

Weiterbildender  
Masterstudiengang  
Informatik, Cybersecurity  
und Datenanalyse





## Weiterbildender Masterstudiengang Informatik, Cybersecurity und Datenanalyse

- » Modalità: online
- » Durata: 2 Jahre
- » Titolo: TECH Università Tecnologica
- » Orario: a scelta
- » Esami: online

Internetzugang: [www.techtitute.com/de/informatik/weiterbildender-masterstudiengang/weiterbildender-masterstudiengang-informatik-cybersecurity-datenanalyse](http://www.techtitute.com/de/informatik/weiterbildender-masterstudiengang/weiterbildender-masterstudiengang-informatik-cybersecurity-datenanalyse)

# Index

01

Präsentation

---

Seite 4

02

Ziele

---

Seite 8

03

Kompetenzen

---

Seite 22

04

Kursleitung

---

Seite 26

05

Struktur und Inhalt

---

Seite 36

06

Methodik

---

Seite 68

07

Qualifizierung

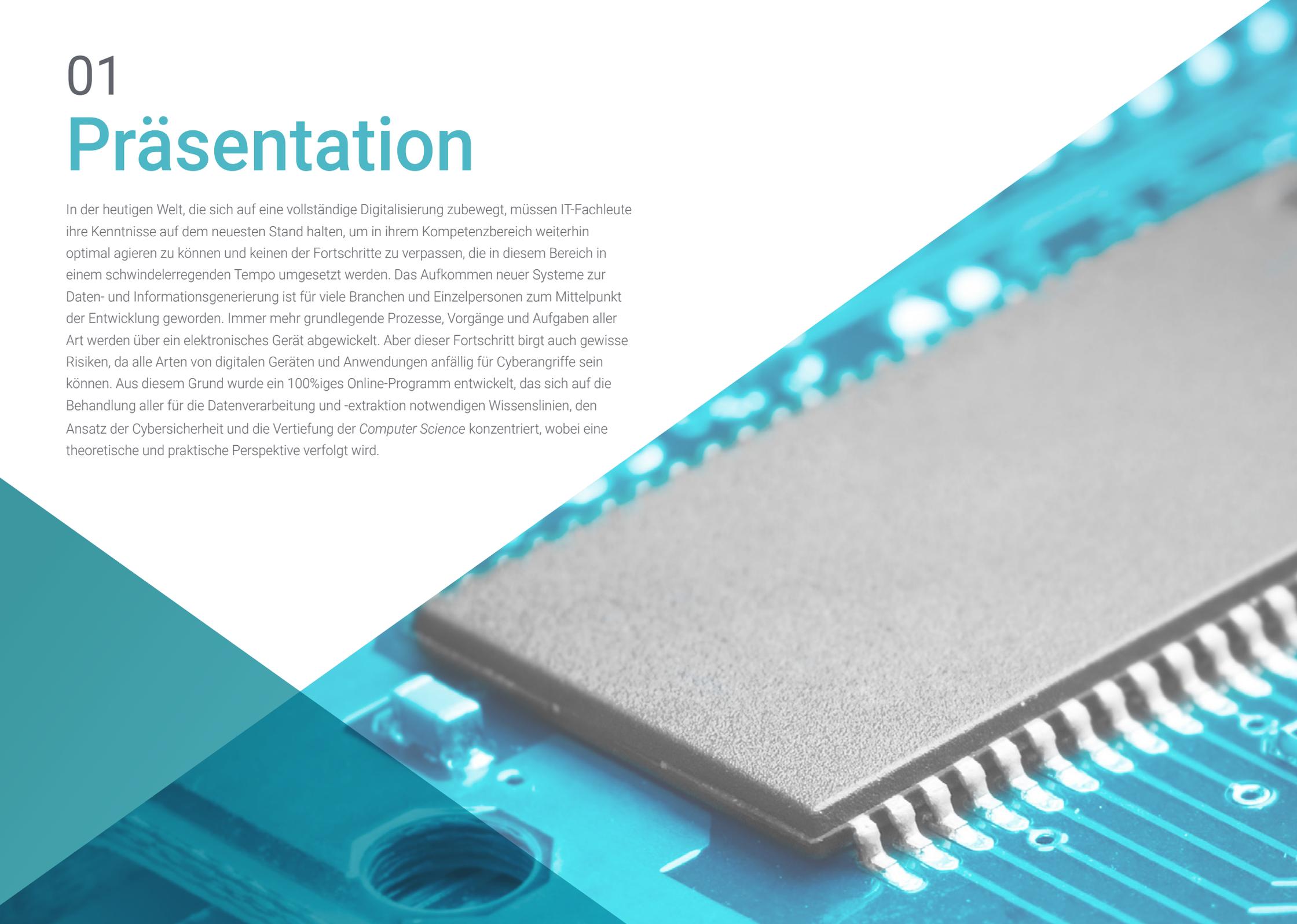
---

Seite 76

# 01

# Präsentation

In der heutigen Welt, die sich auf eine vollständige Digitalisierung zubewegt, müssen IT-Fachleute ihre Kenntnisse auf dem neuesten Stand halten, um in ihrem Kompetenzbereich weiterhin optimal agieren zu können und keinen der Fortschritte zu verpassen, die in diesem Bereich in einem schwindelerregenden Tempo umgesetzt werden. Das Aufkommen neuer Systeme zur Daten- und Informationsgenerierung ist für viele Branchen und Einzelpersonen zum Mittelpunkt der Entwicklung geworden. Immer mehr grundlegende Prozesse, Vorgänge und Aufgaben aller Art werden über ein elektronisches Gerät abgewickelt. Aber dieser Fortschritt birgt auch gewisse Risiken, da alle Arten von digitalen Geräten und Anwendungen anfällig für Cyberangriffe sein können. Aus diesem Grund wurde ein 100%iges Online-Programm entwickelt, das sich auf die Behandlung aller für die Datenverarbeitung und -extraktion notwendigen Wissenslinien, den Ansatz der Cybersicherheit und die Vertiefung der *Computer Science* konzentriert, wobei eine theoretische und praktische Perspektive verfolgt wird.



“

*Werden Sie ein Experte für Cybersicherheit, indem Sie Informatik und Datenanalyse beherrschen und so Ihre Beschäftigungsfähigkeit in einem zunehmend boomenden Sektor erheblich verbessern“*

Angetrieben durch die ständigen Fortschritte in der Informatik hat sich nicht nur die Technologie stark verbessert, sondern auch die digitalen Werkzeuge selbst, mit denen viele Aufgaben heute erledigt werden. Die Kehrseite der Medaille ist, dass diese Fortschritte auch zu einem Anstieg der IT-Schwachstellen geführt haben. Aus diesem Grund suchen immer mehr Unternehmen nach Fachleuten, die auf Cybersicherheit spezialisiert sind und ihnen einen angemessenen Schutz gegen alle Arten von Computerangriffen bieten können.

In diesem weiterbildenden Masterstudiengang wird der Informatiker in der Lage sein, sich mit Aspekten wie der Sicherheit bei der Entwicklung und dem Design von Systemen, den besten kryptographischen Techniken oder der Sicherheit in *Cloud Computing*-Umgebungen zu befassen. Dieses Programm konzentriert sich unter anderem auf die Grundlagen der Programmierung und Datenstruktur, Algorithmen und Komplexität sowie auf den fortgeschrittenen Entwurf von Algorithmen, fortgeschrittene Programmierung, Sprachprozessoren und Computergrafik. All dies mit zahlreichen multimedialen Lehrmitteln, unterrichtet von den renommiertesten und spezialisiertesten Dozenten auf diesem Gebiet.

Andererseits befasst sich diese Qualifizierung aus technischer und geschäftlicher Sicht mit der Datenwissenschaft und bietet alle notwendigen Kenntnisse, um das in ihnen verborgene Wissen zu extrahieren. Auf diese Weise können Informatiker die verschiedenen Algorithmen, Plattformen und aktuellsten Tools für die Erforschung, Visualisierung, Manipulation, Verarbeitung und Analyse von Daten im Detail analysieren. All das, ergänzt durch die Entwicklung von betriebswirtschaftlichen Fähigkeiten, die notwendig sind, um ein Niveau auf Führungsebene zu erreichen, das es ermöglicht, wichtige Entscheidungen in einem Unternehmen zu treffen.

Diese Weiterbildung vermittelt den Fachleuten also die spezifischen Werkzeuge und Fähigkeiten, um ihre berufliche Tätigkeit in der breiten Umgebung der Informatik erfolgreich zu entwickeln. Es wird an Schlüsselkompetenzen wie der Kenntnis der Realität und der täglichen Praxis in verschiedenen IT-Bereichen und die Entwicklung von Verantwortung bei der Überwachung und Beaufsichtigung ihrer Arbeit sowie von spezifischen Fähigkeiten in jedem Bereich gearbeitet.

Mit dieser Qualifikation können sich Informatiker auf Informatik, Cybersecurity und Datenanalyse spezialisieren und so ihre berufliche Karriere vorantreiben. All dies wird dank eines 100%igen Online-Programms greifbar, das sich an die täglichen Bedürfnisse von Berufstätigen anpasst, so dass Sie nur ein Gerät mit Internetanschluss benötigen, um mit der Arbeit an einem vollständigen Berufsprofil mit internationaler Projektion zu beginnen.

Dieser **Weiterbildender Masterstudiengang in Informatik, Cybersecurity und Datenanalyse** enthält das vollständigste und aktuellste Programm auf dem Markt.

Die hervorstechendsten Merkmale sind:

- ♦ Die Entwicklung von Fallstudien, die von Experten der Informatik präsentiert werden
- ♦ Der anschauliche, schematische und äußerst praxisnahe Inhalt soll wissenschaftliche und praktische Informationen zu den für die berufliche Praxis wesentlichen Disziplinen vermitteln
- ♦ Er enthält praktische Übungen in denen der Selbstbewertungsprozess durchgeführt werden kann um das Lernen zu verbessern
- ♦ Ein besonderer Schwerpunkt liegt auf innovativen Methoden für Cybersecurity und Datenanalyse
- ♦ Theoretische Vorträge, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- ♦ Die Verfügbarkeit des Zugangs zu Inhalten von jedem festen oder tragbaren Gerät mit Internetanschluss



*Erwerben Sie auf bequeme und einfache Weise die notwendigen Kenntnisse in Informatik, Cybersicherheit und Datenanalyse, um eine qualitativ hochwertige Computerprogrammierung durchzuführen“*



*TECH stellt Ihnen ein umfangreiches und übersichtliches didaktisches Material zur Verfügung, das alle aktuellen Themen von Interesse enthält, damit Sie sich im Bereich der Informatik weiterentwickeln können“*

Das Dozententeam besteht aus Fachleuten aus dem Bereich der Informatik, die ihre Berufserfahrung in dieses Programm einbringen, sowie aus anerkannten Spezialisten aus führenden Unternehmen und renommierten Universitäten.

Die multimedialen Inhalte, die mit den neuesten Bildungstechnologien entwickelt wurden, ermöglichen den Fachleuten ein situiertes und kontextbezogenes Lernen, d.h. eine simulierte Umgebung, die ein immersives Studium ermöglicht, das auf die Fortbildung in realen Situationen ausgerichtet ist.

Das Konzept dieses Studiengangs konzentriert sich auf problemorientiertes Lernen, bei dem der Student versuchen muss, die verschiedenen Situationen der beruflichen Praxis zu lösen, die im Laufe des akademischen Jahres auftreten. Dabei wird die Fachkraft durch ein innovatives interaktives Videosystem unterstützt, das von anerkannten Experten entwickelt wurde.

*Steigern Sie Ihre Karriere, indem Sie die Erstellung von Dashboards und KPIs abhängig von der Abteilung, in der Sie arbeiten, bestimmen.*

*Erfahren Sie aus erster Hand mehr über die besten Sicherheitstechniken für Cloud Computing-Umgebungen oder die Blockchain-Technologie.*



# 02 Ziele

Der Weiterbildender Masterstudiengang in Informatik, Cybersecurity und Datenanalyse wurde speziell für Informatiker entwickelt, die in diesem Bereich schnell und mit echter Qualität vorankommen wollen. Aus diesem Grund wurde ein Programm mit realistischen und hochwertigen Zielen organisiert, das Sie auf eine neue Ebene der Arbeit in diesem Bereich bringen wird. Die Fachkraft wird sich auf das Studium der verschiedenen Techniken, Technologien und Phasen konzentrieren, die für die Informatik notwendig sind, und zwar aus einer störungsfreien, vollständigen und aktuellen Perspektive.





“

*TECH bietet Ihnen eine hochwertige Qualifikation, die es Ihnen ermöglicht, mit Solvenz in die Informatik einzugreifen und die Sicherheit Ihres Unternehmens zu gewährleisten“*



## Allgemeine Ziele

---

- ♦ Wissenschaftlich und technologisch auf dem neuesten Stand zu sein, sowie sich auf die berufliche Praxis der Informatik und der Sprachen in einer transversalen und vielseitigen Weise vorzubereiten, die an die neuen Technologien und Innovationen in diesem Bereich angepasst ist
- ♦ Fachwissen über ein Informationssystem, Typen und Sicherheitsaspekte, die berücksichtigt werden müssen, generieren
- ♦ Die Schwachstellen eines Informationssystems identifizieren
- ♦ Entwicklung der gesetzlichen Bestimmungen und Typisierung von Verbrechen, die ein Informationssystem angreifen
- ♦ Bewertung der verschiedenen Sicherheitsarchitekturmodelle, um das für das Unternehmen am besten geeignete Modell zu ermitteln
- ♦ Identifizierung der regulatorischen Rahmenbedingungen für die Anwendung und deren Rechtsgrundlagen
- ♦ Analyse der organisatorischen und funktionalen Struktur eines Informationssicherheitsbereichs (das Büro des CISO)
- ♦ Analyse und Entwicklung des Konzepts des Risikos und der Ungewissheit in der Umwelt, in der wir leben
- ♦ Prüfung des Risikomanagementmodells auf der Grundlage von Iso 31.000
- ♦ Untersuchung der Wissenschaft der Kryptologie und der Beziehung zu ihren Zweigen: Kryptographie, Kryptoanalyse, Steganographie und Stegoanalyse
- ♦ Analyse der Arten von Kryptographie nach der Art des Algorithmus und nach ihrer Verwendung
- ♦ Digitale Zertifikate prüfen
- ♦ Untersuchung der Public Key Infrastructure (PKI)
- ♦ Entwicklung des Konzepts des Identitätsmanagements
- ♦ Identifizierung von Authentifizierungsmethoden
- ♦ Spezialwissen über das Ökosystem der IT-Sicherheit generieren
- ♦ Wissen in Bezug auf Cybersicherheit auswerten
- ♦ Die Sicherheitsbereiche in der *Cloud* identifizieren
- ♦ Analyse der Dienste und Tools in jedem der Sicherheitsbereiche
- ♦ Entwicklung der Sicherheitspezifikationen für jede LPWAN-Technologie
- ♦ Vergleichende Analyse der Sicherheit von LPWAN-Technologien
- ♦ Analyse der Vorteile der Anwendung von Datenanalysetechniken in jeder Abteilung des Unternehmens
- ♦ Die Grundlage für das Verständnis der Bedürfnisse und Anwendungen der einzelnen Abteilungen entwickeln
- ♦ Fachwissen generieren, um das richtige Werkzeug auszuwählen
- ♦ Techniken und Ziele vorschlagen, um je nach Abteilung so produktiv wie möglich zu sein



## Spezifische Ziele

---

### Modul 1. Grundlagen der Programmierung

- ♦ Die Grundstruktur eines Computers, Software und allgemeine Programmiersprachen verstehen
- ♦ Algorithmen entwerfen und interpretieren lernen, die die notwendige Grundlage für die Entwicklung von Computerprogrammen sind
- ♦ Die wesentlichen Elemente eines Computerprogramms verstehen, wie z.B. die verschiedenen Datentypen, Operatoren, Ausdrücke, Anweisungen, E/A- und Steueranweisungen
- ♦ Verstehen der verschiedenen Datenstrukturen, die in allgemeinen Programmiersprachen zur Verfügung stehen, sowohl statisch als auch dynamisch, und Erwerb der wesentlichen Kenntnisse für den Umgang mit Dateien
- ♦ Die verschiedenen Softwaretesttechniken und die Bedeutung der Erstellung einer guten Dokumentation zusammen mit einem guten Quellcode verstehen
- ♦ Erlernen der grundlegenden Konzepte der Programmiersprache C++, einer der am häufigsten verwendeten Sprachen der Welt

### Modul 2. Datenstruktur

- ♦ Die Grundlagen der Programmierung in der Sprache C++, einschließlich Klassen, Variablen, bedingte Ausdrücke und Objekte
- ♦ Abstrakte Datentypen, lineare Datenstrukturtypen, einfache und komplexe hierarchische Datenstrukturen und deren Implementierung in C++ verstehen
- ♦ Verstehen der Funktionsweise von fortgeschrittenen Datenstrukturen, die nicht den üblichen entsprechen
- ♦ Die Theorie und Praxis im Zusammenhang mit der Verwendung von Prioritätsheaps und Prioritätswarteschlangen verstehen
- ♦ Die Funktionsweise von *Hash*-Tabellen als abstrakte Datentypen und Funktionen kennenlernen
- ♦ Die Graphentheorie sowie fortgeschrittene Graph-Algorithmen und Konzepte verstehen

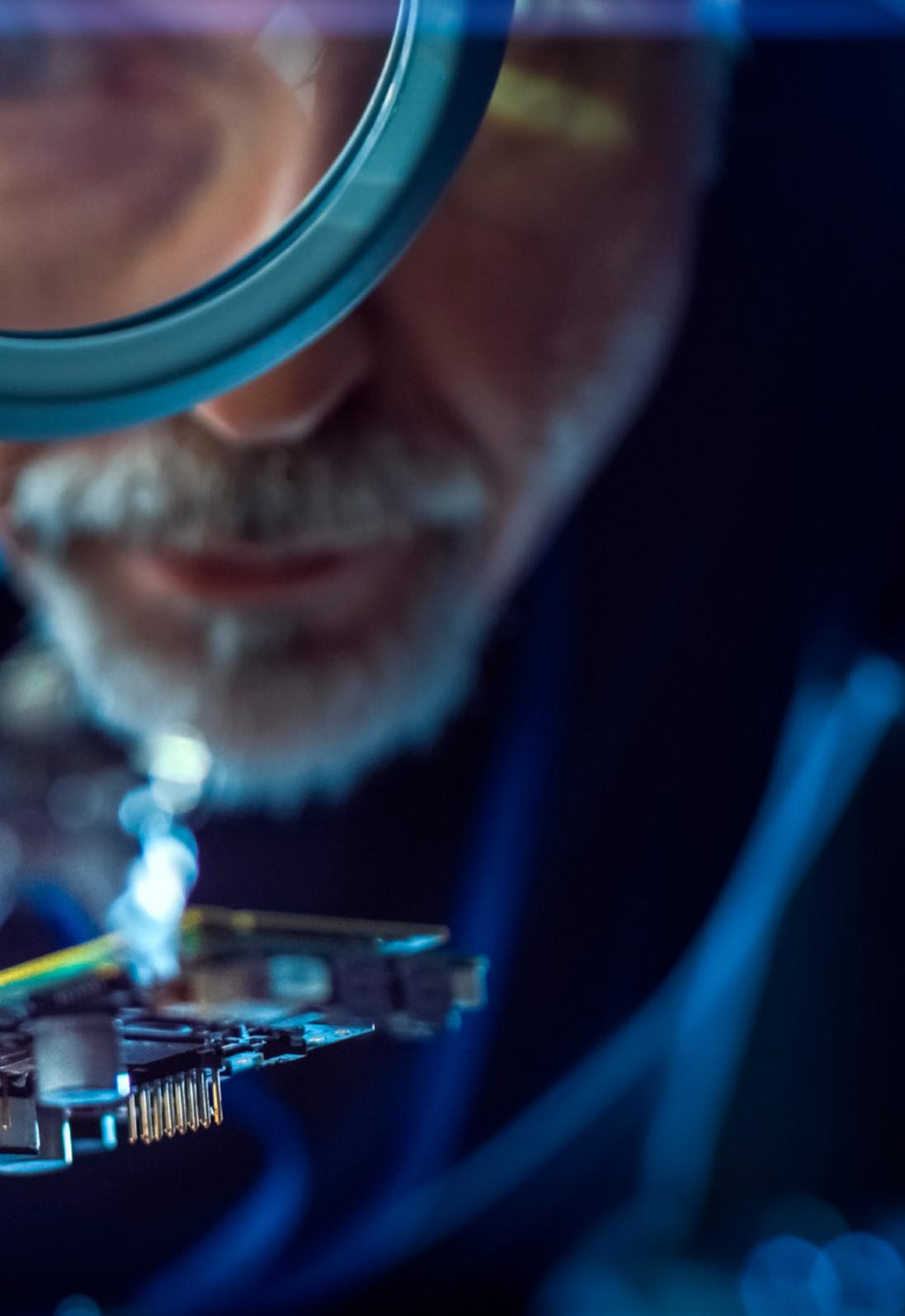
### Modul 3. Algorithmen und Komplexität

- ◆ Erlernen der wichtigsten Strategien für den Entwurf von Algorithmen sowie der verschiedenen Methoden und Maße für die Berechnung von Algorithmen
- ◆ Die wichtigsten Sortieralgorithmen, die in der Softwareentwicklung verwendet werden, kennenlernen
- ◆ Verstehen, wie verschiedene Algorithmen mit Bäumen, *Heaps* und Graphen arbeiten
- ◆ Die Funktionsweise von *Greedy*-Algorithmen, ihre Strategie und Beispiele für ihre Anwendung bei den wichtigsten bekannten Problemen verstehen Die Verwendung von *Greedy*-Algorithmen auf Graphen kennenlernen
- ◆ Die wichtigsten Strategien der Suche nach minimalen Pfaden kennen, mit der Annäherung an wesentliche Probleme des Feldes und Algorithmen zu deren Lösung
- ◆ Verstehen der *Backtracking*-Technik und ihrer wichtigsten Anwendungen sowie anderer alternativer Techniken

### Modul 4. Fortgeschrittener Algorithmusentwurf

- ◆ Vertiefung in den fortgeschrittenen Entwurf von Algorithmen, Analyse von rekursiven Algorithmen und Divide-and-Conquer-Algorithmen sowie Durchführung von amortisierten Analysen
- ◆ Konzepte der dynamischen Programmierung und Algorithmen für NP-Probleme verstehen
- ◆ Die Funktionsweise der kombinatorischen Optimierung, sowie die verschiedenen Randomisierungsalgorithmen und parallelen Algorithmen verstehen
- ◆ Die Funktionsweise der verschiedenen lokalen und Kandidaten-Suchmethoden kennen und verstehen
- ◆ Erlernen der Mechanismen der formalen Verifikation von Programmen und iterativen Programmen, einschließlich der Logik erster Ordnung und des formalen Systems von Hoare
- ◆ Die Funktionsweise einiger der wichtigsten numerischen Methoden wie die Bisektionsmethode, die Newton-Raphson-Methode und die Sekantenmethode kennen lernen





### **Modul 5. Fortgeschrittene Programmierung**

- ◆ Die Kenntnisse der Programmierung vertiefen, insbesondere in Bezug auf die objektorientierte Programmierung und die verschiedenen Arten von Beziehungen zwischen bestehenden Klassen
- ◆ Die verschiedenen Entwurfsmuster für objektorientierte Probleme kennenlernen
- ◆ Ereignisgesteuerte Programmierung und die Entwicklung von Benutzer-*Interfaces* mit Qt erlernen
- ◆ Grundlegende Kenntnisse über nebenläufige Programmierung, Prozesse und Threads erwerben
- ◆ Die Verwendung von Threads und Synchronisierung sowie die Lösung gängiger Probleme bei der gleichzeitigen Programmierung
- ◆ Die Bedeutung von Dokumentation und Tests bei der Softwareentwicklung verstehen

### **Modul 6. Theoretische Informatik**

- ◆ Die wesentlichen theoretischen mathematischen Konzepte der Informatik verstehen, wie z.B. Aussagenlogik, Mengenlehre und numerierbare und nicht numerierbare Mengen
- ◆ Die Konzepte von formalen Sprachen und Grammatiken sowie von Turing-Maschinen in ihren verschiedenen Varianten verstehen
- ◆ Die verschiedenen Arten von unentscheidbaren und unlösbaren Problemen kennenlernen, einschließlich ihrer verschiedenen Varianten und Annäherungen
- ◆ Die Funktionsweise verschiedener randomisierungsbasierter Sprachen und anderer Arten von Klassen und Grammatiken verstehen
- ◆ Andere fortschrittliche Rechensysteme wie z.B. Membran-Computing, DNA-Computing und Quanten-Computing verstehen

### Modul 7. Automatentheorie und formalen Sprachen

- ♦ Verständnis der Automatentheorie und der formalen Sprachen, Erlernen der Konzepte von Alphabeten, Zeichenketten und Sprachen sowie der Durchführung von formalen Demonstrationen
- ♦ Die verschiedenen Arten von endlichen Automaten kennenlernen, sowohl deterministische als auch nicht-deterministische
- ♦ Die grundlegenden und fortgeschrittenen Konzepte im Zusammenhang mit Sprachen und regulären Ausdrücken sowie die Anwendung des Pumping-Lemmas und die Schließung regulärer Sprachen erlernen
- ♦ Verstehen kontextunabhängiger Grammatiken sowie der Funktionsweise von Stapelautomaten
- ♦ Vertiefung der Normalformen, des Pump-Lemmas der kontextunabhängigen Grammatiken und der Eigenschaften kontextunabhängiger Sprachen

### Modul 8. Sprachprozessoren

- ♦ Einführung in die Konzepte im Zusammenhang mit dem Kompilierungsprozess und den verschiedenen Arten der Analyse: lexikalisch, syntaktisch und semantisch
- ♦ Die Funktionsweise eines lexikalischen Analysators, seine Implementierung und Fehlerbehebung lernen
- ♦ Vertiefung der Kenntnisse der syntaktischen Analyse, sowohl top-down als auch bottom-up, aber mit besonderem Schwerpunkt auf den verschiedenen Arten von bottom-up syntaktischen Analysatoren
- ♦ Verstehen, wie semantische Parser funktionieren, die syntaxorientierte Tradition, die Symboltabelle und die verschiedenen Arten von Parsern
- ♦ Die verschiedenen Mechanismen der Codegenerierung kennenlernen, sowohl in Laufzeitumgebungen als auch für die Generierung von Zwischencode
- ♦ Die Grundlagen der Code-Optimierung, einschließlich der Neuordnung von Ausdrücken und der Optimierung von Schleifen

### Modul 9. Computergrafik und Visualisierung

- ♦ Einführung in die grundlegenden Konzepte der Computergrafik und Computervisualisierung, wie z.B. die Theorie der Farbe und ihrer Modelle und die Eigenschaften des Lichts
- ♦ Die Funktionsweise der Ausgabepipeline und ihrer Algorithmen zu verstehen, sowohl für das Zeichnen von Linien als auch für das Zeichnen von Kreisen und Füllungen
- ♦ Vertiefung des Studiums der verschiedenen Transformationen, sowohl 2D als auch 3D, und ihrer Koordinatensysteme und Computervisualisierung
- ♦ Das Erstellen von Projektionen und Schnitten in 3D sowie das Eliminieren von verdeckten Flächen erlernen
- ♦ Erlernen der Theorie im Zusammenhang mit Interpolation und parametrischen Kurven, sowie Bézier-Kurven und *B-Splines*

### Modul 10. Bio-inspiriertes Rechnen

- ♦ Einführung in das Konzept des bio-inspirierten Computings sowie Verständnis für die Funktionsweise der verschiedenen Arten von sozialen Anpassungsalgorithmen und genetischen Algorithmen
- ♦ Vertiefung des Studiums der verschiedenen Modelle der evolutionären Berechnung, Kenntnis ihrer Strategien, Programmierung, Algorithmen und Modelle, die auf der Schätzung von Verteilungen basieren
- ♦ Die wichtigsten Strategien zur Erkundung und Ausnutzung des Raums für genetische Algorithmen verstehen
- ♦ Die Funktionsweise der evolutionären Programmierung bei Lernproblemen und Mehrzielproblemen verstehen
- ♦ Die grundlegenden Konzepte neuronaler Netze kennen und verstehen Sie die Funktionsweise realer Anwendungsfälle in so unterschiedlichen Bereichen wie medizinische Forschung, Wirtschaft und künstliches Sehen erlernen



### Modul 11. Sicherheit in Design und Entwicklung von Systemen

- ◆ Die Sicherheit eines Informationssystems in all seinen Komponenten und Schichten bewerten
- ◆ Identifizierung aktueller Arten von Sicherheitsbedrohungen und Trends
- ◆ Festlegung von Sicherheitsrichtlinien durch Definition von Sicherheits- und Notfallrichtlinien und -plänen
- ◆ Analyse von Strategien und Tools zur Gewährleistung der Integrität und Sicherheit von Informationssystemen
- ◆ Anwendung spezifischer Techniken und Tools für jede Art von Angriff oder Sicherheitsschwachstelle
- ◆ Schutz der im Informationssystem gespeicherten vertraulichen Informationen
- ◆ Den rechtlichen Rahmen und die Typisierung des Verbrechens kennen, um die Vision mit der Typisierung des Täters und seines Opfers zu vervollständigen

### Modul 12. Architekturen und Modelle für die Informationssicherheit

- ◆ Abstimmung des Sicherheitsmasterplans auf die strategischen Ziele des Unternehmens
- ◆ Einrichtung eines kontinuierlichen Risikomanagement-Rahmens als integraler Bestandteil des Master Security Plan
- ◆ Festlegung geeigneter Indikatoren für die Überwachung der Umsetzung des ISMS
- ◆ Einrichtung einer richtlinienbasierten Sicherheitsstrategie
- ◆ Analyse der Ziele und Verfahren im Zusammenhang mit dem Plan zur Sensibilisierung von Mitarbeitern, Lieferanten und Partnern
- ◆ Identifizierung der in jeder Organisation geltenden Vorschriften, Zertifizierungen und Gesetze innerhalb des gesetzlichen Rahmens
- ◆ Entwicklung der Schlüsselemente, die in der Norm ISO 27001:2013 gefordert werden
- ◆ Implementierung eines Modells zur Verwaltung des Datenschutzes in Übereinstimmung mit der europäischen GDPR/RGPD-Verordnung

### Modul 13. IT-Sicherheitsmanagement

- ◆ Die verschiedenen Strukturen, die ein Bereich der Informationssicherheit haben kann, identifizieren
- ◆ Entwicklung eines Sicherheitsmodells, das auf drei Verteidigungslinien basiert
- ◆ Vorstellung der verschiedenen periodischen und außerordentlichen Ausschüsse, in denen der Bereich Cybersicherheit vertreten ist
- ◆ Angabe der technologischen Hilfsmittel, die die Hauptfunktionen des Security Operations Team (SOT) unterstützen
- ◆ Bewertung der für jedes Szenario geeigneten Maßnahmen zur Kontrolle der Schwachstellen
- ◆ Entwicklung des Rahmenwerks für Sicherheitsoperationen auf der Grundlage des NIST CSF
- ◆ Den Umfang der verschiedenen Arten von Audits festlegen (*Red Team*, Pentesting, Bug Bounty, usw.)
- ◆ Vorschläge für die Aktivitäten nach einem Sicherheitsvorfall
- ◆ Einrichtung einer Kommandozentrale für Informationssicherheit, die alle relevanten Akteure (Behörden, Kunden, Lieferanten usw.) einbezieht

### Modul 14. Risikoanalyse und IT-Sicherheitsumgebung

- ◆ Das Umfeld, in dem wir tätig sind, mit einem ganzheitlichen Blick zu untersuchen
- ◆ Die wichtigsten Risiken und Potenziale identifizieren, die das Erreichen unserer Ziele beeinträchtigen können
- ◆ Analyse der Risiken auf der Grundlage der besten uns zur Verfügung stehenden Methoden
- ◆ Bewertung der potenziellen Auswirkungen dieser Risiken und Chancen
- ◆ Entwicklung von Techniken, um die Risiken und Potenziale so anzugehen, dass der Mehrwert maximiert wird
- ◆ Vertiefung der verschiedenen Techniken zur Übertragung von Risiko und Wert
- ◆ Wertschöpfung durch die Entwicklung eigener Modelle für agiles Risikomanagement
- ◆ Prüfung der Ergebnisse, um kontinuierliche Verbesserungen im Projekt- und Prozessmanagement auf der Grundlage risikoorientierter oder *Risk-Driven* Managementmodelle vorzuschlagen
- ◆ Innovation und Umwandlung allgemeiner Daten in relevante Informationen für eine risikobasierte Entscheidungsfindung

### Modul 15. Kryptographie in der IT

- ♦ Die grundlegenden Operationen (XOR, große Zahlen, Substitution und Transposition) und die verschiedenen Komponenten (*One-Way-Funktionen*, *Hash*, Zufallszahlengeneratoren) zusammenstellen
- ♦ Analyse kryptographischer Techniken
- ♦ Verschiedene kryptographische Algorithmen entwickeln
- ♦ Demonstration der Verwendung digitaler Signaturen und ihrer Anwendung in digitalen Zertifikaten
- ♦ Bewertung von Schlüsselverwaltungssystemen und der Bedeutung von kryptographischen Schlüssellängen
- ♦ Untersuchung von Algorithmen zur Schlüsselableitung
- ♦ Analyse des Lebenszyklus von Schlüsseln
- ♦ Auswertung von Blockchiffre- und Stromchiffre-Modi
- ♦ Pseudo-Zufallszahlengeneratoren bestimmen
- ♦ Entwicklung realer Kryptographie-Anwendungen, wie Kerberos, PGP oder Smart Cards
- ♦ Prüfung verwandter Verbände und Gremien, wie ISO, NIST oder NCSC
- ♦ Die Herausforderungen in der Kryptographie des Quantencomputings bestimmen

### Modul 16. Identitäts- und Zugriffsmanagement in der IT-Sicherheit

- ♦ Das Konzept der digitalen Identität entwickeln
- ♦ Bewertung der physischen Zugangskontrolle zu Informationen
- ♦ Grundlagen der biometrischen Authentifizierung und MFA-Authentifizierung
- ♦ Bewertung von Angriffen auf die Vertraulichkeit von Informationen
- ♦ Analyse des Identitätsverbundes
- ♦ Netzwerkzugangskontrolle einrichten

### Modul 17. Sicherheit bei Kommunikation und Softwarebetrieb

- ♦ Entwicklung von Fachwissen über physische und logische Sicherheit
- ♦ Demonstration von Kenntnissen über Kommunikation und Netzwerke
- ♦ Identifizierung größerer bössartiger Angriffe
- ♦ Einen sicheren Entwicklungsrahmen einrichten
- ♦ Nachweis von Kenntnissen über die wichtigsten Vorschriften zum Management von Informationssicherheitssystemen
- ♦ Demonstration der Gründe für den Betrieb eines Betriebszentrums für Cybersicherheit
- ♦ Die Bedeutung von Cybersicherheitspraktiken für organisatorische Katastrophen demonstrieren

### Modul 18. Sicherheit in *Cloud*-Umgebungen

- ◆ Identifizierung der Risiken bei der Bereitstellung einer öffentlichen *Cloud*-Infrastruktur
- ◆ Sicherheitsanforderungen definieren
- ◆ Entwicklung eines Sicherheitsplans für eine *Cloud*-Bereitstellung
- ◆ Identifizierung der *Cloud*-Dienste, die für die Ausführung eines Sicherheitsplans eingesetzt werden sollen
- ◆ Bestimmung der operativen Anforderungen für Präventionsmechanismen
- ◆ Festlegung von Richtlinien für ein Protokollierungs- und Überwachungssystem
- ◆ Maßnahmen zur Reaktion auf Vorfälle vorschlagen

### Modul 19. Sicherheit der Kommunikation von IoT-Geräten

- ◆ Einführung in die vereinfachte IoT-Architektur
- ◆ Erklärung der Unterschiede zwischen allgemeinen Konnektivitätstechnologien und Konnektivitätstechnologien für das IoT
- ◆ Das Konzept des Eisernen Dreiecks der IoT-Konnektivität etablieren
- ◆ Analyse der Sicherheitsspezifikationen der LoRaWAN-Technologie, NB-IoT-Technologie und WiSUN-Technologie
- ◆ Die Wahl der richtigen IoT-Technologie für jedes Projekt begründen

### Modul 20. Business Continuity Plan in Verbindung mit Sicherheit

- ◆ Die wichtigsten Elemente jeder Phase vorstellen und die Merkmale des Business Continuity Plan (BCP) analysieren
- ◆ Die Notwendigkeit eines Business Continuity Plans begründen
- ◆ Bestimmung der Erfolgs- und Risikokarten für jede Phase des Business Continuity Plans
- ◆ Festlegung eines Aktionsplans für die Umsetzung
- ◆ Bewertung der Vollständigkeit eines Business Continuity Plans (BCP)
- ◆ Entwicklung des Plans für die erfolgreiche Implementierung eines Business Continuity Plans

### Modul 21. Datenanalytik in der Unternehmensorganisation

- ◆ Entwicklung analytischer Fähigkeiten, um hochwertige Entscheidungen zu treffen
- ◆ Untersuchung von effektiven Marketing- und Kommunikationskampagnen
- ◆ Die Erstellung von abteilungsspezifischen Dashboards und KPIs bestimmen
- ◆ Fachwissen generieren, um prädiktive Analysen zu entwickeln
- ◆ Vorschlagen von Geschäfts- und Loyalitätsplänen auf der Grundlage von Marktstudien
- ◆ Die Fähigkeit entwickeln, dem Kunden zuzuhören
- ◆ Statistisches, quantitatives und technisches Wissen in realen Situationen anwenden

## Modul 22. Datenmanagement, Datenmanipulation und Informationen für Data Science

- ◆ Durchführen der Datenanalyse
- ◆ Verschiedene Daten vereinheitlichen: Konsistenz der Informationen erreichen
- ◆ Bereitstellung relevanter, effektiver Informationen für die Entscheidungsfindung
- ◆ Bestimmung der besten Praktiken für die Datenverwaltung je nach Typologie und Verwendungszweck
- ◆ Festlegung von Richtlinien für den Datenzugriff und die Wiederverwendung
- ◆ Gewährleistung von Sicherheit und Verfügbarkeit: Verfügbarkeit, Integrität und Vertraulichkeit von Informationen
- ◆ Untersuchung von Tools zur Datenverwaltung mit Hilfe von Programmiersprachen

## Modul 23. IoT-Geräte und Plattformen als Grundlage für Data Science

- ◆ Identifizierung, was IoT (*Internet of Things*) und IIoT (*Industrial Internet of Things*) ist
- ◆ Das industrielle Internet-Konsortium untersuchen
- ◆ Analyse der IoT-Referenzarchitektur
- ◆ Besprechung von IoT-Sensoren und -Geräten und deren Klassifizierung
- ◆ Identifizierung der im IoT verwendeten Kommunikationsprotokolle und Technologien
- ◆ Untersuchung der verschiedenen *Cloud*-Plattformen im IoT: Allzweck, Industrie, Open Source
- ◆ Entwicklung von Mechanismen zum Datenaustausch
- ◆ Festlegung von Sicherheitsanforderungen und -strategien
- ◆ Einführung in die verschiedenen IoT- und IIoT-Anwendungsbereiche

## Modul 24. Grafische Darstellung für die Datenanalyse

- ◆ Fachwissen über Datendarstellung und -analyse aufbauen
- ◆ Die verschiedenen Arten von gruppierten Daten untersuchen
- ◆ Ermittlung der am häufigsten verwendeten grafischen Darstellungen in verschiedenen Bereichen
- ◆ Bestimmung der Gestaltungsprinzipien bei der Datenvisualisierung
- ◆ Einführung in die grafische Erzählung als Werkzeug
- ◆ Analyse der verschiedenen Softwaretools für die grafische Darstellung und explorative Datenanalyse

## Modul 25. Data Science Tools

- ◆ Entwicklung von Fähigkeiten zur Umwandlung von Daten in Informationen, aus denen Wissen gewonnen werden kann
- ◆ Bestimmung der Hauptmerkmale eines *Dataset*, seiner Struktur, seiner Komponenten und der Auswirkungen seiner Verteilung auf die Modellierung
- ◆ Unterstützung der Entscheidungsfindung durch eine vollständige vorherige Analyse der Daten
- ◆ Entwicklung von Fähigkeiten zur Lösung von Fallstudien mit Hilfe von Data Science-Techniken
- ◆ Festlegung der am besten geeigneten allgemeinen Tools und Methoden für die Modellierung jedes *Datasets* auf der Grundlage der durchgeführten Vorverarbeitungen
- ◆ Ergebnisse analytisch auswerten und die Auswirkungen der gewählten Strategie auf die verschiedenen Metriken verstehen
- ◆ Demonstration der Kritikfähigkeit an den Ergebnissen, die nach Anwendung von Vorverarbeitungs- oder Modellierungsmethoden erzielt wurden

### **Modul 26. Data Mining. Auswahl, Vorverarbeitung und Transformation**

- ♦ Fachwissen über die vorherige Statistik für die Datenanalyse und -auswertung generieren
- ♦ Die notwendigen Fähigkeiten zur Identifizierung, Vorbereitung und Umwandlung von Daten entwickeln
- ♦ Die verschiedenen vorgestellten Methoden bewerten und Vor- und Nachteile identifizieren
- ♦ Untersuchung von Problemen in hochdimensionalen Datenumgebungen
- ♦ Entwicklung der Implementierung der Algorithmen für die Datenvorverarbeitung
- ♦ Demonstration der Fähigkeit, Datenvisualisierungen für die deskriptive Analyse zu interpretieren
- ♦ Entwicklung fortgeschrittener Kenntnisse über die verschiedenen vorhandenen Datenaufbereitungstechniken zur Datenbereinigung, Normalisierung und Datentransformation

### **Modul 27. Vorhersagbarkeit und Analyse von stochastischen Phänomenen**

- ♦ Zeitreihen analysieren
- ♦ Entwicklung der Formulierung und der grundlegenden Eigenschaften von univariaten Zeitreihenmodellen
- ♦ Untersuchung der Methodik der Modellierung und Vorhersage von Echtzeitreihen
- ♦ Bestimmung von univariaten Modellen einschließlich Ausreißern
- ♦ Anwendung dynamischer Regressionsmodelle und der Methodik zur Erstellung solcher Modelle aus beobachteten Reihen
- ♦ Spektralanalyse von univariaten Zeitreihen sowie die Grundlagen der periodogrammbasierten Inferenz und deren Interpretation
- ♦ Schätzung der Wahrscheinlichkeit und des Trends einer Zeitreihe für einen bestimmten Zeithorizont

### **Modul 28. Design und Entwicklung von intelligenten Systemen**

- ♦ Den Übergang von Informationen zu Wissen analysieren
- ♦ Entwicklung der verschiedenen Arten von Techniken des maschinellen Lernens
- ♦ Untersuchung von Metriken und Scores zur Quantifizierung der Qualität von Modellen
- ♦ Implementierung der verschiedenen Algorithmen für maschinelles Lernen
- ♦ Probabilistische Argumentationsmodelle identifizieren
- ♦ Die Grundlagen des Deep Learning legen
- ♦ Demonstration der erworbenen Fähigkeiten, um die verschiedenen Algorithmen des maschinellen Lernens zu verstehen

### **Modul 29. Datenintensive Architekturen und Systeme**

- ♦ Anforderungen für datenintensive Systeme festlegen
- ♦ Untersuchung verschiedener Datenmodelle und Analyse von Datenbanken
- ♦ Analyse der wichtigsten Funktionen für verteilte Systeme und ihrer Bedeutung in verschiedenen Systemtypen
- ♦ Bewertung, welche weit verbreiteten Anwendungen die Grundlagen verteilter Systeme nutzen, um ihre Systeme zu gestalten
- ♦ Analyse, wie Datenbanken Informationen speichern und abrufen
- ♦ Die verschiedenen Replikationsmodelle und die damit verbundenen Probleme identifizieren
- ♦ Entwicklung von Möglichkeiten der Partitionierung und verteilten Transaktionen
- ♦ Identifizierung von Batch-Systemen und (nahezu) Echtzeit-Systemen

### Modul 30. Praktische Anwendung von Data Science in Geschäftsbereichen

- ◆ Analyse des Stands der Technik bei Künstlicher Intelligenz (KI) und Datenanalyse
- ◆ Entwicklung von Fachwissen über die am häufigsten verwendeten Technologien
- ◆ Ein besseres Verständnis der Technologie durch Anwendungsfälle schaffen
- ◆ Analyse der gewählten Strategien zur Auswahl der besten Technologien für die Implementierung
- ◆ Anwendungsbereiche festlegen
- ◆ Untersuchung der tatsächlichen und potenziellen Risiken der angewandten Technologie
- ◆ Vorschläge zu den Vorteilen, die sich aus der Nutzung ergeben
- ◆ Identifizierung von Zukunftstrends in bestimmten Sektoren

“

*Erzielen Sie Spitzenleistungen, indem Sie ein Programm studieren, das Sie in die Lage versetzt, spezialisierte Kenntnisse in Informatik, Cybersicherheit und Datenanalyse zu erwerben"*

# 03

# Kompetenzen

Nach Bestehen der Prüfungen in diesem Programm haben die Informatiker die notwendigen Fähigkeiten erworben, um die grundlegenden Prinzipien der Informatik zu verstehen und mit Programmiersprachen und Daten zu arbeiten. So können sie ihre tägliche Arbeit in diesem Spezialgebiet verbessern und bei Entscheidungen, die sich auf das Funktionieren der Abteilungen eines Unternehmens auswirken, wertvolles Wissen einbringen.



“

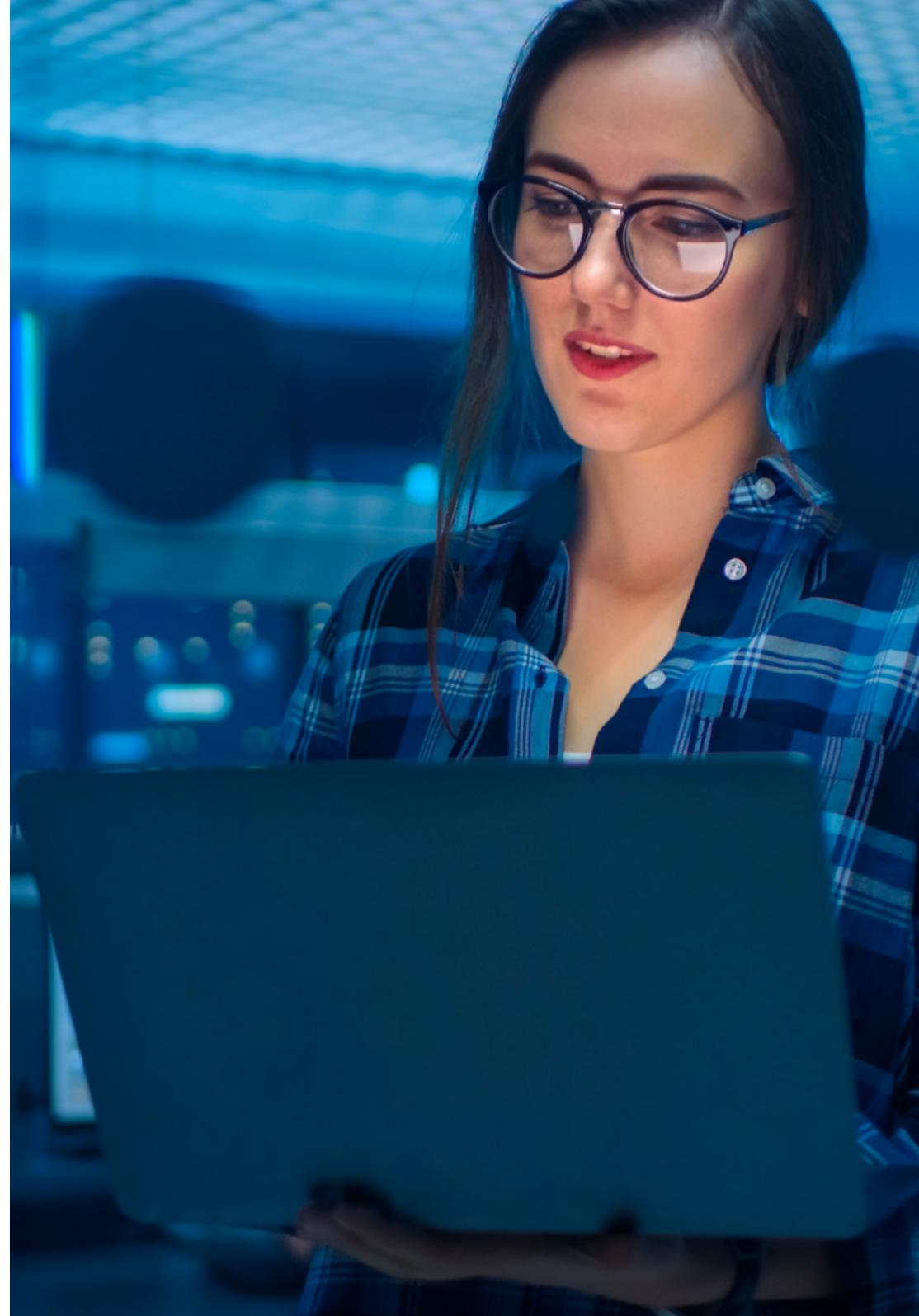
*Erwerben Sie die notwendigen Fähigkeiten, um Ihren Beruf auf das höchste Niveau zu bringen, dank dieses weiterbildenden Masterstudiengangs, der es Ihnen ermöglichen wird, sich zu aktualisieren und an die neue IT-Umgebung anzupassen"*



## Allgemeine Kompetenzen

---

- ◆ Korrektes Ausführen von Aufgaben im Zusammenhang mit Computern und Computersprachen
- ◆ Anwendung der am besten geeigneten Sicherheitsmaßnahmen in Abhängigkeit von den Bedrohungen
- ◆ Festlegung der Sicherheitspolitik und des Sicherheitsplans eines Unternehmens für Informationssysteme und Vervollständigung des Entwurfs und der Umsetzung des Notfallplans
- ◆ Erstellung eines Audit-Programms, das den Selbstbewertungsbedarf der Organisation in Bezug auf die Cybersicherheit abdeckt
- ◆ Entwicklung eines Programms zum Scannen und Überwachen von Schwachstellen und eines Plans zur Reaktion auf Cyber-Sicherheitsvorfälle
- ◆ Maximierung der sich bietenden Chancen und Eliminierung aller potenziellen Risiken durch Design
- ◆ Schlüsselverwaltungssysteme zusammenstellen
- ◆ Bewertung der Informationssicherheit eines Unternehmens
- ◆ Analyse der Systeme für den Informationszugang
- ◆ Entwicklung von Best Practices für die sichere Entwicklung
- ◆ Darstellung der Risiken, die Unternehmen eingehen, wenn sie nicht über eine sichere Informationssicherheitsumgebung verfügen
- ◆ Entwicklung einer technischen und geschäftlichen Perspektive der Datenanalyse
- ◆ Die neuesten Algorithmen, Plattformen und Tools zur Erkundung, Visualisierung, Manipulation, Verarbeitung und Analyse von Daten verstehen
- ◆ Implementierung einer für die Wertschöpfung notwendigen Geschäftsvision als Schlüsselement für die Entscheidungsfindung
- ◆ In der Lage sein, spezifische Probleme der Datenanalyse zu lösen





## Spezifische Kompetenzen

---

- ◆ Algorithmen entwerfen, um Computerprogramme zu entwickeln und die Programmiersprache anzuwenden
- ◆ Computerdatenstruktur verstehen und verwenden
- ◆ Algorithmen verwenden, die zur Lösung von Computerproblemen benötigt werden
- ◆ Gründliches Verständnis von fortgeschrittenem Algorithmusdesign und Suchmethoden
- ◆ Durchführung von Computerprogrammieraufgaben
- ◆ Verstehen und Anwenden der Theorie hinter der Informatik, wie z.B. der Mathematik
- ◆ Die Theorie der Automaten kennen und die Computersprache anwenden
- ◆ Verstehen der theoretischen Grundlagen von Programmiersprachen und der damit verbundenen lexikalischen, syntaktischen und semantischen Verarbeitungstechniken
- ◆ Die grundlegenden Konzepte der Mathematik und der rechnerischen Komplexität verstehen, um sie bei der Lösung von Computerproblemen anzuwenden
- ◆ Die grundlegenden Prinzipien des Rechnens kennen und anwenden, um neue Entwicklungen in der Informatik durchzuführen
- ◆ Entwicklung eines Informationssicherheits-Managementsystems (ISMS)
- ◆ Identifizierung der Schlüsselemente, aus denen ein ISMS besteht
- ◆ Anwendung der MAGERIT Methodik, um das Modell weiterzuentwickeln und einen Schritt weiter zu gehen
- ◆ Entwicklung neuer Risikomanagement-Methoden auf der Grundlage des Konzepts des *Agile Risk Management*
- ◆ Identifizierung, Analyse, Bewertung und Behandlung der Risiken, mit denen die Fachleute konfrontiert sind, aus einer neuen Geschäftsperspektive auf der Grundlage eines *Risk-Driven* oder risikoorientierten Modells, das es nicht nur ermöglicht, in seinem eigenen Umfeld zu überleben, sondern auch seinen eigenen Wertbeitrag zu steigern
- ◆ Untersuchung des Prozesses der Entwicklung einer Sicherheitsstrategie bei der Bereitstellung von *Cloud*-Diensten für Unternehmen
- ◆ Bewertung der Unterschiede in den spezifischen Implementierungen der verschiedenen *Public Cloud*-Anbieter
- ◆ Bewertung der IoT-Konnektivitätsoptionen für ein Projekt, mit Schwerpunkt auf LPWAN-Technologien
- ◆ Einführung in die grundlegenden Spezifikationen der wichtigsten LPWAN-Technologien für das IoT
- ◆ Spezialisierung auf *Data Science* aus technischer und geschäftlicher Sicht
- ◆ Visualisierung von Daten auf die am besten geeignete Weise, um die gemeinsame Nutzung und das Verständnis durch verschiedene Profile zu unterstützen
- ◆ Die wichtigsten Funktionsbereiche des Unternehmens, in denen *Data Science* den größten Nutzen bringen kann, ansprechen
- ◆ Entwicklung des Datenlebenszyklus, seiner Typologie und der für seine Verwaltung erforderlichen Technologien und Phasen
- ◆ Verarbeitung und Manipulation von Daten mit speziellen Sprachen und Bibliotheken
- ◆ Entwicklung fortgeschrittener Kenntnisse in den grundlegenden *Data-Mining*-Techniken für Datenauswahl, Vorverarbeitung und Datentransformation
- ◆ Spezialisierung auf die wichtigsten Algorithmen des *Machine Learning* zur Extraktion von verborgenem Wissen in Daten
- ◆ Fachwissen über die Software-Architekturen und -Systeme, die für die datenintensive Nutzung von Daten erforderlich sind, generieren
- ◆ Bestimmung, wie das IoT eine Quelle für die Erzeugung von Daten und Schlüsselinformationen sein kann, auf die *Data Science* zur Wissensextraktion angewendet werden kann
- ◆ Analyse der verschiedenen Möglichkeiten der Anwendung von *Data Science* in verschiedenen Sektoren oder Branchen anhand von Beispielen aus der Praxis

# 04 Kursleitung

Um das Gebiet der Informatik, Cybersicherheit und Datenanalyse erfolgreich anzugehen, ist ein vollständiges und detailliertes Studium erforderlich. Aus diesem Grund hat TECH die besten, auf die einzelnen Bereiche spezialisierten Dozenten zusammengebracht. So wird der Informatiker von renommierten Fachleuten begleitet, die ihre jahrelange Erfahrung und Ausbildung einbringen. Auf diese Weise können Informatiker sicher sein, aktuelle und spezifische Kenntnisse über einen Sektor zu erhalten, der auf internationaler Ebene boomt.



“

*Sie werden von einem Dozententeam begleitet und betreut, das auf dem neuesten Stand der Entwicklungen in den Bereichen Cybersicherheit und Datenanalyse ist“*

## Internationaler Gastdirektor

Dr. Jeremy Gibbons gilt als **internationale Eminenz** für seine Beiträge im Bereich der **Programmiermethodik** und ihrer Anwendungen im **Software Engineering**. Seit mehr als zwei Jahrzehnten treibt dieser mit dem Fachbereich Informatik der Universität von Oxford verbundene Experte verschiedene **Entwicklungsprojekte** voran, deren greifbarste Ergebnisse von Informatikern in verschiedenen Teilen der Welt angewendet werden.

Seine Arbeit umfasst Bereiche wie **generische Programmierung**, formale Methoden, computergestützte Biologie, Bioinformatik und Algorithmenentwurf mit Haskell. Letzteres wurde in Zusammenarbeit mit seinem Mentor, Dr. Richard Bird, umfassend entwickelt.

In seiner Funktion als **Direktor der Programmieralgebra-Forschungsgruppe** hat Gibbons die Fortschritte bei den **funktionalen Programmiersprachen** und der **Mustertheorie in der Programmierung** vorangetrieben. Gleichzeitig wurden Anwendungen seiner Innovationen mit dem Gesundheitswesen in Verbindung gebracht, wie seine Zusammenarbeit mit **CancerGrid** und **Datatype Generic Programming** beweist. Diese und andere Initiativen wiederum spiegeln sein Interesse an der Lösung praktischer Probleme in der **Krebsforschung** und der **klinischen Informatik** wider.

Gibbons hat sich auch als **Chefredakteur** von **wissenschaftlichen Veröffentlichungen** in The Journal of Functional Programming und The Programming Journal: The Art, Science, and Engineering of Programming einen Namen gemacht. Im Rahmen dieser Aufgaben hat er sich intensiv um die **Verbreitung von Wissen** gekümmert. Darüber hinaus hatte er mehrere Lehrstühle inne, die mit renommierten Einrichtungen wie der Universität Oxford Brookes und der Universität von Auckland, Neuseeland, verbunden sind.

Darüber hinaus ist dieser Spezialist Mitglied der Arbeitsgruppe 2.1 über Algorithmische Sprachen und Berechnungen der **International Federation for Information Processing (IFIP)**. Bei dieser Organisation ist er für die Wartung der Programmiersprachen ALGOL 60 und ALGOL 68 zuständig.



## Dr. Gibbons, Jeremy

---

- Direktor des Software-Engineering-Programms an der Universität von Oxford, UK
- Stellvertretender Leiter des Informatiklabors und der Fakultät für Informatik, Universität von Oxford
- Professor am Kellogg College, an der Universität Oxford Brookes und an der Universität von Auckland in Neuseeland
- Direktor der Forschungsgruppe Programmieralgebra
- Redakteur und Chef der Zeitschriften The Art, Science, and Engineering of Programming und Journal of Functional Programming
- Promotion in Computerwissenschaften an der Universität von Oxford
- Masterstudiengang in Informatik an der Universität von Edinburgh
- Mitglied von: Internationale Föderation für Informationsverarbeitung (IFIP) Arbeitsgruppe 2.1 über Algorithmische Sprachen und Berechnungen (WG2.1)



*Dank TECH werden Sie mit den besten Fachleuten der Welt lernen können"*

## Kursleitung



### Dr. Peralta Martín-Palomino, Arturo

- ♦ CEO und CTO bei Prometheus Global Solutions
- ♦ CTO bei Korporate Technologies
- ♦ CTO bei AI Shephers GmbH
- ♦ Promotion in technischer Informatik an der Universität von Castilla la Mancha
- ♦ Promotion in Wirtschaftswissenschaften, Unternehmen und Finanzen an der Universität Camilo José Cela Außerordentlicher Promotionspreis
- ♦ Doktor der Psychologie an der Universität von Castilla la Mancha
- ♦ Masterstudiengang in fortgeschrittenen Informationstechnologien von der Universität von Castilla la Mancha
- ♦ Masterstudiengang MBA+E (Master in Business Administration and Organisational Engineering) an der Universität von Castilla la Mancha
- ♦ Außerordentlicher Professor, der an der Universität von Castilla la Mancha Bachelor- und Masterstudiengänge in Computertechnik unterrichtet
- ♦ Professor für den Masterstudiengang in Big Data und Datenwissenschaft an der Internationalen Universität von Valencia
- ♦ Professor für den Masterstudiengang in Industrie 4.0 und den Masterstudiengang in Industriedesign und Produktentwicklung
- ♦ Mitglied der SMILe-Forschungsgruppe der Universität von Castilla la Mancha



### Hr. Olalla Bonal, Martín

- Technischer Spezialist in *Blockchain* bei IBM SPGI
- Technischer Vertriebsspezialist für *Blockchain*. IBM
- Direktor für Architektur *Blocknitive*
- Techniker für digitale Elektronik
- *Blockchain Architekt -IT Infrastruktur Architekt - IT Projektmanager* Geschäftsbereiche: Software, Infrastruktur, Telekommunikation

## Professoren

### Hr. Tobal Redondo, Javier

- ♦ Manager des HUAWEI-Anwendungsinnovationsprogramms
- ♦ Leitung der Abteilung Informationssicherheit der Abteilung Zahlungsmittel Amadeus IT Group
- ♦ Leitung der Abteilung Informationssicherheit FINTONIC, Finanzdienstleistungen
- ♦ Serviceingenieur und Architekt im Bereich Planung und Architektur von Diensten und Sicherheit bei Amena / Orange Spanien
- ♦ Hochschulabschluss in Informatik an der Universität von Deusto (Bilbao, Spanien)
- ♦ Postgraduiertenabschluss in Industrieinformatik Hochschule für Wirtschaftsingenieurwesen Bilbao

### Hr. Gonzalo Alonso, Félix

- ♦ Generaldirektor und Gründer Smart REM Solutions
- ♦ Gründungspartner und Leitung von Risk Engineering und Innovation Dynargy
- ♦ Geschäftsführender Direktor und Gründungspartner Risknova (Spezialisiertes Sachverständigenbüro für Technologie)
- ♦ Hochschulabschluss in Ingenieurwesen für industrielle Organisation an der Pontificaluniversität von Comillas ICAI
- ♦ Hochschulabschluss in Industrietechnik, Spezialisierung auf Industrieelektronik, Pontificaluniversität von Comillas ICAI
- ♦ Masterstudiengang in Versicherungsmanagement von ICEA (Institut für die Zusammenarbeit von Versicherungsgesellschaften)

#### **Hr. Sevillano Izquierdo, Javier**

- ◆ Globaler Architekt für Cybersicherheit bei Vodafone Spanien
- ◆ Chief Technology Security Office (CTSO) bei Vodafone Spanien
- ◆ Verantwortlich für technologische Sicherheit bei Bankia
- ◆ Verantwortlich für technologische Sicherheit bei Caja Madrid
- ◆ Sicherheitsmanager bei Sistema 4B
- ◆ SEINCA - Senior Analyst
- ◆ Höherer Techniker für Wirtschaftsinformatik bei Instituto Cibernos

#### **Hr. Entrenas, Alejandro**

- ◆ Entelgy Innotec
- ◆ Hochschulabschluss in Technischem Ingenieurwesen im Bereich Computersysteme an der Universität von Cordoba
- ◆ Masterstudiengang in Informationssicherheitsmanagement von der Polytechnischen Universität Madrid

#### **Hr. Nogales Ávila, Javier**

- ◆ Enterprise Cloud and sourcing senior consultant Quint
- ◆ Cloud and Technology Consultant Indra
- ◆ Associate Technology Consultant Accenture
- ◆ Hochschulabschluss an der Universität von Jaén und der University of Technology and Economics of Budapest (BME)
- ◆ Hochschulabschluss in Ingenieurwesen für industrielle Organisation

#### **Hr. Gómez Rodríguez, Antonio**

- ◆ Ingenieur für Cloud-Lösungen bei Oracle
- ◆ Projektleitung bei der Sopra-Gruppe
- ◆ Projektleitung bei Everis
- ◆ Projektleitung bei der öffentlichen Gesellschaft für die Verwaltung von Kulturprogrammen im andalusischen Kulturministerium
- ◆ Analyst für Informationssysteme bei der Sopra-Gruppe
- ◆ Hochschulabschluss in Telekommunikationstechnik an der Polytechnischen Universität von Katalonien
- ◆ Postgraduiertenabschluss in Informationstechnologien und -systemen vom Katalanischen Institut für Technologie
- ◆ *E-Business* Masterstudiengang der La Salle Wirtschaftsschule

#### **Hr. del Valle Arias, Jorge**

- ◆ Leitung der IoT-Abteilung bei Diode Spanien
- ◆ Smart Cities Business Growth Manager Spain in Itron Inc
- ◆ IoT-Berater
- ◆ Vertriebsleitung IoT & Cellular bei Aicox Soluciones
- ◆ Gründung und CEO von Sensor Intelligence
- ◆ Betriebsleitung bei Codium Networks
- ◆ Bereichsleitung Elektronik bei Aitemin
- ◆ Ingenieur für Telekommunikation von der Polytechnischen Universität von Madrid
- ◆ Executive MBA von der International Graduate School von La Salle in Madrid

**Hr. Gozalo Fernández, Juan Luis**

- ◆ Computer-Ingenieur
- ◆ Außerordentlicher Professor für DevOps und Blockchain am UNIR
- ◆ Ehemaliger Blockchain DevOps Direktor bei Alastria
- ◆ Manager für die Entwicklung mobiler Anwendungen Tinkerlink bei Cronos Telecom
- ◆ IT-Direktor bei Banco Santander
- ◆ Technischer Direktor für IT-Service-Management bei Barclays Bank Spanien
- ◆ Hochschulabschluss in Computertechnik von der Nationalen Universität für Bildung und Fernunterricht (UNED)

**Fr. Jurado Jabonero, Lorena**

- ◆ Leitung der Informationssicherheit (CISO) bei Grupo Pascual
- ◆ Hochschulabschluss in Computertechnik an der Universität Alfonso X El Sabio
- ◆ Technische Ingenieurin in Computer Management von der Polytechnischen Universität von Madrid
- ◆ Kenntnisse: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, usw.

**Hr. Armero Fernández, Rafael**

- ◆ Business Intelligence Consultant bei SDG Group
- ◆ Digital Engineer bei Mi-GSO
- ◆ Logistic Engineer bei Torrecid S.A
- ◆ Quality Intern bei INDRA
- ◆ Hochschulabschluss in Luft- und Raumfahrttechnik an der Polytechnischen Universität von Valencia
- ◆ Masterstudiengang in Professional Development 4.0 von der Universität Alcalá de Henares

**Hr. Peris Morillo, Luis Javier**

- ◆ Technical Lead bei Capitele Consulting. Er leitet ein Team bei Inditex in der Logistikeinheit seiner offenen Plattform
- ◆ Senior Technical Lead und Delivery Lead Support bei HCL
- ◆ Agile Coach und Leiter des operativen Geschäfts bei Mirai Advisory
- ◆ Mitglied des Leitungsausschusses als Chief Operating Officer
- ◆ Entwickler, Team Lead, Scrum Masterstudiengang, Agile Coach, Produkt Manager bei DocPath
- ◆ Höhere Ingenieurausbildung in Informatik an der ESI von Ciudad Real (UCLM)
- ◆ Nachdiplomstudium in Projektmanagement von CEOE - Confederación Española de Organizaciones Empresariales (Spanischer Verband der Unternehmensorganisationen)
- ◆ 50+ MOOCs, die von renommierten Universitäten wie der Stanford University, der Michigan University, der Yonsei University der Polytechnischen Universität Madrid, etc. angeboten werden.
- ◆ Verschiedene Zertifizierungen, einige der bemerkenswertesten oder neuesten sind Azure Fundamentals

**Fr. Pedrajas Parabás, Elena**

- ◆ Business Analyst bei Management Solutions in Madrid
- ◆ Forscherin in der Abteilung für Informatik und numerische Analyse an der Universität von Cordoba
- ◆ Forscherin am Singular Centre for Research in Intelligent Technologies in Santiago de Compostela
- ◆ Hochschulabschluss in Computertechnik Masterstudiengang in Datenwissenschaft Computertechnik

### Hr. Montoro Montarroso, Andrés

- ◆ Forscher in der SMILe-Gruppe an der Universität von Castilla La Mancha
- ◆ Datenwissenschaftler bei Prometheus Global Solutions
- ◆ Abschluss in Computertechnik an der Universität von Kastilien-La Mancha
- ◆ Masterstudiengang in Datenwissenschaft und Computertechnik an der Universität Granada
- ◆ Gastprofessor für das Fach Wissensbasierte Systeme an der Hochschule für Informatik in Ciudad Real, der die Vorlesung hält: "Fortgeschrittene Techniken der künstlichen Intelligenz: Suche und Analyse potenzieller Radikaler in den sozialen Medien"
- ◆ Gastprofessor für das Fach Data Mining an der Hochschule für Informatik in Ciudad Real, der die Vorlesung hält: "Anwendungen der Verarbeitung natürlicher Sprache: Fuzzy Logic zur Analyse von Nachrichten in sozialen Netzwerken"
- ◆ Referent auf dem Seminar über Korruptionsprävention in öffentlichen Verwaltungen und künstliche Intelligenz. Fakultät für Rechts- und Sozialwissenschaften von Toledo. Konferenz mit dem Titel "Techniken der künstlichen Intelligenz". Referent auf dem ersten internationalen Seminar über Verwaltungsrecht und künstliche Intelligenz (DAIA), organisiert von dem Europäischen Studienzentrum (Centro de Estudios Europeos Luis Ortega Álvarez) und dem Forschungsinstitut (Institut de Recerca TransJus). Konferenz mit dem Titel "Analyse von Gefühlen zur Verhinderung von Hassreden in sozialen Medien"

### Hr. Fondón Alcalde, Rubén

- ◆ Business Analyst für das KMU-Segment bei Vodafone Spanien
- ◆ Business Analyst für Südeuropa bei Vodafone Global Enterprise
- ◆ Senior Process Consultant bei Unisys für Telefónica Global Solutions
- ◆ Service Integration Leader bei Entelgy für Telefónica Global Solutions
- ◆ Hochschulabschluss in Telekommunikationstechnik an der Europäischen Universität Madrid
- ◆ Masterstudiengang in *Big Data* und Analytics an der Internationalen Universität von Valencia

### Fr. Fernández Meléndez, Galina

- ◆ Datenanalytikerin bei ADN Mobile Solution
- ◆ ETL-Prozesse, Data Mining, Datenanalyse und -visualisierung, Erstellung von KPIs, Entwurf und Implementierung von Dashboards, Managementkontrolle R-Entwicklung, SQL-Verwaltung und andere
- ◆ Musterbestimmung, prädiktive Modellierung, maschinelles Lernen
- ◆ Hochschulabschluss in Betriebswirtschaftslehre. Universität Bicentenario von Aragua-Caracas
- ◆ Universitätskurs in Planung und öffentlichen Finanzen Venezolanische Schule für Planung - Schule für Finanzen
- ◆ Masterstudiengang in Datenanalyse und Business Intelligence. Universität von Oviedo
- ◆ MBA en Administración y Dirección De Empresas (Europäische Wirtschaftshochschule Barcelona)
- ◆ Masterstudiengang in Big Data und Business Intelligence (Europäische Wirtschaftshochschule Barcelona)

**Hr. Díaz Díaz-Chirón, Tobías**

- ◆ Forscher im ArCO-Labor der Universität von Castilla La Mancha, einer Gruppe, die sich mit Projekten im Zusammenhang mit Computerarchitekturen und -netzen befasst
- ◆ Berater bei Blue Telecom, einem Unternehmen, das sich auf den Telekommunikationssektor spezialisiert hat
- ◆ Hochschulabschluss in Fortgeschrittenenkurs in Computertechnik an der Universität von Kastilien-La Mancha

**Fr. Martínez Cerrato, Yésica**

- ◆ Technikerin für elektronische Sicherheitsprodukte bei Securitas Seguridad Spanien
- ◆ Business Intelligence-Analyst bei Ricopia Technologies
- ◆ Verantwortlich für die Schulung neuer Mitarbeiter in Vertriebsmanagement-Software (CRM, ERP, INTRANET), Produkte und Verfahren bei Ricopia Technologies (Alcalá de Henares)
- ◆ Verantwortlich für Schulung neuer Stipendiaten, die in die Computer-Klassen integriert werden an der Universität von Alcalá
- ◆ Projektmanagerin im Bereich Großkundenintegration bei Correos y Telégrafos (Madrid)
- ◆ Dozentin für Computerkurse bei ASALUMA Association
- ◆ IT-Technik - Verantwortlich für die OTEC-Computerräume an der Universität von Alcalá
- ◆ Hochschulabschluss in elektronischer Kommunikationstechnik an der Polytechnischen Hochschule der Universität von Alcalá
- ◆ Spezialisierungsstipendium als Computertechniker in OTEC von der Universität von Alcalá

**Hr. Tato Sánchez, Rafael**

- ◆ Projektmanagement INDRA SISTEMAS S.A.
- ◆ Technischer Direktor INDRA SISTEMAS S.A.
- ◆ Systemingenieur ENA TRÁFICO S.A.U.
- ◆ IFCD048PO: Management Methoden und Software-Projektentwicklung mit SCRUM
- ◆ Coursera: Machine Learning
- ◆ Udey: Deep Learning A-Z. Hands-on Artificial Neural Networks
- ◆ Coursera: IBM: Fundamentals of Scalable Data Science
- ◆ Coursera: IBM: Applied AI with Deep Learning
- ◆ Coursera: IBM: Advance Machine Learning and Signal Processing
- ◆ Ingenieur für industrielle Elektronik und Automatisierungstechnik an der Europäischen Universität Madrid
- ◆ Masterstudiengang in Wirtschaftsingenieurwesen an der Europäischen Universität Madrid
- ◆ Masterstudiengang in Industrie 4.0 von der Internationalen Universität von La Rioja (UNIR)
- ◆ Berufliche Zertifizierung. SSCE0110: Lehrtätigkeit in der beruflichen Bildung für die Erwerbstätigkeit

# 05 Struktur und Inhalt

Dieser weiterbildende Masterstudiengang vereint eine Reihe von spezialisierten Modulen, die es dem Informatiker ermöglichen, sich mit Aspekten wie der digitalen Identifizierung, Zugangskontrollsystemen, der Architektur der Informationssicherheit, der Struktur des Sicherheitsbereichs, Managementsystemen für die Informationssicherheit in der Kommunikation und im Softwarebetrieb oder der Entwicklung des mit der Sicherheit verbundenen Business Continuity Plans zu beschäftigen. Gleichzeitig werden die vollständigsten und aktuellsten Techniken zur Datenverarbeitung und Wissensextraktion sowohl aus theoretischer als auch aus praktischer Sicht behandelt.



“

*Alle Interessensgebiete, die Sie beherrschen müssen, um erfolgreich in der Informatik zu arbeiten, zusammengefasst in einem hochwertigen Studienplan“*

## Modul 1. Grundlagen der Programmierung

- 1.1. Einführung in die Programmierung
  - 1.1.1. Grundlegende Struktur eines Computers
  - 1.1.2. Software
  - 1.1.3. Programmiersprachen
  - 1.1.4. Lebenszyklus einer Softwareanwendung
- 1.2. Algorithmusentwurf
  - 1.2.1. Lösung von Problemen
  - 1.2.2. Deskriptive Techniken
  - 1.2.3. Elemente und Struktur eines Algorithmus
- 1.3. Elemente eines Programms
  - 1.3.1. Ursprung und Merkmale der Sprache C++
  - 1.3.2. Die Entwicklungsumgebung
  - 1.3.3. Konzept des Programms
  - 1.3.4. Arten von grundlegender Daten
  - 1.3.5. Betreiber
  - 1.3.6. Ausdrücke
  - 1.3.7. Sätze
  - 1.3.8. Dateneingabe und -ausgabe
- 1.4. Kontrollsätze
  - 1.4.1. Sätze
  - 1.4.2. Verzweigungen
  - 1.4.3. Schleifen
- 1.5. Abstraktion und Modularität: Funktionen
  - 1.5.1. Modularer Aufbau
  - 1.5.2. Konzept der Funktion und des Nutzens
  - 1.5.3. Definition einer Funktion
  - 1.5.4. Ausführungsablauf beim Aufruf einer Funktion
  - 1.5.5. Prototyp einer Funktion
  - 1.5.6. Rückgabe der Ergebnisse
  - 1.5.7. Aufrufen einer Funktion: Parameter
  - 1.5.8. Übergabe von Parametern per Referenz und per Wert
  - 1.5.9. Kennung des Geltungsbereichs
- 1.6. Statische Datenstrukturen
  - 1.6.1. *Arrays*
  - 1.6.2. Matrizen, Polyeder
  - 1.6.3. Suchen und Sortieren
  - 1.6.4. Zeichenketten, E/A-Funktionen für Zeichenketten
  - 1.6.5. Strukturen, Verbindungen
  - 1.6.6. Neue Datentypen
- 1.7. Dynamische Datenstrukturen: Zeiger
  - 1.7.1. Konzept, Definition von Zeiger
  - 1.7.2. Operatoren und Operationen mit Zeigern
  - 1.7.3. *Arrays* von Zeigern
  - 1.7.4. Zeiger und *Arrays*
  - 1.7.5. Zeiger auf Zeichenketten
  - 1.7.6. Zeiger auf Strukturen
  - 1.7.7. Multiple Indirektion
  - 1.7.8. Zeiger auf Funktionen
  - 1.7.9. Übergabe von Funktionen, Strukturen und *Arrays* als Funktionsparameter
- 1.8. Dateien
  - 1.8.1. Grundlegende Konzepte
  - 1.8.2. Dateioperationen
  - 1.8.3. Datentypen
  - 1.8.4. Organisation von Dateien
  - 1.8.5. Einführung in C++ Dateien
  - 1.8.6. Handhabung von Dateien
- 1.9. Rekursion
  - 1.9.1. Definition von Rekursion
  - 1.9.2. Arten der Rekursion
  - 1.9.3. Vorteile und Nachteile
  - 1.9.4. Überlegungen
  - 1.9.5. Rekursiv-iterative Umwandlung
  - 1.9.6. Der Rekursionsstapel

- 1.10. Prüfung und Dokumentation
  - 1.10.1. Programm-Tests
  - 1.10.2. White Box-Tests
  - 1.10.3. Black Box-Tests
  - 1.10.4. Test-Tools
  - 1.10.5. Programm-Dokumentation

## Modul 2. Datenstruktur

- 2.1. Einführung in die Programmierung in C++
  - 2.1.1. Klassen, Konstruktoren, Methoden und Attribute
  - 2.1.2. Variablen
  - 2.1.3. Bedingte Ausdrücke und Schleifen
  - 2.1.4. Objekte
- 2.2. Abstrakte Datentypen (ADT)
  - 2.2.1. Datentypen
  - 2.2.2. Grundlegende Strukturen und ADTs
  - 2.2.3. Vektoren und *Arrays*
- 2.3. Lineare Datenstrukturen
  - 2.3.1. ADT-Liste. Definition
  - 2.3.2. Verknüpfte und doppelt verknüpfte Listen
  - 2.3.3. Geordnete Listen
  - 2.3.4. Listen in C++
  - 2.3.5. ADT-Stapel
  - 2.3.6. ADT-Warteschlange
  - 2.3.7. C++ Stapel und Warteschlange
- 2.4. Hierarchische Datenstrukturen
  - 2.4.1. ADT-Baum
  - 2.4.2. Pfade
  - 2.4.3. n-äre Bäume
  - 2.4.4. Binäre Bäume
  - 2.4.5. Binäre Suchbäume
- 2.5. Hierarchische Datenstrukturen: Komplexe Bäume
  - 2.5.1. Perfekt ausbalancierte oder minimal hohe Bäume
  - 2.5.2. Bäume mit mehreren Pfaden
  - 2.5.3. Bibliografische Referenzen
- 2.6. Heaps und Prioritätswarteschlange
  - 2.6.1. ADT-Heaps
  - 2.6.2. ADT-Prioritätswarteschlange
- 2.7. *Hash*-Tabellen
  - 2.7.1. ADT in *Hash*-Tabellen
  - 2.7.2. *Hash*-Funktionen
  - 2.7.3. *Hash*-Funktion in *Hash*-Tabellen
  - 2.7.4. Redispersion
  - 2.7.5. Offene *Hash*-Tabellen
- 2.8. Graph
  - 2.8.1. ADT-Graph
  - 2.8.2. Arten von Graphen
  - 2.8.3. Grafische Darstellung und Grundoperationen
  - 2.8.4. Graphischer Entwurf
- 2.9. Graph-Algorithmen und fortgeschrittene Graph-Konzepte
  - 2.9.1. Graph Probleme
  - 2.9.2. Pfad-Algorithmen
  - 2.9.3. Such- oder Pfad-Algorithmen
  - 2.9.4. Andere Algorithmen
- 2.10. Andere Datenstrukturen
  - 2.10.1. Sets
  - 2.10.2. Parallele *Arrays*
  - 2.10.3. Symboltabellen
  - 2.10.4. *Tries*

## Modul 3. Algorithmen und Komplexität

- 3.1. Einführung in Algorithmus-Design-Strategien
  - 3.1.1. Rekursion
  - 3.1.2. Aufteilen und erobern
  - 3.1.3. Andere Strategien
- 3.2. Effizienz und Analyse von Algorithmen
  - 3.2.1. Maßnahmen zur Steigerung der Effizienz
  - 3.2.2. Messung der Eingabegröße
  - 3.2.3. Messung der Ausführungszeit
  - 3.2.4. Schlimmster, bester und durchschnittlicher Fall
  - 3.2.5. Asymptotische Notation
  - 3.2.6. Kriterien für die mathematische Analyse von nicht-rekursiven Algorithmen
  - 3.2.7. Mathematische Analyse von rekursiven Algorithmen
  - 3.2.8. Empirische Analyse von Algorithmen
- 3.3. Sortieralgorithmen
  - 3.3.1. Konzept der Sortierung
  - 3.3.2. Blase sortieren
  - 3.3.3. Sortieren nach Auswahl
  - 3.3.4. Reihenfolge der Insertion
  - 3.3.5. *Merge Sort*
  - 3.3.6. *Quicksort*)
- 3.4. Algorithmen mit Bäumen
  - 3.4.1. Konzept des Baumes
  - 3.4.2. Binäre Bäume
  - 3.4.3. Baumpfade
  - 3.4.4. Ausdrücke darstellen
  - 3.4.5. Geordnete binäre Bäume
  - 3.4.6. Ausgeglichene binäre Bäume





- 3.5. Algorithmen mit *Heaps*
  - 3.5.1. *Heaps*
  - 3.5.2. Der *Heapsort*-Algorithmus
  - 3.5.3. Prioritätswarteschlangen
- 3.6. Graph Algorithmen
  - 3.6.1. Vertretung
  - 3.6.2. Lauf in Breite
  - 3.6.3. Lauf in Tiefe
  - 3.6.4. Topologische Anordnung
- 3.7. *Greedy*-Algorithmen
  - 3.7.1. Die *Greedy*-Strategie
  - 3.7.2. Elemente der *Greedy*-Strategie
  - 3.7.3. Währungsumtausch
  - 3.7.4. Das Problem des Reisenden
  - 3.7.5. Problem mit dem Rucksack
- 3.8. Minimale Pfadsuche
  - 3.8.1. Das Problem des minimalen Pfades
  - 3.8.2. Negative Bögen und Zyklen
  - 3.8.3. Dijkstras Algorithmus
- 3.9. *Greedy*-Algorithmen auf Graphen
  - 3.9.1. Der minimal aufspannende Baum
  - 3.9.2. Prims Algorithmus
  - 3.9.3. Kruskals Algorithmus
  - 3.9.4. Komplexitätsanalyse
- 3.10. *Backtracking*
  - 3.10.1. Das *Backtracking*
  - 3.10.2. Alternative Techniken

## Modul 4. Fortgeschrittener Algorithmentwurf

- 4.1. Analyse von rekursiven und Teilen-und-Erobern-Algorithmen
  - 4.1.1. Aufstellen und Lösen von homogenen und nicht-homogenen Rekursionsgleichungen
  - 4.1.2. Überblick über die Strategie des Teilens und Eroberns
- 4.2. Amortisierte Analyse
  - 4.2.1. Aggregierte Analyse
  - 4.2.2. Die Buchhaltungsmethode
  - 4.2.3. Die potenzielle Methode
- 4.3. Dynamische Programmierung und Algorithmen für NP-Probleme
  - 4.3.1. Merkmale der dynamischen Programmierung
  - 4.3.2. Rückverfolgung: backtracking
  - 4.3.3. Verzweigung und Beschneidung
- 4.4. Kombinatorische Optimierung
  - 4.4.1. Problemdarstellung
  - 4.4.2. 1D-Optimierung
- 4.5. Randomisierungsalgorithmen
  - 4.5.1. Beispiele für Randomisierungsalgorithmen
  - 4.5.2. Das Buffonsche Theorem
  - 4.5.3. Monte-Carlo-Algorithmus
  - 4.5.4. Las Vegas Algorithmus
- 4.6. Lokale Suche und Kandidatensuche
  - 4.6.1. *Gradient Ascent*
  - 4.6.2. *Hill Climbing*
  - 4.6.3. *Simulated Annealing*
  - 4.6.4. *Tabu Search*
  - 4.6.5. Suche mit Kandidaten

- 4.7. Formale Überprüfung von Programmen
  - 4.7.1. Spezifikation von funktionalen Abstraktionen
  - 4.7.2. Die Sprache der Logik erster Ordnung
  - 4.7.3. Hoare's formales System
- 4.8. Verifizierung von iterativen Programmen
  - 4.8.1. Regeln des formalen Hoare-Systems
  - 4.8.2. Konzept der invarianten Iterationen
- 4.9. Numerische Methoden
  - 4.9.1. Die Methode der Halbierung
  - 4.9.2. Die Newton-Raphson-Methode
  - 4.9.3. Die Sekantenmethode
- 4.10. Parallele Algorithmen
  - 4.10.1. Parallele binäre Operationen
  - 4.10.2. Parallele Operationen mit Diagrammen
  - 4.10.3. Parallelität in Teilen und Erobern
  - 4.10.4. Parallelität in der dynamischen Programmierung

## Modul 5. Fortgeschrittene Programmierung

- 5.1. Einführung in die objektorientierte Programmierung
  - 5.1.1. Einführung in die objektorientierte Programmierung
  - 5.1.2. Klassen-Design
  - 5.1.3. Einführung in UML für die Modellierung von Problemen
- 5.2. Beziehungen zwischen Klassen
  - 5.2.1. Abstraktion und Vererbung
  - 5.2.2. Fortgeschrittene Konzepte der Vererbung
  - 5.2.3. Polymorphismen
  - 5.2.4. Zusammensetzung und Aggregation

- 5.3. Einführung in Design Patterns für objektorientierte Probleme
  - 5.3.1. Was sind Entwurfsmuster?
  - 5.3.2. *Factory*-Muster
  - 5.3.4. *Singleton*-Muster
  - 5.3.5. *Observer*-Muster
  - 5.3.6. *Composite*-Muster
- 5.4. Ausnahmen
  - 5.4.1. Was sind Ausnahmen?
  - 5.4.2. Abfangen und Behandlung von Ausnahmen
  - 5.4.3. Werfen von Ausnahmen
  - 5.4.4. Erstellung von Ausnahmen
- 5.5. Benutzeroberflächen
  - 5.5.1. Einführung in Qt
  - 5.5.2. Positionierung
  - 5.5.3. Was sind Ereignisse?
  - 5.5.4. Ereignisse: Definition und Erfassung
  - 5.5.5. Entwicklung von Benutzeroberflächen
- 5.6. Einführung in die gleichzeitige Programmierung
  - 5.6.1. Einführung in die gleichzeitige Programmierung
  - 5.6.2. Der Prozess und das Thread-Konzept
  - 5.6.3. Interaktion zwischen Prozessen oder Threads
  - 5.6.4. Threads in C++
  - 5.6.5. Vor- und Nachteile der gleichzeitigen Programmierung
- 5.7. Thread-Verwaltung und Synchronisierung
  - 5.7.1. Lebenszyklus eines Threads
  - 5.7.2. Die Klasse *Thread*
  - 5.7.3. Planung des Threads
  - 5.7.4. Gruppen von Threads
  - 5.7.5. Daemon Threads
  - 5.7.6. Synchronisierung
  - 5.7.7. Verriegelungsmechanismen
  - 5.7.8. Kommunikationsmechanismen
  - 5.7.9. Monitore

- 5.8. Häufige Probleme bei der gleichzeitigen Programmierung
  - 5.8.1. Das Erzeuger-Verbraucher-Problem
  - 5.8.2. Das Problem von Lesern und Schriftstellern
  - 5.8.3. Das Problem mit dem Philosophenproblem
- 5.9. Software-Dokumentation und -Tests
  - 5.9.1. Warum ist es wichtig, Software zu dokumentieren?
  - 5.9.2. Design-Dokumentation
  - 5.9.3. Verwendung von Tools zur Dokumentation
- 5.10. Software-Tests
  - 5.10.1. Einführung in das Testen von Software
  - 5.10.2. Arten von Tests
  - 5.10.3. Einheitstest
  - 5.10.4. Integrationstests
  - 5.10.5. Validierungstest
  - 5.10.6. Systemprüfung

## Modul 6. Theoretische Informatik

- 6.1. Verwendete mathematische Konzepte
  - 6.1.1. Einführung in die Aussagenlogik
  - 6.1.2. Theorie der Beziehungen
  - 6.1.3. Abzählbare und nicht abzählbare Mengen
- 6.2. Formale Sprachen und Grammatiken und Einführung in Turingmaschinen
  - 6.2.1. Formale Sprachen und Grammatiken
  - 6.2.2. Problem der Entscheidung
  - 6.2.3. Die Turingmaschine
- 6.3. Erweiterungen für Turing-Maschinen, eingeschränkte Turing-Maschinen und Computer
  - 6.3.1. Programmiertechniken für Turingmaschinen
  - 6.3.2. Erweiterungen für Turingmaschinen
  - 6.3.3. Eingeschränkte Turingmaschinen
  - 6.3.4. Turingmaschinen und Computer

- 6.4. Unsagbarkeit
  - 6.4.1. Nicht rekursiv aufzählbare Sprache
  - 6.4.2. Ein rekursiv aufzählbares unsagbares Problem
- 6.5. Andere unsagbare Probleme
  - 6.5.1. Unsagbare Probleme für Turingmaschinen
  - 6.5.2. Postkorrespondenz-Problem (PCP)
- 6.6. Unlösbare Probleme
  - 6.6.1. Die Klassen P und NP
  - 6.6.2. Ein NP-komplettes Problem
  - 6.6.3. Problem der eingeschränkten Erfüllbarkeit
  - 6.6.4. Andere NP-komplette Probleme
- 6.7. Co-NP und PS Probleme
  - 6.7.1. Komplementär zu NP-Sprachen
  - 6.7.2. Im Polynomraum lösbare Probleme
  - 6.7.3. Vollständige PS-Probleme
- 6.8. Klassen von randomisierungs-basierten Sprachen
  - 6.8.1. MT-Modell mit Randomisierung
  - 6.8.2. Die Klassen RP und ZPP
  - 6.8.3. Primzahl-Test
  - 6.8.4. Komplexität des Primzahltests
- 6.9. Andere Klassen und Grammatiken
  - 6.9.1. Probabilistische endliche Automaten
  - 6.9.2. Zelluläre Automaten
  - 6.9.3. *McCulloch* und *Pitts* Zellen
  - 6.9.4. Lindenmayer-Grammatiken
- 6.10. Fortgeschrittene Rechensysteme
  - 6.10.1. Berechnung der Membranen: P-Systeme
  - 6.10.2. DNA-Computing
  - 6.10.3. Quantencomputing



## Modul 7. Automatentheorie und formalen Sprachen

- 7.1. Einführung in die Automatentheorie
  - 7.1.1. Warum Automaten-Theorie studieren?
  - 7.1.2. Einführung in formale Beweise
  - 7.1.3. Andere Formen des Nachweises
  - 7.1.4. Mathematische Induktion
  - 7.1.5. Alphabete, Zeichenketten und Sprachen
- 7.2. Deterministische endliche Automaten
  - 7.2.1. Einführung in endliche Automaten
  - 7.2.2. Deterministische endliche Automaten
- 7.3. Nicht-deterministische endliche Automaten
  - 7.3.1. Nicht-deterministische endliche Automaten
  - 7.3.2. Äquivalenz zwischen AFD und AFND
  - 7.3.3. Endliche Automaten mit Übergängen  $\epsilon$
- 7.4. Sprachen und reguläre Begriffe (I)
  - 7.4.1. Sprachen und reguläre Begriffe
  - 7.4.2. Endliche Automaten und reguläre Begriffe
- 7.5. Sprachen und reguläre Begriffe (II)
  - 7.5.1. Umwandlung von regulären Begriffen in Automaten
  - 7.5.2. Anwendungen von regulären Begriffen
  - 7.5.3. Algebra der regulären Begriffe
- 7.6. Pumping-Lemma und Abschluss von regulären Sprachen
  - 7.6.1. Pumping-Lemma
  - 7.6.2. Abschlusseigenschaften von regulären Sprachen
- 7.7. Äquivalenz und Minimierung von Automaten
  - 7.7.1. FA Äquivalenz
  - 7.7.2. FA Minimierung
- 7.8. Kontextunabhängige Grammatiken (KUG)
  - 7.8.1. Kontextunabhängige Grammatiken
  - 7.8.2. Ableitungsbäume
  - 7.8.3. Anwendungen von KUGs
  - 7.8.4. Mehrdeutigkeit in Grammatiken und Sprachen

- 7.9. Stapelautomaten und KUG
  - 7.9.1. Definition von Stapelautomaten
  - 7.9.2. Von einem Stapelautomaten akzeptierte Sprachen
  - 7.9.3. Äquivalenz zwischen Stapelautomaten und KUG
  - 7.9.4. Deterministische gestapelte Automaten
- 7.10. Normalformen, Pump-Lemma von KUGs und Eigenschaften von LICs
  - 7.10.1. Normale Formen von KUGs
  - 7.10.2. Pumping-Lemma
  - 7.10.3. Abschlusseigenschaften von regulären Sprachen
  - 7.10.4. Entscheidungseigenschaften von LICs

## Modul 8. Sprachprozessoren

- 8.1. Einführung in den Kompilierungsprozess
  - 8.1.1. Zusammenstellung und Interpretation
  - 8.1.2. Compiler-Ausführungsumgebung
  - 8.1.3. Analyse-Prozess
  - 8.1.4. Prozess der Synthese
- 8.2. Lexikalischer Analysator
  - 8.2.1. Was ist ein lexikalischer Analysator?
  - 8.2.2. Implementierung des lexikalischen Analysators
  - 8.2.3. Semantische Aktionen
  - 8.2.4. Fehlerbehebung
  - 8.2.5. Fragen der Implementierung
- 8.3. Parsing
  - 8.3.1. Was ist ein Parser?
  - 8.3.2. Vorläufige Konzepte
  - 8.3.3. Top-down-Parser
  - 8.3.4. Bottom-up-Analysatoren
- 8.4. Top-down-Parsing und Bottom-up-Parsing
  - 8.4.1. LL-Parser(1)
  - 8.4.2. LR-Parser(0)
  - 8.4.3. Beispiel für einen Parser
- 8.5. Erweitertes Bottom-up-Parsing
  - 8.5.1. SLR-Parser
  - 8.5.2. LR-Parser (1)
  - 8.5.3. LR-Parser (k)
  - 8.5.4. LALR-Parser
- 8.6. Semantische Analyse (I)
  - 8.6.1. Syntaxgesteuerte Übersetzung
  - 8.6.2. Symboltabelle
- 8.7. Semantische Analyse (II)
  - 8.7.1. Typenprüfung
  - 8.7.2. Das Subsystem Typ
  - 8.7.3. Typ-Äquivalenz und Konvertierungen
- 8.8. Codegenerierung und Ausführungsumgebung
  - 8.8.1. Design-Aspekte
  - 8.8.2. Ausführungsumgebung
  - 8.8.3. Speicherorganisation
  - 8.8.4. Speicherzuweisung
- 8.9. Zwischencodegenerierung
  - 8.9.1. Synthesegesteuerte Übersetzung
  - 8.9.2. Zwischendarstellungen
  - 8.9.3. Beispiele für Übersetzungen
- 8.10. Code-Optimierung
  - 8.10.1. Register Zuweisung
  - 8.10.2. Eliminierung toter Zuweisungen
  - 8.10.3. Ausführung zur Kompilierzeit
  - 8.10.4. Neuordnung von Ausdrücken
  - 8.10.5. Schleifen-Optimierung

**Modul 9. Computergrafik und Visualisierung**

- 9.1. Farbtheorie
  - 9.1.1. Eigenschaften von Licht
  - 9.1.2. Farbige Modelle
  - 9.1.3. Der CIE-Standard
  - 9.1.4. *Profiling*
- 9.2. Ausgabe-Primitive
  - 9.2.1. Der Videotreiber
  - 9.2.2. Algorithmen zum Zeichnen von Linien
  - 9.2.3. Algorithmen zum Zeichnen von Kreisen
  - 9.2.4. Algorithmen zum Füllen
- 9.3. 2D-Transformationen und 2D-Koordinatensysteme und 2D-Clipping
  - 9.3.1. Geometrische Grundtransformationen
  - 9.3.2. Homogene Koordinaten
  - 9.3.3. Inverse Transformation
  - 9.3.4. Komposition von Transformationen
  - 9.3.5. Andere Transformationen
  - 9.3.6. Koordinate ändern
  - 9.3.7. 2D-Koordinatensysteme
  - 9.3.8. Koordinatenverschiebung
  - 9.3.9. Normalisierung
  - 9.3.10. Algorithmen zum Trimmen
- 9.4. 3D-Transformationen
  - 9.4.1. Übertragung
  - 9.4.2. Rotation
  - 9.4.3. Skalierung
  - 9.4.4. Reflexion
  - 9.4.5. Scheren
- 9.5. Anzeige und Änderung von 3D-Koordinaten
  - 9.5.1. 3D-Koordinatensysteme
  - 9.5.2. Visualisierung
  - 9.5.3. Änderung koordinieren
  - 9.5.4. Projektion und Normalisierung
- 9.6. Projektion und 3D-Clipping
  - 9.6.1. Orthogonale Projektion
  - 9.6.2. Schräge Parallelprojektion
  - 9.6.3. Perspektivische Projektion
  - 9.6.4. 3D-Beschneidungsalgorithmen
- 9.7. Entfernen von verdeckten Flächen
  - 9.7.1. *Entfernung des Rückseitengesichts*
  - 9.7.2. *Z-Buffer*
  - 9.7.3. Algorithmus des Malers
  - 9.7.4. Warnock-Algorithmus
  - 9.7.5. Erkennung verdeckter Linien
- 9.8. Interpolation und parametrische Kurven
  - 9.8.1. Interpolation und polynomielle Approximation
  - 9.8.2. Parametrische Darstellung
  - 9.8.3. Lagrange-Polynom
  - 9.8.4. Natürliche kubische *Splines*
  - 9.8.5. Basis-Funktionen
  - 9.8.6. Matrix-Darstellung
- 9.9. Bézier-Kurven
  - 9.9.1. Algebraische Konstruktion
  - 9.9.2. Matrix-Formular
  - 9.9.3. Zusammensetzung
  - 9.9.4. Geometrische Konstruktion
  - 9.9.5. Algorithmus zum Zeichnen
- 9.10. *B-Splines*
  - 9.10.1. Das Problem der lokalen Kontrolle
  - 9.10.2. Gleichmäßige kubische B-Splines
  - 9.10.3. Basisfunktionen und Kontrollpunkte
  - 9.10.4. Ableitung zum Ursprung und Multiplizität
  - 9.10.5. Matrix-Darstellung
  - 9.10.6. Nicht-einheitliche B-Splines

## Modul 10. Bio-inspiriertes Rechnen

- 10.1. Einführung in das bio-inspirierte Computing
  - 10.1.1. Einführung in das bio-inspirierte Computing
- 10.2. Algorithmen zur sozialen Anpassung
  - 10.2.1. Bio-inspiriertes Rechnen auf der Basis von Ameisenkolonien
  - 10.2.2. Varianten von Ameisenkolonie-Algorithmen
  - 10.2.3. Cloud-basiertes Computing auf Partikelebene
- 10.3. Genetische Algorithmen
  - 10.3.1. Allgemeine Struktur
  - 10.3.2. Implementierungen der wichtigsten Operatoren
- 10.4. Explorations-Ausbeutungsraum-Strategien für genetische Algorithmen
  - 10.4.1. CHC-Algorithmus
  - 10.4.2. Multimodale Probleme
- 10.5. Evolutionäre Berechnungsmodelle (I)
  - 10.5.1. Evolutionäre Strategien
  - 10.5.2. Evolutionäre Programmierung
  - 10.5.3. Algorithmen auf der Grundlage der differentiellen Evolution
- 10.6. Evolutionäre Berechnungsmodelle (II)
  - 10.6.1. Evolutionäre Modelle auf der Grundlage der Schätzung von Verteilungen (EDA)
  - 10.6.2. Genetische Programmierung
- 10.7. Evolutionäre Programmierung angewandt auf Lernprobleme
  - 10.7.1. Regelbasiertes Lernen
  - 10.7.2. Evolutionäre Methoden bei Instanzauswahlproblemen
- 10.8. Multi-Objektive Probleme
  - 10.8.1. Konzept der Dominanz
  - 10.8.2. Anwendung evolutionärer Algorithmen auf multikriterielle Probleme
- 10.9. Neuronale Netze (I)
  - 10.9.1. Einführung in neuronale Netzwerke
  - 10.9.2. Praktisches Beispiel mit neuronalen Netzwerken
- 10.10. Neuronale Netze
  - 10.10.1. Anwendungsbeispiele für neuronale Netze in der medizinischen Forschung
  - 10.10.2. Anwendungsbeispiele für neuronale Netze in der Wirtschaft
  - 10.10.3. Anwendungsfälle für neuronale Netze in der industriellen Bildverarbeitung



## Modul 11. Sicherheit in Design und Entwicklung von Systemen

- 11.1. Informationssysteme
  - 11.1.1. Domains eines Informationssystems
  - 11.1.2. Komponenten eines Informationssystems
  - 11.1.3. Aktivitäten eines Informationssystems
  - 11.1.4. Lebenszyklus eines Informationssystems
  - 11.1.5. Ressourcen eines Informationssystems
- 11.2. Informationssysteme. Typologie
  - 11.2.1. Typen von Informationssystemen
    - 11.2.1.1. Unternehmerisch
    - 11.2.1.2. Strategisch
    - 11.2.1.3. Je nach Anwendungsbereich
    - 11.2.1.4. Spezifisch
  - 11.2.2. Informationssysteme. Beispiele aus der Praxis
  - 11.2.3. Entwicklung von Informationssystemen: Etappen
  - 11.2.4. Methoden von Informationssystemen
- 11.3. Sicherheit von Informationssystemen. Rechtliche Implikationen
  - 11.3.1. Zugang zu Daten
  - 11.3.2. Sicherheitsbedrohungen: Schwachstellen
  - 11.3.3. Rechtliche Implikationen: Straftaten
  - 11.3.4. Verfahren zur Wartung von Informationssystemen
- 11.4. Sicherheit von Informationssystemen. Sicherheitsprotokolle
  - 11.4.1. Sicherheit von Informationssystemen
    - 11.4.1.1. Integrität
    - 11.4.1.2. Vertraulichkeit
    - 11.4.1.3. Verfügbarkeit
    - 11.4.1.4. Authentifizierung
  - 11.4.2. Sicherheitsdienste
  - 11.4.3. Protokolle zur Informationssicherheit. Typologie
  - 11.4.4. Empfindlichkeit von Informationssystemen
- 11.5. Sicherheit von Informationssystemen. Maßnahmen und Systeme zur Zugangskontrolle
  - 11.5.1. Sicherheitsmaßnahmen
  - 11.5.2. Art der Sicherheitsmaßnahmen
    - 11.5.2.1. Prävention
    - 11.5.2.2. Erkennung
    - 11.5.2.3. Korrektheit
  - 11.5.3. Kontrollsysteme für den Zugang. Typologie
  - 11.5.4. Kryptographie
- 11.6. Netzwerk- und Internetsicherheit
  - 11.6.1. *Firewalls*
  - 11.6.2. Digitale Identifizierung
  - 11.6.3. Viren und Würmer
  - 11.6.4. *Hacking*
  - 11.6.5. Beispiele und reale Fälle
- 11.7. Computerkriminalität
  - 11.7.1. Computerkriminalität
  - 11.7.2. Computerkriminalität. Typologie
  - 11.7.3. Computerkriminalität Angriff. Typologien
  - 11.7.4. Der Fall der virtuellen Realität
  - 11.7.5. Profile von Tätern und Opfern. Typisierung von Verbrechen
  - 11.7.6. Computerkriminalität. Beispiele und reale Fälle
- 11.8. Sicherheitsplan für ein Informationssystem
  - 11.8.1. Sicherheitsplan. Ziele
  - 11.8.2. Sicherheitsplan. Planung
  - 11.8.3. Risikoplan. Analyse
  - 11.8.4. Sicherheitspolitik. Implementierung in der Organisation
  - 11.8.5. Sicherheitsplan. Implementierung in der Organisation
  - 11.8.6. Sicherheitsverfahren. Typen
  - 11.8.7. Sicherheitsplan. Beispiele

- 11.9. Plan für unvorhergesehene Ereignisse
  - 11.9.1. Plan für unvorhergesehene Ereignisse. Funktionen
  - 11.9.2. Notfallplan: Elemente und Ziele
  - 11.9.3. Plan für unvorhergesehene Ereignisse in der Organisation. Implementierung
  - 11.9.4. Plan für unvorhergesehene Ereignisse. Beispiele
- 11.10. Verwaltung der Sicherheit von Informationssystemen
  - 11.10.1. Gesetzliche Bestimmungen
  - 11.10.2. Normen
  - 11.10.3. Zertifizierungen
  - 11.10.4. Technologien

## Modul 12. Architekturen und Modelle für die Informationssicherheit

- 12.1. Architektur der Informationssicherheit
  - 12.1.1. ISMS / ISDP
  - 12.1.2. Strategische Ausrichtung
  - 12.1.3. Risikomanagement
  - 12.1.4. Leistungsmessung
- 12.2. Modelle der Informationssicherheit
  - 12.2.1. Richtlinienbasierte Sicherheitsmodelle
  - 12.2.2. Basierend auf Schutz-Tools
  - 12.2.3. Teambasiert
- 12.3. Sicherheitsmodell. Wichtige Komponenten
  - 12.3.1. Identifizierung von Risiken
  - 12.3.2. Definition von Kontrollen
  - 12.3.3. Kontinuierliche Bewertung des Risikoniveaus
  - 12.3.4. Sensibilisierungsplan für Mitarbeiter, Lieferanten, Partner usw.
- 12.4. Prozess der Risikoverwaltung
  - 12.4.1. Identifizierung von Vermögenswerten
  - 12.4.2. Identifizierung von Bedrohungen
  - 12.4.3. Risikobewertung
  - 12.4.4. Priorisierung der Kontrollen
  - 12.4.5. Neubeurteilung und Restrisiko

- 12.5. Geschäftsprozesse und Informationssicherheit
  - 12.5.1. Geschäftsprozesse
  - 12.5.2. Risikobewertung auf der Grundlage geschäftlicher Parameter
  - 12.5.3. Analyse der Auswirkungen auf das Geschäft
  - 12.5.4. Geschäftsbetrieb und Informationssicherheit
- 12.6. Prozess zur kontinuierlichen Verbesserung
  - 12.6.1. Der Deming-Zyklus
    - 12.6.1.1. Planung
    - 12.6.1.2. Machen
    - 12.6.1.3. Prüfen
    - 12.6.1.4. Agieren
- 12.7. Sicherheitsarchitekturen
  - 12.7.1. Auswahl und Homogenisierung von Technologien
  - 12.7.2. Identitätsmanagement. Authentifizierung
  - 12.7.3. Zugriffsverwaltung. Autorisierung
  - 12.7.4. Sicherheit der Netzwerkinfrastruktur
  - 12.7.5. Verschlüsselungstechnologien und -lösungen
  - 12.7.6. Sicherheit der Endgeräte (EDR)
- 12.8. Der rechtliche Rahmen
  - 12.8.1. Regulatorischer Rahmen
  - 12.8.2. Zertifizierungen
  - 12.8.3. Gesetzgebung
- 12.9. Der ISO 27001-Standard
  - 12.9.1. Implementierung
  - 12.9.2. Zertifizierung
  - 12.9.3. Audits und Penetrationstests
  - 12.9.4. Laufendes Risikomanagement
  - 12.9.5. Klassifizierung der Informationen
- 12.10. Gesetzgebung zum Datenschutz. RGPD (GDPR)
  - 12.10.1. Anwendungsbereich der Allgemeinen Datenschutzverordnung (GDPR)
  - 12.10.2. Persönliche Daten
  - 12.10.3. Rollen bei der Verarbeitung von personenbezogenen Daten
  - 12.10.4. ARCO-Rechte
  - 12.10.5. Der DSB. Funktionen

## Modul 13. IT-Sicherheitsmanagement

- 13.1. Sicherheitsmanagement
  - 13.1.1. Sicherheitsmaßnahmen
  - 13.1.2. Rechtliche und regulatorische Aspekte
  - 13.1.3. Geschäftliche Freigabe
  - 13.1.4. Risikomanagement
  - 13.1.5. Identitäts- und Zugriffsmanagement
- 13.2. Struktur des Sicherheitsbereichs. Das Büro des CISO
  - 13.2.1. Organisatorische Struktur. Position des CISO in der Struktur
  - 13.2.2. Verteidigungslinien
  - 13.2.3. Organigramm des Büros des CISO
  - 13.2.4. Haushaltsführung
- 13.3. Sicherheitsmanagement
  - 13.3.1. Sicherheitsausschuss
  - 13.3.2. Ausschuss für Risikoüberwachung
  - 13.3.3. Prüfungsausschuss
  - 13.3.4. Krisenausschuss
- 13.4. Security Governance. Funktionen
  - 13.4.1. Politiken und Standards
  - 13.4.2. Masterplan Sicherheit
  - 13.4.3. Dashboards
  - 13.4.4. Sensibilisierung und Schulung
  - 13.4.5. Sicherheit der Lieferkette
- 13.5. Sicherheitsmaßnahmen
  - 13.5.1. Identitäts- und Zugriffsmanagement
  - 13.5.2. Konfiguration von Netzwerksicherheitsregeln. *Firewalls*
  - 13.5.3. Verwaltung der IDS/IPS-Plattform
  - 13.5.4. Scannen auf Schwachstellen
- 13.6. Cybersecurity-Rahmenwerk. NIST CSF
  - 13.6.1. NIST-Methodik
    - 13.6.1.1. Identifizieren
    - 13.6.1.2. Schützen
    - 13.6.1.3. Erkennen
    - 13.6.1.4. Reagieren
    - 13.6.1.5. Zurückgewinnen
- 13.7. Sicherheitsoperationszentrum (SOC). Funktionen
  - 13.7.1. Schutz. *Red Team, Pentesting, Threat Intelligence*
  - 13.7.2. Erkennung. *SIEM, user behavior analytics, fraud prevention*
  - 13.7.3. Antwort
- 13.8. Sicherheitsaudits
  - 13.8.1. Penetrationstests
  - 13.8.2. Übungen des *Red Team*
  - 13.8.3. Quellcode-Prüfungen. Sichere Entwicklung
  - 13.8.4. Komponentensicherheit (*Software Supply Chain*)
  - 13.8.5. Forensische Analyse
- 13.9. Reaktion auf Vorfälle
  - 13.9.1. Vorbereitung
  - 13.9.2. Erkennung, Analyse und Berichterstattung
  - 13.9.3. Eindämmung, Ausrottung und Wiederherstellung
  - 13.9.4. Aktivitäten nach dem Vorfall
    - 13.9.4.1. Aufbewahrung von Beweisen
    - 13.9.4.2. Forensische Analyse
    - 13.9.4.3. Lücken-Management
  - 13.9.5. Offizielle Leitfäden für das Management von Cyberfällen
- 13.10. Management von Schwachstellen
  - 13.10.1. Scannen auf Schwachstellen
  - 13.10.2. Bewertung der Anfälligkeit
  - 13.10.3. Verstärkung des Systems
  - 13.10.4. Zero-Day-Sicherheitslücken. *Zero-Day*

## Modul 14. Risikoanalyse und IT-Sicherheitsumgebung

- 14.1. Analyse des Umfelds
  - 14.1.1. Analyse der wirtschaftlichen Lage
    - 14.1.1.1. VUCA-Umgebungen
      - 14.1.1.1.1. Volatil
      - 14.1.1.1.2. Ungewiss
      - 14.1.1.1.3. Komplex
      - 14.1.1.1.4. Mehrdeutig
    - 14.1.1.2. BANI-Umgebungen
      - 14.1.1.2.1. Spröde
      - 14.1.1.2.2. Ängstlich
      - 14.1.1.2.3. Nicht-linear
      - 14.1.1.2.4. Unverständlich
  - 14.1.2. Analyse des allgemeinen Umfelds. PESTEL
    - 14.1.2.1. Politisch
    - 14.1.2.2. Wirtschaft
    - 14.1.2.3. Sozial
    - 14.1.2.4. Technologisch
    - 14.1.2.5. Ökologisch/Umweltbezogen
    - 14.1.2.6. Legal
  - 14.1.3. Analyse der internen Situation. SWOT
    - 14.1.3.1. Ziele
    - 14.1.3.2. Bedrohungen
    - 14.1.3.3. Gelegenheiten
    - 14.1.3.4. Stärken
- 14.2. Risiko und Unsicherheit
  - 14.2.1. Risiko
  - 14.2.2. Risikomanagement
  - 14.2.3. Standards für das Risikomanagement
- 14.3. ISO 31.000:2018 Richtlinien zum Risikomanagement
  - 14.3.1. Objekt
  - 14.3.2. Grundsätze
  - 14.3.3. Referenzrahmen
  - 14.3.4. Prozess



- 14.4. Methodik für die Analyse und das Management von Risiken in Informationssystemen (MAGERIT)
  - 14.4.1. MAGERIT Methodik
    - 14.4.1.1. Ziele
    - 14.4.1.2. Methode
    - 14.4.1.3. Elemente
    - 14.4.1.4. Techniken
    - 14.4.1.5. Verfügbare Tools (PILAR)
- 14.5. Übertragung von Cyber-Risiken
  - 14.5.1. Risikotransfer
  - 14.5.2. Cyberrisiken. Typologie
  - 14.5.3. Versicherung gegen Cyberrisiken
- 14.6. Agile Methoden für das Risikomanagement
  - 14.6.1. Agile Methodologien
  - 14.6.2. Scrum für das Risikomanagement
  - 14.6.3. *Agile Risk Management*
- 14.7. Technologien für das Risikomanagement
  - 14.7.1. Künstliche Intelligenz für das Risikomanagement
  - 14.7.2. *Blockchain* und Kryptographie. Methoden zur Werterhaltung
  - 14.7.3. Quantencomputing. Potenzial oder Bedrohung
- 14.8. IT-Risiko-Mapping auf der Grundlage agiler Methoden
  - 14.8.1. Darstellung von Wahrscheinlichkeiten und Auswirkungen in agilen Umgebungen
  - 14.8.2. Risiko als Bedrohung für den Wert
  - 14.8.3. Neuentwicklung von agilem Projektmanagement und agilen Prozessen auf der Grundlage von KRIs
- 14.9. *Risk Driven* im Risikomanagement
  - 14.9.1. *Risk Driven*
  - 14.9.2. *Risk Driven* im Risikomanagement
  - 14.9.3. Entwicklung eines risikoorientierten Geschäftsführungsmodells
- 14.10. Innovation und digitale Transformation im IT-Risikomanagement
  - 14.10.1. Agiles Risikomanagement als Quelle für geschäftliche Innovation
  - 14.10.2. Umwandlung von Daten in entscheidungsrelevante Informationen
  - 14.10.3. Ganzheitliche Betrachtung des Unternehmens durch Risiko

## Modul 15. Kryptographie in der IT

- 15.1. Kryptographie
  - 15.1.1. Kryptographie
  - 15.1.2. Mathematische Grundlagen
- 15.2. Kryptologie
  - 15.2.1. Kryptologie
  - 15.2.2. Kryptoanalyse
  - 15.2.3. Steganographie und Stegoanalyse
- 15.3. Kryptographische Protokolle
  - 15.3.1. Grundlegende Blöcke
  - 15.3.2. Grundlegende Protokolle
  - 15.3.3. Zwischengeschaltete Protokolle
  - 15.3.4. Erweiterte Protokolle
  - 15.3.5. Esoterische Protokolle
- 15.4. Kryptographische Techniken
  - 15.4.1. Länge des Schlüssels
  - 15.4.2. Handhabung der Tasten
  - 15.4.3. Arten von Algorithmen
  - 15.4.4. Zusammenfassende Funktionen. *Hash*
  - 15.4.5. Pseudo-Zufallszahlengeneratoren
  - 15.4.6. Verwendung von Algorithmen
- 15.5. Symmetrische Kryptographie
  - 15.5.1. Blockchiffren
  - 15.5.2. DES (*Data Encryption Standard*)
  - 15.5.3. RC4 Algorithmus
  - 15.5.4. AES (*Advanced Encryption Standard*)
  - 15.5.5. Kombination von Blockchiffren
  - 15.5.6. Ableitung des Schlüssels
- 15.6. Asymmetrische Kryptographie
  - 15.6.1. Diffie-Hellman
  - 15.6.2. DSA (*Digital Signature Algorithm*)
  - 15.6.3. RSA (Rivest, Shamir y Adleman)
  - 15.6.4. Elliptische Kurve
  - 15.6.5. Asymmetrische Kryptographie. Typologie
- 15.7. Digitale Zertifikate
  - 15.7.1. Digitale Unterschrift
  - 15.7.2. X509-Zertifikate
  - 15.7.3. Infrastruktur für öffentliche Schlüssel (PKI)
- 15.8. Implementierungen
  - 15.8.1. Kerberos
  - 15.8.2. IBM CCA
  - 15.8.3. *Pretty Good Privacy* (PGP)
  - 15.8.4. *ISO Authentication Framework*
  - 15.8.5. SSL und TLS
  - 15.8.6. Chipkarten als Zahlungsmittel (EMV)
  - 15.8.7. Protokolle für Mobiltelefonie
  - 15.8.8. *Blockchain*
- 15.9. Steganographie
  - 15.9.1. Steganographie
  - 15.9.2. Stegano-Analyse
  - 15.9.3. Anwendungen und Einsatzmöglichkeiten
- 15.10. Quantenkryptographie
  - 15.10.1. Quanten-Algorithmen
  - 15.10.2. Schutz von Algorithmen vor Quantenberechnungen
  - 15.10.3. Quantum Key Distribution

**Modul 16. Identitäts- und Zugriffsmanagement in der IT-Sicherheit**

- 16.1. Identitäts- und Zugriffsmanagement (IAM)
  - 16.1.1. Digitale Identität
  - 16.1.2. Identitätsmanagement
  - 16.1.3. Identitätsföderation
- 16.2. Physische Zugangskontrolle
  - 16.2.1. Schutzsysteme
  - 16.2.2. Bereichssicherheit
  - 16.2.3. Wiederherstellungseinrichtungen
- 16.3. Logische Zugriffskontrolle
  - 16.3.1. Authentifizierung: Typologie
  - 16.3.2. Authentifizierungsprotokolle
  - 16.3.3. Angriffe zur Authentifizierung
- 16.4. Logische Zugriffskontrolle. Authentifizierung MFA
  - 16.4.1. Logische Zugriffskontrolle. Authentifizierung MFA
  - 16.4.2. Passwörter. Bedeutung
  - 16.4.3. Angriffe zur Authentifizierung
- 16.5. Logische Zugriffskontrolle. Biometrische Authentifizierung
  - 16.5.1. Logische Zugriffskontrolle. Biometrische Authentifizierung
    - 16.5.1.1. Biometrische Authentifizierung. Anforderungen
  - 16.5.2. Funktionsweise
  - 16.5.3. Modelle und Techniken
- 16.6. Systeme zur Verwaltung der Authentifizierung
  - 16.6.1. *Single Sign On*
  - 16.6.2. Kerberos
  - 16.6.3. AAA-Systeme
- 16.7. Authentifizierung-Management-Systeme: AAA-Systeme
  - 16.7.1. TACACS
  - 16.7.2. RADIUS
  - 16.7.3. DIAMETER

- 16.8. Kontrollsysteme für den Zugang
  - 16.8.1. FW - Firewalls
  - 16.8.2. VPN - Virtuelle private Netzwerke
  - 16.8.3. IDS - Intrusion Detection System
- 16.9. Netzwerk-Zugangskontrollsysteme
  - 16.9.1. NAC
  - 16.9.2. Architektur und Elemente
  - 16.9.3. Betrieb und Standardisierung
- 16.10. Zugang auf drahtlose Netzwerke
  - 16.10.1. Arten von drahtlosen Netzwerken
  - 16.10.2. Sicherheit für drahtlose Netzwerke
  - 16.10.3. Angriffe auf drahtlose Netzwerke

**Modul 17. Sicherheit bei Kommunikation und Softwarebetrieb**

- 17.1. Computersicherheit in der Kommunikation und im Softwarebetrieb
  - 17.1.1. Computersicherheit
  - 17.1.2. Cybersicherheit
  - 17.1.3. Cloud-Sicherheit
- 17.2. Computersicherheit in der Kommunikation und im Softwarebetrieb. Typologie
  - 17.2.1. Physische Sicherheit
  - 17.2.2. Logische Sicherheit
- 17.3. Sicherheit in der Kommunikation
  - 17.3.1. Wichtigste Elemente
  - 17.3.2. Netzwerksicherheit
  - 17.3.3. Bewährte Praktiken
- 17.4. Cyberintelligenz
  - 17.4.1. Social Engineering
  - 17.4.2. *Deep Web*
  - 17.4.3. *Phishing*
  - 17.4.4. *Malware*

- 17.5. Sichere Entwicklung in Kommunikation und Softwarebetrieb
  - 17.5.1. Sichere Entwicklung. HTTP-Protokoll
  - 17.5.2. Sichere Entwicklung. Lebenszyklus
  - 17.5.3. Sichere Entwicklung. PHP-Sicherheit
  - 17.5.4. Sichere Entwicklung. NET-Sicherheit
  - 17.5.5. Sichere Entwicklung. Bewährte Praktiken
- 17.6. Informationssicherheits-Managementsysteme in Kommunikation und Software
  - 17.6.1. GDPR
  - 17.6.2. ISO 27021
  - 17.6.3. ISO 27017/18
- 17.7. SIEM-Technologien
  - 17.7.1. SIEM-Technologien
  - 17.7.2. SOC Betrieb
  - 17.7.3. SIEM *Vendors*
- 17.8. Die Rolle der Sicherheit in Organisationen
  - 17.8.1. Rollen in Organisationen
  - 17.8.2. Die Rolle von IoT-Spezialisten in Unternehmen
  - 17.8.3. Anerkannte Zertifizierungen auf dem Markt
- 17.9. Forensische Analyse
  - 17.9.1. Forensische Analyse
  - 17.9.2. Forensische Analyse. Methodik
  - 17.9.3. Forensische Analyse. Tools und Implementierung
- 17.10. Cybersecurity heute
  - 17.10.1. Große Cyberangriffe
  - 17.10.2. Prognosen zur Beschäftigungsfähigkeit
  - 17.10.3. Herausforderungen



**Modul 18. Sicherheit in *Cloud*-Umgebungen**

- 18.1. Sicherheit in *Cloud Computing*-Umgebungen
  - 18.1.1. Sicherheit in *Cloud Computing*-Umgebungen
  - 18.1.2. Sicherheit in *Cloud Computing*-Umgebungen. Bedrohungen und Sicherheitsrisiken
  - 18.1.3. Sicherheit in *Cloud Computing*-Umgebungen Wichtige Sicherheitsaspekte
- 18.2. Arten von *Cloud* Infrastruktur
  - 18.2.1. Publikum
  - 18.2.2. Öffentlich
  - 18.2.3. Privat
- 18.3. Hybrid
  - 18.3.1. Vom Anbieter verwaltete Sicherheitselemente
  - 18.3.2. Vom Kunden verwaltete Elemente
  - 18.3.3. Definition der Sicherheitsstrategie
- 18.4. Mechanismen der Prävention
  - 18.4.1. Systeme zur Verwaltung der Authentifizierung
  - 18.4.2. Berechtigungsverwaltungssystem: Zugriffsrichtlinien
  - 18.4.3. Systeme zur Schlüsselverwaltung
- 18.5. Verbriefung von Systemen
  - 18.5.1. Verbriefung von Speichersystemen
  - 18.5.2. Sicherung von Datenbanksystemen
  - 18.5.3. Sichern von Daten bei der Übermittlung
- 18.6. Schutz der Infrastruktur
  - 18.6.1. Entwurf und Implementierung eines sicheren Netzwerks
  - 18.6.2. Sicherheit von Computerressourcen
  - 18.6.3. Tools und Ressourcen zum Schutz der Infrastruktur
- 18.7. Erkennung von Bedrohungen und Angriffen
  - 18.7.1. Auditing, *Logging* und Überwachungssysteme
  - 18.7.2. Ereignis- und Alarmsysteme
  - 18.7.3. SIEM-Systeme

- 18.8. Reaktion auf Vorfälle
  - 18.8.1. Plan zur Reaktion auf Vorfälle
  - 18.8.2. Geschäftskontinuität
  - 18.8.3. Forensische Analyse und Behebung von Vorfällen der gleichen Art
- 18.9. Sicherheit in öffentlichen *Clouds*
  - 18.9.1. AWS (Amazon Web Services)
  - 18.9.2. Microsoft Azure
  - 18.9.3. Google GCP
  - 18.9.4. Oracle *Cloud*
- 18.10. Regulierung und Compliance
  - 18.10.1. Compliance im Bereich Sicherheit
  - 18.10.2. Risikomanagement
  - 18.10.3. Menschen und Prozesse in Organisationen

**Modul 19. Sicherheit der Kommunikation von IoT-Geräten**

- 19.1. Von der Telemetrie zum IoT
  - 19.1.1. Telemetrie
  - 19.1.2. M2M-Konnektivität
  - 19.1.3. Demokratisierung der Telemetrie
- 19.2. IoT-Referenzmodelle
  - 19.2.1. IoT-Referenzmodelle
  - 19.2.2. Vereinfachte IoT-Architektur
- 19.3. IoT-Sicherheitsschwachstellen
  - 19.3.1. IoT-Geräte
  - 19.3.2. IoT-Geräte. Kasuistik der Verwendung
  - 19.3.3. IoT-Geräte. Schwachstellen
- 19.4. IoT-Konnektivität
  - 19.4.1. PAN, LAN, WAN-Netzwerke
  - 19.4.2. Drahtlose Technologien außerhalb des IoT
  - 19.4.3. Drahtlose LPWAN-Technologien

- 19.5. LPWAN-Technologien
  - 19.5.1. Das eiserne Dreieck der LPWANs
  - 19.5.2. Freie Frequenzbänder vs. Lizenzierte Bänder
  - 19.5.3. LPWAN Technologie Optionen
- 19.6. LoRaWAN-Technologie
  - 19.6.1. LoRaWAN-Technologie
  - 19.6.2. LoRaWAN Anwendungsfälle. Ökosystem
  - 19.6.3. LoRaWAN Sicherheit
- 19.7. Sigfox Technologie
  - 19.7.1. Sigfox Technologie
  - 19.7.2. Sigfox Anwendungsfälle. Ökosystem
  - 19.7.3. Sicherheit in Sigfox
- 19.8. IoT-Mobilfunktechnologie
  - 19.8.1. IoT-Mobilfunktechnologie (NB-IoT und LTE-M)
  - 19.8.2. Anwendungsfälle für IoT-Mobilfunktechnologie Ökosystem
  - 19.8.3. IoT-Mobilfunktechnologie-Sicherheit
- 19.9. Wi-SUN Technologie
  - 19.9.1. Wi-SUN Technologie
  - 19.9.2. Wi-SUN Anwendungsfälle. Ökosystem
  - 19.9.3. Wi-SUN Sicherheit
- 19.10. Andere IoT-Technologien
  - 19.10.1. Andere IoT-Technologien
  - 19.10.2. Anwendungsfälle und Ökosystem anderer IoT-Technologien
  - 19.10.3. Sicherheit in anderen IoT-Technologien

## Modul 20. Business Continuity Plan in Verbindung mit Sicherheit

- 20.1. Business Continuity Plan
  - 20.1.1. Pläne für die Geschäftskontinuität (BCP)
  - 20.1.2. Plan für die Geschäftskontinuität (BCP). Schlüsselaspekte
  - 20.1.3. Business Continuity Plan (BCP) für die Unternehmensbewertung
- 20.2. Metriken in einem Business Continuity Plan (BCP)
  - 20.2.1. *Recovery Time Objective* (RTO) und *Recovery Point Objective* (RPO)
  - 20.2.2. Maximal verträgliche Zeit (MTD)
  - 20.2.3. Mindestanforderungen für die Wiederherstellung (ROL)
  - 20.2.4. Wiederherstellungspunkt-Ziel (RPO)

- 20.3. Kontinuitätsprojekte. Typologie
  - 20.3.1. Plan für die Geschäftskontinuität (BCP)
  - 20.3.2. IKT-Kontinuitätsplan (ICTCP)
  - 20.3.3. Plan zur Wiederherstellung im Katastrophenfall (DRP)
- 20.4. Risikomanagement im Zusammenhang mit dem BCP
  - 20.4.1. Analyse der Auswirkungen auf das Geschäft
  - 20.4.2. Vorteile der Implementierung eines BCP
  - 20.4.3. Risikobasiertes Denken
- 20.5. Lebenszyklus eines Business Continuity Plans
  - 20.5.1. Phase 1: Analyse der Organisation
  - 20.5.2. Phase 2: Festlegung der Kontinuitätsstrategie
  - 20.5.3. Phase 3: Reaktion auf Notfälle
  - 20.5.4. Phase 4: Tests, Wartung und Überprüfung
- 20.6. Phase der Organisationsanalyse eines BCP
  - 20.6.1. Identifizierung der Prozesse, die in den Geltungsbereich des BCP fallen
  - 20.6.2. Identifizierung von kritischen Geschäftsbereichen
  - 20.6.3. Identifizierung von Abhängigkeiten zwischen Bereichen und Prozessen
  - 20.6.4. Bestimmung der geeigneten MTD
  - 20.6.5. Liefergegenstände. Erstellung eines Plans
- 20.7. Phase der Festlegung der Kontinuitätsstrategie in einer BCP
  - 20.7.1. Rollen in der Phase der Strategiebestimmung
  - 20.7.2. Aufgaben in der Phase der Strategiefestlegung
  - 20.7.3. Liefergegenstände
- 20.8. Phase der Notfallmaßnahmen eines BCP
  - 20.8.1. Rollen in der Reaktionsphase
  - 20.8.2. Aufgaben in dieser Phase
  - 20.8.3. Liefergegenstände
- 20.9. Test-, Wartungs- und Überarbeitungsphase eines BCP
  - 20.9.1. Rollen in der Test-, Wartungs- und Überprüfungsphase
  - 20.9.2. Aufgaben in der Test-, Wartungs- und Überprüfungsphase
  - 20.9.3. Liefergegenstände
- 20.10. ISO-Normen im Zusammenhang mit Business Continuity Plans (BCP)
  - 20.10.1. ISO 22301:2019
  - 20.10.2. ISO 22313:2020
  - 20.10.3. Andere verwandte ISO- und internationale Normen

## Modul 21. Datenanalytik in der Unternehmensorganisation

- 21.1. Business-Analyse
  - 21.1.1. Business-Analyse
  - 21.1.2. Datenstruktur
  - 21.1.3. Phasen und Elemente
- 21.2. Datenanalytik im Unternehmen
  - 21.2.1. Dashboards und KPIs nach Abteilungen
  - 21.2.2. Operative, taktische und strategische Berichterstattung
  - 21.2.3. Datenanalytik für jede Abteilung
    - 21.2.3.1. Marketing und Kommunikation
    - 21.2.3.2. Verkauf
    - 21.2.3.3. Kundendienst
    - 21.2.3.4. Einkauf
    - 21.2.3.5. Verwaltung
    - 21.2.3.6. Personalwesen
    - 21.2.3.7. Produktion
    - 21.2.3.8. IT
- 21.3. Marketing und Kommunikation
  - 21.3.1. Zu messende KPIs, Anwendungen und Vorteile
  - 21.3.2. Marketing-Systeme und *Data Warehouse*
  - 21.3.3. Implementierung einer Struktur zur Datenanalyse im Marketing
  - 21.3.4. Marketing- und Kommunikationsplan
  - 21.3.5. Strategien, Prognosen und Kampagnenmanagement
- 21.4. Kommerziell und Verkauf
  - 21.4.1. Beiträge der Datenanalytik im kommerziellen Bereich
  - 21.4.2. Bedürfnisse der Verkaufsabteilung
  - 21.4.3. Marktstudien
- 21.5. Kundendienst
  - 21.5.1. Loyalität
  - 21.5.2. Persönliche Qualität und emotionale Intelligenz
  - 21.5.3. Kundenzufriedenheit

- 21.6. Einkauf
  - 21.6.1. Datenanalytik für die Marktforschung
  - 21.6.2. Datenanalytik für die Wettbewerbsforschung
  - 21.6.3. Andere Anwendungen
- 21.7. Verwaltung
  - 21.7.1. Bedürfnisse der Verwaltungsabteilung
  - 21.7.2. *Data Warehouse* und finanzielle Risikoanalyse
  - 21.7.3. *Data Warehouse* und finanzielle Risikoanalyse
- 21.8. Personalwesen
  - 21.8.1. Personalwesen und Vorteile der Datenanalyse
  - 21.8.2. Datenanalysetools in der Personalabteilung
  - 21.8.3. Anwendung von Datenanalysen im Personalwesen
- 21.9. Produktion
  - 21.9.1. Datenanalyse in einer Produktionsabteilung
  - 21.9.2. Anwendungen
  - 21.9.3. Vorteile
- 21.10. IT
  - 21.10.1. IT-Abteilung
  - 21.10.2. Datenanalytik und digitale Transformation
  - 21.10.3. Innovation und Produktivität

## Modul 22. Datenmanagement, Datenmanipulation und Informationen für Data Science

- 22.1. Statistik. Variablen, Indizes und Kennziffern
  - 22.1.1. Die Statistik
  - 22.1.2. Statistische Dimensionen
  - 22.1.3. Variablen, Indizes und Kennziffern
- 22.2. Daten-Typologie
  - 22.2.1. Qualitative
  - 22.2.2. Quantitative
  - 22.2.3. Charakterisierung und Kategorien

- 22.3. Wissen über Daten aus Messungen
  - 22.3.1. Maßnahmen der Zentralisierung
  - 22.3.2. Maße der Streuung
  - 22.3.3. Korrelation
- 22.4. Wissen über Daten aus Diagrammen
  - 22.4.1. Visualisierung nach Datentyp
  - 22.4.2. Interpretation von grafischen Informationen
  - 22.4.3. Anpassung von Grafiken mit R
- 22.5. Wahrscheinlichkeit
  - 22.5.1. Wahrscheinlichkeit
  - 22.5.2. Wahrscheinlichkeitsfunktion
  - 22.5.3. Verteilungen
- 22.6. Datenerhebung
  - 22.6.1. Methodik der Erhebung
  - 22.6.2. Erhebungsinstrumente
  - 22.6.3. Kanäle für die Erhebung
- 22.7. Datenbereinigung
  - 22.7.1. Phasen der Datenbereinigung
  - 22.7.2. Qualität der Daten
  - 22.7.3. Datenmanipulation (mit R)
- 22.8. Datenanalyse, Interpretation und Bewertung der Ergebnisse
  - 22.8.1. Statistische Maßnahmen
  - 22.8.2. Beziehungsindizes
  - 22.8.3. Data Mining
- 22.9. Datenlager (*Data Warehouse*)
  - 22.9.1. Elemente
  - 22.9.2. Entwurf
- 22.10. Verfügbarkeit von Daten
  - 22.10.1. Zugang
  - 22.10.2. Nützlichkeit
  - 22.10.3. Sicherheit



**Modul 23. IoT-Geräte und Plattformen als Grundlage für Data Science**

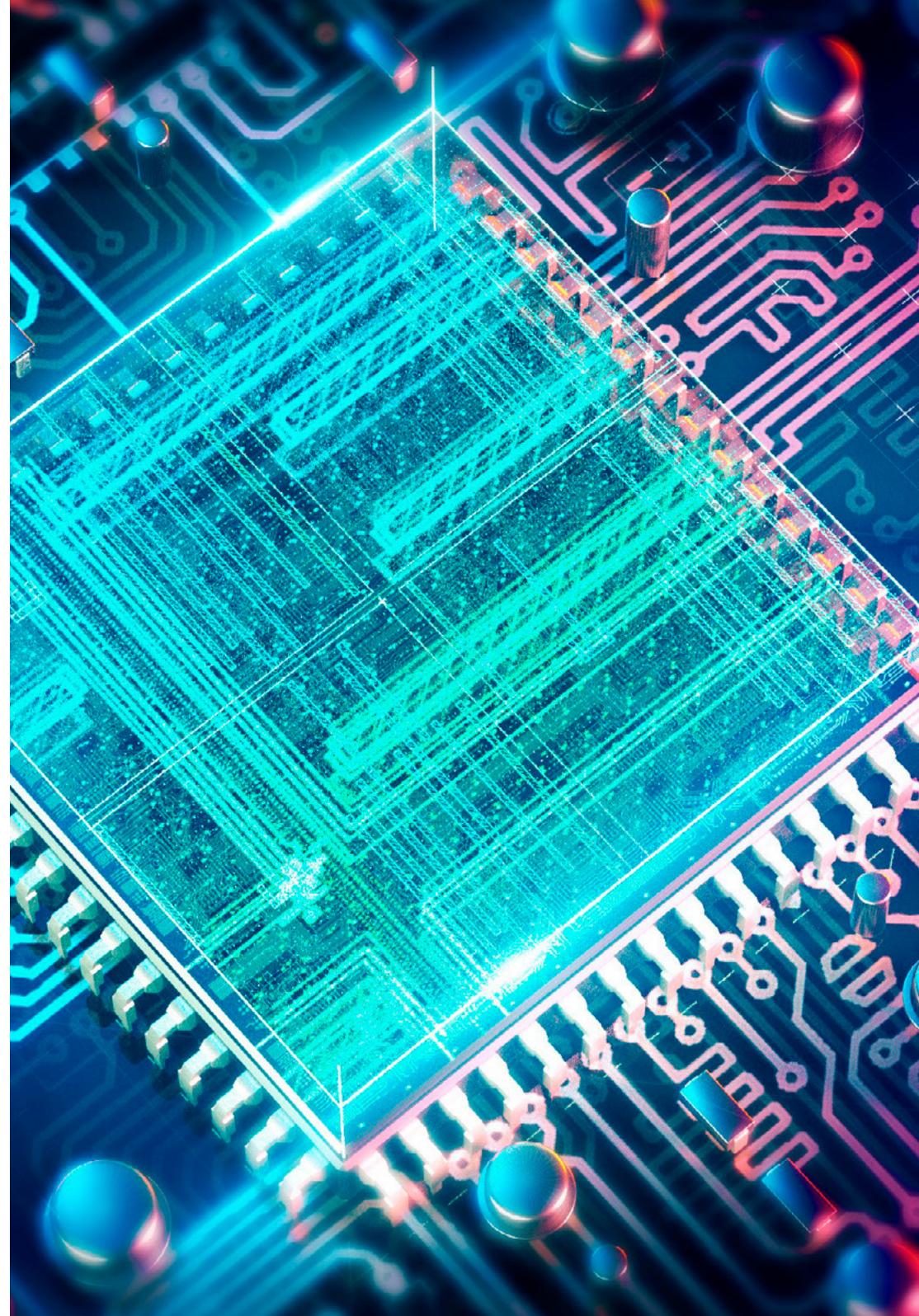
- 23.1. *Internet of Things*
  - 23.1.1. Internet der Zukunft, *Internet of Things*
  - 23.1.2. Das Konsortium Industrielles Internet
- 23.2. Referenzarchitektur
  - 23.2.1. Referenzarchitektur
  - 23.2.2. Schichten
  - 23.2.3. Komponenten
- 23.3. Sensoren und IoT-Geräte
  - 23.3.1. Hauptkomponenten
  - 23.3.2. Sensoren und Aktuatoren
- 23.4. Kommunikation und Protokolle
  - 23.4.1. Protokolle. OSI-Modell
  - 23.4.2. Kommunikationstechnologien
- 23.5. Cloud-Plattformen für IoT und IIoT
  - 23.5.1. Allzweck-Plattformen
  - 23.5.2. Industrielle Plattformen
  - 23.5.3. Open-Source-Plattformen
- 23.6. Datenverwaltung in IoT-Plattformen
  - 23.6.1. Mechanismen zur Datenverwaltung. Offene Daten
  - 23.6.2. Datenaustausch und Visualisierung
- 23.7. IoT-Sicherheit
  - 23.7.1. Sicherheitsanforderungen und -bereiche
  - 23.7.2. IIoT-Sicherheitsstrategien
- 23.8. IoT-Anwendungen
  - 23.8.1. Intelligente Städte
  - 23.8.2. Gesundheit und Fitness
  - 23.8.3. Intelligentes Zuhause
  - 23.8.4. Andere Anwendungen

- 23.9. IIoT-Anwendungen
  - 23.9.1. Herstellung
  - 23.9.2. Transport
  - 23.9.3. Energie
  - 23.9.4. Landwirtschaft und Viehzucht
  - 23.9.5. Andere Sektoren
- 23.10. Industrie 4.0
  - 23.10.1. IoRT (*Internet of Robotics Things*)
  - 23.10.2. 3D Additive Fertigung
  - 23.10.3. *Big Data-Analytics*

**Modul 24. Grafische Darstellung für die Datenanalyse**

- 24.1. Explorative Analyse
  - 24.1.1. Repräsentation für die Informationsanalyse
  - 24.1.2. Der Wert der grafischen Darstellung
  - 24.1.3. Neue Paradigmen der grafischen Darstellung
- 24.2. Optimierung für Data Science
  - 24.2.1. Farbpalette und Design
  - 24.2.2. Gestalt in der grafischen Darstellung
  - 24.2.3. Zu vermeidende Fehler und Tipps
- 24.3. Grundlegende Datenquellen
  - 24.3.1. Für die Qualitätsdarstellung
  - 24.3.2. Für die Mengendarstellung
  - 24.3.3. Für die Zeitdarstellung
- 24.4. Komplexe Datenquellen
  - 24.4.1. Dateien, Listen und DB
  - 24.4.2. Offene Daten
  - 24.4.3. Kontinuierlich generierte Daten

- 24.5. Arten von Grafiken
  - 24.5.1. Grundlegende Darstellungen
  - 24.5.2. Blockdarstellung
  - 24.5.3. Darstellung für die Ausbreitungsanalyse
  - 24.5.4. Zirkuläre Darstellungen
  - 24.5.5. Blasen-Darstellungen
  - 24.5.6. Geografische Darstellungen
- 24.6. Arten der Visualisierung
  - 24.6.1. Vergleichend und relational
  - 24.6.2. Verteilung
  - 24.6.3. Hierarchisch
- 24.7. Berichtsentwurf mit grafischer Darstellung
  - 24.7.1. Anwendung von Diagrammen in Marketingberichten
  - 24.7.2. Anwendung von Diagrammen in Dashboards und KPIs
  - 24.7.3. Anwendung von Grafiken in strategischen Plänen
  - 24.7.4. Andere Verwendungen: Wissenschaft, Gesundheit, Wirtschaft
- 24.8. Grafisches Geschichtenerzählen
  - 24.8.1. Grafisches Geschichtenerzählen
  - 24.8.2. Entwicklung
  - 24.8.3. Nützlichkeit
- 24.9. Visualisierungsorientierte Tools
  - 24.9.1. Erweiterte Tools
  - 24.9.2. Online-Software
  - 24.9.3. *Open Source*
- 24.10. Neue Technologien zur Datenvisualisierung
  - 24.10.1. Systeme zur Virtualisierung der Realität
  - 24.10.2. Systeme für Realitätserweiterung und -verbesserung
  - 24.10.3. Intelligente Systeme



## Modul 25. Data Science Tools

- 25.1. Datenwissenschaft
  - 25.1.1. Datenwissenschaft
  - 25.1.2. Fortgeschrittene Tools für den Data Scientist
- 25.2. Daten, Informationen und Wissen
  - 25.2.1. Daten, Informationen und Wissen
  - 25.2.2. Datentypen
  - 25.2.3. Daten-Quellen
- 25.3. Von Daten zu Informationen
  - 25.3.1. Datenanalyse
  - 25.3.2. Arten der Analyse
  - 25.3.3. Extraktion von Informationen aus einem *Dataset*
- 25.4. Extraktion von Informationen durch Visualisierung
  - 25.4.1. Visualisierung als Analyseinstrument
  - 25.4.2. Methoden der Visualisierung
  - 25.4.3. Visualisierung eines Datensatzes
- 25.5. Datenqualität
  - 25.5.1. Datenqualität
  - 25.5.2. Datenbereinigung
  - 25.5.3. Grundlegende Datenvorverarbeitung
- 25.6. *Dataset*
  - 25.6.1. *Dataset*-Anreicherung
  - 25.6.2. Der Fluch der Dimensionalität
  - 25.6.3. Ändern unseres Datensatzes
- 25.7. Ungleichgewicht
  - 25.7.1. Ungleichgewicht der Klassen
  - 25.7.2. Techniken zur Begrenzung von Ungleichgewichten
  - 25.7.3. *Dataset*-Abgleich
- 25.8. Unüberwachte Modelle
  - 25.8.1. Unüberwachtes Modell
  - 25.8.2. Methoden
  - 25.8.3. Klassifizierung mit unüberwachten Modellen

- 25.9. Überwachte Modelle
  - 25.9.1. Überwachtes Modell
  - 25.9.2. Methoden
  - 25.9.3. Klassifizierung mit überwachten Modellen
- 25.10. Tools und bewährte Verfahren
  - 25.10.1. Bewährte Praktiken für einen Data Scientist
  - 25.10.2. Das beste Modell
  - 25.10.3. Nützliche Tools

## Modul 26. Data Mining. Auswahl, Vorverarbeitung und Transformation

- 26.1. Statistische Inferenz
  - 26.1.1. Deskriptive Statistik vs. statistische Inferenz
  - 26.1.2. Parametrische Verfahren
  - 26.1.3. Nicht-parametrische Verfahren
- 26.2. Explorative Analyse
  - 26.2.1. Deskriptive Analyse
  - 26.2.2. Visualisierung
  - 26.2.3. Vorbereitung der Daten
- 26.3. Datenaufbereitung
  - 26.3.1. Datenintegration und -bereinigung
  - 26.3.2. Normalisierung der Daten
  - 26.3.3. Attribute umwandeln
- 26.4. Verlorene Werte
  - 26.4.1. Umgang mit verlorenen Werten
  - 26.4.2. Maximum-Likelihood-Imputationsmethoden
  - 26.4.3. Imputation verlorener Werte durch maschinelles Lernen
- 26.5. Datenrauschen
  - 26.5.1. Lärmklassen und Attribute
  - 26.5.2. Rauschfilterung
  - 26.5.3. Rauscheffekt

- 26.6. Der Fluch der Dimensionalität
    - 26.6.1. *Oversampling*
    - 26.6.2. *Undersampling*
    - 26.6.3. Multidimensionale Datenreduktion
  - 26.7. Kontinuierliche zu diskreten Attributen
    - 26.7.1. Kontinuierliche vs. Diskrete Daten
    - 26.7.2. Prozess der Diskretisierung
  - 26.8. Die Daten
    - 26.8.1. Datenauswahl
    - 26.8.2. Perspektiven und Auswahlkriterien
    - 26.8.3. Methoden der Auswahl
  - 26.9. Auswahl der Instanzen
    - 26.9.1. Methoden für die Instanzauswahl
    - 26.9.2. Auswahl der Prototypen
    - 26.9.3. Erweiterte Methoden für die Instanzauswahl
  - 26.10. Vorverarbeitung von Daten in *Big Data*-Umgebungen
    - 26.10.1. *Big Data*
    - 26.10.2. Klassische vs. Massive Vorverarbeitung
    - 26.10.3. *Smart Data*
- Modul 27. Vorhersagbarkeit und Analyse von stochastischen Phänomenen**
- 27.1. Zeitreihen
    - 27.1.1. Zeitreihen
    - 27.1.2. Nützlichkeit und Anwendbarkeit
    - 27.1.3. Verwandte Kasuistik
  - 27.2. Die Zeitreihen
    - 27.2.1. Saisonaler Trend von ZR
    - 27.2.2. Typische Variationen
    - 27.2.3. Residuale Analyse
  - 27.3. Typologien
    - 27.3.1. Stationär
    - 27.3.2. Nicht stationär
    - 27.3.3. Transformationen und Anpassungen
  - 27.4. Schemata für Zeitreihen
    - 27.4.1. Additives (Modell) Schema
    - 27.4.2. Multiplikatives (Modell) Schema
    - 27.4.3. Verfahren zur Bestimmung der Art des Modells
  - 27.5. Grundlegende Methoden des *Forecast*
    - 27.5.1. Durchschnitt
    - 27.5.2. *Naiv*
    - 27.5.3. Saisonale *Naive*
    - 27.5.4. Vergleich der Methoden
  - 27.6. Rückstandsanalyse
    - 27.6.1. Autokorrelation
    - 27.6.2. ACF der Residuen
    - 27.6.3. Korrelationstest
  - 27.7. Regression im Kontext von Zeitreihen
    - 27.7.1. ANOVA
    - 27.7.2. Grundlagen
    - 27.7.3. Praktische Anwendung
  - 27.8. Prädiktive Zeitreihenmodelle
    - 27.8.1. ARIMA
    - 27.8.2. Exponentiale Glättung
  - 27.9. Zeitreihenmanipulation und -analyse mit R
    - 27.9.1. Vorbereitung der Daten
    - 27.9.2. Muster-Identifizierung
    - 27.9.3. Modell-Analyse
    - 27.9.4. Vorhersage
  - 27.10. Grafische Analyse kombiniert mit R
    - 27.10.1. Typische Situationen
    - 27.10.2. Praktische Anwendung zum Lösen einfacher Probleme
    - 27.10.3. Praktische Anwendung für fortgeschrittene Problemlösungen

**Modul 28. Design und Entwicklung von intelligenten Systemen**

- 28.1. Vorverarbeitung der Daten
  - 28.1.1. Vorverarbeitung der Daten
  - 28.1.2. Datenumwandlung
  - 28.1.3. Data Mining
- 28.2. Automatisches Lernen
  - 28.2.1. Überwachtes und unüberwachtes Lernen
  - 28.2.2. Verstärkungslernen
  - 28.2.3. Andere Lern-Paradigma
- 28.3. Klassifizierungsalgorithmen
  - 28.3.1. Induktives maschinelles Lernen
  - 28.3.2. SVM und KNN
  - 28.3.3. Metriken und Punktzahlen für die Rangliste
- 28.4. Regressionsalgorithmen
  - 28.4.1. Lineare Regression, logistische Regression und nicht-lineare Modelle
  - 28.4.2. Zeitreihen
  - 28.4.3. Regressionsmetriken und -werte
- 28.5. Clustering-Algorithmen
  - 28.5.1. Hierarchische Clustering-Techniken
  - 28.5.2. Partitionelle Clustering-Techniken
  - 28.5.3. *Clustering*-Metriken und -Bewertungen
- 28.6. Assoziationsregel-Techniken
  - 28.6.1. Methoden zur Extraktion von Regeln
  - 28.6.2. Metriken und Punktzahlen für Assoziationsregel-Algorithmen
- 28.7. Erweiterte Klassifizierungstechniken. Multiklassifizierer
  - 28.7.1. *Bagging*-Algorithmen
  - 28.7.2. "*Random Forests*" Klassifikator
  - 28.7.3. "*Boosting*" für Entscheidungsbäume

- 28.8. Probabilistische grafische Modelle
  - 28.8.1. Probabilistische Modelle
  - 28.8.2. Bayes'sche Netzwerke. Eigenschaften, Darstellung und Parametrisierung
  - 28.8.3. Andere probabilistische grafische Modelle
- 28.9. Neuronale Netze
  - 28.9.1. Maschinelles Lernen mit künstlichen neuronalen Netzen
  - 28.9.2. *Feedforward*-Netzwerke
- 28.10. Tiefes Lernen
  - 28.10.1. Tiefe *Feedforward*-Netzwerke
  - 28.10.2. Faltungsneuronale Netze und Sequenzmodelle
  - 28.10.3. Tools für die Implementierung tiefer neuronaler Netze

**Modul 29. Datenintensive Architekturen und Systeme**

- 29.1. Nicht-funktionale Anforderungen. Säulen der Big Data-Anwendungen
  - 29.1.1. Verlässlichkeit
  - 29.1.2. Anpassungsfähigkeit
  - 29.1.3. Instandhaltbarkeit
- 29.2. Datenmodelle
  - 29.2.1. Relationales Modell
  - 29.2.2. Dokumentarisches Modell
  - 29.2.3. Graph-Datenmodell
- 29.3. Datenbanken. Verwaltung der Speicherung und des Abrufs von Daten
  - 29.3.1. *Hash*-Indizes
  - 29.3.2. Strukturierte Speicherung in *Log*
  - 29.3.3. B-Bäume
- 29.4. Datenverschlüsselungsformate
  - 29.4.1. Sprachspezifische Formate
  - 29.4.2. Standardisierte Formate
  - 29.4.3. Binäre Kodierungsformate
  - 29.4.4. Prozessübergreifender Datenfluss

- 29.5. Replikation
  - 29.5.1. Ziele der Replikation
  - 29.5.2. Replikationsmodelle
  - 29.5.3. Probleme mit der Replikation
- 29.6. Verteilte Transaktionen
  - 29.6.1. Transaktion
  - 29.6.2. Protokolle für verteilte Transaktionen
  - 29.6.3. Serialisierbare Transaktionen
- 29.7. Partitionierung
  - 29.7.1. Formulare unterteilen
  - 29.7.2. Interaktion von Sekundärindex und Partitionierung
  - 29.7.3. Partitionierung neu ausbalancieren
- 29.8. *Offline* Datenverarbeitung
  - 29.8.1. Stapelverarbeitung
  - 29.8.2. Verteilte Dateisysteme
  - 29.8.3. MapReduce
- 29.9. Datenverarbeitung in Echtzeit
  - 29.9.1. Message *Broker*-Typen
  - 29.9.2. Darstellung von Datenbanken als Datenströme
  - 29.9.3. Datenstromverarbeitung
- 29.10. Praktische Anwendungen im Unternehmen
  - 29.10.1. Konsistenz bei der Lektüre
  - 29.10.2. Ganzheitlicher Ansatz für Daten
  - 29.10.3. Skalierung eines verteilten Dienstes

## Modul 30. Praktische Anwendung von Data Science in Geschäftsbereichen

- 30.1. Gesundheitssektor
  - 30.1.1. Auswirkungen von KI und Datenanalyse im Gesundheitssektor
  - 30.1.2. Potenzial und Herausforderungen
- 30.2. Risiken und Trends in der Gesundheitsbranche
  - 30.2.1. Verwendung im Gesundheitssektor
  - 30.2.2. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI





- 30.3. Finanzdienstleistungen
  - 30.3.1. Auswirkungen von KI und Datenanalyse auf den Finanzdienstleistungssektor
  - 30.3.2. Verwendung bei Finanzdienstleistungen
  - 30.3.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI
- 30.4. *Retail*
  - 30.4.1. Auswirkungen von KI und Datenanalyse auf den *Retail*
  - 30.4.2. Verwendung im *Retail*
  - 30.4.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI
- 30.5. Industrie 4.0
  - 30.5.1. Auswirkungen von KI und Datenanalyse in der Industrie 4.0
  - 30.5.2. Einsatz in der Industrie 4.0
- 30.6. Risiken und Trends in der Industrie 4.0
  - 30.6.1. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI
- 30.7. Öffentliche Verwaltung
  - 30.7.1. Auswirkungen von KI und Datenanalyse in der öffentlichen Verwaltung
  - 30.7.2. Verwendung in der öffentlichen Verwaltung
  - 30.7.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI
- 30.8. Bildung
  - 30.8.1. Auswirkungen von KI und Datenanalyse im Bildungswesen
  - 30.8.2. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI
- 30.9. Forst- und Landwirtschaft
  - 30.9.1. Auswirkungen von KI und Datenanalyse auf Forst- und Landwirtschaft
  - 30.9.2. Verwendung in Forst- und Landwirtschaft
  - 30.9.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI
- 30.10. Personalwesen
  - 30.10.1. Auswirkungen von KI und Datenanalyse auf das Personalmanagement
  - 30.10.2. Praktische Anwendungen in der Geschäftswelt
  - 30.10.3. Potenzielle Risiken im Zusammenhang mit dem Einsatz von KI

# 06 Methodik

Dieses Fortbildungsprogramm bietet eine andere Art des Lernens. Unsere Methodik wird durch eine zyklische Lernmethode entwickelt: **das Relearning**.

Dieses Lehrsystem wird z. B. an den renommiertesten medizinischen Fakultäten der Welt angewandt und wird von wichtigen Publikationen wie dem **New England Journal of Medicine** als eines der effektivsten angesehen.



“

*Entdecken Sie Relearning, ein System, das das herkömmliche lineare Lernen aufgibt und Sie durch zyklische Lehrsysteme führt: eine Art des Lernens, die sich als äußerst effektiv erwiesen hat, insbesondere in Fächern, die Auswendiglernen erfordern"*

## Fallstudie zur Kontextualisierung aller Inhalte

Unser Programm bietet eine revolutionäre Methode zur Entwicklung von Fähigkeiten und Kenntnissen. Unser Ziel ist es, Kompetenzen in einem sich wandelnden, wettbewerbsorientierten und sehr anspruchsvollen Umfeld zu stärken.

“

*Mit TECH werden Sie eine Art des Lernens erleben, die die Grundlagen der traditionellen Universitäten in der ganzen Welt verschiebt”*



*Sie werden Zugang zu einem Lernsystem haben, das auf Wiederholung basiert, mit natürlichem und progressivem Unterricht während des gesamten Lehrplans.*



*Die Studenten lernen durch gemeinschaftliche Aktivitäten und reale Fälle die Lösung komplexer Situationen in realen Geschäftsumgebungen.*

## Eine innovative und andersartige Lernmethode

Dieses TECH-Programm ist ein von Grund auf neu entwickeltes, intensives Lehrprogramm, das die anspruchsvollsten Herausforderungen und Entscheidungen in diesem Bereich sowohl auf nationaler als auch auf internationaler Ebene vorsieht. Dank dieser Methodik wird das persönliche und berufliche Wachstum gefördert und ein entscheidender Schritt in Richtung Erfolg gemacht. Die Fallmethode, die Technik, die diesem Inhalt zugrunde liegt, gewährleistet, dass die aktuellste wirtschaftliche, soziale und berufliche Realität berücksichtigt wird.



*Unser Programm bereitet Sie darauf vor, sich neuen Herausforderungen in einem unsicheren Umfeld zu stellen und in Ihrer Karriere erfolgreich zu sein"*

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Informatikschulen der Welt, seit es sie gibt. Die Fallmethode wurde 1912 entwickelt, damit die Jurastudenten das Recht nicht nur anhand theoretischer Inhalte erlernen, sondern ihnen reale, komplexe Situationen vorlegen, damit sie fundierte Entscheidungen treffen und Werturteile darüber fällen können, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard eingeführt.

Was sollte eine Fachkraft in einer bestimmten Situation tun? Mit dieser Frage konfrontieren wir Sie in der Fallmethode, einer handlungsorientierten Lernmethode. Während des gesamten Kurses werden die Studierenden mit mehreren realen Fällen konfrontiert. Sie müssen Ihr gesamtes Wissen integrieren, recherchieren, argumentieren und Ihre Ideen und Entscheidungen verteidigen.

## Relearning Methodik

TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

Wir ergänzen die Fallstudie mit der besten 100%igen Online-Lehrmethode: Relearning.

*Im Jahr 2019 erzielten wir die besten  
Lernergebnisse aller spanischsprachigen  
Online-Universitäten der Welt.*

Bei TECH lernen Sie mit einer hochmodernen Methodik, die darauf ausgerichtet ist, die Führungskräfte der Zukunft auszubilden. Diese Methode, die an der Spitze der weltweiten Pädagogik steht, wird Relearning genannt.

Unsere Universität ist die einzige in der spanischsprachigen Welt, die für die Anwendung dieser erfolgreichen Methode zugelassen ist. Im Jahr 2019 ist es uns gelungen, die Gesamtzufriedenheit unserer Studenten (Qualität der Lehre, Qualität der Materialien, Kursstruktur, Ziele...) in Bezug auf die Indikatoren der besten Online-Universität in Spanisch zu verbessern.



In unserem Programm ist das Lernen kein linearer Prozess, sondern erfolgt in einer Spirale (lernen, verlernen, vergessen und neu lernen). Daher wird jedes dieser Elemente konzentrisch kombiniert. Mit dieser Methode wurden mehr als 650.000 Hochschulabsolventen mit beispiellosem Erfolg in so unterschiedlichen Bereichen wie Biochemie, Genetik, Chirurgie, internationales Recht, Managementfähigkeiten, Sportwissenschaft, Philosophie, Recht, Ingenieurwesen, Journalismus, Geschichte, Finanzmärkte und -Instrumente ausgebildet. Dies alles in einem sehr anspruchsvollen Umfeld mit einer Studentenschaft mit hohem sozioökonomischem Profil und einem Durchschnittsalter von 43,5 Jahren.

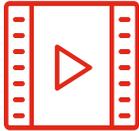
*Das Relearning ermöglicht es Ihnen, mit weniger Aufwand und mehr Leistung zu lernen, sich mehr auf Ihr Fachgebiet einzulassen, einen kritischen Geist zu entwickeln, Argumente zu verteidigen und Meinungen zu kontrastieren: eine direkte Gleichung zum Erfolg.*

Nach den neuesten wissenschaftlichen Erkenntnissen der Neurowissenschaften wissen wir nicht nur, wie wir Informationen, Ideen, Bilder und Erinnerungen organisieren, sondern auch, dass der Ort und der Kontext, in dem wir etwas gelernt haben, von grundlegender Bedeutung dafür sind, dass wir uns daran erinnern und es im Hippocampus speichern können, um es in unserem Langzeitgedächtnis zu behalten.

Auf diese Weise sind die verschiedenen Elemente unseres Programms im Rahmen des so genannten neurokognitiven kontextabhängigen E-Learnings mit dem Kontext verbunden, in dem der Teilnehmer seine berufliche Praxis entwickelt.



Dieses Programm bietet die besten Lehrmaterialien, die sorgfältig für Fachleute aufbereitet sind:



### Studienmaterial

Alle didaktischen Inhalte werden von den Fachleuten, die den Kurs unterrichten werden, speziell für den Kurs erstellt, so dass die didaktische Entwicklung wirklich spezifisch und konkret ist.

Diese Inhalte werden dann auf das audiovisuelle Format angewendet, um die TECH-Online-Arbeitsmethode zu schaffen. Und das alles mit den neuesten Techniken, die dem Studenten qualitativ hochwertige Stücke aus jedem einzelnen Material zur Verfügung stellen.



### Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

Das sogenannte Learning from an Expert baut Wissen und Gedächtnis auf und schafft Vertrauen für zukünftige schwierige Entscheidungen.



### Fertigkeiten und Kompetenzen Praktiken

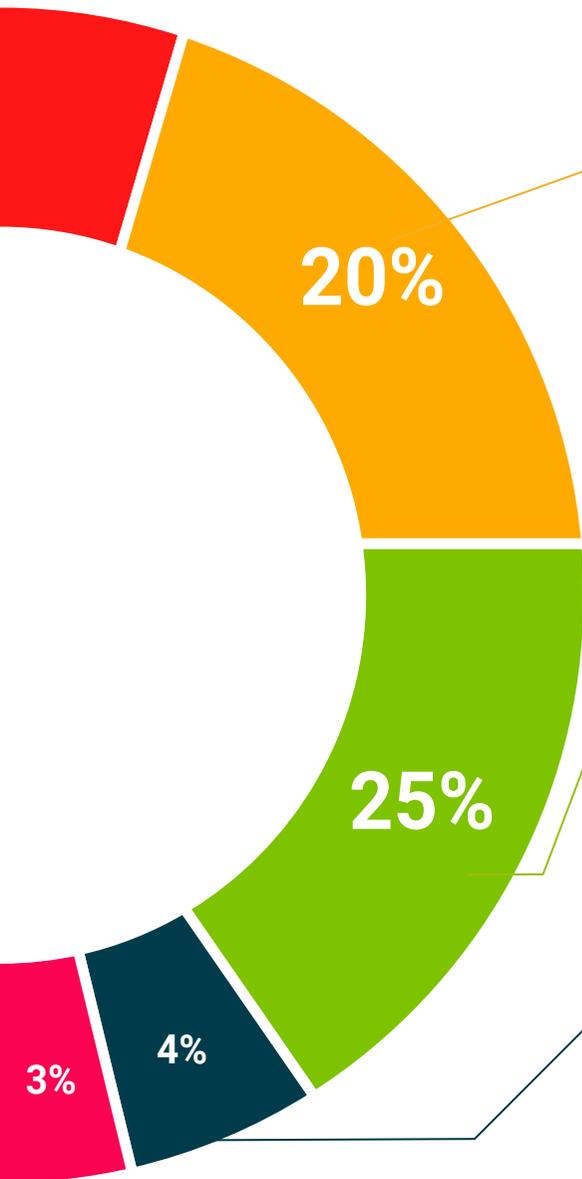
Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Praktiken und Dynamiken zum Erwerb und zur Entwicklung der Fähigkeiten und Fertigkeiten, die ein Spezialist im Rahmen der Globalisierung, in der wir leben, entwickeln muss.



### Weitere Lektüren

Aktuelle Artikel, Konsensdokumente und internationale Leitfäden, u.a. In der virtuellen Bibliothek von TECH haben die Studenten Zugang zu allem, was sie für ihre Ausbildung benötigen.





#### Fallstudien

Sie werden eine Auswahl der besten Fallstudien vervollständigen, die speziell für diese Qualifizierung ausgewählt wurden. Die Fälle werden von den besten Spezialisten der internationalen Szene präsentiert, analysiert und betreut.



#### Interaktive Zusammenfassungen

Das TECH-Team präsentiert die Inhalte auf attraktive und dynamische Weise in multimedialen Pillen, die Audios, Videos, Bilder, Diagramme und konzeptionelle Karten enthalten, um das Wissen zu vertiefen.

Dieses einzigartige Bildungssystem für die Präsentation multimedialer Inhalte wurde von Microsoft als "europäische Erfolgsgeschichte" ausgezeichnet.



#### Prüfung und Nachprüfung

Die Kenntnisse der Studenten werden während des gesamten Programms regelmäßig durch Bewertungs- und Selbsteinschätzungsaktivitäten und -übungen beurteilt und neu bewertet, so dass die Studenten überprüfen können, wie sie ihre Ziele erreichen.



07

# Qualifizierung

Der Weiterbildender Masterstudiengang in Informatik, Cybersecurity und Datenanalyse garantiert neben der strengsten und aktuellsten Ausbildung auch den Zugang zu einem von der TECH Technologischen Universität ausgestellten Diplom.



“

*Schließen Sie dieses Programm erfolgreich ab  
und erhalten Sie Ihren Universitätsabschluss  
ohne lästige Reisen oder Formalitäten"*

Dieser **Weiterbildender Masterstudiengang in Informatik, Cybersecurity und Datenanalyse** enthält das vollständigste und aktuellste Programm auf dem Markt.

Sobald der Student die Prüfungen bestanden hat, erhält er/sie per Post\* mit Empfangsbestätigung das entsprechende Diplom, ausgestellt von der **TECH Technologischen Universität**.

Das von **TECH Technologische Universität** ausgestellte Diplom drückt die erworbene Qualifikation aus und entspricht den Anforderungen, die in der Regel von Stellenbörsen, Auswahlprüfungen und Berufsbildungsausschüssen verlangt werden.

Titel: **Weiterbildender Masterstudiengang in Informatik, Cybersecurity und Datenanalyse**

Anzahl der offiziellen Arbeitsstunden: **3.000 Std.**



\*Haager Apostille. Für den Fall, dass der Student die Haager Apostille für sein Papierdiplom beantragt, wird TECH EDUCATION die notwendigen Vorkerhungen treffen, um diese gegen eine zusätzliche Gebühr zu beschaffen.

zukunft

gesundheit vertrauen menschen  
erziehung information tutoeren  
garantie akkreditierung unterricht  
institutionen technologie lernen  
gemeinschaft verpflichtung  
persönliche betreuung innovation  
wissen gegenwart qualitaet  
online-Ausbildung  
entwicklung institutionen  
virtuelles Klassenzimmer sparten

**tech** technologische  
universität

Weiterbildender  
Masterstudiengang  
Informatik, Cybersecurity  
und Datenanalyse

- » Modalità: online
- » Durata: 2 Jahre
- » Titolo: TECH Università Tecnologica
- » Orario: a scelta
- » Esami: online

Weiterbildender  
Masterstudiengang  
Informatik, Cybersecurity  
und Datenanalyse