation
- 9.1.3. Maintainability

9.2. Data Models
- 9.2.1. Relational Model
- 9.2.2. Documentary Model
- 9.2.3. Network Data Model

9.3. Databases Data Storage and Retrieval Management
- 9.3.1. Hash Indexes
- 9.3.2. Structured Log Storage
- 9.3.3. Trees B

9.4. Data Coding Formats
- 9.4.1. Specific Language Formats
- 9.4.2. Standardized Formats
- 9.4.3. Binary Coding Formats
- 9.4.4. Data Flow between Processes

9.5. Replication
- 9.5.1. Objectives of Replication
- 9.5.2. Replication Models
- 9.5.3. Problems with Replication

9.6. Distributed Transactions
- 9.6.1. Transaction
- 9.6.2. Protocols for Distributed Transactions
- 9.6.3. Serializable Transactions

9.7. Partitions
- 9.7.1. Forms of Partitioning
- 9.7.2. Secondary Index Interaction and Partitioning
- 9.7.3. Partition Rebalancing

9.8. Processing Offline Data
- 9.8.1. Batch Processing
- 9.8.2. Distributed File Systems
- 9.8.3. MapReduce

9.9. Processing Data in Real Time
- 9.9.1. Types of Message Brokers
- 9.9.2. Representation of Databases as Data Flows
- 9.9.3. Data Stream Processing

9.10. Practical Applications of the Enterprise
- 9.10.1. Consistency in Readings
- 9.10.2. Holistic Approach to Data
- 9.10.3. Scaling of a Distributed Service

Module 10. Practical Application of Data Science in Business Sectors

10.1. Healthcare Sector
- 10.1.1. Implications of AI and Data Analytics in the Healthcare Sector
- 10.1.2. Opportunities and Challenges

10.2. Risks and Tendencies of the Healthcare Sector
- 10.2.1. Use in the Healthcare Sector
- 10.2.2. Potential Risks Related to the Use of AI

10.3. Financial Services
- 10.3.1. Implications of AI and Data Analytics in the Financial Services Sector
- 10.3.2. Use of Financial Services
- 10.3.3. Potential Risks Related to the Use of AI

10.4. Retail
- 10.4.1. Implications of AI and Data Analytics in the Retail Sector
- 10.4.2. Use in Retail
- 10.4.3. Potential Risks Related to the Use of AI

10.5. Industry 4.0
- 10.5.1. Implications of AI and Data Analytics in 4.0 Industry
- 10.5.2. Use in 4.0 Industry

10.6. Risks and Tendencies of Industry 4.0
- 10.6.1. Potential Risks Related to the Use of AI

10.7. Public Administration

10.7.1. Implications of AI and Data Analytics in Public Administration

10.7.2. Use in Public Administration

10.7.3. Potential Risks Related to the Use of AI

10.8. Educational

10.8.1. Implications of AI and Data Analytics in Education

10.8.2. Potential Risks Related to the Use of AI

10.9. Forestry and Agriculture

10.9.1. Implications of AI and Data Analytics in Forestry and Agriculture

10.9.2. Use in Forestry and Agriculture

10.9.3. Potential Risks Related to the Use of AI

10.10. Human Resources

10.10.1. Implications of AI and Data Analytics in Human Resources Management

10.10.2. Practical Applications in the Business World

10.10.3. Potential Risks Related to the Use of AI

Module 11. Cyberintelligence and Cybersecurity

11.1. Cyberintelligence

11.1.1. Cyberintelligence

11.1.1.2. Intelligence

11.1.1.2.1. Cycle of Intelligence

11.1.1.3. Cyberintelligence

11.1.1.4. Cyberintelligence and Cybersecurity

11.1.2. The Intelligence Analyst

11.1.2.1. The Role of the Intelligence Analyst

11.1.2.2. The Intelligence Analyst's Biases in Evaluative Activity

11.2. Cybersecurity

11.2.1. Safety Layers

11.2.2. Identification of Cyber Threats

11.2.2.1. External Threats

11.2.2.2. Internal Threats

11.2.3. Adverse Threats

11.2.3.1. Social Engineering

11.2.3.2. Commonly Used Methods

11.3. Intelligence Techniques and Tools

11.3.1. OSINT

11.3.2. SOCMINT

11.3.3. HUMIT

11.3.4. Linux Distributions and Tools

11.3.5. OWISAM

11.3.6. OWISAP

11.3.7. PTES

11.3.8. OSSTM

11.4. Evaluation Methodologies

11.4.1. Intelligence Analysis

11.4.2. Organization Techniques of Acquired Information

11.4.3. Reliability and Credibility of Information Sources

11.4.4. Analysis Methodologies

11.4.5. Presentation of the Intelligence Results

11.5. Audits and Documentation

11.5.1. Audits of IT Security

11.5.2. Documentation and Permits for Auditing

11.5.3. Types of Audits

11.5.4. Deliverables

11.5.4.1. Technical Report

11.5.4.2. Executive Report

11.6. Anonymity in the Network

11.6.1. Use of Anonymity

11.6.2. Anonymity Techniques (Proxy, VPN)

11.6.3. TOR, Freenet and IP2 Networks

11.7. Threats and Types of Security

11.7.1. Types of Threats

11.7.2. Physical Security

11.7.3. Security in Networks

11.7.4. Logical Security

11.7.5. Security in Web Applications

11.7.6. Security in Mobile Devices

11.8. Regulations and Compliance
- 11.8.1. GDPR
- 11.8.2. The National Strategy of Cybersecurity 2011
- 11.8.3. ISO 27000 Families
- 11.8.4. NIST Cybersecurity Framework
- 11.8.5. CIP
- 11.8.6. ISO Business School 27032
- 11.8.7. Cloud Regulations
- 11.8.8. SOX
- 11.8.9. ICP

11.9. Risk Analysis and Metrics
- 11.9.1. Scope of Risks
- 11.9.2. Assets
- 11.9.3. The Threats
- 11.9.4. The Vulnerabilities
- 11.9.5. Risk Evaluation
- 11.9.6. Risk Treatment

11.10. Important Cybersecurity Agencies
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Module 12. Host Security

12.1. Security Copies
- 12.1.1. Strategies for Security Copies
- 12.1.2. Tools for Windows
- 12.1.3. Tools for Linux
- 12.1.4. Tools for MacOS

12.2. User Antivirus
- 12.2.1. Types of Antivirus
- 12.2.2. Antivirus for Windows
- 12.2.3. Antivirus for Linux
- 12.2.4. Antivirus for MacOS
- 12.2.5. Antivirus for Smartphones

12.3. Intrusion Detectors- HIDS
- 12.3.1. Intrusion Detection Methods
- 12.3.2. Sagan
- 12.3.3. Aide
- 12.3.4. Rkhunter

12.4. Local Firewall
- 12.4.1. Firewall for Windows
- 12.4.2. Firewall for Linux
- 12.4.3. Firewall for MacOS

12.5. Password Managers
- 12.5.1. Password
- 12.5.2. LastPass
- 12.5.3. KeePass
- 12.5.4. Sticky Password
- 12.5.5. RoboForm

12.6. Phishing Detectors
- 12.6.1. Manual Detection of Phishing
- 12.6.2. Antiphishing Tools

12.7. Spyware
- 12.7.1. Avoidance Mechanisms
- 12.7.2. Antispyware Tools

12.8. Trackers
- 12.8.1. Measures to Protect the System
- 12.8.2. Anti-tracking Tools

12.9. EDR- End Point Detection and Response
- 12.9.1. Behavior of the EDR System
- 12.9.2. Differences between EDR and Antivirus
- 12.9.3. Future of the EDR Systems

12.10. Control over Software Installation
- 12.10.1. Repositories and Software Stores
- 12.10.2. Lists of Permitted or Prohibited Software
- 12.10.3. Upgrade Criteria
- 12.10.4. Privileges to Install Software

Module 13. Network Security (Perimeter)

- 13.1. Detection Systems and Threat Prevention
    - 13.1.1. General Framework of Security Incidences
    - 13.1.2. Current Defence Systems: Defence in Depth and SOC
    - 13.1.3. Current Network Architectures
    - 13.1.4. Types of Tools for Incident Detection and Prevention
        - 13.1.4.1. Network Based Systems
        - 13.1.4.2. Host Based Systems
        - 13.1.4.3. Centralized Systems
    - 13.1.5. Instance/Host, Container and Serverless Communication and Discovery
- 13.2. Firewall
    - 13.2.1. Types of Firewalls
    - 13.2.2. Attacks and Mitigation
    - 13.2.3. Common Firewalls in Kernel Linux
        - 13.2.3.1. UFW
        - 13.2.3.2. Nftables and Iptables
        - 13.2.3.3. Firewall
    - 13.2.4. Detection Systems Based on System Logs
        - 13.2.4.1. TCP Wrappers
        - 13.2.4.2. BlockHosts and DenyHosts
        - 13.2.4.3. Fai2ban
- 13.3. Detection Systems and Intrusion Prevention (IDS/IPS)
    - 13.3.1. Attacks on IDS/IPS
    - 13.3.2. IDS/IPS Systems
        - 13.3.2.1. Snort
        - 13.3.2.2. Suricata
- 13.4. Next Generation Firewalls (NGFW)
    - 13.4.1. Differences between NGFW and Traditional Firewalls
    - 13.4.2. Main Capabilities
    - 13.4.3. Commercial Solutions
    - 13.4.4. Firewalls for Cloud Services
        - 13.4.4.1. VPC Cloud Architecture
        - 13.4.4.2. ACLS Cloud
        - 13.4.4.3. Security Group
- 13.5. Proxy
    - 13.5.1. Types of Proxy
    - 13.5.2. Proxy Use Advantages and Disadvantages
- 13.6. Antivirus Motors
    - 13.6.1. General Context of Malware and IOCs
    - 13.6.2. Problems of Antivirus Motors
- 13.7. Mail Protection Systems
    - 13.7.1. Antispam
        - 13.7.1.1. White and Black Lists
        - 13.7.1.2. Bayesian Filters
    - 13.7.2. Mail Gateway (MGW)
- 13.8. SIEM
    - 13.8.1. Architecture and Components
    - 13.8.2. Correlation Rules and Use Cases
    - 13.8.3. Current Challenges of SIEM Systems
- 13.9. SOAR
    - 13.9.1. SOAR and SIEM: Enemies or Allies
    - 13.9.2. Future of the SOAR Systems
- 13.10. Others Network Based Systems
    - 13.10.1. WAF
    - 13.10.2. NAC
    - 13.10.3. HoneyPots and HoneyNets
    - 13.10.4. CASB

Module 14. Smartphone Security

- 14.1. The World of the Mobile Device
  - 14.1.1. Types of Mobile Platforms
  - 14.1.2. iOS Devices
  - 14.1.3. Android Devices
- 14.2. Management of Mobile Security
  - 14.2.1. OWASP Mobile Security Project
    - 14.2.1.1. Top 10 Vulnerabilities
  - 14.2.2. Communications, Networks and Connexion Modes
- 14.3. The Mobile Device in the Business World
  - 14.3.1. Risks
  - 14.3.2. Security Policies
  - 14.3.3. Device Monitoring
  - 14.3.4. Mobile Device Management (MDM)
- 14.4. User Privacy and Data Security
  - 14.4.1. Information Statuses
  - 14.4.2. Protection and Confidentiality of Data
    - 14.4.2.1. Licences
    - 14.4.2.2. Encryption
  - 14.4.3. Secure Data Storage
    - 14.4.3.1. Safe iOS Storage
    - 14.4.3.2. Safe Android Storage
  - 14.4.4. Best Practices in the Application Development
- 14.5. Vulnerabilities and Attack Vectors
  - 14.5.1. Vulnerabilities
  - 14.5.2. Attack Vectors
    - 14.5.2.1. Malware
    - 14.5.2.2. Data Exfiltration
    - 14.5.2.3. Data Manipulation
- 14.6. Main Threats
  - 14.6.1. Unforced User
  - 14.6.2. Malware
    - 14.6.2.1. Types of Malware
  - 14.6.3. Social Engineering
  - 14.6.4. Data Leakage
  - 14.6.5. Information Theft
  - 14.6.6. Unsecure Wi-Fi Networks
  - 14.6.7. Outdated Software
  - 14.6.8. Malicious Applications
  - 14.6.9. Insecure Passwords
  - 14.6.10. Weak Configuration or Non-existent Security
  - 14.6.11. Physical Access
  - 14.6.12. Loss or Theft of the Device
  - 14.6.13. Identity Theft (Integrity)
  - 14.6.14. Weak or Broken Cryptography
  - 14.6.15. Denial of Service (DoS)
- 14.7. Main Attacks
  - 14.7.1. Phishing Attacks
  - 14.7.2. Attacks Related to Modes of Communication
  - 14.7.3. Smishing Attacks
  - 14.7.4. Cryptojacking Attacks
  - 14.7.5. Man in The Middle
- 14.8. Hacking
  - 14.8.1. Rooting and Jailbreaking
  - 14.8.2. Anatomy of a Mobile Attack
    - 14.8.2.1. Threat Propagation
    - 14.8.2.2. Installation of Malware on the Device
    - 14.8.2.3. Persistence
    - 14.8.2.4. Payload Execution and Information Extraction

- 14.8.3. Hacking on iOS Devices: Mechanisms and Tools
- 14.8.4. Hacking on Android Devices: Mechanisms and Tools

14.9. Penetration Testing
- 14.9.1. iOS PenTesting
- 14.9.2. Android PenTesting
- 14.9.3. Tools

14.10. Protection and Security
- 14.10.1. Security Configuration
  - 14.10.1.1. In iOS Devices
  - 14.10.1.2. In Android Devices
- 14.10.2. Security Measures
- 14.10.3. Protection Tools

Module 15. IoT Security

15.1. Devices
- 15.1.1. Types of Devices
- 15.1.2. Standardized Architecture
  - 15.1.2.1. ONEM2M
  - 15.1.2.2. IoTWF
- 15.1.3. Application Protocols
- 15.1.4. Connectivity Technologies

15.2. IoT Devices Application Areas
- 15.2.1. SmartHome
- 15.2.2. SmartCity
- 15.2.3. Transports
- 15.2.4. Wearables
- 15.2.5. Healthcare Sector
- 15.2.6. IioT

15.3. Communication Protocols
- 15.3.1. QTTM
- 15.3.2. LWM2M
- 15.3.3. OMA-DM
- 15.3.4. TR-069

15.4. SmartHome
- 15.4.1. Home Automation
- 15.4.2. Networks
- 15.4.3. Electrodomestics
- 15.4.4. Surveillance and Security

15.5. SmartCity
- 15.5.1. Lighting
- 15.5.2. Meteorology
- 15.5.3. Security/safety

15.6. Transports
- 15.6.1. Localization
- 15.6.2. Making Payments and Obtaining Services
- 15.6.3. Connectivity

15.7. Wearables
- 15.7.1. Intelligent Clothes
- 15.7.2. Intelligent Jewellery
- 15.7.3. Intelligent Watches

15.8. Healthcare Sector
- 15.8.1. Exercise Monitoring/Cardiac Rhythm
- 15.8.2. Monitoring of Patients and Elderly People
- 15.8.3. Implantable
- 15.8.4. Surgical Robots

15.9. Connectivity
- 15.9.1. Wi-Fi/Gateway
- 15.9.2. Bluetooth
- 15.9.3. Incorporated Connectivity

15.10. Securitization
- 15.10.1. Dedicated Networks
- 15.10.2. Password Managers
- 15.10.3. Use of Encrypted Protocols
- 15.10.4. Use Tips

Module 16. Ethical Hacking

- 16.1. Work Environment
  - 16.1.1. Linux Distributions
    - 16.1.1.1. Kali Linux - Offensive Security
    - 16.1.1.2. Parrot OS
    - 16.1.1.3. Ubuntu
  - 16.1.2. Virtualization Systems
  - 16.1.3. Sandbox
  - 16.1.4. Deployment of Laboratories
- 16.2. Methods
  - 16.2.1. OSSTM
  - 16.2.2. OWASP
  - 16.2.3. NIST
  - 16.2.4. PTES
  - 16.2.5. ISSAF
- 16.3. Footprinting
  - 16.3.1. Open-Source Intelligence (OSINT)
  - 16.3.2. Search for Data Breaches and Vulnerabilities
  - 16.3.3. Use of Passive Tools
- 16.4. Network Scanning
  - 16.4.1. Scanning Tools
    - 16.4.1.1. Nmap
    - 16.4.1.2. Hping3
    - 16.4.1.3. Other Scanning Tools
  - 16.4.2. Scanning Techniques
  - 16.4.3. Firewall I and IDS Evasion Techniques
  - 16.4.4. Banner Grabbing
  - 16.4.5. Networks Diagrams
- 16.5. Enumeration
  - 16.5.1. SMTP Enumeration
  - 16.5.2. DNS Enumeration
  - 16.5.3. NetBIOS and Samba Enumeration
  - 16.5.4. LDAP Enumeration
  - 16.5.5. SNMP Enumeration
  - 16.5.6. Other Techniques of Enumeration
- 16.6. Vulnerability Analysis
  - 16.6.1. Vulnerability Scanning Solutions
    - 16.6.1.1. Qualys
    - 16.6.1.2. Nessus
    - 16.6.1.3. CFI LanGuard
  - 16.6.2. Vulnerability Scoring Systems
    - 16.6.2.1. CVSS
    - 16.6.2.2. CVE
    - 16.6.2.3. NVD
- 16.7. Attacks on Wireless Networks
  - 16.7.1. Hacking Methodology of Wireless Networks
    - 16.7.1.1. Wi-Fi Discovery
    - 16.7.1.2. Traffic Analysis
    - 16.7.1.3. Aircrack Attacks
      - 16.7.1.3.1. WEP Attacks
      - 16.7.1.3.2. WPA/WPA2 Attacks
    - 16.7.1.4. Evil Twin Attacks
    - 16.7.1.5. WPS Attacks
    - 16.7.1.6. Jamming
  - 16.7.2. Tools for Wireless Security
- 16.8. Hacking of Web Servers
  - 16.8.1. Cross Site Scripting
  - 16.8.2. CSRF
  - 16.8.3. Hijacking Session
  - 16.8.4. SQL Injection

16.9. Exploitation of Vulnerabilities
- 16.9.1. Use of Known Exploits
- 16.9.2. Use of Known Metasploit
- 16.9.3. Use of Malware
  - 16.9.3.1. Definition and Scope
  - 16.9.3.2. MalwareGeneration
  - 16.9.3.3. Bypass of Antivirus Solutions

16.10. Persistence
- 16.10.1. Rootkits Installations
- 16.10.2. Use of Ncat
- 16.10.3. Use of Scheduled Tasks for Backdoors
- 16.10.4. User Creation
- 16.10.5. HIDS Detection

Module 17. Reverse Engineering

17.1. Compilers
- 17.1.1. Types of Codes
- 17.1.2. Phases to a Compiler
- 17.1.3. Table of Symbols
- 17.1.4. Mistake Manager
- 17.1.5. GCC Compiler

17.2. Types of Analysis in Compilers
- 17.2.1. Lexical Analysis
  - 17.2.1.1. Terminology
  - 17.2.1.2. Lexical Components
  - 17.2.1.3. LEX Lexical Analyzer
- 17.2.2. Syntactic Analysis
  - 17.2.2.1. Context-Free Grammars
  - 17.2.2.2. Types of Syntactic Analysis
    - 17.2.2.2.1. Top-Down Analysis
    - 17.2.2.2.2. Bottom-Up Analysis
  - 17.2.2.3. Syntactic Trees and Derivations
  - 17.2.2.4. Types of Syntactic Analyzers
    - 17.2.2.4.1. LR Analyzers (Left to Right)
    - 17.2.2.4.2. LALR Analyzers
- 17.2.3. Semantic Analysis
  - 17.2.3.1. Attribute Grammars
  - 17.2.3.2. S-Attributed
  - 17.2.3.3. L-Attributed

17.3. Data Structures in Assembler
- 17.3.1. Variables
- 17.3.2. Arrays
- 17.3.3. Pointers
- 17.3.4. Structures
- 17.3.5. Objects

17.4. Assembler Code Structures
- 17.4.1. Selection Structures
  - 17.4.1.1. If, Else If, Else
  - 17.4.1.2. Switch
- 17.4.2. Iteration Structures
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Use of the Break
- 17.4.3. Functions

17.5. X86 Hardware Architecture
- 17.5.1. x86 Processor Architecture
- 17.5.2. X86 Data Structures
- 17.5.3. x86 Code Structures

17.6. ARM Hardware Architecture
- 17.6.1. ARM Processor Architecture
- 17.6.2. ARM Data Structures
- 17.6.3. ARM Code Structures

17.7. Static Code Analysis
- 17.7.1. Disassemblers
- 17.7.2. IDA
- 17.7.3. Code Rebuilders

17.8. Dynamics Code Analysis
- 17.8.1. Behavior Analysis
  - 17.8.1.1. Communication
  - 17.8.1.2. Monitoring
- 17.8.2. Linux Code Debuggers
- 17.8.3. Windows Code Debuggers

17.9. Sandbox
- 17.9.1. Sandbox Architecture
- 17.9.2. Sandbox Avoidance
- 17.9.3. Detection Techniques
- 17.9.4. Avoidance Techniques
- 17.9.5. Countermeasures
- 17.9.6. Sandbox in Linux
- 17.9.7. Sandboxin Windows
- 17.9.8. Sandox in MacOS
- 17.9.9. Sandbox in Android

17.10. Malware Analysis
- 17.10.1. Analysis Methods of Malware
- 17.10.2. Malware Obfuscation Techniques
  - 17.10.2.1. Executable Obfuscation
  - 17.10.2.2. Restriction of Execution Environments
- 17.10.3. Malware Analysis Tools

Module 18. Secure Development

18.1. Secure Development
- 18.1.1. Quality, Functionality and Security
- 18.1.2. Confidentiality, Integrity and Availability
- 18.1.3. Software Development Life Cycle

18.2. Requirements Phase
- 18.2.1. Authentication Control
- 18.2.2. Role and Privilege Control
- 18.2.3. Risk-Oriented Requirements
- 18.2.4. Privilege Approval

18.3. Analysis and Design Phases
- 18.3.1. Component Access and System Administration
- 18.3.2. Audit Trails
- 18.3.3. Session Management
- 18.3.4. Historical Data
- 18.3.5. Proper Error Handling
- 18.3.6. Separation of Functions

18.4. Implementation and Coding Phase
- 18.4.1. Ensuring the Development Environment
- 18.4.2. Preparation of Technical Documentation
- 18.4.3. Secure Coding
- 18.4.4. Communications Security

18.5. Good Practices of Secure Coding
- 18.5.1. Validation of Entry Data
- 18.5.2. Coding of Output Data
- 18.5.3. Programming Style
- 18.5.4. Change Log Management
- 18.5.5. Cryptographic Practices
- 18.5.6. Management of Mistakes and Logs
- 18.5.7. File Management
- 18.5.8. Memory Management
- 18.5.9. Standardization and Reuse of Security Functions

18.6. Server Preparation and Hardening

18.6.1. Management of Users, Groups and Roles on the Server

18.6.2. Software Installation

18.6.3. Server Hardening

18.6.4. Robust Configuration of the Application Environment

18.7. DB Preparation and Hardening

18.7.1. DB Engine Optimization

18.7.2. Create Your Own User for the Application

18.7.3. Assignment of the Required Privileges to the User

18.7.4. Hardening of the DB

18.8. Testing Phase

18.8.1. Quality Control in Security Controls

18.8.2. Phased Code Inspection

18.8.3. Checking Configuration Management

18.8.4. Black Box Tests

18.9. Preparing the Transition to Production

18.9.1. Perform Change Control

18.9.2. Carry Out Production Changeover Procedure

18.9.3. Perform Rollback Procedure

18.9.4. Pre-Production Testing

18.10. Maintenance Phase

18.10.1. Risk-Based Assurance

18.10.2. White Box Security Maintenance Tests

18.10.3. Black Box Safety Maintenance Tests

Module 19. Forensic Analysis

19.1. Data Acquisition and Duplication

19.1.1. Volatile Data Acquisition

19.1.1.1. System Information

19.1.1.2. Network Information

19.1.1.3. Volatility Order

19.1.2. Static Data Acquisition

19.1.2.1. Creating a Duplicate Image

19.1.2.2. Preparation of a Chain of Custody Document

19.1.3. Methods for Validation of Acquired Data

19.1.3.1. Methods for Linux

19.1.3.2. Methods for Windows

19.2. Evaluation and Defeat of Antiforensic Techniques

19.2.1. Objectives of Antiforensic Techniques

19.2.2. Data Deletion

19.2.2.1. Data Deletion and Files

19.2.2.2. File Recovery

19.2.2.3. Recovery of Deleted Partitions

19.2.3. Password Protection

19.2.4. Steganography

19.2.5. Secure Device Wiping

19.2.6. Encryption

19.3. Forensic Analysis of the Operating System

19.3.1. Windows Forensic Analysis

19.3.2. Linux Forensic Analysis

19.3.3. Mac Forensic Analysis

19.4. Network Forensic Analysis

19.4.1. Logs Analysis

19.4.2. Correlation of Data

19.4.3. Network Investigation

19.4.4. Steps to Follow in Network Forensic Analysis

- 19.5. Web Forensic Analysis
    - 19.5.1. Investigation of Web Attacks
    - 19.5.2. Attack Detection
    - 19.5.3. IP Address Location
- 19.6. Forensic Analysis of Databases
    - 19.6.1. MSSQL Forensic Analysis
    - 19.6.2. MySQL Forensic Analysis
    - 19.6.3. PostgreSQL Forensic Analysis
    - 19.6.4. MongoDB Forensic Analysis
- 19.7. Cloud Forensic Analysis
    - 19.7.1. Types of Crimes in Cloud
        - 19.7.1.1. Cloud as Subject
        - 19.7.1.2. Cloud as Object
        - 19.7.1.3. Cloud as Tool
    - 19.7.2. Challenges of Cloud Forensics
    - 19.7.3. Investigation of Storage Services in the Cloud
    - 19.7.4. Forensic Analysis Tools for Cloud
- 19.8. Investigation of Email Crimes
    - 19.8.1. Mail Systems
        - 19.8.1.1. Mail Clients
        - 19.8.1.2. Server Clients
        - 19.8.1.3. SMTP Server
        - 19.8.1.4. POP3 Server
        - 19.8.1.5. IMAP4 Server
    - 19.8.2. Mail Crimes
    - 19.8.3. Mail Message
        - 19.8.3.1. Standard Headers
        - 19.8.3.2. Extended Headers
    - 19.8.4. Steps for the Investigation of These Crimes
    - 19.8.5. Forensic Tools for Email
- 19.9. Forensic Analysis of Mobiles
    - 19.9.1. Cellular Networks
        - 19.9.1.1. Types of Networks
        - 19.9.1.2. CDR Contents
    - 19.9.2. Subscriber Identity Module (SIM)
    - 19.9.3. Logical Acquisition
    - 19.9.4. Physical Acquisition
    - 19.9.5. File System Acquisition
- 19.10. Forensic Report Writing and Presentation
    - 19.10.1. Important Aspects of a Forensic Report
    - 19.10.2. Classification and Types of Reports
    - 19.10.3. Guide to Write a Report
    - 19.10.4. Presenting Reports
        - 19.10.4.1. Prior Preparation for Testifying
        - 19.10.4.2. Deposition
        - 19.10.4.3. Dealing with the Media

Module 20. Current and Future Challenges in IT Security

- 20.1. Blockchain Technology
    - 20.1.1. Scope of Application
    - 20.1.2. Confidentiality Guarantee
    - 20.1.3. Non-Repudiation Guarantee
- 20.2. Digital Money
    - 20.2.1. Bitcoins
    - 20.2.2. Cryptocurrencies
    - 20.2.3. Cryptocurrency Mining
    - 20.2.4. Pyramid Schemes
    - 20.2.5. Other Potential Offenses and Problems
- 20.3. Deepfake
    - 20.3.2. Impact of the Media
    - 20.3.3. Dangers for Society
    - 20.3.4. Detection Mechanisms
- 20.4. Future of Artificial Intelligence
    - 20.4.1. Artificial Intelligence and Cognitive Computing
    - 20.4.2. Uses to Simplify Customer Service
- 20.5. Digital Privacy
    - 20.5.1. Value of Data in the Network
    - 20.5.2. Use of Data in the Network
    - 20.5.3. Management of Privacy and Digital Identity

20.6. Cyberconflicts, Cybercriminals and Cyberattacks
- 20.6.1. Impact of Cybersecurity in International Conflicts
- 20.6.2. Consequences of Cyber-Attacks on the General Population
- 20.6.3. Types of Cybercriminals Protection Measures

20.7. Telework
- 20.7.1. Telework Revolution During and After Covid19
- 20.7.2. Access Bottlenecks
- 20.7.3. Variation of the Attacking Surface
- 20.7.4. Employee Needs

20.8. Emergent Wireless Technologies
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Millimeter Waves
- 20.8.4. Tendency of "Get Smart" instead of "Get more"

20.9. Future Addressing in Networks
- 20.9.1. Current Problems with IP Addressing
- 20.9.2. IPv6
- 20.9.2. IPv4+
- 20.9.3. Advantages of Ipv4+ over IPv4
- 20.9.4. Advantages of Ipv6 over IPv4

20.10. The Challenge of Raising Awareness of Early and Continuing Education in the Population
- 20.10.1. Current Strategies of Government
- 20.10.2. Resistance of the Population to Learning
- 20.10.3. Training Plans to Be Adopted by Companies

> *Don't think twice, you know that with this Advanced Master's Degree, you will go far"*

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

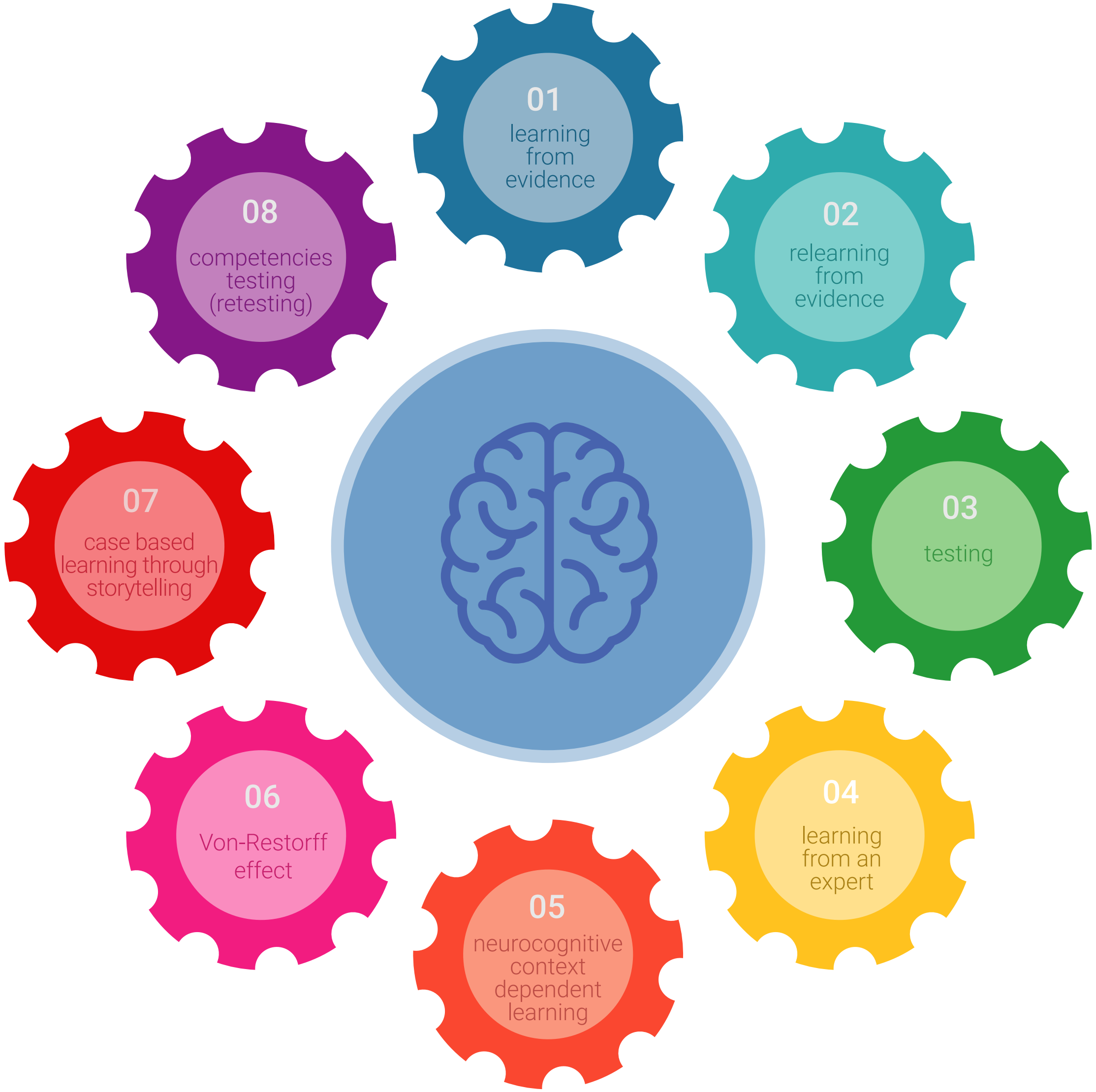
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

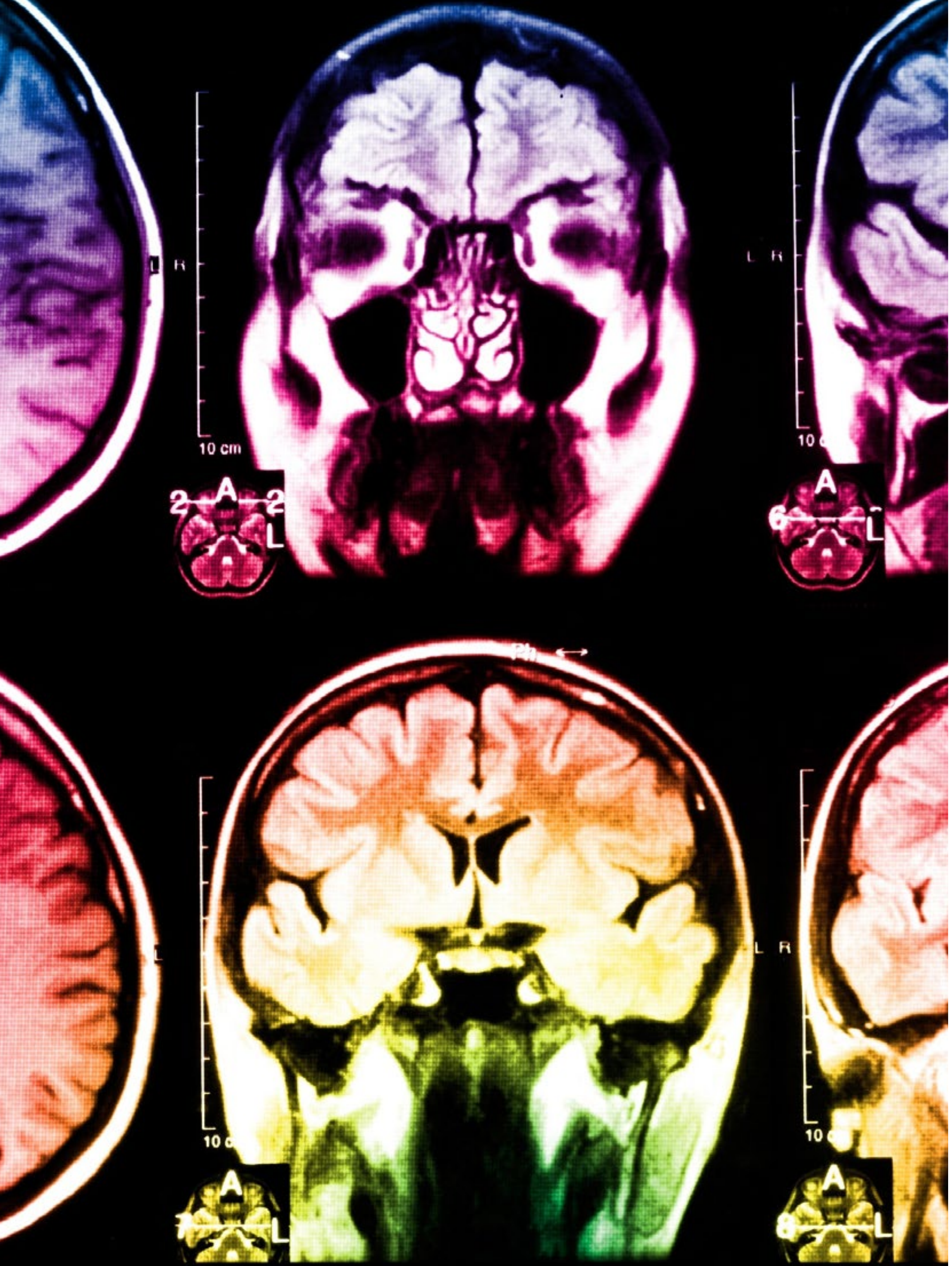
We enhance the Case Study with the best 100% online teaching method: Relearning.

> *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.


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.

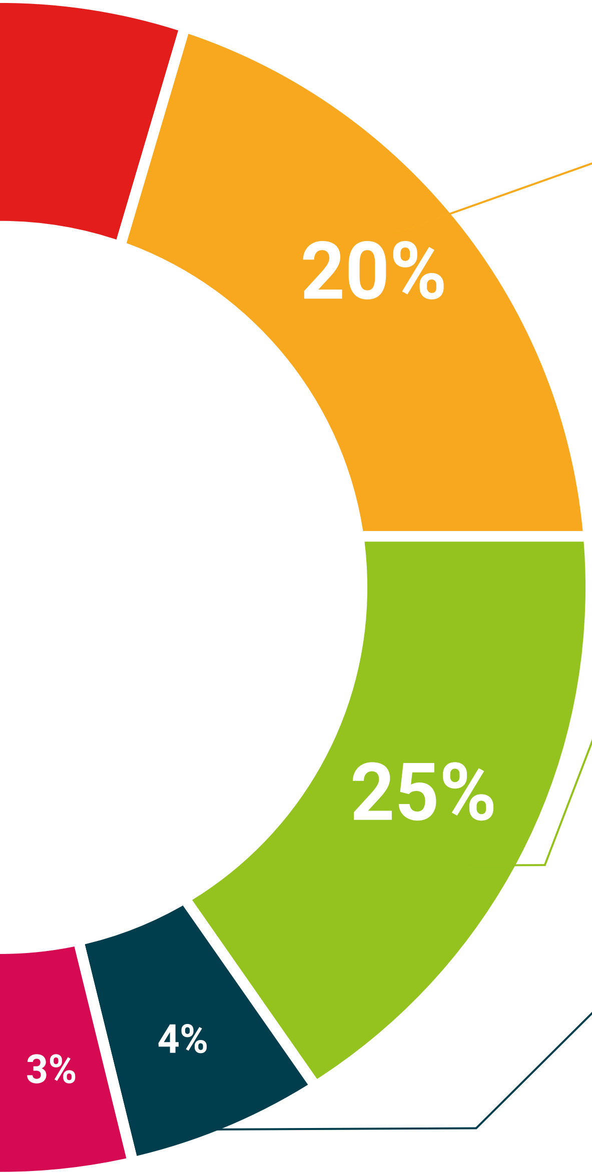
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

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.

07

Certificate

The Advanced Master's Degree in Secure Information Management guarantees you, in addition to the most rigorous and up-to-date training, access to a Advanced Master's Degree issued by TECH Technological University.

Successfully complete this program and receive your university degree without travel or laborious paperwork"

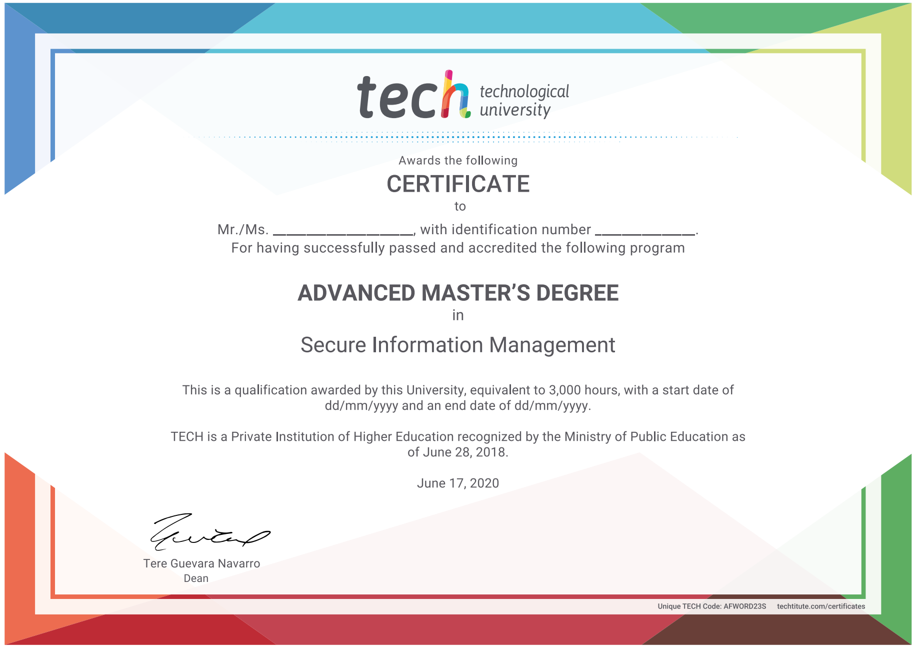
This **Advanced Master's Degree in Secure Information Management** contains the most complete and up-to-date program on the market.

After the student has passed the assessments, they will receive their corresponding **Advanced Master's Degree** issued by **TECH Technological University** via tracked delivery*.

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

Title: **Advanced Master's Degree in Secure Information Management**

Official Nº of hours: **3,000 h.**



tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. _______________, with identification number ___________.
For having successfully passed and accredited the following program

ADVANCED MASTER'S DEGREE

in

Secure Information Management

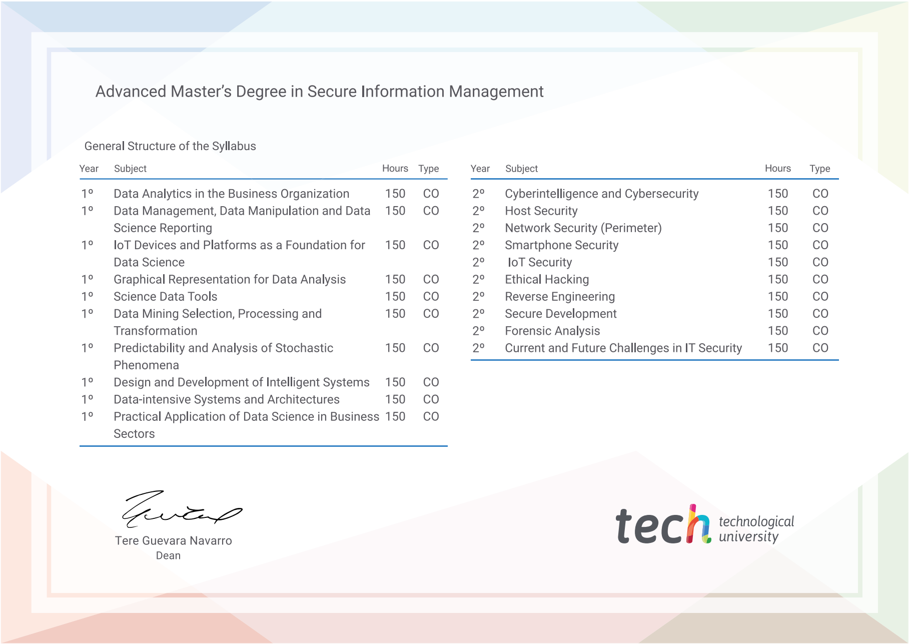
This is a qualification awarded by this University, equivalent to 3,000 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

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



Advanced Master's Degree in Secure Information Management

General Structure of the Syllabus

Year	Subject	Hours	Type
1º	Data Analytics in the Business Organization	150	CO
1º	Data Management, Data Manipulation and Data Science Reporting	150	CO
1º	IoT Devices and Platforms as a Foundation for Data Science	150	CO
1º	Graphical Representation for Data Analysis	150	CO
1º	Science Data Tools	150	CO
1º	Data Mining Selection, Processing and Transformation	150	CO
1º	Predictability and Analysis of Stochastic Phenomena	150	CO
1º	Design and Development of Intelligent Systems	150	CO
1º	Data-intensive Systems and Architectures	150	CO
1º	Practical Application of Data Science in Business Sectors	150	CO

Year	Subject	Hours	Type
2º	Cyberintelligence and Cybersecurity	150	CO
2º	Host Security	150	CO
2º	Network Security (Perimeter)	150	CO
2º	Smartphone Security	150	CO
2º	IoT Security	150	CO
2º	Ethical Hacking	150	CO
2º	Reverse Engineering	150	CO
2º	Secure Development	150	CO
2º	Forensic Analysis	150	CO
2º	Current and Future Challenges in IT Security	150	CO

Tere Guevara Navarro
Dean

tech technological university

*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

Advanced Master's Degree

Secure Information Management

- Modality: **online**
- Duration: **2 years**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Advanced Master’s Degree

Secure Information Management

tech technological university