Advanced Master's Degree
Secure Information Management

Advanced Master's Degree
Secure Information Management

- Modality: **online**
- Duration: **2 years**
- Certificate: **TECH Global University**
- Accreditation: **120 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

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

Index

01

Introduction to the Program

In today's digital age, activities in a variety of fields are managed seamlessly over the Internet. Entertainment, work and communication with friends and family increasingly depend on online tools and resources. Enormous amounts of information are transferred daily, from simple data in conversations on social networks and messaging applications to sensitive personal and professional information hosted on banking or business platforms. This scenario requires specialists capable of handling and protecting information in different contexts, prioritizing its security. That is why TECH has designed this program in Software Engineering, focused on training professionals with the necessary skills to manage and protect information effectively, addressing current digital challenges and contributing to create safer and more reliable technological environments.

> *"Protecting data is key in the face of constant threats. You could be the guardian of that valuable information"*

Every second, thousands of pieces of data are generated, shared and stored in the digital environment. From making online payments and accessing educational services to coordinating business activities or protecting digital identities, technology has become an essential pillar that continually transforms the way we live and work. These interactions generate and transfer massive amounts of data at every instant, from personal information to sensitive files related to companies and institutions. This constant flow of data highlights the need for proper handling to ensure its security and privacy.

Managing and protecting this data is no simple task, as it requires the combination of highly specialized expertise in areas such as cybersecurity and information management. These disciplines, although distinct, must be integrated to address the complex challenges of today's digital environment. In this context, the Advanced Master's Degree in Secure Information Management represents a unique opportunity for engineers and IT professionals interested in acquiring a comprehensive vision that will enable them to master both areas and position themselves as leaders in a constantly growing sector.

Many companies and institutions face the need to protect critical and highly sensitive data, but lack experts who can ensure effective management, preservation and surveillance of their digital information. To respond to this demand, TECH has designed a program that combines the best content with a teaching team of recognized professional experience. This approach ensures that students acquire the tools and knowledge necessary to stand out in the job market and access strategic positions in organizations seeking to strengthen their information security.

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

- The development of practical cases presented by experts in Secure Information Management
- The graphic, schematic, and practical contents with which they are created, provide scientific and practical information on the disciplines that are essential for professional practice
- Practical exercises where self-assessment can be used to improve learning
- Special emphasis on innovative methodologies in Secure Information Management
- 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

> *Acquire the skills needed to secure and effectively manage data in a competitive digital environment"*

Discover the most innovative educational methodology designed by TECH to guarantee immersive and contextualized learning.

Consolidate your theoretical knowledge with the numerous practical resources included in this Advanced Master's Degree in Secure Information Management"

Access a 100% online program that allows you to study at your own pace, at any time and from anywhere in the world.

The teaching staff includes professionals belonging to the field of Finance, who bring to this program the experience of their work, as well as recognized specialists from leading companies 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 an immersive learning experience designed to prepare 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 throughout the program. For this purpose, the professional will be assisted by an innovative interactive video system created by renowned and experienced experts.

02
Why Study at TECH?

TECH is the world's largest online university. With an impressive catalog of more than 14,000 university programs, available in 11 languages, it is positioned as a leader in employability, with a 99% job placement rate. In addition, it has a huge faculty of more than 6,000 professors of the highest international prestige.

> *Study at the largest online university in the world and ensure your professional success. The future begins at TECH"*

The world's best online university, according to FORBES

The prestigious Forbes magazine, specialized in business and finance, has highlighted TECH as "the best online university in the world" This is what they have recently stated in an article in their digital edition in which they echo the success story of this institution, "thanks to the academic offer it provides, the selection of its teaching staff, and an innovative learning method oriented to form the professionals of the future"

The best top international faculty

TECH's faculty is made up of more than 6,000 professors of the highest international prestige. Professors, researchers and top executives of multinational companies, including Isaiah Covington, performance coach of the Boston Celtics; Magda Romanska, principal investigator at Harvard MetaLAB; Ignacio Wistumba, chairman of the department of translational molecular pathology at MD Anderson Cancer Center; and D.W. Pine, creative director of TIME magazine, among others.

The world's largest online university

TECH is the world's largest online university. We are the largest educational institution, with the best and widest digital educational catalog, one hundred percent online and covering most areas of knowledge. We offer the largest selection of our own degrees and accredited online undergraduate and postgraduate degrees. In total, more than 14,000 university programs, in ten different languages, making us the largest educational institution in the world.

Forbes
Mejor universidad
online del mundo

Plan
de estudios
más completo

Profesorado
TOP
Internacional

La metodología
más eficaz

nº1
Mundial
Mayor universidad
online del mundo

The most complete syllabuses on the university scene

TECH offers the most complete syllabuses on the university scene, with programs that cover fundamental concepts and, at the same time, the main scientific advances in their specific scientific areas. In addition, these programs are continuously updated to guarantee students the academic vanguard and the most demanded professional skills. and the most in-demand professional competencies. In this way, the university's qualifications provide its graduates with a significant advantage to propel their careers to success.

A unique learning method

TECH is the first university to use Relearning in all its programs. This is the best online learning methodology, accredited with international teaching quality certifications, provided by prestigious educational agencies. In addition, this innovative academic model is complemented by the "Case Method", thereby configuring a unique online teaching strategy. Innovative teaching resources are also implemented, including detailed videos, infographics and interactive summaries.

The official online university of the NBA

TECH is the official online university of the NBA. Thanks to our agreement with the biggest league in basketball, we offer our students exclusive university programs, as well as a wide variety of educational resources focused on the business of the league and other areas of the sports industry. Each program is made up of a uniquely designed syllabus and features exceptional guest hosts: professionals with a distinguished sports background who will offer their expertise on the most relevant topics.

Leaders in employability

TECH has become the leading university in employability. Ninety-nine percent of its students obtain jobs in the academic field they have studied within one year of completing any of the university's programs. A similar number achieve immediate career enhancement. All this thanks to a study methodology that bases its effectiveness on the acquisition of practical skills, which are absolutely necessary for professional development.

Google Partner
PREMIER 2023
Universidad online oficial de la NBA
NBA
4,9/5
★★★★★
Trustpilot
99%
Garantía de máxima empleabilidad

Google Premier Partner

The American technology giant has awarded TECH the Google Premier Partner badge. This award, which is only available to 3% of the world's companies, highlights the efficient, flexible and tailored experience that this university provides to students. The recognition not only accredits the maximum rigor, performance and investment in TECH's digital infrastructures, but also places this university as one of the world's leading technology companies.

Top-rated by its students

The main review websites have positioned TECH as the best rated university in the world by its students. These review portals, recognized for their reliability and prestige due to the rigorous verification and validation of the authenticity of each opinion, have given TECH highly favorable ratings. These ratings place TECH as the absolute international university reference.

03

Syllabus

The teaching materials that make up this Advanced Master's Degree in Secure Information Management have been developed by a team of experts in cybersecurity and data management. Therefore, the curriculum delves into the main digital threats and the most advanced methodologies for the protection and management of information. This will enable graduates to identify specific risks and develop effective solutions to ensure data security in various professional environments. The syllabus also addresses the most innovative tools in the sector, promoting strategies aimed at protecting the digital assets of organizations.

> *You will contribute to the protection of sensitive data and the creation of secure systems that guarantee the operational continuity of companies and institutions”*

Module 1. Data Analysis in a 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 Analysis in the Business
- 1.2.1. Departmental Scorecards and KPIs
- 1.2.2. Operational, Tactical and Strategic Reports
- 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 for Measurement, 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, Prediction and Campaign Management

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

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

1.6. Purchasing
- 1.6.1. Data Analysis for Market Research
- 1.6.2. Data Analysis for Competency Research
- 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 Credit Risk Analysis

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

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 Analysis and Digital Transformation
- 1.10.3. Innovation and Productivity

Module 2. Data Management, Data Manipulation and Information Management for Data Science

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

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

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

2.4. Data Knowledge from the Graphs
- 2.4.1. Visualization According to Type of Data
- 2.4.2. Interpretation of Graphic Information
- 2.4.3. Customization of Graphics with

2.5. Probability
- 2.5.1. Probability
- 2.5.2. Function of Probability
- 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 Indexes
- 2.8.3. Data Mining

2.9. Datawarehouse
- 2.9.1. Components
- 2.9.2. Design

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

Module 3. Devices and IoT Platforms as a Base 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 LoT and LIoT
- 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 Exchange and Visualization

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

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 of 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 Graphical Representation
- 4.2. Optimization for Data Science
  - 4.2.1. Color Range and Design
  - 4.2.2. Gestalt in Graphic Representation
  - 4.2.3. Errors to Avoid and Advice
- 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 Data Generation
- 4.5. Types of Graphs
  - 4.5.1. Basic Representations
  - 4.5.2. Block Representation
  - 4.5.3. Representation for Dispersion Analysis
  - 4.5.4. Circular Representations
  - 4.5.5. Bubble Representations
  - 4.5.6. Geographical 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 Graphic 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. Tools Oriented Towards 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. Systems for Virtualization of Reality
  - 4.10.2. Reality Enhancement and Improvement Systems
  - 4.10.3. Intelligent Systems

Module 5. Data Science Tools

- 5.1. Data Science
  - 5.1.1. Data Science
  - 5.1.2. Advanced Tools for Data Scientists
- 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. Extraction of Information from a Dataset
- 5.4. Extraction of Information Through Visualization
  - 5.4.1. Visualization as an Analysis Tool
  - 5.4.2. Visualization Methods
  - 5.4.3. Visualization of a Data Set

5.5. Data Quality
- 5.5.1. Quality Data
- 5.5.2. Data Cleaning
- 5.5.3. Basic Data Pre-Processing

5.6. Dataset
- 5.6.1. Dataset Enrichment
- 5.6.2. The Curse of Dimensionality
- 5.6.3. Modification of Our Data Set

5.7. Unbalance
- 5.7.1. Classes of Unbalance
- 5.7.2. Unbalance Mitigation Techniques
- 5.7.3. Balancing a Dataset

5.8. Unsupervised Models
- 5.8.1. Unsupervised Model
- 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 Data Scientists
- 5.10.2. The Best Model
- 5.10.3. Useful Tools

Module 6. Data Mining: Selection, Preprocessing 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 Cleaning
- 6.3.2. Normalization of Data
- 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. Noise in the Data
- 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 Data vs. Discreet 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 Pre-Processing in Big Data Environments
- 6.10.1. Big Data
- 6.10.2. Classical Versus Massive Pre-processing
- 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. Utility and Applicability
- 7.1.3. Related Case Studies

7.2. Time Series
- 7.2.1. Trend Seasonality of TS
- 7.2.2. Typical Variations
- 7.2.3. Waste Analysis

7.3. Typology
- 7.3.1. Stationary
- 7.3.2. Non-Stationary
- 7.3.3. Transformations and Settings

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

7.5. Basic Forecasting Methods
- 7.5.1. Media
- 7.5.2. *Naïve*
- 7.5.3. Seasonal Naivety
- 7.5.4. Method Comparison

7.6. Waste Analysis
- 7.6.1. Autocorrelation
- 7.6.2. ACF of Waste
- 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 Applications

7.8. Predictive Methods of Time Series
- 7.8.1. ARIMA
- 7.8.2. Exponential Smoothing

7.9. Manipulation and Analysis of Time Series with R
- 7.9.1. Data Preparation
- 7.9.2. Identification of Patterns
- 7.9.3. Model Analysis
- 7.9.4. Prediction

7.10. Combined Graphical Analysis with R
- 7.10.1. Normal Situations
- 7.10.2. Practical Application for the Resolution of Simple Problems
- 7.10.3. Practical Application for the Resolution of 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. Machine 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 Machine Learning
- 8.3.2. SVM and KNN
- 8.3.3. Metrics and Scores for Ranking

8.4. Regression Algorithms
- 8.4.1. Lineal Regression, Logistical Regression and Non-Lineal Models
- 8.4.2. Time Series
- 8.4.3. Metrics and Scores for Regression

8.5. Clustering Algorithms
- 8.5.1. Hierarchical Clustering Techniques
- 8.5.2. Partitional Clustering Techniques
- 8.5.3. Metrics and Scores for Clustering

8.6. Association Rules Techniques
- 8.6.1. Methods for Rule 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 Sorter
- 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. Other 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 for Implementing Deep Neural Networks

Module 9. Architecture and Systems for Intensive Use of Data

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. Document Model
- 9.2.3. Graph Type Data Model

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

9.4. Data Coding Formats
- 9.4.1. Language-Specific Formats
- 9.4.2. Standardized Formats
- 9.4.3. Binary Coding Formats
- 9.4.4. Data Stream 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. Offline Data Processing
- 9.8.1. Batch Processing
- 9.8.2. Distributed File Systems
- 9.8.3. *MapReduce*

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

9.10. Practical Applications in Business
- 9.10.1. Consistency in Readings
- 9.10.2. Holistic Focus of Data
- 9.10.3. Scaling of a Distributed Service

Module 10. Practical Application of Data Science in Business Sectors

10.1. Health Sector
- 10.1.1. Implications of AI and Data Analysis in the Health Sector
- 10.1.2. Opportunities and Challenges

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

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

10.4. Retail
- 10.4.1. Implications of AI and Data Analysis 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 Analysis in Industry 4.0
- 10.5.2. Use in Industry 4.0

10.6. Risks and Trends in 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 Analysis 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 Analysis 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 Analysis 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 Analysis in Human Resources
- 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
  - 11.1.1.1. Intelligence
    - 11.1.1.1.1. Intelligence Cycle
  - 11.1.1.2. Cyberintelligence
  - 11.1.1.3. Cyberintelligence and Cybersecurity
- 11.1.2. 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. Layers of Security
- 11.2.2. Identification of Cyber Threats
  - 11.2.2.1. External Threats
  - 11.2.2.2. Internal Threats
- 11.2.3. Adverse Actions
  - 11.2.3.1. Social Engineering
  - 11.2.3.2. Commonly Used Methods

11.3. Techniques and Tools of Intelligences
- 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. Techniques for Organizing Acquired Information
- 11.4.3. Reliability and Credibility of Information Sources
- 11.4.4. Analysis Methodologies
- 11.4.5. Presentation of Intelligence Results

11.5. Audits and Documentation
- 11.5.1. IT Security Audit
- 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. Network Security
- 11.7.4. Logical Security
- 11.7.5. Web Application Security
- 11.7.6. Security on Mobile Devices

11.8. Regulations and Compliance
- 11.8.1. The GDPR
- 11.8.2. BORRAR
- 11.8.3. ISO 27000 Family
- 11.8.4. NIST Cybersecurity Framework
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. Cloud Regulations
- 11.8.8. SOX
- 11.8.9. ICP

11.9. Risk Analysis and Metrics
- 11.9.1. Extent of Risk
- 11.9.2. The Assets
- 11.9.3. Threats
- 11.9.4. 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. BORRAR
- 11.10.4. OEA
- 11.10.5. UNASUR PROSUR

Module 12. Host Security

12.1. Backup Copies
- 12.1.1. Backup Strategies
- 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. Firewalls for Windows
- 12.4.2. Firewalls for Linux
- 12.4.3. Firewalls for MacOS

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

12.6. Detectors for Phishing
 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. EDR System Behavior
 12.9.2. Differences between EDR and Antivirus
 12.9.3. The Future of 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. Update Criteria
 12.10.4. Software Installation Privileges

Module 13. Network Security (Perimeter)

13.1. Threat Detection and Prevention Systems
 13.1.1. General Framework for Security Incidents
 13.1.2. Current Defense Systems: Defense 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 Hosts, Container and Serverless Communication and Detection
13.2. Firewall
 13.2.1. Types of Firewalls
 13.2.2. Attacks and Mitigation

- 13.2.3. Common Firewalls in Linux Kernel
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables and Iptables
  - 13.2.3.3. *Firewalls*
- 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. Intrusion Detection and Prevention Systems (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 Firewall
- 13.4.2. Main Capabilities
- 13.4.3. Commercial Solutions
- 13.4.4. Firewalls for Cloud Services
  - 13.4.4.1. Virtual Private Cloud (VPC) Architecture
  - 13.4.4.2. Cloud ACLs
  - 13.4.4.3. *Security Group*

13.5. Proxy

- 13.5.1. Types of Proxy
- 13.5.2. Use of Proxy Advantages and Disadvantages

13.6. Antivirus Engines

- 13.6.1. General Context of Malware and IOCs
- 13.6.2. Antivirus Engine Problems

13.7. Email Protection Systems

- 13.7.1. Antispam
  - 13.7.1.1. Black and White Lists
  - 13.7.1.2. Bayesian Filters
- 13.7.2. Mail Gateway (MGW)

13.8. SIEM
- 13.8.1. Components and Architecture
- 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. The Future of SOAR Systems

13.10. Other 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 Mobile Devices
- 14.1.1. Types of Mobile Platforms
- 14.1.2. IOS Devices
- 14.1.3. Android Devices

14.2. Mobile Security Management
- 14.2.1. OWASP Mobile Security Project
    - 14.2.1.1. Top 10 Vulnerabilities
- 14.2.2. Communications, Networks and Connection Modes

14.3. Mobile Devices in Business Environments
- 14.3.1. Risk
- 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. Statements of Information
- 14.4.2. Data Protection and Confidentiality
    - 14.4.2.1. Licenses
    - 14.4.2.2. Encryption
- 14.4.3. Secure Data Storage
    - 14.4.3.1. Secure Storage on iOS
    - 14.4.3.2. Secure Storage on Android
- 14.4.4. Best Practices in 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. Unsecured Wi-Fi Networks
- 14.6.7. Outdated Software
- 14.6.8. Malicious Applications
- 14.6.9. Insecure Passwords
- 14.6.10 Weak or No Security Configuration
- 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 Communication Modes
- 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. Malware Installation 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 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. Safety and Security
- 14.10.1. Security Configuration
  - 14.10.1.1. On iOS Devices
  - 14.10.1.2. On Android Devices
- 14.10.2. Safety Measures
- 14.10.3. Protection Tools

Module 15. IoT Security

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

15.2. IoT Devices. Areas of Application
- 15.2.1. *SmartHome*
- 15.2.2. *SmartCity*
- 15.2.3. Transportation
- 15.2.4. *Wearables*
- 15.2.5. Health Sector
- 15.2.6. IioT

15.3. Communication Protocols
- 15.3.1. MQTT
- 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. Household Appliances
- 15.4.4. Surveillance and Security

15.5. *SmartCity*
- 15.5.1. Lighting
- 15.5.2. Meteorology
- 15.5.3. Security

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

15.7. *Wearables*
- 15.7.1. Smart Clothing
- 15.7.2. Smart Jewelry
- 15.7.3. Smart Watches

15.8. Health Sector
- 15.8.1. Exercise/Heart Rate Monitoring
- 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. Built-In Connectivity

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

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 and IDS Avoidance Techniques
- 16.4.4. *Banner Grabbing*
- 16.4.5. Network 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 Enumeration Techniques

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. Methodology of Hacking in 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. Attacks on WPS
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. *Session Hijacking*
16.8.4. *SQLinjection*
16.9. Exploiting Vulnerabilities
16.9.1. Use of Known Exploits
16.9.2. Use of Metasploit
16.9.3. Use of Malware
16.9.3.1. Definition and Scope
16.9.3.2. Malware Generation
16.9.3.3. Bypass of Antivirus Solutions
16.10. Persistence
16.10.1. Rootkits Installation
16.10.2. Use of Ncat
16.10.3. Use of Programmed 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 of a Compiler
17.1.3. Table of Symbols
17.1.4. Error 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. Parsing
17.2.2.1. Context-Free Grammars
17.2.2.2. Types of Parsing
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 Parsers
17.2.2.4.1. LR (Left To Right) Analyzers
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 Break
- 17.4.3. Functions

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

17.6. ARM Architecture Hardware
- 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. Dynamic Code Analysis
- 17.8.1. Behavioral Analysis
  - 17.8.1.1. Communications
  - 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 Evasion
- 17.9.3. Detection Techniques
- 17.9.4. Avoidance Techniques
- 17.9.5. Countermeasures
- 17.9.6. Sandbox in Linux
- 17.9.7. Sandbox in Windows
- 17.9.8. Sandbox in MacOS
- 17.9.9. Sandbox in Android

17.10. Malware Analysis
- 17.10.1. Malware Analysis Methods
- 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 Safety
- 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 Codification
- 18.4.4. Communications Security

18.5. Good Secure Coding Practices
- 18.5.1. Input Data Validation
- 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. Error and Log Management
- 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. Preparing Databases and Hardening
- 18.7.1. DB Engine Optimization
- 18.7.2. Create Your Own User for the Application
- 18.7.3. Assigning the Required Privileges to the User
- 18.7.4. Hardening of the Databases

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 Testing

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 Testing
- 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. Deletion of Data 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 Forensics
- 19.3.2. Linux Forensics
- 19.3.3. Mac Forensics

19.4. Network Forensic Analysis
- 19.4.1. Logs Analysis
- 19.4.2. Data Correlation
- 19.4.3. Network Research
- 19.4.4. Steps to Follow in Network Forensic Analysis

19.5. Web Forensics
- 19.5.1. Investigation of Web Attacks
- 19.5.2. Attack Detection
- 19.5.3. IP Address Location

19.6. Forensic Database Analysis
- 19.6.1. Forensic Analysis in MSSQL
- 19.6.2. MySQL Forensic Analysis
- 19.6.3. PostgreSQL Forensic Analysis
- 19.6.4. Forensic Analysis in MongoDB

19.7. Cloud Forensics
- 19.7.1. Types of Crimes in the Cloud
  - 19.7.1.1. Cloud as a Subject
  - 19.7.1.2. Cloud as an Object
  - 19.7.1.3. Cloud as a Tool
- 19.7.2. Challenges of Cloud Forensics
- 19.7.3. Research on Cloud Storage Services
- 19.7.4. Cloud Forensic Analysis Tools

19.8. Investigation of Email Crimes
- 19.8.1. Mailing Systems
  - 19.8.1.1. Mail Clients
  - 19.8.1.2. Mail Server
  - 19.8.1.3. SMTP Server
  - 19.8.1.4. POP3 Server
  - 19.8.1.5. IMAP4 Server
- 19.8.2. Mailing 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. E-Mail Forensic Tools

19.9. Mobile Forensic Analysis
- 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 Features of a Forensic Report
- 19.10.2. Classification and Types of Reports
- 19.10.3. Guide to Writing a Report
- 19.10.4. Presentation of the Report
  - 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 Information 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 Crimes and Problems

20.3. *Deepfake*
- 20.3.1. Media Impact
- 20.3.2. Dangers to Society
- 20.3.3. Detection Mechanisms

20.4. The 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. Privacy and Digital Identity Management

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

20.7. Telework
- 20.7.1. Remote Work Revolution during and post COVID-19
- 20.7.2. Access Bottlenecks
- 20.7.3. Variation of the Attacking Surface
- 20.7.4. Workers' Needs

20.8. Emerging Wireless Technologies
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Millimeter Waves
- 20.8.4. Trend in Get Smart instead of Get More

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

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

04

Teaching Objectives

The main objective of the Advanced Master's Degree in Secure Information Management is to provide students with excellent knowledge in two fundamental and complementary areas of computer science and engineering: data management in digital environments and cybersecurity. This program combines both disciplines to train professionals in the implementation of advanced solutions, allowing them to face work challenges with the necessary tools to manage and protect sensitive information in their organizations.

Transform your career with this innovative Advanced Master's Degree, designed to mark a before and after in your specialization in data management and cybersecurity"

General Objectives

- Develop advanced knowledge in data analytics and cybersecurity to optimize business processes with innovative tools and technique
- Implement effective security strategies to prevent digital threats in systems, networks, and mobile devices
- Solve cybersecurity challenges through audits, reverse engineering and evidence-based forensic analysis
- Anticipate technology trends by applying disruptive solutions that protect digital assets and advanced systems

> *Lead data management and cybersecurity in the digital environment with this specialization program"*

Specific Objectives

Module 1. Data Analysis in a Business Organization

- Develop skills in the use of data analysis techniques
- Generate valuable information that drives strategic decision making in business organizations, improving efficiency and competitiveness

Module 2. Data and Information Management and Manipulation in Data Science

- Train in the efficient management and manipulation of large volumes of data
- Apply methodologies and tools to structure, clean and transform data into useful information for data science projects

Module 3. IoT Devices and Platforms as the Basis for Data Science

- Provide the necessary knowledge on Internet of Things platforms and devices and their integration into data science
- Delve into the capture, processing and analysis of real-time data

Module 4. Graphical Representation of Data Analysis

- Graphically represent data using advanced visualization tools and techniques
- Facilitate understanding of patterns, trends, and relationships within large data sets

Module 5. Data Science Tools

- Train in the use of specific data science tools and software, such as Python
- Delve into the collection, analysis and presentation of data in various professional contexts

Module 6. Data Mining. Selection, Pre-Processing and Transformation

- Provide the knowledge and skills necessary to apply data mining techniques
- Analyze the selection, preprocessing and transformation of data to extract meaningful patterns and trends

Module 7. Predictability and Analysis of Stochastic Phenomena

- Develop skills in the modeling and analysis of stochastic phenomena
- Use advanced statistical methods to predict behavior and trends in uncertain and dynamic environments

Module 8. Design and Development of Intelligent Systems

- Train in the design and development of intelligent systems, integrating machine learning and artificial intelligence techniques
- Create automatic solutions that solve complex problems efficiently

Module 9. Architecture and Systems for Intensive Use of Data

- Provide knowledge on the creation of system architectures capable of processing large volumes of data efficiently
- Use advanced technologies such as distributed databases and parallel processing

Module 10. Practical Application of Data Science in Business Sectors

- Develop the ability to apply data science practices in various business sectors
- Integrate the acquired knowledge to improve decision making, process optimization and innovation in the enterprise

Module 11. Cyberintelligence and Cybersecurity

- Provide the necessary knowledge and skills to apply cyberintelligence and cybersecurity techniques
- Protect enterprise systems and networks from cyber threats and ensure data integrity

Module 12. Host Security

- Train in the implementation of security measures in host systems
- Ensure the protection of servers and critical applications through the use of IT security tools and best practices

Module 13. Network Security (Perimeter)

- Provide knowledge on the protection of networks and computer systems at the perimeter level
- Manage firewalls, VPNs and other tools to ensure the security of the company's network infrastructure

Module 14. Smartphone Security

- Develop skills to ensure security on mobile devices
- Understand common vulnerabilities and applying preventative measures to protect information and applications on smartphones

Module 15. IoT Security

- Provide the necessary knowledge to implement security solutions in IoT devices
- Protect networks and systems interconnecting devices and ensuring the confidentiality and integrity of the data generated

Module 16. Ethical Hacking

- Train in ethical hacking practices, teaching how to perform controlled penetration tests
- Identify vulnerabilities in computer systems to improve security before they can be exploited by attackers

Module 17. Reverse Engineering

- Provide knowledge on reverse engineering techniques, allowing to analyze and understand the operation of software and hardware
- Detect security flaws or improve the functionality of existing systems

Module 18. Secure Development

- Train in secure software development, teaching good coding and security practices throughout the software lifecycle
- Be able to prevent vulnerabilities and protect computer systems against attacks

Module 19. Forensic Analysis

- Develop the skills necessary to conduct digital forensic investigations
- Utilize advanced tools and techniques to recover, analyze and preserve electronic evidence in computer security incidents

Module 20. Current and Future Challenges in Information Security

- Explore current and future challenges in the field of IT security, analyzing emerging threats and new protection technologies
- Delve into strategies to mitigate risks in an ever-changing technological environment

05

Career Opportunities

Upon completion of this Advanced Master's Degree in Secure Information Management, professionals will have acquired a solid understanding of the most advanced strategies in cybersecurity and digital data management. Graduates will be prepared to design and implement solutions that ensure the protection of sensitive information and optimize analysis and decision-making processes in business environments. In this way, they will improve their job prospects and take on specialized roles as cybersecurity analysts, intelligence consultants or critical data managers.

> *You will ensure the security of digital assets and be key to the digital transformation of organizations"*

Graduate Profile

Graduates of the Advanced Master's Degree in Secure Information Management will be a highly qualified professional to manage and protect information in digital environments. They will possess advanced knowledge in areas such as cybersecurity, digital intelligence and data analysis, as well as practical skills in the design and implementation of threat defense strategies. Their profile combines a deep technical understanding with strategic skills that will enable them to lead projects in key business sectors.

> *You will become a leader in data protection and cybersecurity, collaborating with companies to meet the challenges of the digital environment.*

- **Security Management:** Develop the ability to identify risks, implement multi-layered defense strategies and ensure confidentiality, integrity and availability of data
- **Critical Analysis and Problem Solving:** You will apply advanced techniques to assess systems, detect vulnerabilities and design solutions adapted to different technological environments
- **Technical and Digital Competency:** You will handle advanced tools for data analysis, cybersecurity and intelligence systems, enabling you to lead technological innovation projects
- **Strategic Thinking:** You will design security policies and business strategies that respond to the current and future demands of the digital environment
- **Interdisciplinary Collaboration:** You will work with multidisciplinary teams to address complex challenges and ensure security in networks, IoT platforms and mobile devices

After completing the Advanced Master's Degree, you will be able to apply your knowledge and skills in the following positions:

1. **Cybersecurity Director:** Leader in charge of coordinating teams and designing strategies to protect digital assets in large organizations
2. **Data Analyst:** Designer of predictive analytics and visualization systems to optimize decision making
3. **Digital Intelligence Consultant:** Advisor specialized in offering advanced solutions based on intelligence and risk analysis
4. **IoT and Security Specialist:** Designer of protection measures for connected devices and industrial environments
5. **Ethical Hacker:** Vulnerability assessor who fixes flaws in enterprise systems to prevent cyberattacks
6. **Security Auditor:** Inspector who performs audits and forensic analysis to ensure regulatory compliance
7. **Corporate Data Manager:** Administrator responsible for designing and managing storage and analytics systems to improve operational efficiency

> “*Complete this program and stand out as a specialist in the most demanded areas of the digital environment”*

06
Study Methodology

TECH is the world's first university to combine the **case study** methodology with **Relearning**, a 100% online learning system based on guided repetition.

This disruptive pedagogical strategy has been conceived to offer professionals the opportunity to update their knowledge and develop their skills in an intensive and rigorous way. A learning model that places students at the center of the educational process giving them the leading role, adapting to their needs and leaving aside more conventional methodologies.

TECH will prepare you to face new challenges in uncertain environments and achieve success in your career”

The student: the priority of all TECH programs

In TECH's study methodology, the student is the main protagonist.
The teaching tools of each program have been selected taking into account the demands of time, availability and academic rigor that, today, not only students demand but also the most competitive positions in the market.

With TECH's asynchronous educational model, it is students who choose the time they dedicate to study, how they decide to establish their routines, and all this from the comfort of the electronic device of their choice. The student will not have to participate in live classes, which in many cases they will not be able to attend. The learning activities will be done when it is convenient for them. They can always decide when and from where they want to study.

> *At TECH you will NOT have live classes (which you might not be able to attend)"*

The most comprehensive study plans at the international level

TECH is distinguished by offering the most complete academic itineraries on the university scene. This comprehensiveness is achieved through the creation of syllabi that not only cover the essential knowledge, but also the most recent innovations in each area.

By being constantly up to date, these programs allow students to keep up with market changes and acquire the skills most valued by employers. In this way, those who complete their studies at TECH receive a comprehensive education that provides them with a notable competitive advantage to further their careers.

And what's more, they will be able to do so from any device, pc, tablet or smartphone.

> *TECH's model is asynchronous, so it allows you to study with your pc, tablet or your smartphone wherever you want, whenever you want and for as long as you want”*

Case Studies and Case Method

The case method has been the learning system most used by the world's best business schools. Developed in 1912 so that law students would not only learn the law based on theoretical content, its function was also to present them with real complex situations. In this way, they could make informed decisions and value judgments about how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

With this teaching model, it is students themselves who build their professional competence through strategies such as Learning by Doing or Design Thinking, used by other renowned institutions such as Yale or Stanford.

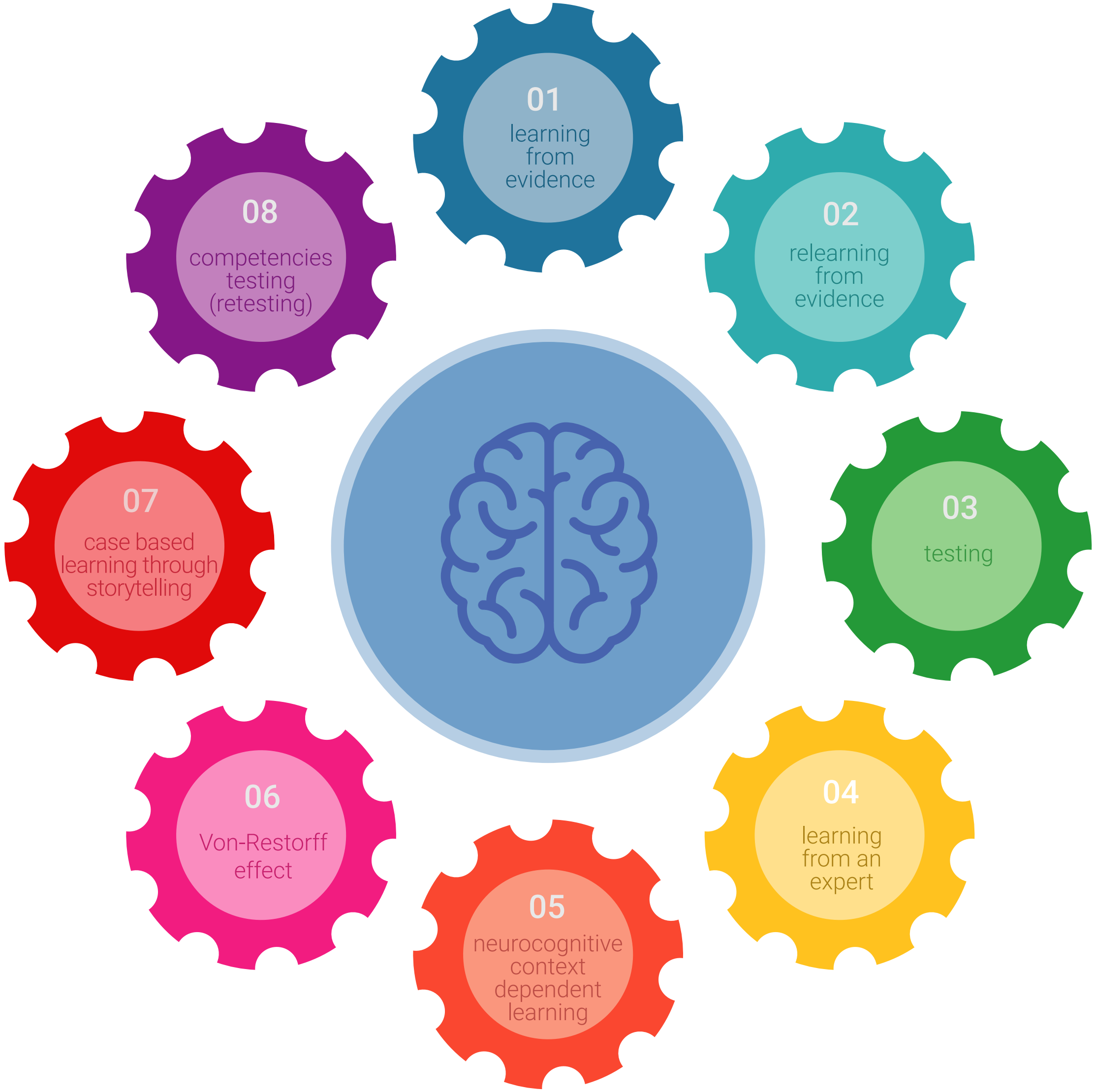
This action-oriented method will be applied throughout the entire academic itinerary that the student undertakes with TECH. Students will be confronted with multiple real-life situations and will have to integrate knowledge, research, discuss and defend their ideas and decisions. All this with the premise of answering the question of how they would act when facing specific events of complexity in their daily work.

Relearning Methodology

At TECH, case studies are enhanced with the best 100% online teaching method: Relearning.

This method breaks with traditional teaching techniques to put the student at the center of the equation, providing the best content in different formats. In this way, it manages to review and reiterate the key concepts of each subject and learn to apply them in a real context.

In the same line, and according to multiple scientific researches, reiteration is the best way to learn. For this reason, TECH offers between 8 and 16 repetitions of each key concept within the same lesson, presented in a different way, with the objective of ensuring that the knowledge is completely consolidated during the study process.


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)

Relearning will allow you to learn with less effort and better performance, involving you more in your specialization, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation to success.

A 100% online Virtual Campus with the best teaching resources

In order to apply its methodology effectively, TECH focuses on providing graduates with teaching materials in different formats: texts, interactive videos, illustrations and knowledge maps, among others. All of them are designed by qualified teachers who focus their work on combining real cases with the resolution of complex situations through simulation, the study of contexts applied to each professional career and learning based on repetition, through audios, presentations, animations, images, etc.

The latest scientific evidence in the field of Neuroscience points to the importance of taking into account the place and context where the content is accessed before starting a new learning process. Being able to adjust these variables in a personalized way helps people to remember and store knowledge in the hippocampus to retain it in the long term. This is a model called Neurocognitive context-dependent e-learning that is consciously applied in this university qualification.

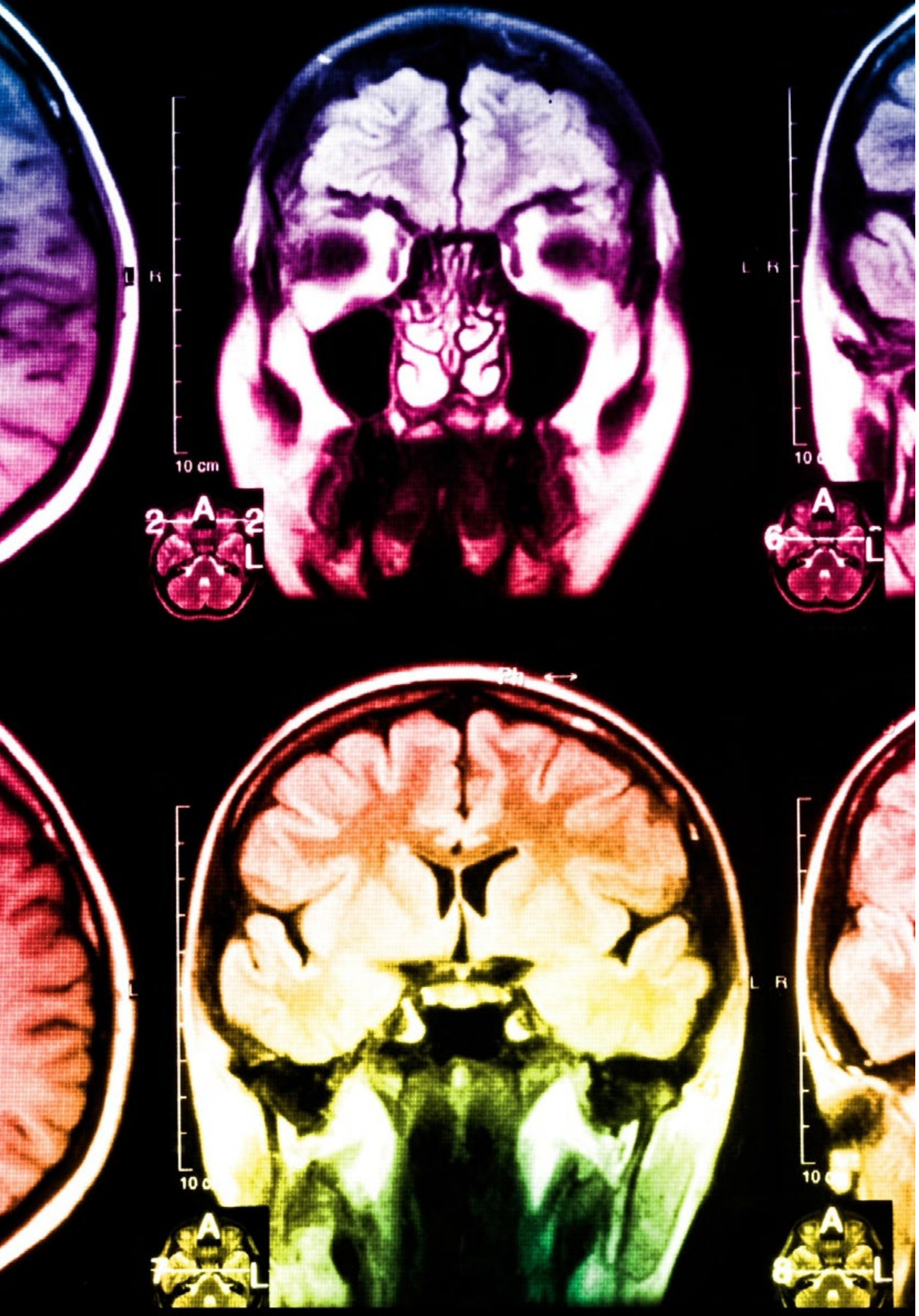
In order to facilitate tutor-student contact as much as possible, you will have a wide range of communication possibilities, both in real time and delayed (internal messaging, telephone answering service, email contact with the technical secretary, chat and videoconferences).

Likewise, this very complete Virtual Campus will allow TECH students to organize their study schedules according to their personal availability or work obligations. In this way, they will have global control of the academic content and teaching tools, based on their fast-paced professional update.

> “*The online study mode of this program will allow you to organize your time and learning pace, adapting it to your schedule”*

The effectiveness of the method is justified by four fundamental achievements:

1. Students who follow this method not only achieve the assimilation of concepts, but also a development of their mental capacity, through exercises that assess real situations and the application of knowledge.
2. Learning is solidly translated into practical skills that allow the student to better integrate into the real world.
3. Ideas and concepts are understood more efficiently, given that the example situations are based on real-life.
4. Students like to feel that the effort they put into their studies is worthwhile. This then translates into a greater interest in learning and more time dedicated to working on the course.



The university methodology top-rated by its students

The results of this innovative teaching model can be seen in the overall satisfaction levels of TECH graduates.

The students' assessment of the quality of teaching, quality of materials, course structure and objectives is excellent. Not surprisingly, the institution became the best rated university by its students on the Trustpilot review platform, obtaining a 4.9 out of 5.

Access the study contents from any device with an Internet connection (computer, tablet, smartphone) thanks to the fact that TECH is at the forefront of technology and teaching.

You will be able to learn with the advantages that come with having access to simulated learning environments and the learning by observation approach, that is, Learning from an expert.

As such, the best educational materials, thoroughly prepared, will be available in this program:

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.

This content is then adapted in an audiovisual format that will create our way of working online, with the latest techniques that allow us to offer you high quality in all of the material that we provide you with.

Practicing Skills and Abilities

You will carry out activities to develop specific competencies and skills in each thematic field. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop within the framework of the globalization we live in.

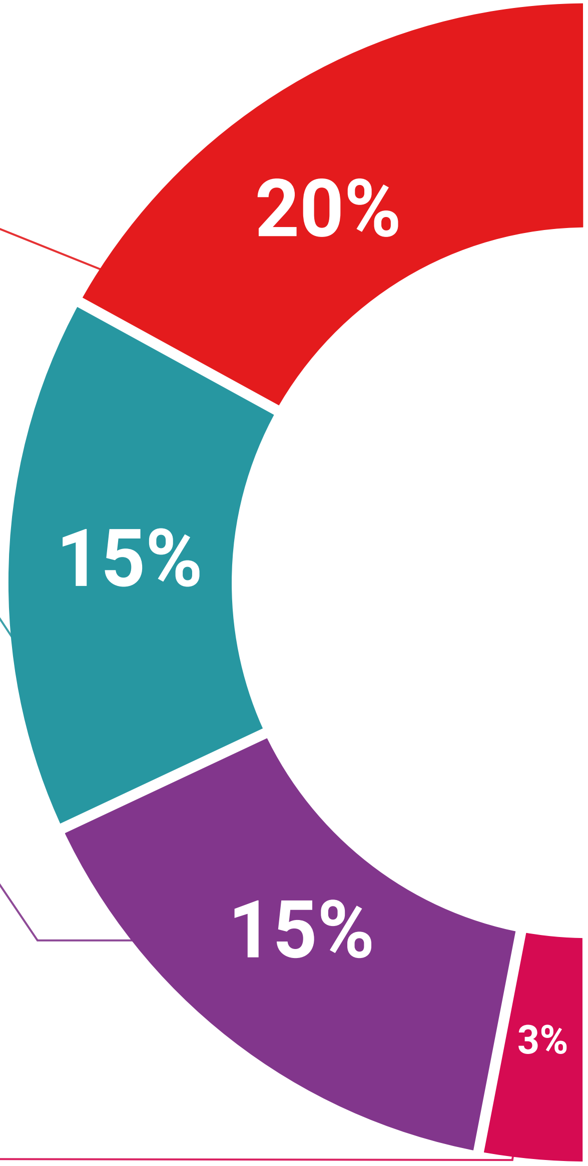
Interactive Summaries

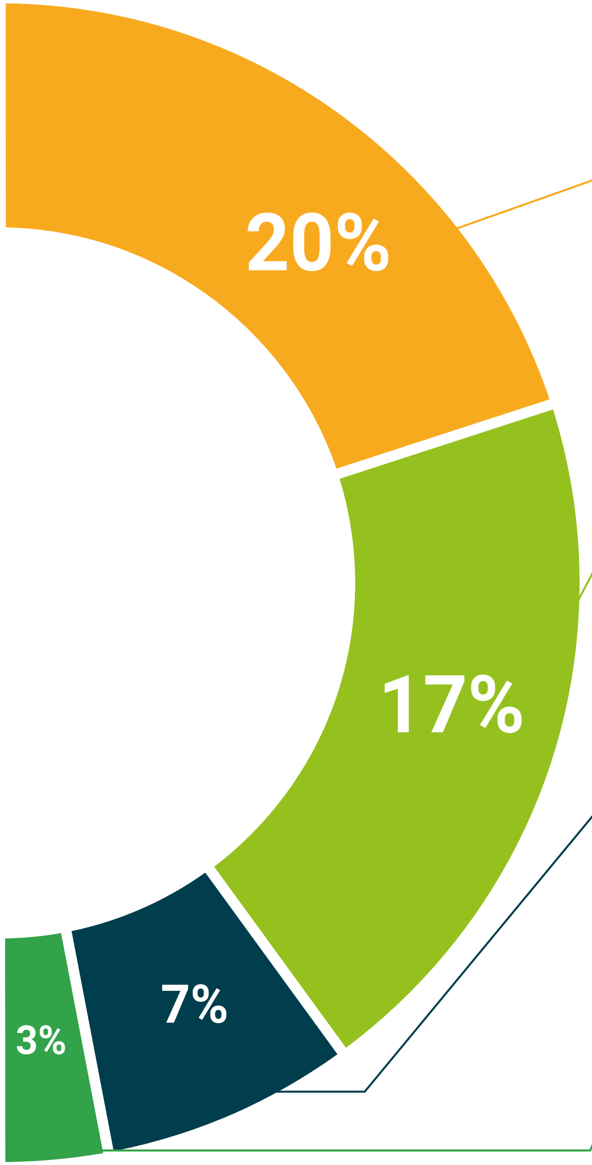
We present the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

This exclusive educational system for presenting multimedia content was awarded by Microsoft as a "European Success Story".

Additional Reading

Recent articles, consensus documents, international guides... In our virtual library you will have access to everything you need to complete your education.





Case Studies

Students will complete a selection of the best case studies in the field. Cases that are presented, analyzed, and supervised by the best specialists in the world.

Testing & Retesting

We periodically assess and re-assess your knowledge throughout the program. We do this on 3 of the 4 levels of Miller's Pyramid.

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 for future difficult decisions.

Quick Action Guides

TECH offers the most relevant contents of the course in the form of worksheets or quick action guides. A synthetic, practical and effective way to help students progress in their learning.

07

Teaching Staff

This program is taught by leading professionals in cybersecurity and digital data management. Their experience ensures that students receive complete and updated content, directly applicable to their careers. In this way, the teachers of this Advanced Master's Degree in Secure Information Management share their knowledge, training highly qualified specialists who are in demand by large international companies.

> *Succeed with the best and acquire the knowledge and key skills to lead in data management and cybersecurity in the digital environment”*

International Guest Director

Dr. Frederic Lemieux is internationally recognized as an innovative expert and inspirational leader in the fields of Intelligence, National 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 the understanding of today's emerging technologies. During his professional career, he has conceptualized and directed cutting-edge academic programs in 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 international security.** He has also made a significant contribution to the field of Cybersecurity with the publication of numerous articles in academic journals, examining crime control during major disasters, counter-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 various 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

- Director of the Master's Degree in Cybersecurity Risk Management at Georgetown, Washington, U.S.A.
- Director of the Master's Degree in Technology Management at Georgetown University
- Director of the Master's Degree in Applied Intelligence at Georgetown University
- Professor of Internships at Georgetown University
- PhD in Criminology from the School of Criminology at the University of Montreal
- B.A. in Sociology and Minor Degree in Psychology from Laval University
- Member of: New Program Roundtable Committee, 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 at Korporate Technologies
- CTO at AI Shepherds GmbH
- Consultant and Strategic Business Advisor at Alliance Medical
- Director of Design and Development at DocPath
- PhD in Psychology from the University of Castilla La Mancha
- PhD in Economics, Business and Finance from the Camilo José Cela University
- PhD in Psychology from University of Castilla La Mancha
- Master's Degree in Executive MBA from the Isabel I University
- Master's Degree in Sales and Marketing Management, Isabel I University
- Expert Master's Degree in Big Data by Hadoop Training
- Master's Degree in Advanced Information Technologies from the University of Castilla La Mancha
- Member of the research group SMILE

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
- Computer Engineer by the University of Alcalá de Henares, Madrid
- Master's Degree in DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Professors

Dr. Montoro Montarroso, Andrés

- Researcher in the SMILe Group at the University of Castilla-La Mancha.
- Researcher at the University of Granada
- Data Scientist at Prometeus Global Solutions
- Vice President and Software Developer at CireBits
- PhD in Advanced Information Technologies from the University of Castilla La Mancha
- Degree in Computer Engineering from the University of Castilla-La Mancha
- Master's Degree in Data Science and Computer Engineering from the University of Granada
- Guest lecturer in the subject of Knowledge-Based Systems at the Escuela Superior de Informática de Ciudad Real, Giving the Lecture: *Advanced Artificial Intelligence Techniques: Search and Analysis of Potential Social Media Radicals*
- Guest lecturer in the subject of Data Mining at the Escuela Superior de Informática de Ciudad Real , giving the lecture: *Applications of Natural Language Processing: Fuzzy logic to the analysis of messages in social networks*
- Speaker at the Seminar on Prevention of Corruption in Public Administrations and Artificial Intelligence at the Faculty of Law and Social Sciences of Toledo, giving the lecture: *Artificial Intelligence Techniques*
- Speaker at the first International Seminar on Administrative Law and Artificial Intelligence (DAIA). Organized by the Luis Ortega Álvarez Centre for European Studies and the TransJus Research Institute. Conference entitled *"Sentiment Analysis for the prevention of hate speech on social media*

Mr. Peris Morillo, Luis Javier

- Senior Technical Lead and Delivery Lead Support at HCL Technologies
- Technical Editor at Baeldung
- Agile Coach and Operations Manager at Mirai Advisory
- Developer, Team Lead, Scrum Master, Agile Coach and Product Manager at DocPath
- Technologist at ARCO
- Degree in Computer Science Engineering from the University of Castilla-La Mancha
- Master's Degree in Project Management from CEOE

Ms. Fernández Meléndez, Galina

- Specialist's Degree in Big Data
- Data Analyst at Aresi Gestión de Fincas
- Data Analyst in ADN Mobile Solution
- Bachelor's Degree in Business Administration at Universidad Bicentenaria Aragua. Caracas, Venezuela
- Diploma in Planning and Public Finance from the Venezuelan School of Planning
- Master's Degree in Data Analysis and Business Intelligence from the University of Oviedo
- MBA in Business Administration and Management by the European Business School of Barcelona
- Master's Degree in Big Data and Business Intelligence from the European Business School of Barcelona

Ms. Pedrajas Parabá, María Elena

- New Technologies and Digital Transformation Consultant en Management Solutions
- 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 from the University of Cordoba
- Master's Degree in Data Science and Computer Engineering from the University of Granada
- Master's Degree in Business Consulting at the Pontificia Comillas University

Ms. Martínez Cerrato, Yésica

- Responsible for Technical Training at Securitas Seguridad España
- Education, Business and Marketing Specialist
- Product Manager in Electronic Security at Securitas Seguridad España
- Business Intelligence Analyst at Ricopia Technologies
- Computer Technician and Responsible for OTEC computer classrooms at the University of Alcalá de Henares
- Collaborator in the ASALUMA Association
- Degree in Electronic Communications Engineering at the Polytechnic School, University of Alcalá de Henares

Mr. Fondón Alcalde, Rubén

- Analyst EMEA at Amazon Web Services
- Business Analyst in Customer Value Management at Vodafone Spain
- Head of Service Integration at Entelgy for Telefónica Global Solutions
- Online Account Manager for Clone Servers at EDM Electronics
- International Services Implementation Manager at Vodafone Global Enterprise
- Solutions Consultant for Spain and Portugal at Telvent Global Services
- Business Analyst for Southern Europe at Vodafone Global Enterprise
- Telecommunications Engineer from the European University of Madrid
- Master's Degree in Big Data and Data Science from the International University of Valencia.

Mr. Díaz Díaz-Chirón, Tobías

- Researcher in the ArCO laboratory of the University of Castilla-La Mancha
- Consultant at Blue Telecom
- Freelance mainly dedicated to the telecommunications sector, specialising in 4G/5G networks.
- OpenStack: deploy and administration
- Computer Engineer from the University of Castilla - la Mancha
- Specialization in Architecture and computer network
- Associate Professor at the University of Castilla-La Mancha
- Speaker at Sepecam course on network administration

Mr. Tato Sánchez, Rafael

- Technical Director at Indra Sistemas SA
- Systems Engineer in ENA TRÁFICO SAU
- Master's Degree in Industry 4.0. by the Online University
- Master's Degree in Industrial Engineering from the European University
- Industrial Electronics and Automation Engineering Degree from the European University
- Industrial Technical Engineer by the Polytechnic University of Madrid

Ms. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applications Developer at B60. UK.
- Analyst Programmer for the Management, Coordination and Documentation of the Virtualized Environment of Security Alarms
- Analyst Programmer of Java Applications for Automatic Teller Machines (ATM)
- Software Development Professional for Signature Validation and Document Management Application
- Systems Technician for Equipment Migration and for Management, Maintenance and Training of PDA Mobile Devices
- Technical Engineer in Computer Systems from the Open University of Catalonia (UOC)
- Master's Degree in Computer Security and Ethical Hacking Official EC- Council and CompTIA from the Professional School of New Technologies CICE

Mr. Catalá Barba, José Francisco

- Electronic Technician Expert in Cybersecurity
- Developer of Applications for Mobile Devices
- Electronic Technician in Intermediate Command at the Ministry of Defense of Spain
- Electronics Technician at Ford Factory in Valencia

Mr. Armero Fernández, Rafael

- Business Intelligence Consultant en SDG Group
- Digital Engineer at MI-GSO
- Logistic Engineer at Torrecid SA
- Quality Intern at INDRA
- Degree in Aerospace Engineering from the Polytechnic University of Valencia
- Master's Degree in Professional Development 4.0 from the University of Alcalá

Mr. Peralta Alonso, Jon

- Senior Data Protection and Cybersecurity Consultant at Altia
- Lawyer/Legal Advisor at Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Legal Advisor/Intern at a professional law firm: Óscar Padura
- Law Degree from the Public University of the Basque Country
- Master's Degree in Data Protection Delegate by EIS Innovative School
- Master's Degree in Law from the Public University of the Basque Country
- Specialist Master's Degree in Civil Litigation Practice from the International University Isabel I of Castilla
- Professor in Master's Degree in Personal Data Protection, Cybersecurity and ICT Law

Mr. Redondo, Jesús Serrano

- Web Developer and Cybersecurity Technician
- Web Developer at Roams, Palencia
- FrontEnd Developer at Telefónica, Madrid
- FrontEnd Developer at Best Pro Consulting SL, Madrid
- Telecommunications Equipment and Services Installer at Grupo Zener, Castilla y León
- Telecommunications Equipment and Services Installer at Lican Comunicaciones SL, Castilla y León
- Certificate in Computer Security by CFTIC Getafe, Madrid
- Senior Technician in Telecommunications and Computer Systems at IES Trinidad Arroyo, Palencia
- Higher Technician in MV and LV Electrotechnical Installations by IES Trinidad Arroyo, Palencia
- Training in Reverse Engineering, Stenography and Encryption by Academia Hacker Incibe

Mr. Jiménez Ramos, Álvaro

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

> *Take the opportunity to learn about the latest advances in this field in order to apply it to your daily practice”*

08

Certificate

The Advanced Master's Degree in Secure Information Management guarantees students, in addition to the most rigorous and up-to-date education, access to an Advanced Master's Degree diploma issued by TECH Global University.

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

This private qualification will allow you to obtain a **Advanced Master's Degree in Secure Information Management** endorsed by **TECH Global University**, the world's largest online university.

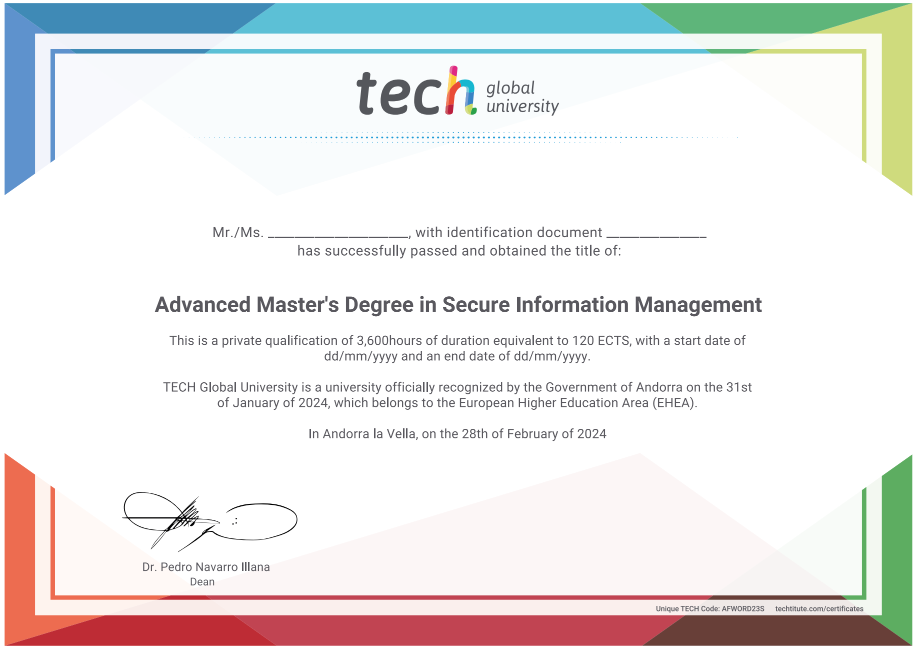
This **TECH Global University** private qualification is a European program of continuing education and professional updating that guarantees the acquisition of competencies in its area of knowledge, providing a high curricular value to the student who completes the program.

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

Modality: **online**

Duration: **2 years**

Accreditation: **120 ECTS**



tech global university

Mr./Ms. __________________, with identification document _____________
has successfully passed and obtained the title of:

Advanced Master's Degree in Secure Information Management

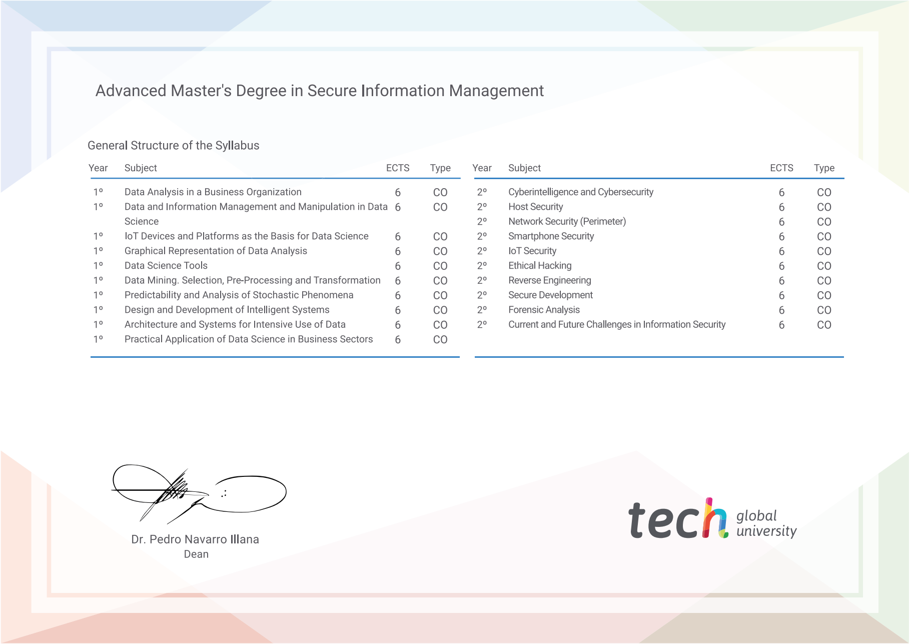
This is a private qualification of 3,600hours of duration equivalent to 120 ECTS, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH Global University is a university officially recognized by the Government of Andorra on the 31st of January of 2024, which belongs to the European Higher Education Area (EHEA).

In Andorra la Vella, on the 28th of February of 2024

Dr. Pedro Navarro Illana
Dean

Unique TECH Code: AFWORD23S techtitute.com/certificates



Advanced Master's Degree in Secure Information Management

General Structure of the Syllabus

Year	Subject	ECTS	Type
1º	Data Analysis in a Business Organization	6	CO
1º	Data and Information Management and Manipulation in Data Science	6	CO
1º	IoT Devices and Platforms as the Basis for Data Science	6	CO
1º	Graphical Representation of Data Analysis	6	CO
1º	Data Science Tools	6	CO
1º	Data Mining. Selection, Pre-Processing and Transformation	6	CO
1º	Predictability and Analysis of Stochastic Phenomena	6	CO
1º	Design and Development of Intelligent Systems	6	CO
1º	Architecture and Systems for Intensive Use of Data	6	CO
1º	Practical Application of Data Science in Business Sectors	6	CO

Year	Subject	ECTS	Type
2º	Cyberintelligence and Cybersecurity	6	CO
2º	Host Security	6	CO
2º	Network Security (Perimeter)	6	CO
2º	Smartphone Security	6	CO
2º	IoT Security	6	CO
2º	Ethical Hacking	6	CO
2º	Reverse Engineering	6	CO
2º	Secure Development	6	CO
2º	Forensic Analysis	6	CO
2º	Current and Future Challenges in Information Security	6	CO

Dr. Pedro Navarro Illana
Dean

tech global university

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

tech global university

Advanced Master's Degree
Secure Information Management

- Modality: **online**
- Duration: **2 years**
- Certificate: **TECH Global University**
- Accreditation: **120 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

Advanced Master's Degree
Secure Information Management

Content Overview

Pages	Pageviews	% Pageviews
/	5,932	23.33%
/information-resources	1,306	5.14%
/decisions	867	3.41%
/information-privacy	697	2.74%
/information-privacy-guidelines	692	2.72%

tech global university