Professional Master's Degree

Artificial Intelligence in Cybersecurity

tech global university

tech global university

Professional Master's Degree
Artificial Intelligence in Cybersecurity

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Global University**
- Accreditation: **90 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/us/information-technology/professional-master-degree/master-artificial-intelligence-cybersecurity

Index

01

Introduction

Artificial Intelligence applied to Cybersecurity is a sector in full expansion due to the increase in digital threats and the need for proactive and effective responses. In this field, intelligent systems not only allow automating repetitive processes, but also analyze large volumes of data to identify anomalous patterns, anticipate attacks and strengthen protection systems. For this reason, TECH has developed a comprehensive university program that prepares computer scientists to face the current challenges in Cybersecurity, offering them the necessary tools to anticipate future threats, leading technological initiatives and ensuring the protection of critical infrastructures at a global level. All this, through a 100% online academic itinerary taught by the best experts in the sector.

With this innovative 100% online university program, you will master the most advanced techniques of modern cryptography, and design robust protection systems to ensure the privacy and authenticity of data"

Artificial Intelligence and Cybersecurity are two fundamental pillars in the digital era. While the former focuses on the development of systems capable of simulating human cognitive processes, Cybersecurity is responsible for protecting computer systems and data from malicious attacks. The combination of both disciplines makes it possible to create advanced solutions that not only detect and mitigate threats in real time, but also anticipate potential vulnerabilities, thus ensuring a safer digital environment. This context drives the need for highly qualified professionals who master both the fundamentals of Artificial Intelligence and its specific applications in cyber defense.

From these demands arises the Professional Master's Degree in Artificial Intelligence in Cybersecurity of TECH, a program structured in 20 comprehensive modules that address from the fundamentals of Artificial Intelligence and data management to deep learning, convolutional neural networks and the application of generative models in Cybersecurity. It also delves into threat detection, digital forensics and modern cryptography, using tools such as TensorFlow and advanced Artificial Intelligence models to meet the challenges of a constantly evolving digital environment. Therefore, this academic path enables computer scientists to anticipate emerging threats and lead security strategies in complex environments.

Regarding the methodology of this university program, TECH offers a 100% online environment that allows professionals to individually plan their schedules and pace of study. In addition, it uses its disruptive Relearning system, which facilitates the progressive assimilation of key concepts through contextualized reiteration and active learning. Along the same lines, graduates will only need an electronic device with an Internet connection to access the Virtual Campus. There they will be able to access a vast library of multimedia resources, such as interactive summaries, explanatory videos or specialized readings based on the latest evidence.

This **Professional Master's Degree in Artificial Intelligence in Cybersecurity** contains the most complete and up-to-date program on the market. The most important features include:

- The development of case studies presented by experts in Artificial Intelligence, Cybersecurity and advanced technologies
- The graphic, schematic and eminently practical contents with which it is conceived gather scientific and practical information on those disciplines that are indispensable for professional practice
- Practical exercises where the self-assessment process can be carried out to improve learning
- Its special emphasis on innovative methodologies
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- Content that is accessible from any fixed or portable device with an Internet connection

You will delve into how Artificial Intelligence transforms Cybersecurity with tools such as Neural Networks and generative models applied to threat detection and prevention"

You will optimize your strategic decision making through predictive analytics and the use of advanced models in cyber attack management"

You will have at your disposal the most cutting-edge multimedia resources, from interactive overviews to explanatory videos and specialized readings.

You'll lead projects in key sectors, such as infrastructure protection and management of connected Internet of Things systems.

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

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

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

02

Syllabus

The syllabus of this Professional Master's Degree addresses both the fundamentals of Artificial Intelligence and its specific applications in the field of Cybersecurity. Throughout this academic course, computer scientists will delve into key topics such as algorithms, data mining and natural language processing. They will also delve into advanced neural networks and intelligent systems applied to forensic analysis, as well as intrusion detection and proactive defense, which will allow them to acquire the necessary tools to develop innovative solutions to digital threats.

With the Relearning methodology, of which TECH is a pioneer, you will specialize in the use of Bio-inspired Systems and Deep Learning to address complex problems in digital protection"

Module 1. Fundamentals of Artificial Intelligence

1.1. History of Artificial Intelligence
- 1.1.1. When Do We Start Talking About Artificial Intelligence?
- 1.1.2. References in Film
- 1.1.3. Importance of Artificial Intelligence
- 1.1.4. Technologies that Enable and Support Artificial Intelligence

1.2. Artificial Intelligence in Games
- 1.2.1. Game Theory
- 1.2.2. Minimax and Alpha-Beta Pruning
- 1.2.3. Simulation: Monte Carlo

1.3. Neural Networks
- 1.3.1. Biological Fundamentals
- 1.3.2. Computational Model
- 1.3.3. Supervised and Unsupervised Neural Networks
- 1.3.4. Simple Perceptron
- 1.3.5. Multilayer Perceptron

1.4. Genetic Algorithms
- 1.4.1. History
- 1.4.2. Biological Basis
- 1.4.3. Problem Coding
- 1.4.4. Generation of the Initial Population
- 1.4.5. Main Algorithm and Genetic Operators
- 1.4.6. Evaluation of Individuals: Fitness

1.5. Thesauri, Vocabularies, Taxonomies
- 1.5.1. Vocabulary
- 1.5.2. Taxonomy
- 1.5.3. Thesauri
- 1.5.4. Ontologies
- 1.5.5. Knowledge Representation: Semantic Web

1.6. Semantic Web
- 1.6.1. Specifications: RDF, RDFS and OWL
- 1.6.2. Inference/ Reasoning
- 1.6.3. *Linked Data*

1.7. Expert Systems and DSS
- 1.7.1. Expert Systems
- 1.7.2. Decision Support Systems

1.8. Chatbots and Virtual Assistants
- 1.8.1. Types of Assistants: Voice and Text Assistants
- 1.8.2. Fundamental Parts for the Development of an Assistant: Intents, Entities and Dialog Flow
- 1.8.3. Integrations: Web, Slack, Whatsapp, Facebook
- 1.8.4. Assistant Development Tools: *Dialog Flow, Watson Assistant*

1.9. AI Implementation Strategy

1.10. Future of Artificial Intelligence
- 1.10.1. Understand How to Detect Emotions Using Algorithms
- 1.10.2. Creating a Personality: Language, Expressions and Content
- 1.10.3. Trends of Artificial Intelligence
- 1.10.4. Reflections

Module 2. Data Types and Life Cycle

2.1. Statistics
- 2.1.1. Statistics: Descriptive Statistics, Statistical Inferences
- 2.1.2. Population, Sample, Individual
- 2.1.3. Variables: Definition, Measurement Scales

2.2. Types of Data Statistics
- 2.2.1. According to Type
  - 2.2.1.1. Quantitative: Continuous Data and Discrete Data
  - 2.2.1.2. Qualitative: Binomial Data, Nominal Data and Ordinal Data
- 2.2.2. According to Its Shape
  - 2.2.2.1. Numeric
  - 2.2.2.2. Text
  - 2.2.2.3. Logical
- 2.2.3. According to Its Source
  - 2.2.3.1. Primary
  - 2.2.3.2. Secondary

2.3. Life Cycle of Data
- 2.3.1. Stages of the Cycle
- 2.3.2. Milestones of the Cycle
- 2.3.3. FAIR Principles

2.4. Initial Stages of the Cycle
- 2.4.1. Definition of Goals
- 2.4.2. Determination of Resource Requirements
- 2.4.3. Gantt Chart
- 2.4.4. Data Structure

2.5. Data Collection
- 2.5.1. Methodology of Data Collection
- 2.5.2. Data Collection Tools
- 2.5.3. Data Collection Channels

2.6. Data Cleaning
- 2.6.1. Phases of Data Cleansing
- 2.6.2. Data Quality
- 2.6.3. Data Manipulation (with R)

2.7. Data Analysis, Interpretation and Evaluation of Results
- 2.7.1. Statistical Measures
- 2.7.2. Relationship Indexes
- 2.7.3. Data Mining

2.8. Datawarehouse
- 2.8.1. Elements that Comprise It
- 2.8.2. Design
- 2.8.3. Aspects to Consider

2.9. Data Availability
- 2.9.1. Access
- 2.9.2. Uses
- 2.9.3. Security

2.10. Regulatory Framework
- 2.10.1. Data Protection Law
- 2.10.2. Good Practices
- 2.10.3. Other Regulatory Aspects

Module 3. Data in Artificial Intelligence

3.1. Data Science
- 3.1.1. Data Science
- 3.1.2. Advanced Tools for Data Scientists

3.2. Data, Information and Knowledge
- 3.2.1. Data, Information and Knowledge
- 3.2.2. Types of Data
- 3.2.3. Data Sources

3.3. From Data to Information
- 3.3.1. Data Analysis
- 3.3.2. Types of Analysis
- 3.3.3. Extraction of Information from a Dataset

3.4. Extraction of Information Through Visualization
- 3.4.1. Visualization as an Analysis Tool
- 3.4.2. Visualization Methods
- 3.4.3. Visualization of a Data Set

3.5. Data Quality
- 3.5.1. Quality Data
- 3.5.2. Data Cleaning
- 3.5.3. Basic Data Pre-Processing

3.6. *Dataset*
- 3.6.1. Dataset Enrichment
- 3.6.2. The Curse of Dimensionality
- 3.6.3. Modification of Our Data Set

3.7. Unbalance
- 3.7.1. Classes of Unbalance
- 3.7.2. Unbalance Mitigation Techniques
- 3.7.3. Balancing a Dataset

3.8. Unsupervised Models
- 3.8.1. Unsupervised Model
- 3.8.2. Methods
- 3.8.3. Classification with Unsupervised Models

3.9. Supervised Models
- 3.9.1. Supervised Model
- 3.9.2. Methods
- 3.9.3. Classification with Supervised Models

3.10. Tools and Good Practices
- 3.10.1. Good Practices for Data Scientists
- 3.10.2. The Best Model
- 3.10.3. Useful Tools

Module 4. Data Mining: Selection, Pre-Processing and Transformation

4.1. Statistical Inference
- 4.1.1. Descriptive Statistics vs. Statistical Inference
- 4.1.2. Parametric Procedures
- 4.1.3. Non-Parametric Procedures

4.2. Exploratory Analysis
- 4.2.1. Descriptive Analysis
- 4.2.2. Visualization
- 4.2.3. Data Preparation

4.3. Data Preparation
- 4.3.1. Integration and Data Cleaning
- 4.3.2. Normalization of Data
- 4.3.3. Transforming Attributes

4.4. Missing Values
- 4.4.1. Treatment of Missing Values
- 4.4.2. Maximum Likelihood Imputation Methods
- 4.4.3. Missing Value Imputation Using Machine Learning

4.5. Noise in the Data
- 4.5.1. Noise Classes and Attributes
- 4.5.2. Noise Filtering
- 4.5.3. The Effect of Noise

4.6. The Curse of Dimensionality
- 4.6.1. Oversampling
- 4.6.2. Undersampling
- 4.6.3. Multidimensional Data Reduction

4.7. From Continuous to Discrete Attributes
- 4.7.1. Continuous Data vs. Discreet Data
- 4.7.2. Discretization Process

4.8. The Data
- 4.8.1. Data Selection
- 4.8.2. Prospects and Selection Criteria
- 4.8.3. Selection Methods

4.9. Instance Selection
- 4.9.1. Methods for Instance Selection
- 4.9.2. Prototype Selection
- 4.9.3. Advanced Methods for Instance Selection

4.10. Data Pre-Processing in Big Data Environments

Module 5. Algorithm and Complexity in Artificial Intelligence

5.1. Introduction to Algorithm Design Strategies
- 5.1.1. Recursion
- 5.1.2. Divide and Conquer
- 5.1.3. Other Strategies

5.2. Efficiency and Analysis of Algorithms
- 5.2.1. Efficiency Measures
- 5.2.2. Measuring the Size of the Input
- 5.2.3. Measuring Execution Time
- 5.2.4. Worst, Best and Average Case
- 5.2.5. Asymptotic Notation
- 5.2.6. Mathematical Analysis Criteria for Non-Recursive Algorithms
- 5.2.7. Mathematical Analysis of Recursive Algorithms
- 5.2.8. Empirical Analysis of Algorithms

5.3. Sorting Algorithms
- 5.3.1. Concept of Sorting
- 5.3.2. Bubble Sorting
- 5.3.3. Sorting by Selection
- 5.3.4. Sorting by Insertion
- 5.3.5. Sorting by Merge (Merge_Sort)
- 5.3.6. Sorting Quickly (Quick_Sort)

5.4. Algorithms with Trees
- 5.4.1. Tree Concept
- 5.4.2. Binary Trees
- 5.4.3. Tree Paths
- 5.4.4. Representing Expressions
- 5.4.5. Ordered Binary Trees
- 5.4.6. Balanced Binary Trees

5.5. Algorithms Using Heaps
- 5.5.1. Heaps
- 5.5.2. The Heapsort Algorithm
- 5.5.3. Priority Queues

5.6. Graph Algorithms
- 5.6.1. Representation
- 5.6.2. Traversal in Width
- 5.6.3. Depth Travel
- 5.6.4. Topological Sorting

5.7. Greedy Algorithms
- 5.7.1. Greedy Strategy
- 5.7.2. Elements of the Greedy Strategy
- 5.7.3. Currency Exchange
- 5.7.4. Traveler's Problem
- 5.7.5. Backpack Problem

5.8. Minimal Path Finding
- 5.8.1. The Minimum Path Problem
- 5.8.2. Negative Arcs and Cycles
- 5.8.3. Dijkstra's Algorithm

5.9. Greedy Algorithms on Graphs
- 5.9.1. The Minimum Covering Tree
- 5.9.2. Prim's Algorithm
- 5.9.3. Kruskal's Algorithm
- 5.9.4. Complexity Analysis

5.10. Backtracking
- 5.10.1. Backtracking
- 5.10.2. Alternative Techniques

Module 6. Intelligent Systems

6.1. Agent Theory
- 6.1.1. Concept History
- 6.1.2. Agent Definition
- 6.1.3. Agents in Artificial Intelligence
- 6.1.4. Agents in Software Engineering

6.2. Agent Architectures
- 6.2.1. The Reasoning Process of an Agent
- 6.2.2. Reactive Agents
- 6.2.3. Deductive Agents
- 6.2.4. Hybrid Agents
- 6.2.5. Comparison

6.3. Information and Knowledge
- 6.3.1. Difference between Data, Information and Knowledge
- 6.3.2. Data Quality Assessment
- 6.3.3. Data Collection Methods
- 6.3.4. Information Acquisition Methods
- 6.3.5. Knowledge Acquisition Methods

6.4. Knowledge Representation
- 6.4.1. The Importance of Knowledge Representation
- 6.4.2. Definition of Knowledge Representation According to Roles
- 6.4.3. Knowledge Representation Features

6.5. Ontologies
- 6.5.1. Introduction to Metadata
- 6.5.2. Philosophical Concept of Ontology
- 6.5.3. Computing Concept of Ontology
- 6.5.4. Domain Ontologies and Higher-Level Ontologies
- 6.5.5. How to Build an Ontology

6.6. Ontology Languages and Ontology Creation Software
- 6.6.1. Triple RDF, Turtle and N
- 6.6.2. RDF Schema
- 6.6.3. OWL
- 6.6.4. SPARQL
- 6.6.5. Introduction to Ontology Creation Tools
- 6.6.6. Installing and Using Protégé

6.7. Semantic Web
- 6.7.1. Current and Future Status of the Semantic Web
- 6.7.2. Semantic Web Applications

6.8. Other Knowledge Representation Models
- 6.8.1. Vocabulary
- 6.8.2. Global Vision
- 6.8.3. Taxonomy
- 6.8.4. Thesauri
- 6.8.5. Folksonomy
- 6.8.6. Comparison
- 6.8.7. Mind Maps

6.9. Knowledge Representation Assessment and Integration
- 6.9.1. Zero-Order Logic
- 6.9.2. First-Order Logic
- 6.9.3. Descriptive Logic
- 6.9.4. Relationship between Different Types of Logic
- 6.9.5. Prolog: Programming Based on First-Order Logic

6.10. Semantic Reasoners, Knowledge-Based Systems and Expert Systems
- 6.10.1. Concept of Reasoner
- 6.10.2. Reasoner Applications
- 6.10.3. Knowledge-Based Systems
- 6.10.4. MYCIN: History of Expert Systems
- 6.10.5. Expert Systems Elements and Architecture
- 6.10.6. Creating Expert Systems

Module 7. Machine Learning and Data Mining

7.1. Introduction to Knowledge Discovery Processes and Basic Concepts of Machine Learning
- 7.1.1. Key Concepts of Knowledge Discovery Processes
- 7.1.2. Historical Perspective of Knowledge Discovery Processes
- 7.1.3. Stages of the Knowledge Discovery Processes
- 7.1.4. Techniques Used in Knowledge Discovery Processes
- 7.1.5. Characteristics of Good Machine Learning Models
- 7.1.6. Types of Machine Learning Information
- 7.1.7. Basic Learning Concepts
- 7.1.8. Basic Concepts of Unsupervised Learning

7.2. Data Exploration and Pre-Processing
- 7.2.1. Data Processing
- 7.2.2. Data Processing in the Data Analysis Flow
- 7.2.3. Types of Data
- 7.2.4. Data Transformations
- 7.2.5. Visualization and Exploration of Continuous Variables
- 7.2.6. Visualization and Exploration of Categorical Variables
- 7.2.7. Correlation Measures
- 7.2.8. Most Common Graphic Representations
- 7.2.9. Introduction to Multivariate Analysis and Dimensionality Reduction

7.3. Decision Trees
- 7.3.1. ID Algorithm
- 7.3.2. Algorithm C
- 7.3.3. Overtraining and Pruning
- 7.3.4. Result Analysis

7.4. Evaluation of Classifiers
- 7.4.1. Confusion Matrices
- 7.4.2. Numerical Evaluation Matrices
- 7.4.3. Kappa Statistic
- 7.4.4. ROC Curves

7.5. Classification Rules
- 7.5.1. Rule Evaluation Measures
- 7.5.2. Introduction to Graphic Representation
- 7.5.3. Sequential Overlay Algorithm

7.6. Neural Networks
- 7.6.1. Basic Concepts
- 7.6.2. Simple Neural Networks
- 7.6.3. Backpropagation Algorithm
- 7.6.4. Introduction to Recurrent Neural Networks

7.7. Bayesian Methods
- 7.7.1. Basic Probability Concepts
- 7.7.2. Bayes' Theorem
- 7.7.3. Naive Bayes
- 7.7.4. Introduction to Bayesian Networks

7.8. Regression and Continuous Response Models
- 7.8.1. Simple Linear Regression
- 7.8.2. Multiple Linear Regression
- 7.8.3. Logistic Regression
- 7.8.4. Regression Trees
- 7.8.5. Introduction to Support Vector Machines (SVM)
- 7.8.6. Goodness-of-Fit Measures

7.9. *Clustering*
- 7.9.1. Basic Concepts
- 7.9.2. Hierarchical Clustering
- 7.9.3. Probabilistic Methods
- 7.9.4. EM Algorithm
- 7.9.5. B-Cubed Method
- 7.9.6. Implicit Methods

7.10. Text Mining and Natural Language Processing (NLP)
- 7.10.1. Basic Concepts
- 7.10.2. Corpus Creation
- 7.10.3. Descriptive Analysis
- 7.10.4. Introduction to Feelings Analysis

Module 8. Neural Networks, the Basis of Deep Learning

8.1. Deep Learning
- 8.1.1. Types of Deep Learning
- 8.1.2. Applications of Deep Learning
- 8.1.3. Advantages and Disadvantages of Deep Learning

8.2. Operations
- 8.2.1. Sum
- 8.2.2. Product
- 8.2.3. Transfer

8.3. Layers
- 8.3.1. Input Layer
- 8.3.2. Hidden Layer
- 8.3.3. Output Layer

8.4. Union of Layers and Operations
- 8.4.1. Architecture Design
- 8.4.2. Connection between Layers
- 8.4.3. Forward Propagation

8.5. Construction of the First Neural Network
- 8.5.1. Network Design
- 8.5.2. Establish the Weights
- 8.5.3. Network Training

8.6. Trainer and Optimizer
- 8.6.1. Optimizer Selection
- 8.6.2. Establishment of a Loss Function
- 8.6.3. Establishing a Metric

8.7. Application of the Principles of Neural Networks
- 8.7.1. Activation Functions
- 8.7.2. Backward Propagation
- 8.7.3. Parameter Adjustment

8.8. From Biological to Artificial Neurons
- 8.8.1. Functioning of a Biological Neuron
- 8.8.2. Transfer of Knowledge to Artificial Neurons
- 8.8.3. Establish Relations Between the Two

8.9. Implementation of MLP (Multilayer Perceptron) with Keras
- 8.9.1. Definition of the Network Structure
- 8.9.2. Model Compilation
- 8.9.3. Model Training

8.10. Fine Tuning Hyperparameters of Neural Networks
- 8.10.1. Selection of the Activation Function
- 8.10.2. Set the Learning Rate
- 8.10.3. Adjustment of Weights

Module 9. Deep Neural Networks Training

9.1. Gradient Problems
- 9.1.1. Gradient Optimization Techniques
- 9.1.2. Stochastic Gradients
- 9.1.3. Weight Initialization Techniques

9.2. Reuse of Pre-Trained Layers
- 9.2.1. Transfer Learning Training
- 9.2.2. Feature Extraction
- 9.2.3. Deep Learning

9.3. Optimizers
- 9.3.1. Stochastic Gradient Descent Optimizers
- 9.3.2. Adam and RMSprop Optimizers
- 9.3.3. Moment Optimizers

9.4. Learning Rate Programming
- 9.4.1. Automatic Learning Rate Control
- 9.4.2. Learning Cycles
- 9.4.3. Smoothing Terms

9.5. Overfitting
- 9.5.1. Cross Validation
- 9.5.2. Regularization
- 9.5.3. Evaluation Metrics

9.6. Practical Guidelines
- 9.6.1. Model Design
- 9.6.2. Selection of Metrics and Evaluation Parameters
- 9.6.3. Hypothesis Testing

9.7. Transfer Learning
- 9.7.1. Transfer Learning Training
- 9.7.2. Feature Extraction
- 9.7.3. Deep Learning

9.8. Data Augmentation
- 9.8.1. Image Transformations
- 9.8.2. Synthetic Data Generation
- 9.8.3. Text Transformation

9.9. Practical Application of Transfer Learning
- 9.9.1. Transfer Learning Training
- 9.9.2. Feature Extraction
- 9.9.3. Deep Learning

9.10. Regularization
- 9.10.1. L and L
- 9.10.2. Regularization by Maximum Entropy
- 9.10.3. Dropout

Module 10. Model Customization and Training with TensorFlow

10.1. *TensorFlow*
- 10.1.1. Use of the TensorFlow Library
- 10.1.2. Model Training with TensorFlow
- 10.1.3. Operations with Graphs in TensorFlow

10.2. TensorFlow and NumPy
- 10.2.1. NumPy Computing Environment for TensorFlow
- 10.2.2. Using NumPy Arrays with TensorFlow
- 10.2.3. NumPy Operations for TensorFlow Graphs

10.3. Model Customization and Training Algorithms
- 10.3.1. Building Custom Models with TensorFlow
- 10.3.2. Management of Training Parameters
- 10.3.3. Use of Optimization Techniques for Training

10.4. TensorFlow Features and Graphs
- 10.4.1. Functions with TensorFlow
- 10.4.2. Use of Graphs for Model Training
- 10.4.3. Graph Optimization with TensorFlow Operations

10.5. Loading and Preprocessing Data with TensorFlow
- 10.5.1. Loading Data Sets with TensorFlow
- 10.5.2. Pre-Processing Data with TensorFlow
- 10.5.3. Using TensorFlow Tools for Data Manipulation

10.6. The tfdata API
- 10.6.1. Using the tf.data API for Data Processing
- 10.6.2. Construction of Data Streams with tf.data
- 10.6.3. Using the tf.data API for Model Training

10.7. The TFRecord Format
- 10.7.1. Using the TFRecord API for Data Serialization
- 10.7.2. TFRecord File Upload with TensorFlow
- 10.7.3. Using TFRecord Files for Model Training

10.8. Keras Pre-Processing Layers
- 10.8.1. Using the Keras Pre-Processing API
- 10.8.2. Pre-Processing Pipelined Construction with Keras
- 10.8.3. Using the Keras Pre-Processing API for Model Training

10.9. The TensorFlow Datasets Project
- 10.9.1. Using TensorFlow Datasets for Data Loading
- 10.9.2. Data Pre-Processing with TensorFlow Datasets
- 10.9.3. Using TensorFlow Datasets for Model Training

10.10. Building a Deep Learning App with TensorFlow
- 10.10.1. Practical Application
- 10.10.2. Building a Deep Learning App with TensorFlow
- 10.10.3. Model Training with TensorFlow
- 10.10.4. Using the Application for the Prediction of Results

Module 11. Deep Computer Vision with Convolutional Neural Networks

11.1. The Cortex Visual Architecture
- 11.1.1. Functions of the Visual Cortex
- 11.1.2. Theories of Computational Vision
- 11.1.3. Models of Image Processing

11.2. Convolutional Layers
- 11.2.1. Reuse of Weights in Convolution
- 11.2.2. Convolution D
- 11.2.3. Activation Functions

11.3. Grouping Layers and Implementation of Grouping Layers with Keras
- 11.3.1. Pooling and Striding
- 11.3.2. *Flattening*
- 11.3.3. Types of Pooling

11.4. CNN Architecture
- 11.4.1. VGG Architecture
- 11.4.2. AlexNet Architecture
- 11.4.3. ResNet Architecture

11.5. Implementing a CNN ResNet- Using Keras
- 11.5.1. Weight Initialization
- 11.5.2. Input Layer Definition
- 11.5.3. Output Definition

11.6. Use of Pre-Trained Keras Models
- 11.6.1. Characteristics of Pre-Trained Models
- 11.6.2. Uses of Pre-Trained Models
- 11.6.3. Advantages of Pre-Trained Models

11.7. Pre-Trained Models for Transfer Learning
- 11.7.1. Transfer Learning
- 11.7.2. Transfer Learning Process
- 11.7.3. Advantages of Transfer Learning

11.8. Deep Computer Vision Classification and Localization
- 11.8.1. Image Classification
- 11.8.2. Localization of Objects in Images
- 11.8.3. Object Detection

11.9. Object Detection and Object Tracking
- 11.9.1. Object Detection Methods
- 11.9.2. Object Tracking Algorithms
- 11.9.3. Tracking and Localization Techniques

11.10. Semantic Segmentation
- 11.10.1. Deep Learning for Semantic Segmentation
- 11.10.1. Edge Detection
- 11.10.1. Rule-Based Segmentation Methods

Module 12. Natural Language Processing (NLP) with Recurrent Neural Networks (RNN) and Attention

12.1. Text Generation Using RNN
- 12.1.1. Training an RNN for Text Generation
- 12.1.2. Natural Language Generation with RNN
- 12.1.3. Text Generation Applications with RNN

12.2. Training Data Set Creation
- 12.2.1. Preparation of the Data for Training an RNN
- 12.2.2. Storage of the Training Dataset
- 12.2.3. Data Cleaning and Transformation
- 12.2.4. Sentiment Analysis

12.3. Classification of Opinions with RNN
- 12.3.1. Detection of Themes in Comments
- 12.3.2. Sentiment Analysis with Deep Learning Algorithms

12.4. Encoder-Decoder Network for Neural Machine Translation
- 12.4.1. Training an RNN for Machine Translation
- 12.4.2. Use of an Encoder-Decoder Network for Machine Translation
- 12.4.3. Improving the Accuracy of Machine Translation with RNNs

12.5. Attention Mechanisms
- 12.5.1. Application of Care Mechanisms in RNN
- 12.5.2. Use of Care Mechanisms to Improve the Accuracy of the Models
- 12.5.3. Advantages of Attention Mechanisms in Neural Networks

12.6. Transformer Models
- 12.6.1. Using Transformers Models for Natural Language Processing
- 12.6.2. Application of Transformers Models for Vision
- 12.6.3. Advantages of Transformers Models

12.7. Transformers for Vision
- 12.7.1. Use of Transformers Models for Vision
- 12.7.2. Image Data Pre-Processing
- 12.7.3. Training a Transformers Model for Vision

12.8. Hugging Face's Transformers Library
- 12.8.1. Using Hugging Face's Transformers Library
- 12.8.2. Hugging Face's Transformers Library Application
- 12.8.3. Advantages of Hugging Face's Transformers Library

12.9. Other Transformers Libraries. Comparison
- 12.9.1. Comparison Between Different Transformers Libraries
- 12.9.2. Use of the Other Transformers Libraries
- 12.9.3. Advantages of the Other Transformers Libraries

12.10. Development of an NLP Application with RNN and Attention. Practical Application
- 12.10.1. Development of a Natural Language Processing Application with RNN and Attention.
- 12.10.2. Use of RNN, Attention Mechanisms and Transformers Models in the Application
- 12.10.3. Evaluation of the Practical Application

Module 13. Autoencoders, GANs and Diffusion Models

13.1. Representation of Efficient Data
- 13.1.1. Dimensionality Reduction
- 13.1.2. Deep Learning
- 13.1.3. Compact Representations

13.2. PCA Realization with an Incomplete Linear Automatic Encoder
- 13.2.1. Training Process
- 13.2.2. Implementation in Python
- 13.2.3. Use of Test Data

13.3. Stacked Automatic Encoders
- 13.3.1. Deep Neural Networks
- 13.3.2. Construction of Coding Architectures
- 13.3.3. Use of Regularization

13.4. Convolutional Autoencoders
- 13.4.1. Design of Convolutional Models
- 13.4.2. Convolutional Model Training
- 13.4.3. Results Evaluation

13.5. Noise Suppression of Automatic Encoders
- 13.5.1. Filter Application
- 13.5.2. Design of Coding Models
- 13.5.3. Use of Regularization Techniques

13.6. Sparse Automatic Encoders
- 13.6.1. Increasing Coding Efficiency
- 13.6.2. Minimizing the Number of Parameters
- 13.6.3. Using Regularization Techniques

13.7. Variational Automatic Encoders
- 13.7.1. Use of Variational Optimization
- 13.7.2. Unsupervised Deep Learning
- 13.7.3. Deep Latent Representations

13.8. Generation of Fashion MNIST Images
- 13.8.1. Pattern Recognition
- 13.8.2. Image Generation
- 13.8.3. Deep Neural Networks Training

13.9. Generative Adversarial Networks and Diffusion Models
- 13.9.1. Content Generation from Images
- 13.9.2. Modeling of Data Distributions
- 13.9.3. Use of Adversarial Networks

13.10. Implementation of the Models
- 13.10.1. Practical Application
- 13.10.2. Implementation of the Models
- 13.10.3. Use of Real Data
- 13.10.4. Results Evaluation

Module 14. Bio-Inspired Computing

14.1. Introduction to Bio-Inspired Computing
- 14.1.1. Introduction to Bio-Inspired Computing

14.2. Social Adaptation Algorithms
- 14.2.1. Bio-Inspired Computation Based on Ant Colonies
- 14.2.2. Variants of Ant Colony Algorithms
- 14.2.3. Particle Cloud Computing

14.3. Genetic Algorithms
- 14.3.1. General Structure
- 14.3.2. Implementations of the Major Operators

14.4. Space Exploration-Exploitation Strategies for Genetic Algorithms
- 14.4.1. CHC Algorithm
- 14.4.2. Multimodal Problems

14.5. Evolutionary Computing Models (I)
- 14.5.1. Evolutionary Strategies
- 14.5.2. Evolutionary Programming
- 14.5.3. Algorithms Based on Differential Evolution

14.6. Evolutionary Computation Models (II)
- 14.6.1. Evolutionary Models Based on Estimation of Distributions (EDA)
- 14.6.2. Genetic Programming

14.7. Evolutionary Programming Applied to Learning Problems
- 14.7.1. Rules-Based Learning
- 14.7.2. Evolutionary Methods in Instance Selection Problems

14.8. Multi-Objective Problems
- 14.8.1. Concept of Dominance
- 14.8.2. Application of Evolutionary Algorithms to Multi-Objective Problems

14.9. Neural Networks (I)
- 14.9.1. Introduction to Neural Networks
- 14.9.2. Practical Example with Neural Networks

14.10. Neural Networks (II)
- 14.10.1. Use Cases of Neural Networks in Medical Research
- 14.10.2. Use Cases of Neural Networks in Economics
- 14.10.3. Use Cases of Neural Networks in Artificial Vision

Module 15. Artificial Intelligence: Strategies and Applications

15.1. Financial Services
- 15.1.1. The Implications of Artificial Intelligence in Financial Services. Opportunities and Challenges
- 15.1.2. Case Studies
- 15.1.3. Potential Risks Related to the Use of Artificial Intelligence
- 15.1.4. Potential Future Developments / Uses of Artificial Intelligence

15.2. Implications of Artificial Intelligence in Healthcare Service
- 15.2.1. Implications of Artificial Intelligence in the Healthcare Sector. Opportunities and Challenges
- 15.2.2. Case Studies

15.3. Risks Related to the Use of Artificial Intelligence in Health Services
- 15.3.1. Potential Risks Related to the Use of Artificial Intelligence
- 15.3.2. Potential Future Developments / Uses of Artificial Intelligence

15.4. *Retail*
- 15.4.1. Implications of Artificial Intelligence in Retail. Opportunities and Challenges
- 15.4.2. Case Studies
- 15.4.3. Potential Risks Related to the Use of Artificial Intelligence
- 15.4.4. Potential Future Developments / Uses of Artificial Intelligence

15.5. Industry
- 15.5.1. Implications of Artificial Intelligence in Industry. Opportunities and Challenges
- 15.5.2. Case Studies

15.6. Potential Risks Related to the Use of Artificial Intelligence in the Industry
- 15.6.1. Case Studies
- 15.6.2. Potential Risks Related to the Use of Artificial Intelligence
- 15.6.3. Potential Future Developments / Uses of Artificial Intelligence

15.7. Public Administration
- 15.7.1. Implications of Artificial Intelligence in Public Administration. Opportunities and Challenges
- 15.7.2. Case Studies
- 15.7.3. Potential Risks Related to the Use of Artificial Intelligence
- 15.7.4. Potential Future Developments / Uses of Artificial Intelligence

15.8. Educational
- 15.8.1. Implications of Artificial Intelligence in Education. Opportunities and Challenges
- 15.8.2. Case Studies
- 15.8.3. Potential Risks Related to the Use of Artificial Intelligence
- 15.8.4. Potential Future Developments / Uses of Artificial Intelligence

15.9. Forestry and Agriculture
- 15.9.1. Implications of Artificial Intelligence in Forestry and Agriculture. Opportunities and Challenges
- 15.9.2. Case Studies
- 15.9.3. Potential Risks Related to the Use of Artificial Intelligence
- 15.9.4. Potential Future Developments / Uses of Artificial Intelligence

15.10. Human Resources
- 15.10.1. Implications of Artificial Intelligence in Human Resources. Opportunities and Challenges
- 15.10.2. Case Studies
- 15.10.3. Potential Risks Related to the Use of Artificial Intelligence
- 15.10.4. Potential Future Developments / Uses of Artificial Intelligence

Module 16. Cybersecurity and Modern Threat Analysis with ChatGPT

16.1. Introduction to Cybersecurity: Current Threats and the Role of Artificial Intelligence
- 16.1.1. Definition and Basic Concepts of Cybersecurity
- 16.1.2. Types of Modern Cybersecurity Threats
- 16.1.3. Role of Artificial Intelligence in the Evolution of Cybersecurity

16.2. Confidentiality, Integrity and Availability (CIA) in the Age of Artificial Intelligence
- 16.2.1. Fundamentals of the CIA Model in Cybersecurity
- 16.2.2. Security Principles Applied in the Artificial Intelligence Context
- 16.2.3. CIA Challenges and Considerations in Artificial Intelligence-Driven Systems

16.3. Use of ChatGPT for Risk Analysis and Threat Scenarios
- 16.3.1. Fundamentals of Risk Analysis in Cybersecurity
- 16.3.2. ChatGPT's Ability to Identify and Evaluate Threat Scenarios
- 16.3.3. Benefits and Limitations of Risk Analysis with Artificial Intelligence

16.4. ChatGPT in the Detection of Critical Vulnerabilities
- 16.4.1. Principles of Vulnerability Detection in Information Systems
- 16.4.2. ChatGPT Functionalities to Support Vulnerability Detection
- 16.4.3. Ethical and Security Considerations When Using Artificial Intelligence in Fault Detection

16.5. AI-Assisted Analysis of Malware and Ransomware
- 16.5.1. Basic Principles of Malware and Ransomware Analysis
- 16.5.2. Artificial Intelligence Techniques Applied in the Identification of Malicious Code
- 16.5.3. Technical and Operational Challenges in AI-Assisted Malware Analysis

16.6. Identification of Common Attacks with Artificial Intelligence: Phishing, Social Engineering and Exploitation
- 16.6.1. Classification of Attacks: Phishing, Social Engineering and Exploitation
- 16.6.2. Artificial Intelligence Techniques for Identification and Analysis of Common Attacks
- 16.6.3. Difficulties and Limitations of Artificial Intelligence Models for Attack Detection

16.7. ChatGPT in Cyberthreat Training and Simulation
- 16.7.1. Fundamentals of Threat Simulation for Cybersecurity Training
- 16.7.2. ChatGPT Capabilities for Designing Simulation Scenarios
- 16.7.3. Benefits of Threat Simulation as a Training Tool

16.8. Cyber Security Policies with Artificial Intelligence Recommendations
- 16.8.1. Principles for Cyber Security Policy Formulation
- 16.8.2. Role of Artificial Intelligence in Generating Security Recommendations
- 16.8.3. Key Components in Artificial Intelligence Oriented Security Policies

16.9. Security in IoT Devices and the Role of Artificial Intelligence
- 16.9.1. Fundamentals of Internet of Things (IoT) Security
- 16.9.2. Artificial Intelligence Capabilities to Mitigate Vulnerabilities in IoT Devices
- 16.9.3. Specific Artificial Intelligence Challenges and Considerations for IoT Security

16.10. Threat Assessment and Responses Assisted by Artificial Intelligence Tools
- 16.10.1. Cybersecurity Threat Assessment Principles
- 16.10.2. Characteristics of Automated Artificial Intelligence Responses
- 16.10.3. Critical Factors in the Effectiveness of Cyber Responses with Artificial Intelligence

Module 17. Intrusion Detection and Prevention Using Generative Artificial Intelligence Models

17.1. Fundamentals of IDS/IPS Systems and the Role of Artificial Intelligence
- 17.1.1. Definition and Basic Principles of IDS and IPS Systems
- 17.1.2. Main Types and Configurations of IDS/IPS
- 17.1.3. Contribution of Artificial Intelligence in the Evolution of Detection and Prevention Systems

17.2. Use of Gemini for Network Anomaly Detection
- 17.2.1. Concepts and Types of Anomalies in Network Traffic
- 17.2.2. Gemini's Features for Network Data Analysis
- 17.2.3. Benefits of Anomaly Detection in Intrusion Prevention

17.3. Gemini and the Identification of Intrusion Patterns
- 17.3.1. Principles of Intrusion Pattern Identification and Classification
- 17.3.2. Artificial Intelligence Techniques Applied in the Detection of Threat Patterns
- 17.3.3. Types of Patterns and Anomalous Behavior in Network Security

17.4. Application of Generative Models in Attack Simulation
- 17.4.1. Fundamentals of Generative Models in Artificial Intelligence
- 17.4.2. Use of Generative Models to Recreate Attack Scenarios
- 17.4.3. Advantages and Limitations of Attack Simulation Using Generative Artificial Intelligence

17.5. Clustering and Event Classification Using Artificial Intelligence
- 17.5.1. Fundamentals of Clustering and Classification in Intrusion Detection
- 17.5.2. Common Clustering Algorithms Applied in Cybersecurity
- 17.5.3. Role of Artificial Intelligence in Improving Event Classification Methods

17.6. Gemini in the Generation of Behavioral Profiles
- 17.6.1. User and Device Profiling Concepts
- 17.6.2. Application of Generative Models in the Creation of Profiles
- 17.6.3. Benefits of Behavioral Profiling in Threat Detection

17.7. Big Data Analysis for Intrusion Prevention
- 17.7.1. Importance of Big Data in Detecting Security Patterns
- 17.7.2. Methods for Processing Large Volumes of Data in Cybersecurity
- 17.7.3. Artificial Intelligence Applications in Analysis and Prevention Based on Big Data

17.8. Data Reduction and Selection of Relevant Features with Artificial Intelligence
- 17.8.1. Principles of Dimensionality Reduction in Large Data Volumes
- 17.8.2. Feature Selection to Improve the Efficiency of Artificial Intelligence Analysis
- 17.8.3. Data Reduction Techniques Applied in Cybersecurity

17.9. Evaluation of Artificial Intelligence Models in Intrusion Detection
- 17.9.1. Evaluation Criteria of Artificial Intelligence Models in Cybersecurity
- 17.9.2. Performance and Accuracy Indicators of the Models
- 17.9.3. Importance of Constant Validation and Evaluation in Artificial Intelligence

17.10. Implementation of an Intrusion Detection System Powered by Generative Artificial Intelligence
- 17.10.1. Basic Concepts of Intrusion Detection System Implementation
- 17.10.2. Integration of Generative Artificial Intelligence in IDS/IPS Systems
- 17.10.3. Key Aspects for the Configuration and Maintenance of Artificial Intelligence-Based Systems

Module 18. Modern Cryptography with ChatGPT Support for Data Protection

18.1. Basic Principles of Cryptography with Artificial Intelligence Applications
- 18.1.1. Fundamental Concepts of Cryptography: Confidentiality and Authenticity
- 18.1.2. Main Cryptographic Algorithms and Their Current Relevance
- 18.1.3. Role of Artificial Intelligence in the Modernization of Cryptography

18.2. ChatGPT in the Teaching and Practice of Symmetric and Asymmetric Cryptography
- 18.2.1. Introduction to Symmetric and Asymmetric Cryptography
- 18.2.2. Comparison between Symmetric and Asymmetric Encryption
- 18.2.3. Use of ChatGPT in Learning Cryptographic Methods

18.3. Advanced Encryption (AES, RSA) and AI-Generated Recommendations
- 18.3.1. Fundamentals of AES and RSA Algorithms in Data Encryption
- 18.3.2. Strengths and Weaknesses of These Algorithms in the Current Context
- 18.3.3. Generation of Security Recommendations in Advanced Cryptography with Artificial Intelligence

18.4. Artificial Intelligence in Key Management and Authentication
- 18.4.1. Principles of Cryptographic Key Management
- 18.4.2. Importance of Secure Key Authentication
- 18.4.3. Application of Artificial Intelligence to Optimize Key Management and Authentication Processes

18.5. Hashing Algorithms and ChatGPT in Integrity Assessment
- 18.5.1. Basic Concepts and Applications of Hashing Algorithms
- 18.5.2. Hashing Functions in Data Integrity Verification
- 18.5.3. Data Integrity Analysis and Verification with the Help of ChatGPT

18.6. ChatGPT in the Detection of Anomalous Encryption Patterns
- 18.6.1. Introduction to Anomalous Pattern Detection in Cryptography
- 18.6.2. ChatGPT's Ability to Identify Irregularities in Cryptographic Data
- 18.6.3. Limitations of Language Models in Anomalous Cipher Detection

18.7. Introduction to Post-Quantum Cryptography with Artificial Intelligence Simulations
- 18.7.1. Fundamentals of Post-Quantum Cryptography and Its Importance
- 18.7.2. Main Post-Quantum Algorithms in Research
- 18.7.3. Use of Artificial Intelligence in Simulations for the Study of Post-Quantum Cryptography

18.8. Blockchain and ChatGPT in the Verification of Secure Transactions
- 18.8.1. Basic Concepts of Blockchain and Its Security Structure
- 18.8.2. Role of Cryptography in Blockchain Integrity
- 18.8.3. Application of ChatGPT to Explain and Analyze Secure Transactions

18.9. Privacy Protection and Federated Learning
- 18.9.1. Definition and Principles of Federated Learning
- 18.9.2. Importance of Privacy in Decentralized Learning
- 18.9.3. Benefits and Challenges of Federated Learning for Data Security

18.10. Development of a Generative Artificial Intelligence Based Encryption System
- 18.10.1. Basic Principles in the Creation of Encryption Systems
- 18.10.2. Advantages of Generative Artificial Intelligence in the Design of Encryption Systems
- 18.10.3. Components and Requirements of an AI-Assisted Encryption System

Module 19. Digital Forensics and Artificial Intelligence-Assisted Incident Response

19.1. ChatGPT Forensic Processes for the Identification of Evidence
- 19.1.1. Basic Concepts of Forensic Analysis in Digital Environments
- 19.1.2. Stages of Evidence Identification and Collection
- 19.1.3. Role of ChatGPT in the Support of Forensic Identification

19.2. Gemini and ChatGPT in Data Identification and Data Mining
- 19.2.1. Fundamentals of Data Extraction for Forensic Analysis
- 19.2.2. Relevant Data Identification Techniques
- 19.2.3. Contribution of Artificial Intelligence to the Automation of the Extraction Process

19.3. Log Analysis and Event Correlation with Artificial Intelligence
- 19.3.1. Importance of Logs in Incident Analysis
- 19.3.2. Event Correlation Techniques for Incident Reconstruction
- 19.3.3. Use of Artificial Intelligence to Identify Patterns in Log Correlation

19.4. Data Recovery and Restoration of Systems Using Artificial Intelligence
- 19.4.1. Data Recovery Principles and Their Importance in Digital Forensics
- 19.4.2. Restoration Techniques of Compromised Systems
- 19.4.3. Application of Artificial Intelligence to Improve Recovery and Restoration Processes

19.5. Machine Learning for Incident Detection and Reconstruction
- 19.5.1. Introduction to Machine Learning in Incident Detection
- 19.5.2. Incident Reconstruction Techniques with Artificial Intelligence Models
- 19.5.3. Ethical and Practical Considerations in Event Detection

19.6. Incident Reconstruction and Simulation with ChatGPT
- 19.6.1. Fundamentals of Incident Reconstruction in Forensic Analysis
- 19.6.2. ChatGPT's Ability to Create Incident Simulations
- 19.6.3. Limitations and Challenges in Complex Incident Simulation

19.7. Detection of Malicious Activity on Mobile Devices
- 19.7.1. Characteristics and Challenges in Forensic Analysis of Mobile Devices
- 19.7.2. Major Malicious Activities in Mobile Environments
- 19.7.3. Application of Artificial Intelligence to Identify Threats in Mobile Devices

19.8. Automated Incident Response with Artificial Intelligence Workflows
- 19.8.1. Principles of Incident Response in Cybersecurity
- 19.8.2. Importance of Automation in Rapid Incident Response
- 19.8.3. Benefits of Artificial Intelligence-Assisted Workflows in Mitigation

19.9. Ethics and Transparency in Forensic Analysis with Generative AI
- 19.9.1. Ethical Principles in the Use of Artificial Intelligence in Forensic Analysis
- 19.9.2. Transparency and Explainability of Generative Models in Forensics
- 19.9.3. Privacy and Accountability Considerations in Analysis

19.10. Forensic Analysis and Incident Recreation Lab with ChatGPT and Gemini
- 19.10.1. Structure and Objectives of a Forensic Analysis Laboratory
- 19.10.2. Benefits of Controlled Environments for Forensics Practice
- 19.10.3. Key Components for Setting Up a Simulation Laboratory

Module 20. Predictive Models for Proactive Defense in Cybersecurity Using ChatGPT

20.1. Predictive Analytics in Cybersecurity: Techniques and Applications with Artificial Intelligence
- 20.1.1. Basic Concepts of Predictive Analytics in Security
- 20.1.2. Predictive Techniques in the Field of Cybersecurity
- 20.1.3. Application of Artificial Intelligence in the Anticipation of Cyber Threats

20.2. Regression and Classification Models with ChatGPT Support
- 20.2.1. Principles of Regression and Classification in Threat Prediction
- 20.2.2. Types of Classification Models in Cybersecurity
- 20.2.3. ChatGPT Assistance in the Interpretation of Predictive Models

20.3. Identifying Emerging Threats with ChatGPT Predictions
- 20.3.1. Emerging Threat Detection Concepts
- 20.3.2. Techniques for Identifying New Attack Patterns
- 20.3.3. Limitations and Precautions in the Prediction of New Threats

20.4. Neural Networks for Anticipation of Cyberattacks
- 20.4.1. Fundamentals of Neural Networks Applied in Cybersecurity
- 20.4.2. Common Architectures for Detection and Prediction of Attacks
- 20.4.3. Challenges in Implementing Neural Networks in Cyber Defense

20.5. Use of ChatGPT for Threat Scenario Simulations
- 20.5.1. Basic Concepts of Threat Simulation in Cybersecurity
- 20.5.2. ChatGPT Capabilities for Developing Predictive Simulations
- 20.5.3. Factors to Consider in the Design of Simulated Scenarios

20.6. Reinforcement Learning Algorithms for Optimization of Defenses
- 20.6.1. Introduction to Reinforcement Learning in Cybersecurity
- 20.6.2. Reinforcement Algorithms Applied to Defense Strategies
- 20.6.3. Benefits and Challenges of Reinforcement Learning in Cybersecurity Environments

20.7. Threat Simulation and Response with ChatGPT
- 20.7.1. Threat Simulation Principles and Their Relevance in Cyber Defense
- 20.7.2. Automated and Optimized Responses to Simulated Attacks
- 20.7.3. Benefits of Simulation for Improving Cyber Preparedness

20.8. Accuracy and Effectiveness Assessment in Predictive Artificial Intelligence Models
- 20.8.1. Key Indicators for the Evaluation of Predictive Models
- 20.8.2. Accuracy Assessment Methodologies in Cybersecurity Models
- 20.8.3. Critical Factors in the Effectiveness of Artificial Intelligence Models in Cybersecurity

20.9. Artificial Intelligence in Incident Management and Automated Response
- 20.9.1. Fundamentals of Incident Management in Cybersecurity
- 20.9.2. Role of Artificial Intelligence in Real-Time Decision Making
- 20.9.3. Challenges and Opportunities in Response Automation

20.10. Creation of a Predictive Defense System with ChatGPT Support
- 20.10.1. Proactive Defense System Design Principles
- 20.10.2. Integration of Predictive Models in Cybersecurity Environments
- 20.10.3. Key Components for an AI-Based Predictive Defense System

You will delve into the integration of ChatGPT in risk analysis and automated incident response, to manage highly complex digital environments with precision"

03

Teaching Objectives

The main objective of this TECH university program is to provide professionals with the necessary skills to lead cybersecurity projects supported by Artificial Intelligence. Thanks to this academic itinerary, computer scientists will be able to design predictive models, implement advanced algorithms and develop effective strategies for the protection of both systems and data. In addition, they will acquire skills for proactive threat detection, digital forensics and optimization of technological resources in highly complex environments.

You will gain key skills to analyze large volumes of data, detect anomalous patterns and manage threats in real time"

General Objectives

- Master the fundamental principles of Artificial Intelligence and its application in Cybersecurity
- Analyze the data lifecycle and its impact on the implementation of intelligent systems
- Design advanced machine learning models for threat detection and mitigation
- Implement deep neural networks and deep learning systems in cybersecurity projects
- Apply data mining and natural language processing techniques to risk analysis
- Develop AI-based strategies for proactive protection of critical infrastructures
- Integrate bio-inspired intelligent systems for complex problem solving in digital environments
- Optimize algorithms and tools such as TensorFlow to customize security solutions
- Implement AI-assisted digital forensic analysis methods
- Design innovative solutions in modern cryptography to ensure data integrity
- Evaluate the effectiveness of predictive and generative models applied to cyber defense
- Encourage innovation in the development of AI-based tools to address emerging threats

Specific Objectives

Module 1. Fundamentals of Artificial Intelligence

- Analyze the historical evolution of Artificial Intelligence, from its beginnings to its current state, identifying key milestones and developments
- Understand the functioning of neural networks and their application in learning models in Artificial Intelligence
- Study the principles and applications of genetic algorithms, analyzing their usefulness in solving complex problems
- Analyze the importance of thesauri, vocabularies and taxonomies in structuring and processing data for Artificial Intelligence systems

Module 2. Data Types and Life Cycle

- Identify and classify the different types of statistical data, from quantitative to qualitative data
- Analyze the life cycle of data, from generation to disposal, identifying key stages
- Explore the initial stages of the data life cycle, highlighting the importance of data planning and structure
- Study data collection processes, including methodology, tools and collection channels
- Explore the Datawarehouse concept, with emphasis on the elements that comprise it and its design
- Analyze the regulatory aspects related to data management, complying with privacy and security regulations, as well as best practices.

Module 3. Data in Artificial Intelligence

- Master the fundamentals of data science, covering tools, types and sources for information analysis
- Explore the process of transforming data into information using data mining and visualization techniques
- Study the structure and characteristics of datasets, understanding their importance in the preparation and use of data for Artificial Intelligence models
- Use specific tools and best practices in data handling and processing, ensuring efficiency and quality in the implementation of Artificial Intelligence

Module 4. Data Mining. Selection, Preprocessing and Transformation

- Master the techniques of statistical inference to understand and apply statistical methods in data mining
- Perform detailed exploratory analysis of data sets to identify relevant patterns, anomalies, and trends
- Develop skills for data preparation, including data cleaning, integration, and formatting for use in data mining
- Implement effective strategies for handling missing values in datasets, applying imputation or elimination methods according to context
- Identify and mitigate noise present in data, using filtering and smoothing techniques to improve the quality of the data set
- Address data pre-processing in Big Data environments

Module 5. Algorithm and Complexity in Artificial Intelligence

- Introduce algorithm design strategies, providing a solid understanding of fundamental approaches to problem solving
- Study and apply sorting algorithms, understanding their performance and comparing their efficiency in different contexts
- Investigate algorithms with Heaps, analyzing their implementation and usefulness in efficient data manipulation
- Analyze graph-based algorithms, exploring their application in the representation and solution of problems involving complex relationships
- Study Greedy algorithms, understanding their logic and applications in solving optimization problems
- Investigate and apply the backtracking technique for systematic problem solving, analyzing its effectiveness in various scenarios

Module 6. Intelligent Systems

- Explore agent theory, understanding the fundamental concepts of its operation and its application in Artificial Intelligence and software engineering
- Analyze the concept of the semantic web and its impact on the organization and retrieval of information in digital environments
- Evaluate and compare different knowledge representations, integrating these to improve the efficiency and accuracy of intelligent systems
- Study semantic reasoners, knowledge-based systems and expert systems, understanding their functionality and applications in intelligent decision making

Module 7. Machine Learning and Data Mining

- Introduce the processes of knowledge discovery and the fundamental concepts of machine learning
- Evaluate classifiers using specific techniques to measure their performance and accuracy in data classification
- Study neural networks, understanding their operation and architecture to solve complex machine learning problems
- Explore Bayesian methods and their application in machine learning, including networks and Bayesian classifiers
- Analyze regression and continuous response models for predicting numerical values from data
- Explore text mining and natural language processing (NLP), understanding how machine learning techniques are applied to analyze and understand text

Module 8. Neural Networks, the Basis of Deep Learning

- Master the fundamentals of Deep Learning, understanding its essential role in Deep Learning
- Explore the fundamental operations in neural networks and understand their application in model building
- Analyze the different layers used in neural networks and learn how to select them appropriately
- Understand the effective linking of layers and operations to design complex and efficient neural network architectures
- Explore the connection between biological and artificial neurons for a deeper understanding of model design
- Tune hyperparameters for Fine Tuning of neural networks, optimizing their performance on specific tasks

Module 9. Deep Neural Networks Training

- Solve gradient-related problems in deep neural network training
- Apply practical guidelines to ensure efficient and effective training of deep neural networks
- Implement Transfer Learning as an advanced technique to improve model performance on specific tasks
- Explore and apply Data Augmentation techniques to enrich datasets and improve model generalization
- Develop practical applications using Transfer Learning to solve real-world problems
- Understand and apply regularization techniques to improve generalization and avoid overfitting in deep neural networks

Module 10. Model Customization and Training with TensorFlow

- Master the fundamentals of TensorFlow and its integration with NumPy for efficient data management and calculations
- Customize models and training algorithms using the advanced capabilities of TensorFlow
- Implement the TFRecord format for storing and accessing large datasets in TensorFlow
- Use Keras preprocessing layers to facilitate the construction of custom models
- Explore the TensorFlow Datasets project to access predefined datasets and improve development efficiency
- Develop a Deep Learning application with TensorFlow, integrating the knowledge acquired in the module

Module 11. Deep Computer Vision with Convolutional Neural Networks

- Understand the architecture of the visual cortex and its relevance in Deep Computer Vision
- Explore and apply convolutional layers to extract key features from images
- Implement clustering layers and their use in Deep Computer Vision models with Keras
- Analyze various Convolutional Neural Network (CNN) architectures and their applicability in different contexts
- Develop and implement a CNN ResNet using the Keras library to improve model efficiency and performance
- Use pre-trained Keras models to leverage transfer learning for specific tasks
- Address object detection and object tracking strategies using Convolutional Neural Networks
- Implement semantic segmentation techniques to understand and classify objects in images in a detailed manner

Module 12. Natural Language Processing (NLP) with Recurrent Neural Networks (RNN) and Attention

- Develop skills in text generation using Recurrent Neural Networks (RNN)
- Apply RNNs in opinion classification for sentiment analysis in texts
- Understand and apply attentional mechanisms in natural language processing models
- Analyze and use Transformers models in specific NLP tasks
- Delve into the application of Transformers models in the context of image processing and computer vision
- Become familiar with the Hugging Face Transformers library for efficient implementation of advanced models
- Compare different Transformers libraries to evaluate their suitability for specific tasks
- Develop a practical application of NLP that integrates RNN and attention mechanisms to solve real-world problems

Module 13. Autoencoders, GANs and Diffusion Models

- Develop efficient representations of data using Autoencoders, GANs and Diffusion Models.
- Perform PCA using an incomplete linear autoencoder to optimize data representation
- Delve and apply convolutional autoencoders for efficient visual data representations
- Generate fashion images from the MNIST dataset using Autoencoders
- Understand the concept of Generative Adversarial Networks (GANs) and Diffusion Models
- Implement and compare the performance of Diffusion Models and GANs in data generation

Module 14. Bio-Inspired Computing

- Introduce the fundamental concepts of bio-inspired computing
- Analyze social adaptation algorithms as a key approach in bio-inspired computing
- Examine models of evolutionary computation in the context of optimization
- Address the complexity of multi-objective problems in the framework of bio-inspired computing
- Explore the application of neural networks in the field of bio-inspired computing
- Delve into the implementation and usefulness of neural networks in bio-inspired computing

Module 15. Artificial Intelligence: Strategies and Applications

- Develop strategies for the implementation of artificial intelligence in financial services
- Analyze the implications of artificial intelligence in the delivery of healthcare services
- Identify and assess the risks associated with the use of Artificial Intelligence in the health care setting
- Assess the potential risks associated with the use of Artificial Intelligence in industry
- Apply artificial intelligence techniques in industry to improve productivity
- Design artificial intelligence solutions to optimize processes in public administration
- Evaluate the implementation of Artificial Intelligence technologies in the education sector
- Apply artificial intelligence techniques in forestry and agriculture to improve productivity

Module 16. Cybersecurity and Modern Threat Analysis with ChatGPT

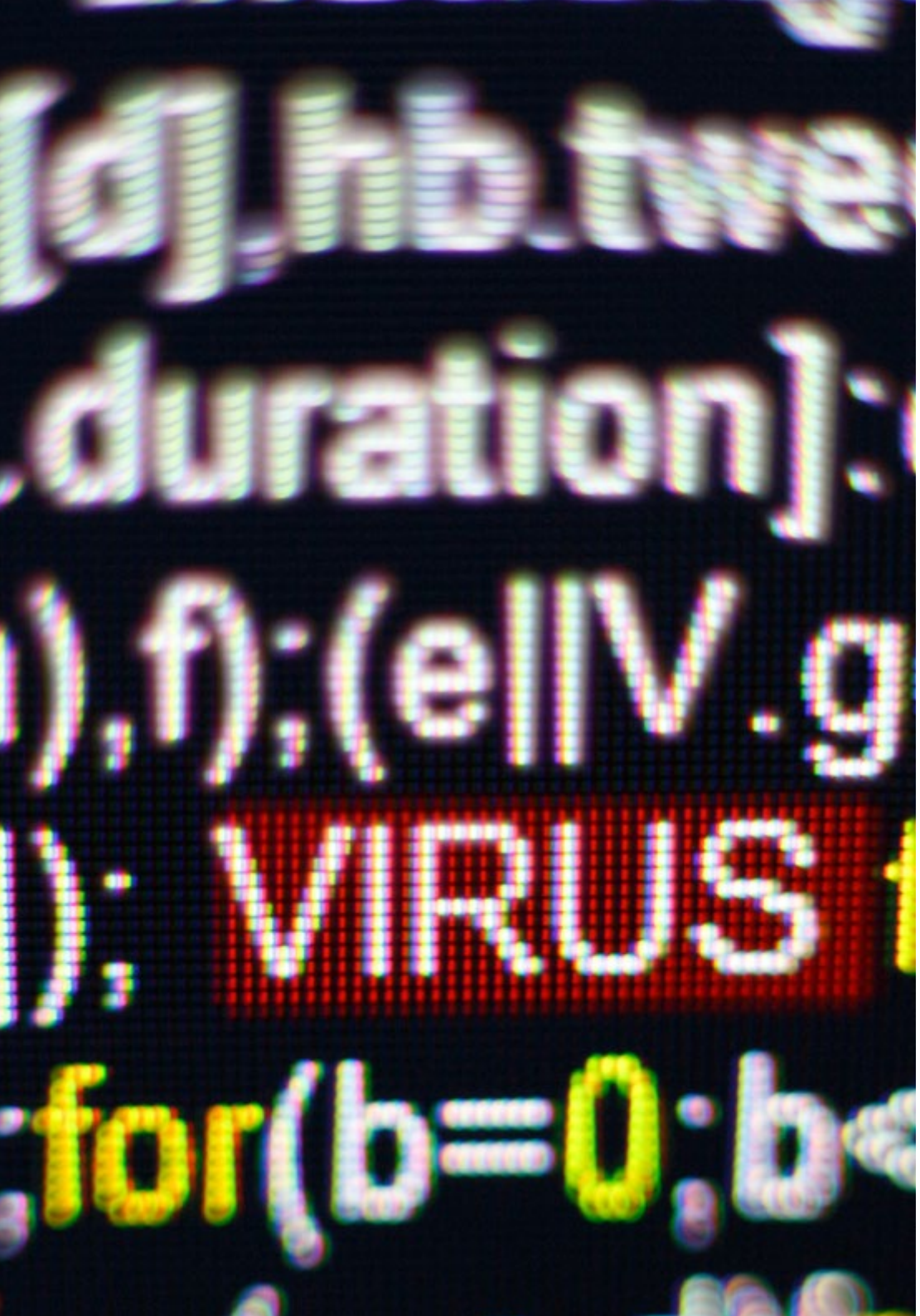
- Understand the fundamental concepts of Cybersecurity, including modern threats and the CIA model
- Use ChatGPT for risk analysis, vulnerability detection and simulation of threat scenarios
- Develop skills to design effective cybersecurity policies and protect IoT devices using Artificial Intelligence
- Implement advanced threat management strategies using generative Artificial Intelligence to anticipate potential attacks
- Assess the impact of modern threats on critical infrastructures using AI-assisted simulation techniques
- Design customized solutions for the protection of corporate networks, based on advanced Artificial Intelligence tools

Module 17. Intrusion Detection and Prevention Using Generative Artificial Intelligence Models

- Master anomaly and intrusion pattern detection techniques with tools such as Gemini
- Apply generative models to simulate cyber-attacks and improve intrusion prevention
- Implement advanced IDS/IPS systems optimized with Artificial Intelligence, developing behavioral profiles and analyzing Big Data in real-time
- Design integrated security architectures with Artificial Intelligence for the protection of multi-user environments and distributed systems
- Use generative models to anticipate targeted attacks and elaborate countermeasures in real time
- Integrate predictive analytics into detection systems for dynamic management of emerging threats

Module 18. Modern Cryptography with ChatGPT Support for Data Protection

- Master the basics of advanced cryptography, including algorithms such as AES, RSA and post-quantum algorithms
- Use ChatGPT to teach, practice and optimize cryptographic methods
- Design and manage AI-assisted encryption systems, ensuring data privacy and authenticity
- Evaluate the resilience of cryptographic algorithms against simulated attack scenarios with generative Artificial Intelligence
- Develop optimized encryption and decryption strategies to protect critical infrastructures and sensitive data
- Implement post-quantum cryptography solutions to mitigate future risks in AI-based systems



Module 19. Digital Forensics and Artificial Intelligence-Assisted Incident Response

- Learn to identify, extract and analyze digital evidence with the support of Artificial Intelligence tools
- Use Artificial Intelligence to automate data retrieval and reconstruction of security incidents
- Design and practice automated response workflows, ensuring speed and effectiveness in mitigating incidents
- Integrate advanced forensic analysis tools for the investigation of complex cyber-attacks
- Develop Artificial Intelligence-based event reconstruction techniques for post-incident audits
- Create automated incident response protocols, prioritizing operational continuity and damage mitigation

Module 20. Predictive Models for Proactive Defense in Cybersecurity Using ChatGPT

- Design advanced predictive models based on neural networks and reinforcement learning
- Implement simulations of threat scenarios to train teams and improve incident preparedness
- Evaluate and optimize proactive defense systems, integrating generative Artificial Intelligence for decision making and response automation
- Develop predictive defense frameworks adaptable to critical infrastructure and enterprise systems
- Use predictive analytics to identify emerging vulnerabilities before they are exploited
- Integrate generative Artificial Intelligence into strategic decision making processes for continuous improvement of defensive systems

04

Career Opportunities

With the skills and knowledge acquired through this university program, computer scientists will be able to access a wide range of job opportunities in key sectors such as Information Security, Risk Analysis and Critical Infrastructure Management. In this way, they will be able to play strategic roles in threat detection, predictive model design and advanced data protection, positioning them as leaders in a highly demanded field.

Your professional profile will enable you to work as a Cybersecurity Consultant, advising organizations on the integration of advanced technological solutions"

Graduate Profile

The graduate of this university program will be a professional specialized in integrating Artificial Intelligence and Cybersecurity to design innovative solutions to digital threats. They will have a deep knowledge of advanced tools, predictive models and modern cryptography, standing out for their ability to implement effective strategies in the protection of critical data and systems. This profile combines technical excellence and practical vision, ensuring your contribution to the transformation of the digital environment.

You will broaden your work horizons with a specialized approach, handling sophisticated methods such as Data Mining, Deep Learning and Digital Forensics.

- **Critical Thinking and Problem Solving:** Ability to analyze complex situations from multiple perspectives to identify patterns in digital threats and design innovative solutions using Artificial Intelligence that accurately and adaptively address technology challenges
- **Data-Driven Decision Making:** Ability to interpret large volumes of data and apply predictive models that inform real-time strategies ensuring actions aimed at mitigating risks efficiently
- **Technological Adaptability:** Competency to quickly integrate new tools, technologies and AI methodologies into professional practice responding in an agile manner to changes in the digital landscape and new forms of cyber attack
- **Ethical and Responsible Management:** In-depth understanding of the legal and ethical aspects related to data protection and the use of Artificial Intelligence acting in an ethical manner and aligned with international regulations to ensure the responsible use of Cybersecurity technologies

After completing the program, you will be able to use your knowledge and skills in the following positions:

1. **Analyst in Cyber Security with Artificial Intelligence:** In charge of identifying, preventing and mitigating digital threats using advanced Artificial Intelligence models for the protection of critical systems.
   Responsibilities: Implement Artificial Intelligence based intrusion detection systems, analyze attack patterns and design effective countermeasures in real time.
2. **Analyst in Digital Forensics with Artificial Intelligence:** Responsible for identifying, extracting and analyzing digital evidence employing advanced Artificial Intelligence technologies.
   Responsibilities: Automate data retrieval and incident reconstruction processes to ensure the integrity of cyber investigations.
3. **Proactive Digital Defense Consultant:** Specialized advisor in the development of Artificial Intelligence based security strategies to anticipate emerging threats in enterprise environments.
   Responsibilities: Perform simulations of attack scenarios and design predictive solutions to protect critical infrastructures.
4. **Expert in Digital Forensic Analysis with Artificial Intelligence:** In charge of investigating and reconstructing cybersecurity incidents using Artificial Intelligence tools to extract and analyze digital evidence.
   Responsibilities: Automate data recovery processes, perform post-incident audits and prepare technical reports for decision making.
5. **Cybersecurity Predictive Model Designer:** Focused on developing and implementing systems based on machine learning and neural networks to anticipate vulnerabilities.
   Responsibilities: Create custom predictive models and optimize Artificial Intelligence tools to identify attack patterns before they materialize.
6. **Critical Infrastructure Security Coordinator:** Responsible for overseeing the implementation of AI-based cybersecurity solutions in strategic sectors such as energy, transportation or finance.
   Responsibilities: Monitor threats in real time, integrate Artificial Intelligence systems into operating platforms and coordinate incident response.
7. **Manager of Cyber Risks with Artificial Intelligence:** Responsible for leading the planning and execution of strategies to identify and minimize cyber risks using Artificial Intelligence.
   Responsibilities: Perform vulnerability assessments and design dynamic security frameworks based on Generative Artificial Intelligence.
8. Responsible for Post Quantum Cryptography: expert in designing robust encryption systems based on quantum computer resistant algorithms, ensuring long term data protection.
   Responsibilities: Assess future threats and develop cryptographic solutions adapted to current and emerging needs.
9. **Administrator of Intrusion Detection Systems with Generative Artificial Intelligence:** Responsible for configuring and optimizing automated security tools that use generative Artificial Intelligence to detect and respond to threats.
   Responsibilities: Monitor IDS/IPS systems, analyze real-time results and update detection algorithms based on emerging patterns.
10. **Artificial Intelligence-Assisted Digital Security Auditor:** Responsible for assessing and certifying digital security systems using advanced AI-assisted analysis tools.
    Responsibilities: Identify security gaps, develop practical recommendations and ensure compliance with international cybersecurity regulations.

Academic and Research Opportunities

In addition to all the jobs you will be qualified for by studying this TECH Professional Master's Degree, you will also be able to pursue a solid academic and research career. After completing this university program, you will be ready to continue your studies associated with this field of knowledge and thus progressively achieve other scientific merits.

05

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.

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 Global Score 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.

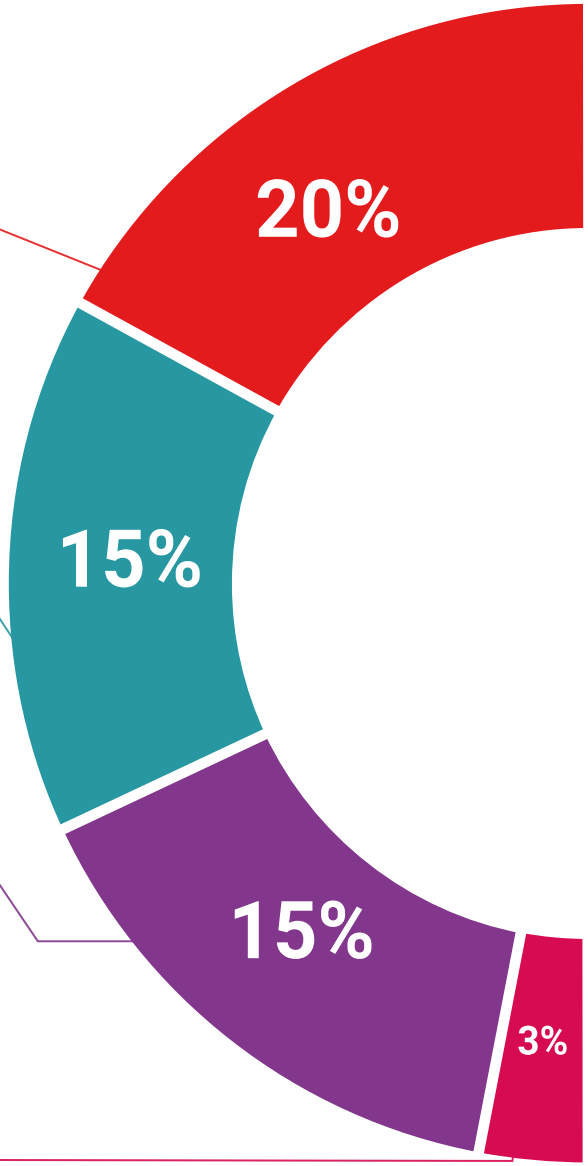
Interactive Summaries

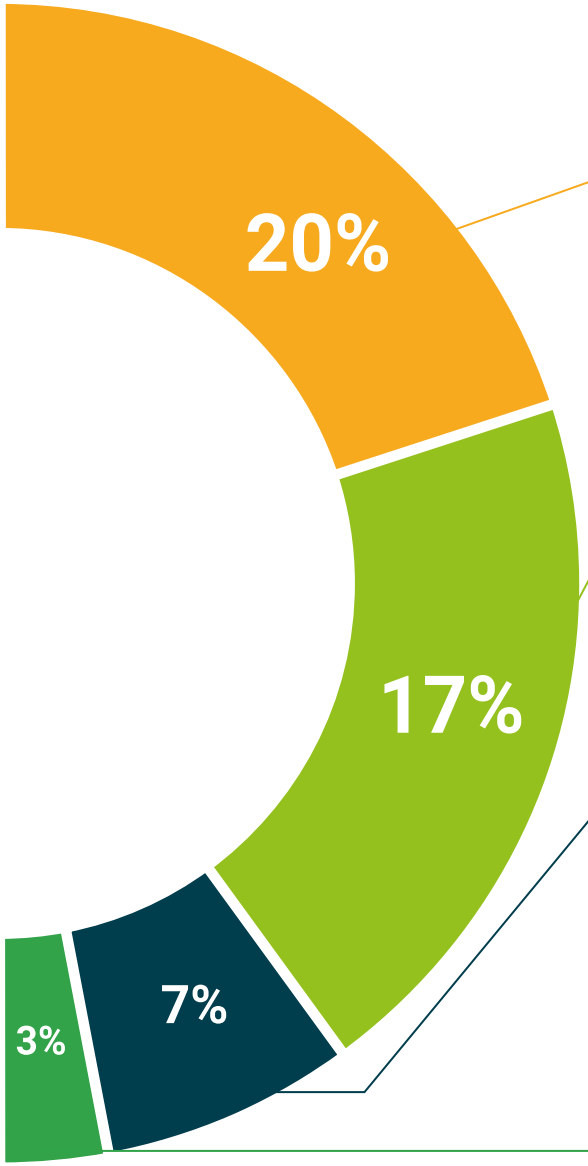
We present the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

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.

06

Teaching Staff

The faculty of this TECH program is composed of internationally renowned experts in the fields of Artificial Intelligence and cybersecurity. With strong backgrounds in both research and the implementation of advanced technological solutions, these professionals bring a practical and strategic approach to the development of key competencies in the sector. Their experience ranges from leading innovative projects to collaborating with industry leaders, ensuring an up-to-date and applied view of the most challenging technology demands.

You will benefit from both the experience and academic background of recognized professionals with a solid reputation in Cybersecurity and Deep Learning"

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: SMILE Research Group

Professors

Mr. Del Rey Sánchez, Alejandro

- Responsible for implementation of programs to improve tactical care in emergencies
- Degree in Industrial Organization Engineering
- Certification in Big Data and Business Analytics
- Certification in Microsoft Excel Advanced, VBA, KPI and DAX
- Certification in CIS Telecommunication and Information Systems

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

07

Certificate

The Professional Master's Degree in Artificial Intelligence in Cybersecurity guarantees students, in addition to the most rigorous and up-to-date education, access to a Professional 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 **Professional Master's Degree diploma in Artificial Intelligence in Cybersecurity** 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: **Professional Master's Degree in Artificial Intelligence in Cybersecurity**

Modality: **online**

Duration: **12 months**

Accreditation: **90 ECTS**

tech global university

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

Professional Master's Degree in Artificial Intelligence in Cybersecurity

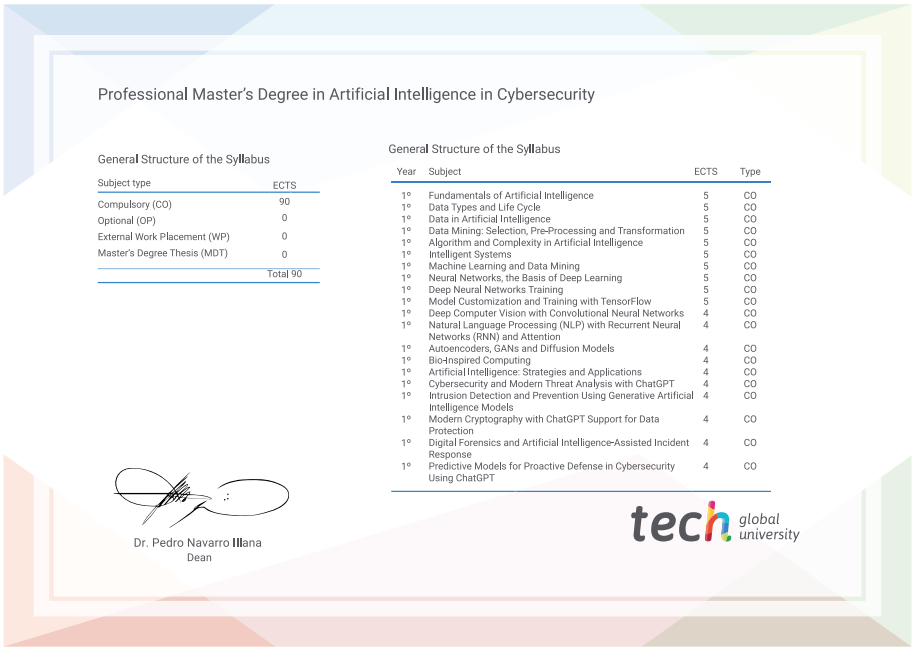
This is a private qualification of 2,700 hours of duration equivalent to 90 ECTS, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

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



Professional Master's Degree in Artificial Intelligence in Cybersecurity

General Structure of the Syllabus

Subject type	ECTS
Compulsory (CO)	90
Optional (OP)	0
External Work Placement (WP)	0
Master's Degree Thesis (MDT)	0
	Total 90

General Structure of the Syllabus

Year	Subject	ECTS	Type
1º	Fundamentals of Artificial Intelligence	5	CO
1º	Data Types and Life Cycle	5	CO
1º	Data in Artificial Intelligence	5	CO
1º	Data Mining: Selection, Pre-Processing and Transformation	5	CO
1º	Algorithm and Complexity in Artificial Intelligence	5	CO
1º	Intelligent Systems	5	CO
1º	Machine Learning and Data Mining	5	CO
1º	Neural Networks, the Basis of Deep Learning	5	CO
1º	Deep Neural Networks Training	5	CO
1º	Model Customization and Training with TensorFlow	5	CO
1º	Deep Computer Vision with Convolutional Neural Networks	4	CO
1º	Natural Language Processing (NLP) with Recurrent Neural Networks (RNN) and Attention	4	CO
1º	Autoencoders, GANs and Diffusion Models	4	CO
1º	Bio-Inspired Computing	4	CO
1º	Artificial Intelligence: Strategies and Applications	4	CO
1º	Cybersecurity and Modern Threat Analysis with ChatGPT	4	CO
1º	Intrusion Detection and Prevention Using Generative Artificial Intelligence Models	4	CO
1º	Modern Cryptography with ChatGPT Support for Data Protection	4	CO
1º	Digital Forensics and Artificial Intelligence-Assisted Incident Response	4	CO
1º	Predictive Models for Proactive Defense in Cybersecurity Using ChatGPT	4	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

Professional Master's Degree
Artificial Intelligence in Cybersecurity

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Global University**
- Accreditation: **90 ECTS**
- Schedule: **at your own pace**
- Exams: **online**

Professional Master's Degree

Artificial Intelligence in Cybersecurity

tech global university