Weiterbildender Masterstudiengang
Telematik

tech global university

tech global university

Weiterbildender Masterstudiengang

Telematik

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Global University**
- Akkreditierung: **60 ECTS**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

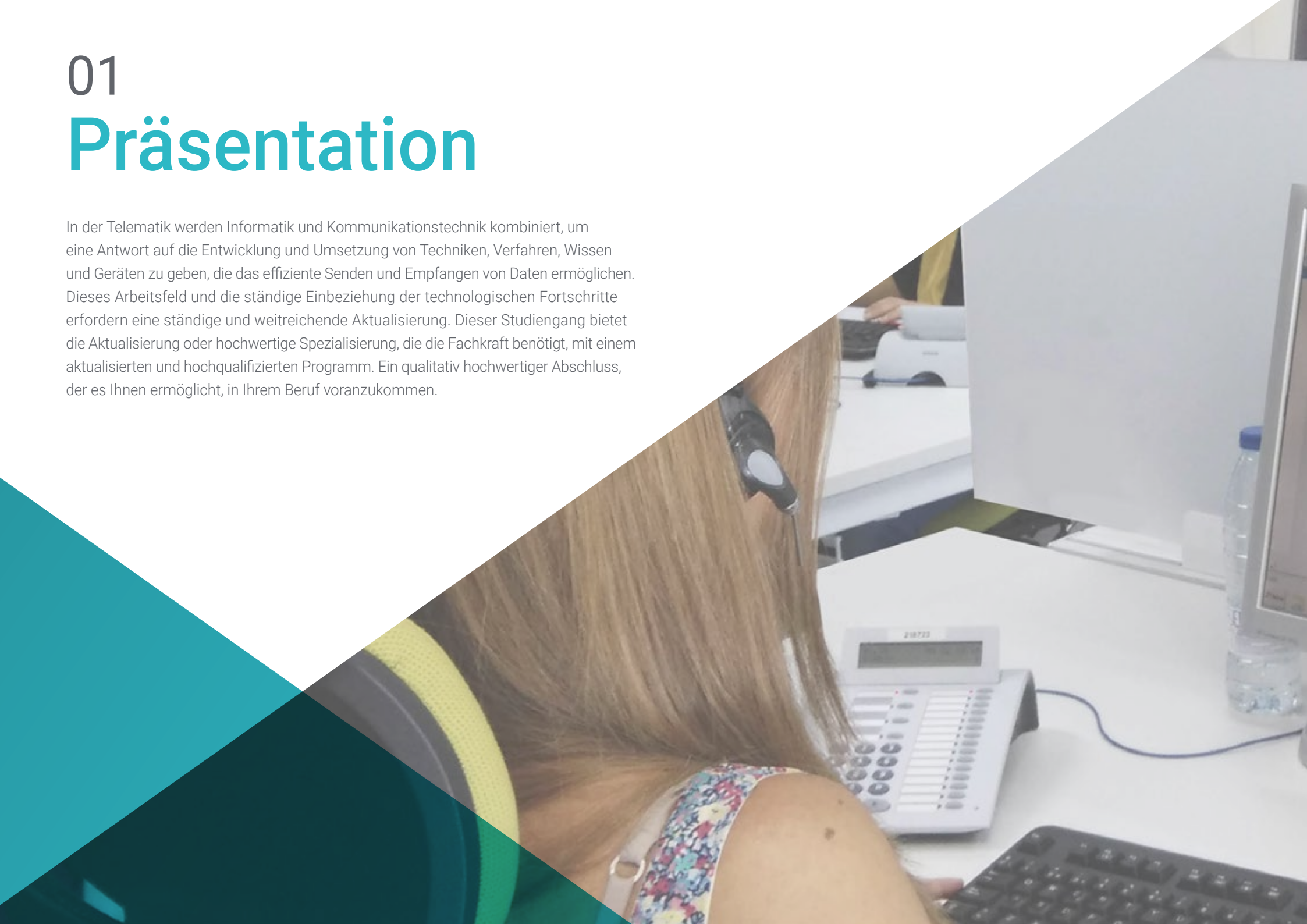
Internetzugang: www.techtitute.com/de/informatik/weiterbildender-masterstudiengang/weiterbildender-masterstudiengang-telematik

Index

01

Präsentation

In der Telematik werden Informatik und Kommunikationstechnik kombiniert, um eine Antwort auf die Entwicklung und Umsetzung von Techniken, Verfahren, Wissen und Geräten zu geben, die das effiziente Senden und Empfangen von Daten ermöglichen. Dieses Arbeitsfeld und die ständige Einbeziehung der technologischen Fortschritte erfordern eine ständige und weitreichende Aktualisierung. Dieser Studiengang bietet die Aktualisierung oder hochwertige Spezialisierung, die die Fachkraft benötigt, mit einem aktualisierten und hochqualifizierten Programm. Ein qualitativ hochwertiger Abschluss, der es Ihnen ermöglicht, in Ihrem Beruf voranzukommen.



Dieses umfassende, vollständig aktualisierte und an Ihre Verfügbarkeit anpassbare Programm ist ein hochwertiges Hilfsmittel für Informatiker, die ihre realen Fähigkeiten erweitern wollen"

In der Telekommunikation, einem der sich am schnellsten entwickelnden Bereiche, gibt es ständig neue Entwicklungen. Es ist daher notwendig, über IT-Experten zu verfügen, die sich an diese Veränderungen anpassen können und die neuen Instrumente und Techniken, die in diesem Bereich entstehen, aus erster Hand kennen.

Das Programm in Telematik umfasst alle Themen, die mit diesem Bereich zu tun haben. Das Studium hat einen klaren Vorteil gegenüber anderen Masterstudiengängen, die sich auf bestimmte Blöcke konzentrieren, wodurch der Student die Zusammenhänge mit anderen Bereichen des multidisziplinären Bereichs der Telekommunikation nicht kennt. Darüber hinaus hat das Dozententeam dieses Programms eine sorgfältige Auswahl der einzelnen Themen getroffen, um dem Studenten ein möglichst umfassendes Studium zu ermöglichen das stets mit dem aktuellen Zeitgeschehen verbunden ist.

Das Programm richtet sich an Personen, die ihr Wissen über die Telematik vertiefen möchten. Das Hauptziel besteht darin, den Studenten in die Lage zu versetzen, das in diesem Programm erworbene Wissen in der realen Welt anzuwenden, und zwar in einem Arbeitsumfeld, das die Bedingungen, die in seiner Zukunft vorzufinden sind, auf präzise und realistische Weise reproduziert.

Da es sich um ein 100%iges Online-Programm handelt, ist der Student nicht an feste Zeiten oder die Notwendigkeit, sich an einen anderen Ort zu begeben, gebunden, sondern kann zu jeder Tageszeit auf die Inhalte zugreifen und so sein Arbeits- oder Privatleben mit seinem akademischen Leben in Einklang bringen.

Dieser **Weiterbildender Masterstudiengang in Telematik** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten für Telematik präsentiert werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren wissenschaftlichen und praktischen Informationen
- Er enthält praktische Übungen, in denen der Selbstbewertungsprozess durchgeführt werden kann, um das Lernen zu verbessern
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden im Bereich Telematik
- 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

Erweitern Sie Ihre Kompetenzen um die Fähigkeit, in den verschiedenen Bereichen der Telematik tätig zu werden, mit einem Lernpfad, der Ihre berufliche Entwicklung fördern wird"

Dieses Programm ist die beste Investition, die Sie tätigen können, wenn Sie sich für ein Fortbildungsprogramm entscheiden, um Ihr Wissen in Telematik zu aktualisieren"

Das didaktische Material, mit dem Sie Ihr Studium entwickeln werden, ist ein Kompendium von hoher Qualität, das es Ihnen ermöglicht, auf bequeme und einfache Weise Fortschritte zu machen.

Dieses 100%ige Online-Programm ermöglicht es Ihnen, Ihr Studium mit Ihrer beruflichen Tätigkeit zu verbinden.

Das Dozententeam setzt sich aus Fachleuten aus dem Bereich der Telekommunikationsinformatik zusammen, die ihre Berufserfahrung in diese Fortbildung einbringen, sowie aus anerkannten Experten von führenden Gesellschaften und renommierten Universitäten.

Die multimedialen Inhalte, die mit der neuesten Bildungstechnologie entwickelt wurden, werden der Fachkraft ein situiertes und kontextbezogenes Lernen ermöglichen, d. h. eine simulierte Umgebung, die eine immersive Fortbildung bietet, die auf die Ausführung von realen Situationen ausgerichtet ist.

Das Konzept dieses Programms konzentriert sich auf problemorientiertes Lernen, bei dem die Fachkraft versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des gesamten Studiengangs gestellt werden. Dabei wird sie von einem innovativen interaktiven Videosystem unterstützt, das von anerkannten und erfahrenen Experten in Telematik entwickelt wurde.

02

Ziele

Das Programm Telematik zielt darauf ab, den IT-Fachleuten ein vollständiges und aktuelles Studium aller Bereiche zu bieten, die mit der Telematik zu tun haben, mit der Sicherheit und Qualität eines Programms, das nach dem Kriterium der absoluten Exzellenz erstellt wurde.

Das Ziel dieses Programm ist es, den Fachleuten einen vollständigen Überblick über die theoretischen und praktischen Kenntnisse zu geben, die sie im Bereich der Telematik benötigen"

Allgemeines Ziel

- Fortbilden der Studenten, damit sie unter anderem in der Lage sind, Telematikanwendungen zu entwickeln, Daten zu analysieren oder Aufgaben der digitalen Sicherheit wahrzunehmen

Eine Gelegenheit, die für Fachleute geschaffen wurde, die einen intensiven und effektiven Kurs suchen, um in ihrem Beruf einen bedeutenden Schritt nach vorne zu machen"

Spezifische Ziele

Modul 1. Computer-Netzwerke

- Aneignen der wesentlichen Kenntnisse über Computernetzwerke im Internet
- Verstehen der Funktionsweise der verschiedenen Schichten, die ein vernetztes System definieren, z. B. Anwendungs-, Transport-, Netzwerk- und Verbindungsschicht
- Verstehen des Aufbaus von LANs, ihrer Topologie, Netzwerk- und Verbindungselemente
- Lernen, wie IP-Adressierung und Subnetting funktionieren
- Verstehen der Struktur von drahtlosen und mobilen Netzen, einschließlich des neuen 5G-Netzes
- Verstehen der verschiedenen Netzwerksicherheitsmechanismen sowie der verschiedenen Internet-Sicherheitsprotokolle

Modul 2. Verteilte Systeme

- Beherrschen der Grundprinzipien verteilter Systeme
- Erlernen der Charakterisierung und Klassifizierung verteilter Systeme in Bezug auf eine Reihe grundlegender Parameter
- Verstehen der verschiedenen Arten von Modellen, die in verteilten Systemen verwendet werden
- Verstehen der aktuellen Architekturen, die das Konzept des verteilten Dateisystems umsetzen
- In der Lage sein, Prozess- und Objektsynchronisationsalgorithmen, die Definition logischer Uhren und die zeitliche Konsistenz von Informationen zu analysieren
- Verstehen des im Internet verwendeten Namensgebungs-systems DNS (Domain Name System)
- Lernen, wie IP-Adressierung und Subnetting funktionieren

Modul 3. Sicherheit in Kommunikationssystemen und -netzen

- Erwerben einer globalen Perspektive auf Sicherheit, Kryptographie und klassische Kryptoanalysen
- Verstehen der Grundlagen der symmetrischen und asymmetrischen Kryptographie sowie deren Hauptalgorithmen
- Analysieren der Art von Netzwerkangriffen und der verschiedenen Arten von Sicherheitsarchitekturen
- Verstehen der verschiedenen Techniken für den Systemschutz und die Entwicklung von sicherem Code
- Verstehen der wesentlichen Komponenten von Botnets und Spam sowie von Malware und bösartigem Code
- Schaffen der Grundlagen für die forensische Analyse in der Welt der Software- und IT-Prüfung

Modul 4. Unternehmensnetze und -infrastrukturen

- Beherrschen fortgeschrittener Aspekte der Infrastrukturzusammenschaltung, die für den Entwurf und die Planung von Hochgeschwindigkeitsnetzen unerlässlich sind
- Kennen der wichtigsten Merkmale und Technologien von Verkehrsnetzen
- Verstehen der klassischen WAN-Architekturen, All-Ethernet, MPLS, VPN
- Analysieren der grundlegenden Aspekte der Entwicklung von Netzen zu NGN (Next Generation Networks)
- Verstehen der fortgeschrittenen QoS-, Routing- und Staukontroll- und Zuverlässigkeitsanforderungen
- Kennen und Anwenden der internationalen Netzwerkstandards

Modul 5. Sicherheitsarchitekturen

- Verstehen der Grundprinzipien der IT-Sicherheit
- Beherrschen von IT-Sicherheitsstandards und Zertifizierungsverfahren
- Analysieren der organisatorischen und kryptographischen Grundlagen, auf denen die Sicherheitstechnologien beruhen
- Identifizieren der wichtigsten Bedrohungen und Schwachstellen der verschiedenen IKT-Elemente sowie deren Ursachen
- Vertiefen der Kenntnisse über Netzsicherheitstools und ihren spezifischen Funktionen
- Anwenden der Technologien, aus denen sich eine IKT-Sicherheitsarchitektur zusammensetzt, in ihren verschiedenen Aspekten

Modul 6. Rechenzentren, Netzbetrieb und Dienstleistungen

- In der Lage sein, Netze, Dienste und Inhalte, die über ein Rechenzentrumbereitgestellt werden, zu entwerfen, zu betreiben, zu verwalten und zu warten
- Kennen aller wesentlichen Elemente, aus denen ein Rechenzentrum besteht, sowie der bestehenden Normen und Zertifizierungen
- Analysieren der wirtschaftlichen Auswirkungen der Infrastruktur eines Rechenzentrums in Bezug auf Leistung und Effizienz
- Identifizieren der Hardware-Elemente eines Rechenzentrums in realen Infrastrukturen
- Verstehen der Sicherheitsaspekte der verschiedenen Lösungen für das Anbieten von Dienstleistungen durch Marktanbieter
- Kennen der Funktionsweise des Virtualisierungsprozesses
- Verstehen der Vorteile, des Nutzens und der Einführungsmodelle der Cloud

Modul 7. Fortgeschrittene Programmierung

- Vertiefen der Kenntnisse in der Programmierung, insbesondere in Bezug auf die objektorientierte Programmierung und die verschiedenen Arten von Beziehungen zwischen bestehenden Klassen
- Kennen der verschiedenen Entwurfsmuster für objektorientierte Probleme
- Kennen der ereignisgesteuerten Programmierung und der Entwicklung von Benutzeroberflächen mit Qt
- Aneignen der grundlegenden Kenntnisse über nebenläufige Programmierung, Prozesse und Threads
- Lernen, wie man die Verwendung von Threads und die Synchronisierung handhabt, sowie die Lösung gängiger Probleme bei der gleichzeitigen Programmierung
- Verstehen der Bedeutung von Dokumentation und Tests bei der Softwareentwicklung

Modul 8. Technik für Systeme und Netzdienste

- Beherrschen der grundlegenden Konzepte der Dienstleistungstechnik
- Kennen der Grundprinzipien des Konfigurationsmanagements von sich entwickelnden Softwaresystemen
- Kennen der Technologien und Instrumente für die Bereitstellung von Telematikdiensten
- Kennen der verschiedenen architektonischen Stile eines Softwaresystems, Verstehen ihrer Unterschiede und Wissen, wie man den am besten geeigneten Stil je nach den Systemanforderungen auswählt
- Verstehen der Validierungs- und Verifizierungsprozesse und ihrer Beziehung zu anderen Phasen des Lebenszyklus
- In der Lage sein, Systeme zur Erfassung, Darstellung, Verarbeitung, Speicherung, Verwaltung und Präsentation multimedialer Informationen für den Aufbau von Telekommunikationsdiensten und Telematikanwendungen zu integrieren

- Kennen allgemeiner Elemente für den detaillierten Entwurf eines Softwaresystems
- Erwerben von Programmier-, Simulations- und Validierungskenntnissen für telematische, vernetzte und verteilte Dienste und Anwendungen
- Kennen des Prozesses und der Aktivitäten der Umstellung, Konfiguration, Bereitstellung und des Betriebs
- Verstehen der Prozesse der Netzverwaltung, -automatisierung und -optimierung

Modul 9. Prüfung von Informationssystemen

- Beherrschen der wichtigsten Konzepte, Normen und Methoden der Systemprüfung
- Kennen der organisatorischen Elemente und des rechtlichen Rahmens von Audits
- Erhalten eines Leitfadens für die Gestaltung neuer interner IT-Kontrollsysteme
- Verstehen und Identifizieren der Risiken, die durch technologische Entwicklungen entstehen
- Erkennen, wie verschiedene Informationssysteme die gewünschten Sicherheitsanforderungen erfüllen oder nicht erfüllen
- Durchführen eines Prozesses zur kontinuierlichen Verbesserung der Cybersicherheit

Modul 10. Projektmanagement

- Kennen der grundlegenden Konzepte des Projektmanagements und des Lebenszyklus des Projektmanagements
- Verstehen der verschiedenen Phasen des Projektmanagements wie Initiierung, Planung, *Stakeholder*-Management und Scoping
- Lernen, einen Zeitplan für das Zeitmanagement, die Budgetentwicklung und die Reaktion auf Risiken zu erstellen
- Verstehen der Funktionsweise des Qualitätsmanagements in Projekten, einschließlich Planung, Sicherung, Kontrolle, statistischer Konzepte und verfügbarer Instrumente
- Verstehen, wie die Prozesse der Projektbeschaffung, -durchführung, -überwachung, -kontrolle und -abschluss funktionieren
- Aneignen der wesentlichen Kenntnisse im Zusammenhang mit der beruflichen Verantwortung, die sich aus dem Projektmanagement ergibt

03

Kompetenzen

Nach Bestehen der Bewertungen des Weiterbildender Masterstudiengangs in Telematik werden die Studenten die notwendigen Kompetenzen erworben haben, um in den verschiedenen Arbeitsbereichen der Telematik sicher und zeitgemäß zu agieren. Ein Prozess der Kompetenzerweiterung, der ihre berufliche Laufbahn entscheidend beeinflussen wird.

Erwerben Sie die Kompetenzen eines Telematikspezialisten und beginnen Sie, in diesem Bereich mit dem Weitblick einer Spitzenfachkraft tätig zu werden"

Allgemeine Kompetenz

- Entwickeln von Telematikanwendungen und Durchführen von Aufgaben der digitalen Sicherheit

Spezialisieren Sie sich mit den Besten und stehen Sie an der Spitze der professionellen Intervention"

Spezifische Kompetenzen

- Kennen der gesamten Struktur von Computernetzen
- Beherrschen verteilter Systeme und Wissen, wie man sie klassifiziert
- Durchführen von Sicherheitsaufgaben in Kommunikationssystemen und -netzen
- Anwenden internationaler Normen für Netzwerke
- Beherrschen aller IT-Sicherheitsverfahren
- Planen und Verwalten von Datenzentren
- Erstellen von Programmierungen und Erkennen möglicher Probleme und deren Lösung
- Verstehen des gesamten Prozesses der Systementwicklung
- Durchführen von Systemaudits und Verbessern der Cybersicherheit
- Kennen aller Phasen des Projektmanagements und seines Lebenszyklus, um zu wissen, wie man sie steuert

04

Kursleitung

Dieses akademische Programm verfügt über den spezialisiertesten Lehrkörper auf dem aktuellen Bildungsmarkt. Es handelt sich um Spezialisten, die von TECH ausgewählt wurden, um den gesamten Studiengang zu entwickeln. Auf diese Weise haben sie auf der Grundlage ihrer eigenen Erfahrung und der neuesten Erkenntnisse die aktuellsten Inhalte entworfen, die eine Qualitätsgarantie für ein so relevantes Thema bieten.

TECH bietet Ihnen den spezialisiertesten Lehrkörper in diesem Fachgebiet. Schreiben Sie sich jetzt ein und genießen Sie die Qualität, die Sie verdienen"

Internationaler Gastdirektor

Kevin Jackson ist ein hervorragender Produktmanager mit einer starken Erfolgsbilanz bei der Integration von technischen und kommerziellen Fähigkeiten. Als Spezialist für Marktanalysen, Produktplanung und -innovation sowie für die Entwicklung von Geschäftsszenarien hat er sich in seiner Karriere auf die Entwicklung fortschrittlicher Technologielösungen für die Bereiche Telekommunikation und Konnektivität konzentriert. Darüber hinaus hat er durch seine Fähigkeit, komplexe Teams und Projekte zu leiten, bedeutende Ergebnisse im Bereich der Fahrzeug- und Anlagentelematik erzielt.

Er hatte auch Schlüsselpositionen bei Verizon Connect inne, wo er als stellvertretender Direktor für Produktmanagement tätig war. In dieser Funktion leitete er die Entwicklung der Fahrzeug- und Anlagentelematiklösung und trieb Innovationen bei Web-, Mobil- und IoT-Geräteanwendungen voran. Außerdem war er Produktmanager im Bereich Connected Devices und leitete ein Team zur Entwicklung von Technologielösungen, die die Konnektivität und Benutzerfreundlichkeit verbessern

International wurde er für seine Fähigkeit, innovative Ideen in erfolgreiche Produkte zu verwandeln, anerkannt. In der Tat hat seine Arbeit dazu beigetragen, das Unternehmen Accenture als Referenz bei der Entwicklung fortschrittlicher Lösungen für den Video- und Telekommunikationsmarkt zu positionieren. Seine Erfahrung in der Zusammenarbeit mit globalen Vertriebskanälen und seine Beherrschung agiler Methoden haben seinen Ruf als einflussreiche Führungspersönlichkeit im Bereich des technologischen Produktmanagements gefestigt.

Er hat sein Wissen auch durch Veröffentlichungen und Präsentationen auf Branchenkonferenzen weitergegeben und dabei Themen wie die Qualität der Benutzererfahrung und die Entwicklung der digitalen Konnektivität angesprochen. Sein Fokus auf Innovation und Produktentwicklung treibt den Fortschritt in der Branche weiter voran und macht ihn zu einem der führenden Köpfe bei der Entwicklung innovativer Technologielösungen.

Hr. Jackson, Kevin

- Stellvertretender Direktor für Produktmanagement bei Verizon Connect, Dublin, Irland
- Produktmanager für vernetzte Geräte bei Verizon Connect
- Produktlinienleiter bei Accenture
- Manager für Software-Produktmanagement bei Accenture
- Produktmanager bei S3 Group
- Produktmanager bei Harris Broadcast
- Produktmanager bei Zandar Technologies
- Masterstudiengang in Produktmanagement von der Technologischen Universität von Dublin
- Masterstudiengang in Elektrotechnik mit Telekommunikation an der Universität von Hull
- Hochschulabschluss in Elektrotechnik von der Technologischen Universität von Dublin

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

05

Struktur und Inhalt

Die Struktur der Inhalte wurde von den besten Fachleuten des Sektors der Telekommunikationsinformatik entworfen. Ein intensiver und vollständiger Studiengang, der alle Aspekte umfasst, die ein Informatiker, der in der Telematik tätig ist, mit Sicherheit beherrschen muss, und der für den Studenten strukturiert und effizient entwickelt wurde.

Wir haben das vollständigste und aktuellste Programm auf dem Markt. Wir streben nach Exzellenz und wollen, dass auch Sie sie erreichen"

Modul 1. Computer-Netzwerke

1.1. Computernetzwerke im Internet
- 1.1.1. Netzwerke und das Internet
- 1.1.2. Protokoll-Architektur

1.2. Die Anwendungsschicht
- 1.2.1. Modell und Protokolle
- 1.2.2. FTP- und SMTP-Dienste
- 1.2.3. DNS-Dienst
- 1.2.4. HTTP-Operationsmodell
- 1.2.5. HTTP-Nachrichtenformate
- 1.2.6. Interaktion mit fortgeschrittenen Methoden

1.3. Die Transportschicht
- 1.3.1. Kommunikation zwischen Prozessen
- 1.3.2. Verbindungsorientierter Transport: TCP und SCTP

1.4. Die Netzwerkschicht
- 1.4.1. Leitungsvermittlung und Paketvermittlung
- 1.4.2. Das IP-Protokoll (v4 und v6)
- 1.4.3. Routing-Algorithmen

1.5. Die Verbindungsschicht
- 1.5.1. Verbindungsschicht und Techniken zur Fehlererkennung und -korrektur
- 1.5.2. Mehrfachzugriffsverbindungen und -protokolle
- 1.5.3. Adressierung auf Verbindungsebene

1.6. LAN-Netzwerke
- 1.6.1. Netzwerk-Topologien
- 1.6.2. Netzwerk- und Zusammenschaltungselemente

1.7. IP-Adressierung
- 1.7.1. IP-Adressierung und *Subnetting*
- 1.7.2. Überblick: eine HTTP-Anfrage

1.8. Drahtlose und mobile Netzwerke
- 1.8.1. 2G-, 3G- und 4G-Mobilfunknetze und -dienste
- 1.8.2. 5G-Netze

1.9. Netzwerksicherheit
- 1.9.1. Grundlagen der Kommunikationssicherheit
- 1.9.2. Zugangskontrolle
- 1.9.3. Sicherheit des Systems
- 1.9.4. Grundlagen der Kryptographie
- 1.9.5. Digitale Unterschrift

1.10. Internet-Sicherheitsprotokolle
- 1.10.1. IP-Sicherheit und virtuelle private Netzwerke (VPNs)
- 1.10.2. Web-Sicherheit mit SSL/TLS

Modul 2. Verteilte Systeme

2.1. Einführung in das verteilte Rechnen
- 2.1.1. Grundlegende Konzepte
- 2.1.2. Monolithisches, verteiltes, paralleles und kooperatives Rechnen
- 2.1.3. Vorteile, Nachteile und Herausforderungen von verteilten Systemen
- 2.1.4. Vorläufige Konzepte zu Betriebssystemen: Prozesse und Gleichzeitigkeit
- 2.1.5. Hintergrund der Vernetzung
- 2.1.6. Vorläufige Konzepte zur Softwareentwicklung
- 2.1.7. Aufbau des Handbuchs

2.2. Verteiltes Rechnen und Kommunikationsparadigmen zwischen Prozessen
- 2.2.1. Kommunikation zwischen Prozessen
- 2.2.2. Synchronisierung der Ereignisse
  - 2.2.2.1. Beispiel 1: Synchrones Senden und synchroner Empfang
  - 2.2.2.2. Beispiel 2: Asynchrones Senden und synchroner Empfang
  - 2.2.2.3. Beispiel 3: Synchrones Senden und asynchrones Empfangen
  - 2.2.2.4. Beispiel 4: Asynchrones Senden und asynchrones Empfangen
- 2.2.3. Verriegelungen und Zeitschaltuhren
- 2.2.4. Datendarstellung und Kodierung
- 2.2.5. Klassifizierung und Beschreibung von Paradigmen der verteilten Datenverarbeitung
- 2.2.6. Java als Entwicklungsumgebung für verteilte Systeme

2.3. *Socket*-APIs
- 2.3.1. Sockets-APIs, Typen und Unterschiede
- 2.3.2. Sockets für Datagramme
- 2.3.3. Sockets für *Streams*
- 2.3.4. Interlock-Lösung: Zeitgeber und nicht blockierende Ereignisse
- 2.3.5. *Socket*-Sicherheit

2.4. Paradigma der Kunden-Server-Kommunikation
- 2.4.1. Grundlegende Merkmale und Konzepte von verteilten Kunden-Server-Systemen
- 2.4.2. Prozess der Konzeption und Implementierung eines Kunden-Server-Systems
- 2.4.3. Nicht verbindungsorientierte Adressierungsprobleme mit anonymen Kunden
- 2.4.4. Iterative und konkurrierende Server
- 2.4.5. Informationen zu Staat und Sitzung
  - 2.4.5.1. Sitzungsinformationen
  - 2.4.5.2. Globale Statusinformationen
- 2.4.6. Komplexe Kunden, die asynchrone Antworten von der Serverseite erhalten
- 2.4.7. Komplexe Server, die als Vermittler zwischen mehreren Kunden fungieren

2.5. Kommunikation in der Gruppe
- 2.5.1. Einführung in Multicast und häufige Verwendungen
- 2.5.2. Verlässlichkeit und Ordnung in Multicast-Systemen
- 2.5.3. Java-Implementierung von Multicast-Systemen
- 2.5.4. Beispiel für den Einsatz der Peer-to-Peer-Gruppenkommunikation
- 2.5.5. Zuverlässige Multicast-Implementierungen
- 2.5.6. Multicast auf Anwendungsebene

2.6. Verteilte Objekte
- 2.6.1. Einführung in verteilte Objekte
- 2.6.2. Architektur einer auf verteilten Objekten basierenden Anwendung
- 2.6.3. Technologien für verteilte Objektsysteme
- 2.6.4. Java RMI Client-seitige und Server-seitige Software-Schichten
- 2.6.5. Java RMI-APIs für verteilte Objekte
- 2.6.6. Schritte zur Erstellung einer RMI-Anwendung
- 2.6.7. Verwendung von *Callback* in RMI
- 2.6.8. Dynamisches Offloading von entfernten Objekt-Stubs und RMI-Sicherheitsmanager

2.7. Internetanwendungen I: HTML, XML, HTTP
- 2.7.1. Einführung in Internetanwendungen I
- 2.7.2. HTML-Sprache
- 2.7.3. XML-Sprache
- 2.7.4. HTTP-Internetprotokoll
- 2.7.5. Verwendung von dynamischen Inhalten: Formularverarbeitung und CGI
- 2.7.6. Handhabung von Status- und Sitzungsdaten im Internet

2.8. CORBA
- 2.8.1. Einführung in CORBA
- 2.8.2. CORBA-Architektur
- 2.8.3. Schnittstellenbeschreibungssprache in CORBA
- 2.8.4. GIOP-Interoperabilitätsprotokolle
- 2.8.5. IOR Entfernte Objektreferenzen
- 2.8.6. CORBA-Benennungsdienst
- 2.8.7. Java IDL-Beispiel
- 2.8.8. Entwerfen, Kompilieren und Ausführen von Schritten in Java IDL

2.9. Internetanwendungen II: Applets, Servlets und SOA
- 2.9.1. Einführung in Internetanwendungen II
- 2.9.2. Applets
- 2.9.3. Einführung in Servlets
- 2.9.4. HTTP-Servlets und wie sie funktionieren
- 2.9.5. Beibehaltung von Zustandsinformationen in Servlets
  - 2.9.5.1. Ausgeblendete Formularfelder
  - 2.9.5.2. *Cookies*
  - 2.9.5.3. Servlet-Variablen
  - 2.9.5.4. Sitzungsobjekt
- 2.9.6. Webdienste
- 2.9.7. SOAP-Protokoll
- 2.9.8. Kurzer Überblick über die REST-Architektur

2.10. Fortgeschrittene Paradigmen
- 2.10.1. Einführung in fortgeschrittene Paradigmen
- 2.10.2. MOM-Paradigma
- 2.10.3. Paradigma des mobilen Software-Agenten
- 2.10.4. Paradigma des Objektraums
- 2.10.5. Kollaboratives Rechnen
- 2.10.6. Künftige Trends im verteilten Rechnen

Modul 3. Sicherheit in Kommunikationssystemen und -netzen

3.1. Ein Überblick über Sicherheit, Kryptographie und klassische Kryptoanalyse
- 3.1.1. Computersicherheit: Historische Perspektive
- 3.1.2. Aber was genau ist mit Sicherheit gemeint?
- 3.1.3. Geschichte der Kryptographie
- 3.1.4. Substitutions-Chiffren
- 3.1.5. Fallstudie: Die Enigma-Maschine

3.2. Symmetrische Kryptographie
- 3.2.1. Einführung und grundlegende Terminologie
- 3.2.2. Symmetrische Verschlüsselung
- 3.2.3. Betriebsarten
- 3.2.4. DES
- 3.2.5. Der neue AES-Standard
- 3.2.6. Stream-Verschlüsselung
- 3.2.7. Kryptoanalyse

3.3. Asymmetrische Kryptographie
- 3.3.1. Die Ursprünge der Public Key-Kryptographie
- 3.3.2. Grundlegende Konzepte und Bedienung
- 3.3.3. Der RSA-Algorithmus
- 3.3.4. Digitale Zertifikate
- 3.3.5. Speicherung und Verwaltung von Schlüsseln

3.4. Netzwerk-Angriffe
- 3.4.1. Bedrohungen und Angriffe aus dem Netzwerk
- 3.4.2. Aufzählung
- 3.4.3. Verkehrsüberwachung: *Sniffers*
- 3.4.4. Denial-of-Service-Angriffe
- 3.4.5. ARP-Poisoning-Angriffe

3.5. Sicherheitsarchitekturen
- 3.5.1. Traditionelle Sicherheitsarchitekturen
- 3.5.2. Secure Socket Layer: SSL
- 3.5.3. SSH-Protokoll
- 3.5.4. Virtuelle private Netzwerke (VPN)
- 3.5.5. Schutzmechanismen für externe Speicherlaufwerke
- 3.5.6. Hardware-Schutzmechanismen

3.6. Systemschutztechniken und Entwicklung von sicherem Code
- 3.6.1. Sicherheit bei Operationen
- 3.6.2. Ressourcen und Kontrollen
- 3.6.3. Überwachung
- 3.6.4. Intrusion Detection Systeme
- 3.6.5. *Host*-IDS
- 3.6.6. Netzwerk-IDS
- 3.6.7. Signatur-basiertes IDS
- 3.6.8. Decoy-Systeme
- 3.6.9. Grundlegende Sicherheitsprinzipien bei der Code-Entwicklung
- 3.6.10. Störungsmanagement
- 3.6.11. Staatsfeind Nummer 1: Der Buffer Overflow
- 3.6.12. Kryptographische Botschaften

3.7. Botnets und *Spam*
- 3.7.1. Ursprung des Problems
- 3.7.2. Spam-Prozess
- 3.7.3. Spam verschicken
- 3.7.4. Verfeinerung der Verteilerlisten
- 3.7.5. Methoden zum Schutz
- 3.7.6. Von Dritten angebotener *Antispam*-Service
- 3.7.7. Fallstudien
- 3.7.8. Exotischer Spam

3.8. Web-Auditing und -Angriffe
- 3.8.1. Sammeln von Informationen
- 3.8.2. Angriffs-Techniken
- 3.8.3. Tools

3.9. Malware und bösartiger Code
- 3.9.1. Was ist Malware?
- 3.9.2. Arten von Malware
- 3.9.3. Virus
- 3.9.4. Kryptoviren
- 3.9.5. Würmer
- 3.9.6. *Adware*
- 3.9.7. *Spyware*
- 3.9.8. *Hoaxes*
- 3.9.9. *Phishing*
- 3.9.10. Trojaner
- 3.9.11. Die Malware-Wirtschaft
- 3.9.12. Mögliche Lösungen

3.10. Forensische Analyse
- 3.10.1. Sammeln von Beweisen
- 3.10.2. Analyse der Beweise
- 3.10.3. Anti-Forensik-Techniken
- 3.10.4. Praktische Fallstudie

Modul 4. Unternehmensnetze und -infrastrukturen

4.1. Verkehrsnetze
- 4.1.1. Funktionelle Architektur von Verkehrsnetzen
- 4.1.2. Netzwerkknoten-Schnittstelle in SDH
- 4.1.3. Netzwerkelement
- 4.1.4. Netzqualität und Verfügbarkeit
- 4.1.5. Verwaltung der Verkehrsnetze
- 4.1.6. Entwicklung der Verkehrsnetze

4.2. Klassische WAN-Architekturen
- 4.2.1. WAN-Weitverkehrsnetze
- 4.2.2. WAN-Standards
- 4.2.3. WAN-Kapselung
- 4.2.4. WAN-Geräte
  - 4.2.4.1. Router
  - 4.2.4.2. Modem
  - 4.2.4.3. *Switch*
  - 4.2.4.4. Kommunikationsserver
  - 4.2.4.5. *Gateway*
  - 4.2.4.6. *Firewall*
  - 4.2.4.7. *Proxy*
  - 4.2.4.8. NAT
- 4.2.5. Anschlussarten
  - 4.2.5.1. Punkt-zu-Punkt-Verbindungen
  - 4.2.5.2. Leitungsvermittlung
  - 4.2.5.3. Paketvermittlung
  - 4.2.5.4. Virtuelle WAN-Schaltungen

4.3. ATM-basierte Netze
- 4.3.1. Einführung, Merkmale und Schichtenmodell
- 4.3.2. Physikalische ATM-Zugangsschicht
  - 4.3.2.1. Physische mediumsabhängige PM-Teilschicht
  - 4.3.2.2. TC, Übertragungskonvergenz-Unterschicht

4.3.3. ATM-Zelle
4.3.3.1. Überschrift
4.3.3.2. Virtuelle Verbindung
4.3.3.3. ATM-Switching-Knoten
4.3.3.4. Flusskontrolle (Link Loading)
4.3.4. AAL-Zellanpassung
4.3.4.1. Arten von AAL-Diensten
4.4. Erweiterte Warteschlangenmodelle
4.4.1. Einführung
4.4.2. Grundlagen der Warteschlangentheorie
4.4.3. Warteschlangentheorie, grundlegende Systeme
4.4.3.1. Systeme M/M/1, M/M/m und M/M/∞
4.4.3.2. Systeme M/M/1/k und M/M/m/m/m
4.4.4. Warteschlangentheorie, fortgeschrittene Systeme
4.4.4.1. M/G/1-System
4.4.4.2. M/G/1-System mit Prioritäten
4.4.4.3. Warteschlangen-Netzwerke
4.4.4.4. Modellierung von Kommunikationsnetzen
4.5. Dienstqualität in Unternehmensnetzen
4.5.1. Grundlagen
4.5.2. QoS-Faktoren in konvergenten Netzen
4.5.3. QoS-Konzepte
4.5.4. QoS-Richtlinien
4.5.5. Methoden zur Implementierung von QoS
4.5.6. QoS-Modelle
4.5.7. Mechanismen für den Einsatz von DiffServ QoS
4.5.8. Beispiel einer Anwendung
4.6. Unternehmensnetze und All-Ethernet-Infrastrukturen
4.6.1. Ethernet-Netzwerk-Topologien
4.6.1.1. Bus-Topologie
4.6.1.2. Sterntopologie
4.6.2. Ethernet und IEEE 802.3-Rahmenformat

4.6.3. Geschaltetes Ethernet-Netzwerk
4.6.3.1. Virtuelle VLANs
4.6.3.2. Anschlussaggregation
4.6.3.3. Redundanz der Verbindungen
4.6.3.4. QoS-Verwaltung
4.6.3.5. Sicherheitsfunktionen
4.6.4. Fast Ethernet
4.6.5. Gigabit Ethernet
4.7. MPLS-Infrastrukturen
4.7.1. Einführung
4.7.2. MPLS
4.7.2.1. Hintergrund zu MPLS und Entwicklung
4.7.2.2. MPLS-Architektur
4.7.2.3. Etikettierte Paketweiterleitung
4.7.2.4. Protokoll zur Etikettenverteilung (LDP)
4.7.3. MPLS-VPN
4.7.3.1. Definition einer VPN
4.7.3.2. VPN-Modelle
4.7.3.3. MPLS-VPN-Modell
4.7.3.4. MPLS-VPN-Architektur
4.7.3.5. *Virtual Routing Forwarding* (VRF)
4.7.3.6. RD
4.7.3.7. Route Target (RT)
4.7.3.8. VPNv4-Routenausbreitung in einem MPLS-VPN
4.7.3.9. Weiterleitung von Paketen in einem MPLS-VPN-Netz
4.7.3.10. BGP
4.7.3.11. Erweiterte BGP-Gemeinschaft RT
4.7.3.12. BGP-Etikettentransport
4.7.3.13. Route Reflector (RR)
4.7.3.14. RR-Gruppe
4.7.3.15. BGP-Routenauswahl
4.7.3.16. Paketweiterleitung

4.7.4. Gemeinsame *Routing*-Protokolle in MPLS-Umgebungen
4.7.4.1. Routing-Protokolle mit Vektorentfernung
4.7.4.2. Routing-Protokolle im Verbindungszustand
4.7.4.3. OSPF
4.7.4.4. ISIS
4.8. Netzbetreiberdienste und VPN
4.8.1. Einführung
4.8.2. Grundlegende VPN-Anforderungen
4.8.3. Arten von VPNs
4.8.3.1. Fernzugriff-VPN
4.8.3.2. Punkt-zu-Punkt-VPN
4.8.3.3. Internes VPN (über LAN)
4.8.4. In VPN verwendete Protokolle
4.8.5. Implementierungen und Verbindungsarten
4.9. NGN (Next Generation Networks)
4.9.1. Einführung
4.9.2. Hintergrund
4.9.2.1. Definition und Merkmale des NGN-Netzes
4.9.2.2. Migration zu Netzen der nächsten Generation
4.9.3. NGN-Architektur
4.9.3.1. Primäre Konnektivitätsschicht
4.9.3.2. Zugangsebene
4.9.3.3. Dienst-Ebene
4.9.3.4. Verwaltungsebene
4.9.4. IMS
4.9.5. Normensetzende Organisationen
4.9.6. Regulatorische Trends
4.10. Überprüfung der ITU- und IETF-Normen
4.10.1. Einführung
4.10.2. Normalisierung
4.10.3. Einige Standardorganisationen
4.10.4. Protokolle und Standards der physikalischen WAN-Schicht
4.10.5. Beispiele für medienorientierte Protokolle

Modul 5. Sicherheitsarchitekturen

5.1. Grundprinzipien der IT-Sicherheit
5.1.1. Was versteht man unter IT-Sicherheit?
5.1.2. Ziele der IT-Sicherheit
5.1.3. IT-Sicherheitsdienste
5.1.4. Folgen der mangelnden Sicherheit
5.1.5. Grundsatz der Verteidigung in Sicherheit
5.1.6. Sicherheitspolitik, -pläne und -verfahren
5.1.6.1. Verwaltung von Benutzerkonten
5.1.6.2. Benutzeridentifizierung und -authentifizierung
5.1.6.3. Autorisierung und logische Zugriffskontrolle
5.1.6.4. Server-Überwachung
5.1.6.5. Datenschutz
5.1.6.6. Sicherheit von Remote-Verbindungen
5.1.7. Die Bedeutung des menschlichen Faktors
5.2. Standardisierung und Zertifizierung der IT-Sicherheit
5.2.1. Sicherheitsstandards
5.2.1.1. Ziel der Standards
5.2.1.2. Zuständige Stellen
5.2.2. Standards in den USA
5.2.2.1. TCSEC
5.2.2.2. Federal Criteria
5.2.2.3. FISCAM
5.2.2.4. NIST SP 800
5.2.3. Europäische Standards
5.2.3.1. ITSEC
5.2.3.2. ITSEM
5.2.3.3. Europäische Agentur für Netz- und Informationssicherheit (ENISA)
5.2.4. Internationale Standards
5.2.5. Prozess der Zertifizierung

5.3. Bedrohungen der Computersicherheit: Schwachstellen und Malware
- 5.3.1. Einführung
- 5.3.2. Schwachstellen der Systeme
  - 5.3.2.1. Sicherheitsvorfälle im Netz
  - 5.3.2.2. Ursachen für Schwachstellen in Informatiksystemen
  - 5.3.2.3. Arten von Schwachstellen
  - 5.3.2.4. Verantwortlichkeiten der Softwarehersteller
  - 5.3.2.5. Tools zur Schwachstellenbewertung
- 5.3.3. Bedrohungen der IT-Sicherheit
  - 5.3.3.1. Klassifizierung von Eindringlingen in das Netz
  - 5.3.3.2. Motivationen der Angreifer
  - 5.3.3.3. Phasen eines Angriffs
  - 5.3.3.4. Arten von Angriffen
- 5.3.4. Computerviren
  - 5.3.4.1. Allgemeine Merkmale
  - 5.3.4.2. Arten von Viren
  - 5.3.4.3. Schäden, die durch Viren verursacht werden
  - 5.3.4.4. Wie man Viren bekämpft

5.4. Cyber-Terrorismus und Reaktion auf Vorfälle
- 5.4.1. Einführung
- 5.4.2. Die Bedrohung durch Cyber-Terrorismus und Cyber-Kriegsführung
- 5.4.3. Folgen von Misserfolgen und Angriffen auf Unternehmen
- 5.4.4. Spionage in Computernetzen

5.5. Benutzeridentifizierung und biometrische Systeme
- 5.5.1. Einführung in die Benutzerauthentifizierung, -autorisierung und -registrierung
- 5.5.2. AAA-Sicherheitsmodell
- 5.5.3. Zugangskontrolle
- 5.5.4. Benutzeridentifikation
- 5.5.5. Überprüfung von Passwörtern
- 5.5.6. Authentifizierung mit digitalen Zertifikaten
- 5.5.7. Remote-Benutzeridentifikation
- 5.5.8. Einmalige Anmeldung
- 5.5.9. Passwortmanager
- 5.5.10. Biometrische Systeme
  - 5.5.10.1. Allgemeine Merkmale
  - 5.5.10.2. Typen von biometrischen Systemen
  - 5.5.10.3. Einführung von Systemen

5.6. Grundlagen der Kryptographie und kryptographische Protokolle
- 5.6.1. Einführung in die Kryptographie
  - 5.6.1.1. Kryptographie, Kryptoanalyse und Kryptologie
  - 5.6.1.2. Betrieb eines kryptografischen Systems
  - 5.6.1.3. Geschichte der kryptografischen Systeme
- 5.6.2. Kryptoanalyse
- 5.6.3. Klassifizierung von kryptografischen Systemen
- 5.6.4. Symmetrische und asymmetrische kryptografische Systeme
- 5.6.5. Authentifizierung mit kryptografischen Systemen
- 5.6.6. Elektronische Unterschrift
  - 5.6.6.1. Was ist eine elektronische Unterschrift?
  - 5.6.6.2. Merkmale von elektronischen Unterschriften
  - 5.6.6.3. Zertifizierungsstellen
  - 5.6.6.4. Digitale Zertifikate
  - 5.6.6.5. Vertrauenswürdige Systeme von Drittanbietern
  - 5.6.6.6. Verwendung der elektronischen Unterschrift
  - 5.6.6.7. Elektronischer Ausweis
  - 5.6.6.8. Elektronische Rechnung

5.7. Tools für die Netzsicherheit
- 5.7.1. Das Problem der Sicherheit von Internetverbindungen
- 5.7.2. Sicherheit im externen Netz
- 5.7.3. Die Rolle von Proxyservern
- 5.7.4. Die Rolle von Firewalls
- 5.7.5. Authentifizierungsserver für Fernverbindungen
- 5.7.6. Analyse der Aktivitätsprotokolle
- 5.7.7. Systeme zur Erkennung von Eindringlingen
- 5.7.8. Köder

5.8. Bezpieczeństwo w wirtualnych sieciach prywatnych i bezprzewodowych
- 5.8.1. Bezpieczeństwo w wirtualnych sieciach prywatnych
  - 5.8.1.1. Rola VPN
  - 5.8.1.2. Protokoły dla VPN
- 5.8.2. Tradycyjne bezpieczeństwo w bezprzewodowych sieciach
- 5.8.3. Możliwe ataki na bezprzewodowe sieci
- 5.8.4. Protokół WEP
- 5.8.5. Standardy bezpieczeństwa bezprzewodowych sieci
- 5.8.6. Zalecenia dotyczące poprawy bezpieczeństwa

5.9. Bezpieczeństwo w korzystaniu z usług internetowych
- 5.9.1. Bezpieczne surfowanie po Internecie
  - 5.9.1.1. Usługa WWW
  - 5.9.1.2. Problemy bezpieczeństwa w WWW
  - 5.9.1.3. Zalecenia bezpieczeństwa
  - 5.9.1.4. Ochrona prywatności w Internecie
- 5.9.2. Bezpieczeństwo poczty e-mail
  - 5.9.2.1. Cechy poczty e-mail
  - 5.9.2.2. Problemy bezpieczeństwa poczty e-mail
  - 5.9.2.3. Zalecenia dotyczące bezpieczeństwa poczty e-mail
  - 5.9.2.4. Rozszerzone usługi poczty e-mail
  - 5.9.2.5. Użycie poczty e-mail w miejscu pracy
- 5.9.3. SPAM
- 5.9.4. *Phishing*

5.10. Kontrola treści
- 5.10.1. Rozpowszechnianie treści w Internecie
- 5.10.2. Środki prawne w walce z nielegalnymi treściami
- 5.10.3. Filtrowanie, katalogowanie i blokowanie treści
- 5.10.4. Szkody wizerunkowe

Moduł 6. Centra przetwarzania danych, eksploatacja i usługi

6.1. Centrum przetwarzania danych: podstawowe koncepcje i komponenty
- 6.1.1. Wprowadzenie
- 6.1.2. Podstawowe koncepcje
  - 6.1.2.1. Definicja centrum przetwarzania danych
  - 6.1.2.2. Klasyfikacja i znaczenie
  - 6.1.2.3. Katastrofy i straty
  - 6.1.2.4. Trend ewolucyjny
  - 6.1.2.5. Koszty złożoności
  - 6.1.2.6. Filary i warstwy redundancji
- 6.1.3. Filozofia projektowania
  - 6.1.3.1. Cele
  - 6.1.3.2. Wybór lokalizacji
  - 6.1.3.3. Dostępność
  - 6.1.3.4. Krytyczne elementy
  - 6.1.3.5. Ocena kosztów i analiza
  - 6.1.3.6. Budżet IT
- 6.1.4. Podstawowe komponenty
  - 6.1.4.1. Podłoga techniczna
  - 6.1.4.2. Rodzaje płytek
  - 6.1.4.3. Rozważania ogólne
  - 6.1.4.4. Rozmiar centrum przetwarzania danych
  - 6.1.4.5. *Racks*
  - 6.1.4.6. Serwery i urządzenia komunikacyjne
  - 6.1.4.7. Monitoring

6.2. *Data Center*: systemy sterowania
- 6.2.1. Wprowadzenie
- 6.2.2. Zasilanie
  - 6.2.2.1. Sieć elektryczna
  - 6.2.2.2. Moc elektryczna
  - 6.2.2.3. Strategie dystrybucji energii elektrycznej
  - 6.2.2.4. UPS
  - 6.2.2.5. Generatory
  - 6.2.2.6. Problemy elektryczne

6.2.3. Überwachung der Umgebung
6.2.3.1. Temperatur
6.2.3.2. Feuchtigkeit
6.2.3.3. Klimatisierung
6.2.3.4. Kalorische Schätzung
6.2.3.5. Strategien zur Kühlung
6.2.3.6. Gestaltung der Korridore. Luftzirkulation
6.2.3.7. Sensoren und Wartung
6.2.4. Sicherheit und Brandverhütung
6.2.4.1. Physische Sicherheit
6.2.4.2. Feuer und seine Klassifizierung
6.2.4.3. Klassifizierung und Typen von Feuerlöschanlagen
6.3. *Data Centers*: Gestaltung und Organisation
6.3.1. Einführung
6.3.2. Netzwerk-Design
6.3.2.1. Typologien
6.3.2.2. Strukturierte Verkabelung
6.3.2.3. Backbone
6.3.2.4. UTP- und STP-Netzwerkkabel
6.3.2.5. Telefoniekabel
6.3.2.6. Terminal-Elemente
6.3.2.7. Optische Faserkabel
6.3.2.8. Koaxialkabel
6.3.2.9. Drahtlose Übertragung
6.3.2.10. Empfehlungen und Kennzeichnung
6.3.3. Organisation
6.3.3.1. Einführung
6.3.3.2. Grundlegende Maßnahmen
6.3.3.3. Strategien für das Kabelmanagement
6.3.3.4. Richtlinien und Verfahren
6.3.4. Verwaltung des Rechenzentrums
6.3.5. Standards im *Data Center*
6.4. *Data Center*: Geschäftsmodelle und Geschäftskontinuität
6.4.1. Einführung
6.4.2. Optimierung
6.4.2.1. Optimierungstechniken
6.4.2.2. Ökologische *Data Centers*
6.4.2.3. Aktuelle Herausforderungen
6.4.2.4. Modulare *Data Centers*
6.4.2.5. Housing
6.4.2.6. Konsolidierung von *Data Centers*
6.4.2.7. Überwachung
6.4.3. Geschäftskontinuität
6.4.3.1. BCP. Geschäftskontinuitätsplan. Wichtige Punkte
6.4.3.2. DR. Plan zur Wiederherstellung im Katastrophenfall
6.4.3.3. Implementierung eines DR
6.4.3.4. *Backup* und Strategien
6.4.3.5. Backup-*Data Center*
6.4.4. Bewährte Praktiken
6.4.4.1. Empfehlungen
6.4.4.2. Anwendung der ITIL-Methodik
6.4.4.3. Metriken zur Verfügbarkeit
6.4.4.4. Überwachung der Umgebung
6.4.4.5. Risikomanagement
6.4.4.6. Verantwortlicher des Rechenzentrums
6.4.4.7. Tools
6.4.4.8. Tipps zur Implementierung
6.4.4.9. Charakterisierung

6.5. *Cloud Computing*: Einführung und Grundlagen
- 6.5.1. Einführung
- 6.5.2. Grundlegende Konzepte und Terminologie
- 6.5.3. Zielsetzung und Nutzen
  - 6.5.3.1. Verfügbarkeit
  - 6.5.3.2. Verlässlichkeit
  - 6.5.3.3. Skalierbarkeit
- 6.5.4. Risiken und Herausforderungen
- 6.5.5. Roles. Provider. Consumer
- 6.5.6. Merkmale der Cloud
- 6.5.7. Modelle der Dienstleistungserbringung
  - 6.5.7.1. IaaS
  - 6.5.7.2. PaaS
  - 6.5.7.3. SaaS
- 6.5.8. Arten von Cloud
  - 6.5.8.1. Öffentliche
  - 6.5.8.2. Private
  - 6.5.9.3. Hybride
- 6.5.9. Technologien für die Cloud
  - 6.5.9.1. Netzarchitekturen
  - 6.5.9.2. Breitbandnetze. Interkonnektivität
  - 6.5.9.3. Technologien für Rechenzentren
    - 6.5.9.3.1. *Computing*
    - 6.5.9.3.2. *Storage*
    - 6.5.9.3.3. *Networking*
    - 6.5.9.3.4. Hohe Verfügbarkeit
    - 6.5.9.3.5. *Backup*-Systeme
    - 6.5.9.3.6. Verteiler
  - 6.5.9.4. Virtualisierung
  - 6.5.9.5. Web-Technologien
  - 6.5.9.6. Mehrmandanten-Technologie
  - 6.5.9.7. Servicetechnologie

6.5.9.8. Cloud-Sicherheit
6.5.9.8.1. Begriffe und Konzepte
6.5.9.8.2. Integrität und Authentifizierung
6.5.9.8.3. Sicherheitsmechanismen
6.5.9.8.4. Sicherheitsbedrohungen
6.5.9.8.5. Angriffe auf die Cloud-Sicherheit
6.5.9.8.6. Fallstudie

6.6. *Cloud Computing*: Technologie und Sicherheit in der Cloud
6.6.1. Einführung
6.6.2. Cloud-Infrastruktur-Mechanismen
6.6.2.1. Perimeter des Netzwerks
6.6.2.2. Speicherung
6.6.2.3. Server-Umgebung
6.6.2.4. Cloud-Überwachung
6.6.2.5. Hohe Verfügbarkeit
6.6.3. Sicherheitsmechanismen in der Cloud (Teil I)
6.6.3.1. Automatisierung
6.6.3.2. Lastverteiler
6.6.3.3. SLA-Monitor
6.6.3.4. Pay-per-Use-Mechanismen
6.6.4. Sicherheitsmechanismen in der Cloud (Teil II)
6.6.4.1. Rückverfolgbarkeit und Auditsysteme
6.6.4.2. Failover-Systeme
6.6.4.3. Hypervisor
6.6.4.4. Clustering
6.6.4.5. Mehrmandanten-Systeme

6.7. *Cloud Computing*: Infrastruktur. Kontroll- und Sicherheitsmechanismen
6.7.1. Einführung in die Cloud-Verwaltungsmechanismen
6.7.2. Systeme zur Fernverwaltung
6.7.3. Systeme zur Ressourcenverwaltung
6.7.4. Systeme zur Verwaltung von Service Level Agreements
6.7.5. Systeme zur Verwaltung von Rechnungen
6.7.6. Cloud-Sicherheitsmechanismen
6.7.6.1. Verschlüsselung
6.7.6.2. *Hashing*
6.7.6.3. Digitale Unterschrift
6.7.6.4. PKI
6.7.6.5. Identitäts- und Zugangsmanagement
6.7.6.6. SSO
6.7.6.7. Cloud-basierte Sicherheitsgruppen
6.7.6.8. Bastionierungssysteme

6.8. *Cloud Computing*: Cloud-Architekturen
6.8.1. Einführung
6.8.2. Grundlegende Cloud-Architekturen
6.8.2.1. Architekturen zur Verteilung der Arbeitslast
6.8.2.2. Architekturen zur Ressourcennutzung
6.8.2.3. Skalierbare Architekturen
6.8.2.4. Architekturen für den Lastausgleich
6.8.2.5. Redundante Architekturen
6.8.2.6. Beispiele
6.8.3. Erweiterte Cloud-Architekturen
6.8.3.1. Hypervisor-Cluster-Architekturen
6.8.3.2. Virtuelle Architekturen zum Lastausgleich
6.8.3.3. *Non-Stop*-Architekturen
6.8.3.4. Architekturen mit hoher Verfügbarkeit
6.8.3.5. Bare-Metal-Architekturen
6.8.3.6. Redundante Architekturen
6.8.3.7. Hybride Architekturen
6.8.4. Spezialisierte Cloud-Architekturen
6.8.4.1. Architekturen mit direktem E/A-Zugriff
6.8.4.2. LUN-Direktzugriffsarchitekturen
6.8.4.3. Elastische Netzarchitekturen
6.8.4.4. SDDC-Architektur
6.8.4.5. Besondere Architekturen
6.8.4.6. Beispiele

6.9. *Cloud Computing*: Modelle der Dienstbereitstellung
- 6.9.1. Einführung
- 6.9.2. Bereitstellung von Cloud-Diensten
- 6.9.3. Perspektive des Dienstleisters
- 6.9.4. Perspektive der Verbraucher dieser Dienstleistungen
- 6.9.5. Fallstudien

6.10. *Cloud Computing*: Vertragsmodelle, Metriken und Anbieter von Dienstleistungen
- 6.10.1. Einführung in Abrechnungsmodelle und Metriken
- 6.10.2. Modelle für die Rechnungsstellung
- 6.10.3. Pay-per-use-Metriken
- 6.10.4. Überlegungen zum Kostenmanagement
- 6.10.5. Einführung in QoS-Metriken und SLAs
- 6.10.6. Metriken für die Dienstqualität
- 6.10.7. Leistungsmetriken für Dienstleistungen
- 6.10.8. Metriken zur Skalierbarkeit von Diensten
- 6.10.9. Dienstleistungsmodell SLAs
- 6.10.10. Fallstudien

Modul 7. Fortgeschrittene Programmierung

7.1. Einführung in die objektorientierte Programmierung
- 7.1.1. Einführung in die objektorientierte Programmierung
- 7.1.2. Klassen-Design
- 7.1.3. Einführung in UML für die Modellierung von Problemen

7.2. Beziehungen zwischen Klassen
- 7.2.1. Abstraktion und Vererbung
- 7.2.2. Fortgeschrittene Konzepte der Vererbung
- 7.2.3. Polymorphismen
- 7.2.4. Zusammensetzung und Aggregation

7.3. Einführung in Entwurfsmuster für objektorientierte Probleme
- 7.3.1. Was sind Entwurfsmuster?
- 7.3.2. Factory-Muster
- 7.3.3. Singleton-Muster
- 7.3.4. Observer-Muster
- 7.3.5. Composite-Muster

7.4. Ausnahmen
- 7.4.1. Was sind Ausnahmen?
- 7.4.2. Abfangen und Behandlung von Ausnahmen
- 7.4.3. Start von Ausnahmen
- 7.4.4. Erstellung von Ausnahmen

7.5. Benutzeroberflächen
- 7.5.1. Einführung in Qt
- 7.5.2. Positionierung
- 7.5.3. Was sind Ereignisse?
- 7.5.4. Ereignisse: Definition und Erfassung
- 7.5.5. Entwicklung von Benutzeroberflächen

7.6. Einführung in die gleichzeitige Programmierung
- 7.6.1. Einführung in die gleichzeitige Programmierung
- 7.6.2. Der Prozess und das Thread-Konzept
- 7.6.3. Interaktion zwischen Prozessen oder Threads
- 7.6.4. Threads in C++
- 7.6.5. Vor- und Nachteile der gleichzeitigen Programmierung

7.7. Thread-Verwaltung und Synchronisierung
- 7.7.1. Lebenszyklus eines Threads
- 7.7.2. Die Klasse Thread
- 7.7.3. Planung des Threads
- 7.7.4. Gruppen von Threads
- 7.7.5. Daemon-Threads
- 7.7.6. Synchronisierung
- 7.7.7. Verriegelungsmechanismen
- 7.7.8. Kommunikationsmechanismen
- 7.7.9. Monitore

7.8. Häufige Probleme bei der gleichzeitigen Programmierung
- 7.8.1. Das Erzeuger-Verbraucher-Problem
- 7.8.2. Das Problem von Lesern und Schriftstellern
- 7.8.3. Das Problem der speisenden Philosophen

7.9. Software-Dokumentation und -Tests
- 7.9.1. Warum ist es wichtig, Software zu dokumentieren?
- 7.9.2. Design-Dokumentation
- 7.9.3. Verwendung von Tools zur Dokumentation

7.10. Software-Tests
- 7.10.1. Einführung in das Testen von Software
- 7.10.2. Arten von Tests
- 7.10.3. Einheitstest
- 7.10.4. Integrationstests
- 7.10.5. Validierungstest
- 7.10.6. Systemprüfung

Modul 8. Technik für Systeme und Netzdienste

8.1. Einführung in die Systemtechnik und Netzdienste
- 8.1.1. Computersystemkonzept und Computertechnik
- 8.1.2. Die Software und ihre Eigenschaften
  - 8.1.2.1. Eigenschaften der Software
- 8.1.3. Die Entwicklung der Software
  - 8.1.3.1. Die Anfänge der Softwareentwicklung
  - 8.1.3.2. Die Softwarekrise
  - 8.1.3.3. Die Softwaretechnik
  - 8.1.3.4. Die Tragödie der Software
  - 8.1.3.5. Die Aktualität von Software
- 8.1.4. Die Mythen der Software
- 8.1.5. Die neuen Herausforderungen der Software
- 8.1.6. Berufsethik in der Softwareentwicklung
- 8.1.7. SWEBOK. Der Bestand an Wissen über Softwareentwicklung

8.2. Der Entwicklungsprozess
- 8.2.1. Der Problemlösungsprozess
- 8.2.2. Der Softwareentwicklungsprozess
- 8.2.3. Softwareprozess versus Lebenszyklus
- 8.2.4. Lebenszyklen. Prozessmodelle (traditionell)
  - 8.2.4.1. Wasserfall-Modell
  - 8.2.4.2. Prototypische Modelle
  - 8.2.4.3. Inkrementelles Entwicklungsmodell
  - 8.2.4.4. Schnelle Anwendungsentwicklung (RAD)
  - 8.2.4.5. Spiralförmiges Modell
  - 8.2.4.6. Vereinheitlichter Entwicklungsprozess oder Rational Unified Process (RUP)
  - 8.2.4.7. Komponentenbasierte Software-Entwicklung
- 8.2.5. Das agile Manifest. Agile Methoden
  - 8.2.5.1. Extreme Programmierung (XP)
  - 8.2.5.2. Scrum
  - 8.2.5.3. Feature Driven Development (FDD)
- 8.2.6. Software-Prozess-Standards
- 8.2.7. Definition eines Softwareprozesses
- 8.2.8. Reifegrad von Software-Prozessen

8.3. Planung und Management von agilen Projekten
- 8.3.1. Was ist Agile?
  - 8.3.1.1. Geschichte von Agile
  - 8.3.1.2. Das Agile Manifest
- 8.3.2. Agile Grundlagen
  - 8.3.2.1. Die "agile" Denkweise
  - 8.3.2.2. Anpassung an Agile
  - 8.3.2.3. Lebenszyklus der Produktentwicklung
  - 8.3.2.4. Das Eiserne Dreieck
  - 8.3.2.5. Umgang mit Unsicherheit und Volatilität
  - 8.3.2.6. Definierte Prozesse und empirische Prozesse
  - 8.3.2.7. Die Mythen von Agile
- 8.3.3. Das Umfeld von Agile
  - 8.3.3.1. Operatives Modell
  - 8.3.3.2. Agile Rollen
  - 8.3.3.3. Agile Techniken
  - 8.3.3.4. Agile Praktiken

8.3.4. Agile Rahmenwerke
8.3.4.1. e-Xtreme Programming (XP)
8.3.4.2. Scrum
8.3.4.3. Dynamic Systems Development Method (DSDM)
8.3.4.4. Agile Project Management
8.3.4.5. Kanban
8.3.4.6. Lean Software Development
8.3.4.7. Lean Start-up
8.3.4.8. Scaled Agile Framework (SAFe)

8.4. Konfigurationsmanagement und kollaborative Repositories
8.4.1. Grundlegende Konzepte des Software-Konfigurationsmanagements
8.4.1.1. Was ist Software-Konfigurationsmanagement?
8.4.1.2. Softwarekonfiguration und Elemente der Softwarekonfiguration
8.4.1.3. Grundlinien
8.4.1.4. Versionen, Revisionen, Varianten und *releases*
8.4.2. Aktivitäten des Konfigurationsmanagements
8.4.2.1. Identifizierung der Konfiguration
8.4.2.2. Änderungskontrolle der Konfiguration
8.4.2.3. Erstellung von Statusberichten
8.4.2.4. Überprüfung der Konfiguration
8.4.3. Der Konfigurationsmanagementplan
8.4.4. Werkzeuge zur Konfigurationsverwaltung
8.4.5. Konfigurationsmanagement im Rahmen der Metric v.3-Methodik
8.4.6. Konfigurationsmanagement in SWEBOK

8.5. Prüfung von Systemen und Diensten
8.5.1. Allgemeine Prüfkonzepte
8.5.1.1. Überprüfen und Validieren
8.5.1.2. Definition von Tests
8.5.1.3. Grundsätze der Tests
8.5.2. Ansätze für die Tests
8.5.2.1. White-Box-Tests
8.5.2.2. Black-Box-Tests

8.5.3. Statische Tests oder Revisionen
8.5.3.1. Formelle technische Überprüfungen
8.5.3.2. *Walkthroughs*
8.5.3.3. Code-Inspektionen
8.5.4. Dynamische Prüfung
8.5.4.1. Einheitliche Prüfung
8.5.4.2. Integrationstests
8.5.4.3. Systemprüfung
8.5.4.4. Abnahmetests
8.5.4.5. Regressionstests
8.5.5. Alphatests und Betatests
8.5.6. Das Prüfverfahren
8.5.7. Fehler, Defekt und Versagen
8.5.8. Automatisierte Prüfwerkzeuge
8.5.8.1. Junit
8.5.8.2. LoadRunner
8.6. Modellierung und Entwurf von Netzarchitekturen
8.6.1. Einführung
8.6.2. Merkmale der Systeme
8.6.2.1. Beschreibung der Systeme
8.6.2.2. Beschreibung und Merkmale der Dienstleistungen
8.6.2.3. Anforderungen an die Betriebsfähigkeit
8.6.3. Analyse der Anforderungen
8.6.3.1. Anforderungen der Benutzer
8.6.3.2. Anforderungen an die Anwendungen
8.6.3.3. Anforderungen an das Netz
8.6.4. Entwurf von Netzarchitekturen
8.6.4.1. Referenzarchitektur und Komponenten
8.6.4.2. Architektur-Modelle
8.6.4.3. System- und Netzarchitekturen

8.7. Modellierung und Entwurf verteilter Systeme
- 8.7.1. Einführung
- 8.7.2. Adressierung und *Routing*-Architektur
  - 8.7.2.1. Adressierungsstrategie
  - 8.7.2.2. Routing-Strategie
  - 8.7.2.3. Überlegungen zum Design
- 8.7.3. Netzwerkdesign-Konzepte
- 8.7.4. Design-Prozess

8.8. Plattformen und Einsatzumgebungen
- 8.8.1. Einführung
- 8.8.2. Verteilte Computersysteme
  - 8.8.2.1. Grundlegende Konzepte
  - 8.8.2.2. Computer-Modelle
  - 8.8.2.3. Vorteile, Nachteile und Herausforderungen
  - 8.8.2.4. Grundlagen des Betriebssystems
- 8.8.3. Virtualisierte Netzwerkimplementierungen
  - 8.8.3.1. Notwendigkeit des Wandels
  - 8.8.3.2. Transformation der Netze: von „All-IP" zur Cloud
  - 8.8.3.3. Bereitstellung eines Cloud-Netzwerks
- 8.8.4. Beispiel: Netzwerkarchitektur in Azure

8.9. E2E-Leistung: Verzögerung und Bandbreite. QoS
- 8.9.1. Einführung
- 8.9.2. Leistungsanalyse
- 8.9.3. QoS
- 8.9.4. Prioritätensetzung und Verkehrsmanagement
- 8.9.5. Vereinbarungen über das Dienstleistungsniveau
- 8.9.6. Überlegungen zum Design
  - 8.9.6.1. Leistungsbewertung
  - 8.9.6.2. Beziehungen und Interaktionen

8.10. Netzautomatisierung und -optimierung
- 8.10.1. Einführung
- 8.10.2. Verwaltung des Netzes
  - 8.10.2.1. Verwaltungs- und Konfigurationsprotokolle
  - 8.10.2.2. Netzverwaltungsarchitekturen
- 8.10.3. Orchestrierung und Automatisierung
  - 8.10.3.1. ONAP-Architektur
  - 8.10.3.2. Steuerungen und Funktionen
  - 8.10.3.3. Politiken
  - 8.10.3.4. Netzinventar
- 8.10.4. Optimierung

Modul 9. Prüfung von Informationssystemen

9.1. Prüfung von Informationssystemen. Standards der guten Praxis
- 9.1.1. Einführung
- 9.1.2. Rechnungsprüfung und COBIT
- 9.1.3. Audit der IKT-Verwaltungssysteme
- 9.1.4. Zertifizierungen

9.2. Konzepte und Methoden der Systemprüfung
- 9.2.1. Einführung
- 9.2.2. Methoden der Systembewertung: quantitativ und qualitativ
- 9.2.3. IT-Audit-Methoden
- 9.2.4. Der Prüfungsplan

9.3. Der Prüfungsvertrag
- 9.3.1. Rechtlicher Charakter des Auftrags
- 9.3.2. Parteien eines Prüfungsauftrags
- 9.3.3. Gegenstand des Prüfungsvertrags
- 9.3.4. Der Prüfbericht

9.4. Organisatorische Elemente von Prüfungen
- 9.4.1. Einführung
- 9.4.2. Auftrag des Auditdienstes
- 9.4.3. Audit-Planung
- 9.4.4. IS-Audit-Methodik

9.5. Rechtlicher Rahmen für Audits
- 9.5.1. Schutz von personenbezogenen Daten
- 9.5.2. Rechtlicher Schutz von Software
- 9.5.3. Technologische Kriminalität
- 9.5.4. Vertragsabschluss, Unterschrift und elektronischer Ausweis

9.6. Outsourcing-Audit und Bezugsrahmen
- 9.6.1. Einführung
- 9.6.2. Grundlagen des Outsourcing
- 9.6.3. Prüfung von IT-Outsourcing
- 9.6.4. Referenzrahmen: CMMI, ISO27001, ITIL

9.7. Sicherheitsaudit
- 9.7.1. Einführung
- 9.7.2. Physische und logische Sicherheit
- 9.7.3. Sicherheit in der Umgebung
- 9.7.4. Planung und Durchführung des Audits der physischen Sicherheit

9.8. Netzwerk- und Internet-Audits
- 9.8.1. Einführung
- 9.8.2. Schwachstellen im Netzwerk
- 9.8.3. Grundsätze und Rechte im Internet
- 9.8.4. Datenkontrolle und -verarbeitung

9.9. Prüfung von IT-Anwendungen und -Systemen
- 9.9.1. Einführung
- 9.9.2. Referenzmodelle
- 9.9.3. Bewertung der Qualität der Anwendungen
- 9.9.4. Audit der Organisation und Verwaltung des Bereichs Entwicklung und Instandhaltung

9.10. Prüfung der personenbezogenen Daten
- 9.10.1. Einführung
- 9.10.2. Gesetze und Vorschriften zum Datenschutz
- 9.10.3. Die Durchführung des Audits
- 9.10.4. Verstöße und Sanktionen

Modul 10. Projektmanagement

10.1. Grundlegende Konzepte des Projektmanagements und des Lebenszyklus des Projektmanagements
- 10.1.1. Was ist ein Projekt?
- 10.1.2. Gemeinsame Methodik
- 10.1.3. Was ist Projektmanagement?
- 10.1.4. Was ist ein Projektplan?
- 10.1.5. Vorteile
- 10.1.6. Projektlebenszyklus
- 10.1.7. Prozessgruppen oder Lebenszyklus des Projektmanagements
- 10.1.8. Die Beziehung zwischen Prozessgruppen und Wissensgebieten
- 10.1.9. Beziehung zwischen Produkt- und Projektlebenszyklus

10.2. Inbetriebnahme und Planung
- 10.2.1. Von der Idee zum Projekt
- 10.2.2. Entwicklung der Projektcharta
- 10.2.3. Projekt-Kick-off-Meeting
- 10.2.4. Aufgaben, Kenntnisse und Fähigkeiten im Gründungsprozess
- 10.2.5. Der Projektplan
- 10.2.6. Entwicklung des Basisplans. Schritte
- 10.2.7. Aufgaben, Kenntnisse und Fähigkeiten im Planungsprozess

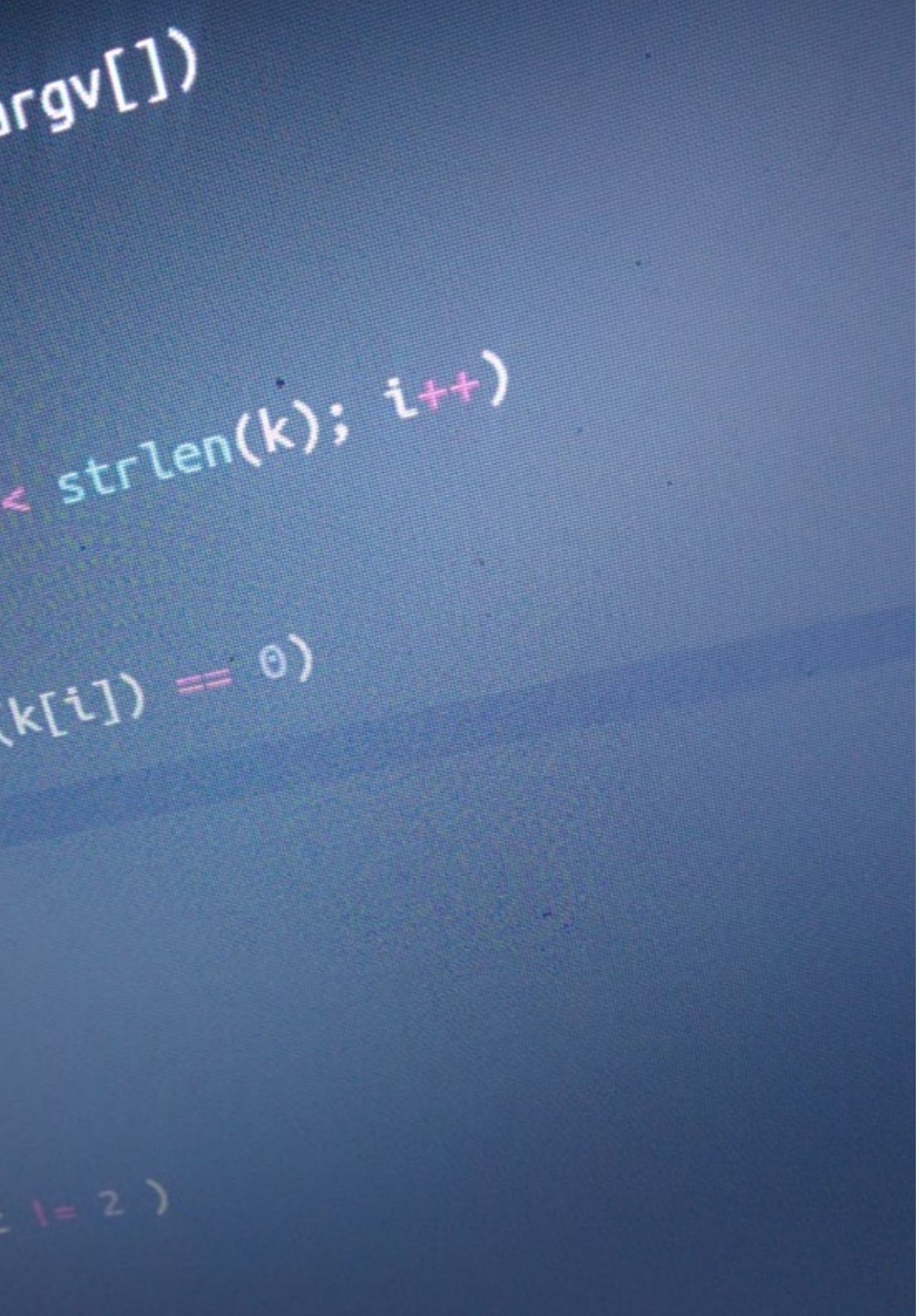
10.3. Management von *Stakeholdern* und Reichweite
- 10.3.1. Identifizierung von Interessengruppen
- 10.3.2. Entwicklung des *Stakeholder*-Management-Plans
- 10.3.3. Management der Einbindung von *Stakeholdern*
- 10.3.4. Überwachung des Engagements der *Stakeholder*
- 10.3.5. Das Projektziel
- 10.3.6. Umfangsmanagement und sein Plan
- 10.3.7. Erfassen von Anforderungen
- 10.3.8. Definieren Sie den Geltungsbereich
- 10.3.9. Erstellen des Projektstrukturplans
- 10.3.10. Überprüfung und Kontrolle des Umfangs

10.4. Die Entwicklung des Zeitplans
- 10.4.1. Zeitmanagement und sein Plan
- 10.4.2. Definieren der Aktivitäten
- 10.4.3. Festlegung der Reihenfolge der Aktivitäten
- 10.4.4. Schätzung der Ressourcen für die Aktivitäten
- 10.4.5. Geschätzte Dauer der Aktivitäten
- 10.4.6. Entwicklung des Zeitplans und Berechnung des kritischen Pfades
- 10.4.7. Terminplan-Kontrolle

10.5. Budgetentwicklung und Risikobewältigung
- 10.5.1. Schätzung der Kosten
- 10.5.2. Entwicklung des Budgets und der S-Kurve
- 10.5.3. Kostenkontrolle und *Earned-Value*-Methode
- 10.5.4. Risikokonzepte
- 10.5.5. Wie man eine Risikoanalyse durchführt
- 10.5.6. Die Entwicklung des Reaktionsplans

10.6. Qualitätsmanagement
- 10.6.1. Planung der Qualität
- 10.6.2. Qualitätssicherung
- 10.6.3. Qualitätskontrolle
- 10.6.4. Grundlegende statistische Konzepte
- 10.6.5. Instrumente des Qualitätsmanagements

10.7. Kommunikation und Personalwesen
- 10.7.1. Planung des Kommunikationsmanagements
- 10.7.2. Analyse der Kommunikationsanforderungen
- 10.7.3. Technologie der Kommunikation
- 10.7.4. Kommunikationsmodelle
- 10.7.5. Kommunikationsmethoden
- 10.7.6. Plan für das Kommunikationsmanagement
- 10.7.7. Verwaltung der Kommunikation
- 10.7.8. Verwaltung des Personalwesens
- 10.7.9. Hauptakteure und ihre Rolle in den Projekten
- 10.7.10. Arten von Organisationen
- 10.7.11. Projektorganisation
- 10.7.12. Das Projektteam



10.8. Beschaffung
- 10.8.1. Der Beschaffungsprozess
- 10.8.2. Planung
- 10.8.3. Beschaffung von Lieferanten und Einholung von Angeboten
- 10.8.4. Vergabe des Auftrags
- 10.8.5. Vertragsverwaltung
- 10.8.6. Verträge
- 10.8.7. Arten von Verträgen
- 10.8.8. Vertragsverhandlungen

10.9. Durchführung, Überwachung und Kontrolle sowie Abschluss
- 10.9.1. Prozessgruppen
- 10.9.2. Projektdurchführung
- 10.9.3. Projektüberwachung und -kontrolle
- 10.9.4. Abschluss des Projekts

10.10. Berufliche Verantwortung
- 10.10.1. Berufliche Verantwortung
- 10.10.2. Merkmale der sozialen und beruflichen Verantwortung
- 10.10.3. Ethischer Kodex für Projektleiter
- 10.10.4. Verantwortung vs. PMP®
- 10.10.5. Beispiele für Rechenschaftspflicht
- 10.10.6. Vorteile der Professionalisierung

Ein Prozess des beruflichen und persönlichen Wachstums, der Ihre Wettbewerbsfähigkeit enorm steigern wird"

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 hinter sich lässt 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 an den Grundlagen der traditionellen Universitäten auf der ganzen Welt rüttelt"

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

Der Student wird durch gemeinschaftliche Aktivitäten und reale Fälle lernen, wie man komplexe Situationen in realen Geschäftsumgebungen löst.

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 Jurastudenten das Recht nicht nur auf der Grundlage theoretischer Inhalte erlernen. Sie bestand darin, ihnen reale komplexe Situationen zu präsentieren, damit sie fundierte Entscheidungen treffen und Werturteile darüber fällen konnten, wie diese zu lösen sind. Sie wurde 1924 als Standardlehrmethode in Harvard etabliert.

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 Studenten mit mehreren realen Fällen konfrontiert. Sie müssen ihr gesamtes Wissen integrieren, recherchieren, argumentieren und ihre Ideen und Entscheidungen verteidigen.

Relearning Methodology

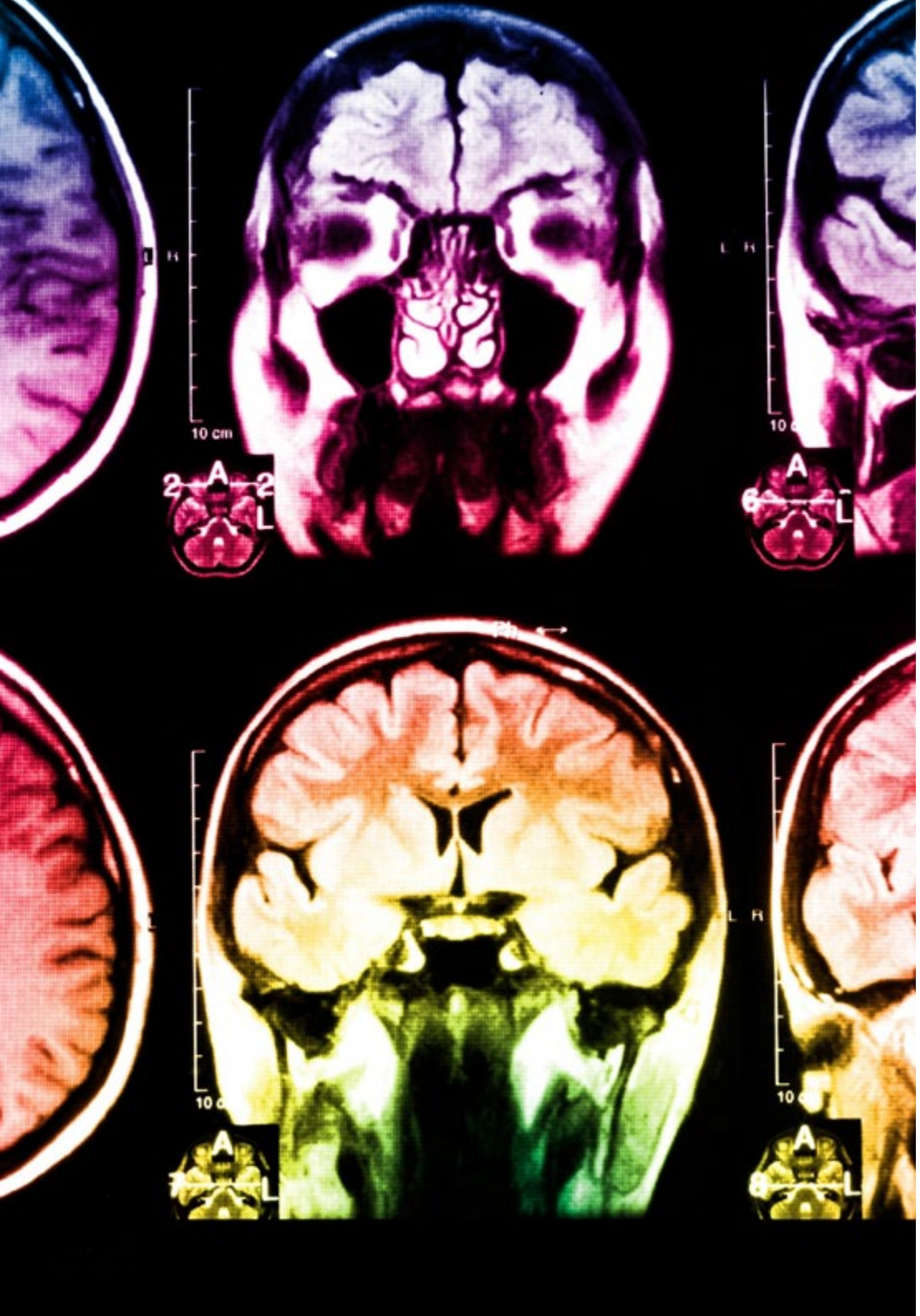
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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 zu spezialisieren. 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 spanischsprachigen Online-Universität 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 fortgebildet. 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 Ihre Spezialisierung 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 Neurocognitive Context-Dependent E-Learning 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 Online-Arbeitsmethode von TECH zu schaffen. All dies mit den neuesten Techniken, die in jedem einzelnen der Materialien, die dem Studenten zur Verfügung gestellt werden, qualitativ hochwertige Elemente bieten.

Meisterklassen

Die Nützlichkeit der Expertenbeobachtung ist wissenschaftlich belegt.

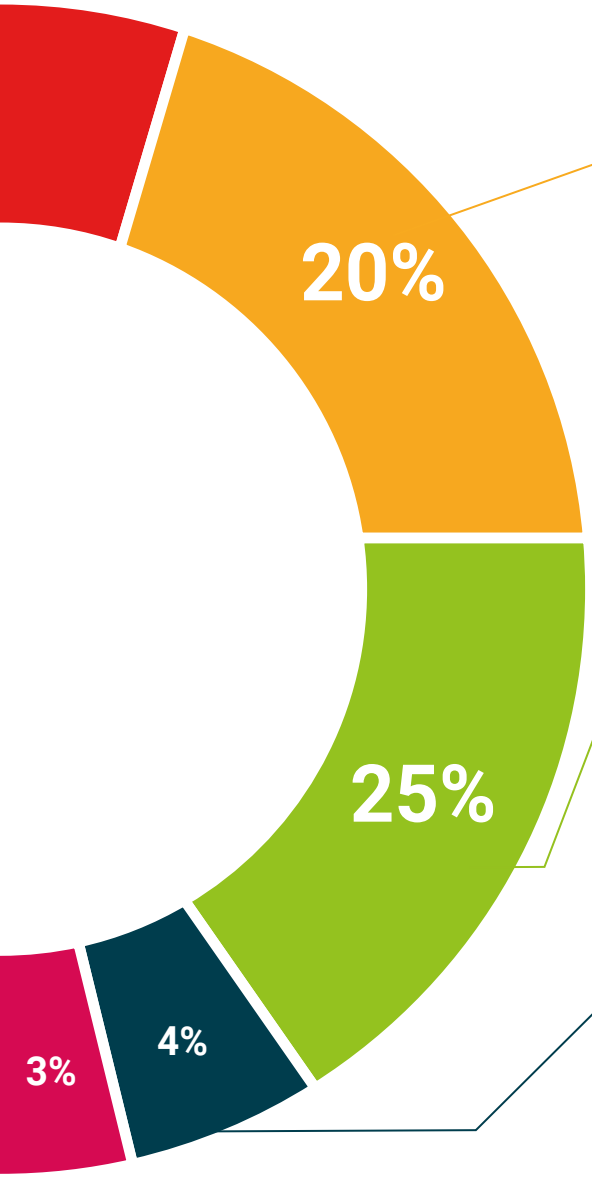
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

Übungen für Fertigkeiten und Kompetenzen

Sie werden Aktivitäten durchführen, um spezifische Kompetenzen und Fertigkeiten in jedem Fachbereich zu entwickeln. Übungen und Aktivitäten 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 hat der Student Zugang zu allem, was er für seine Fortbildung benötigt.



Case Studies

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.

Testing & Retesting

Die Kenntnisse des Studenten werden während des gesamten Programms regelmäßig durch Bewertungs- und Selbsteinschätzungsaktivitäten und -übungen beurteilt und neu bewertet, so dass der Student überprüfen kann, wie er seine Ziele erreicht.

07

Qualifizierung

Der Weiterbildender Masterstudiengang in Telematik garantiert neben der präzisesten und aktuellsten Fortbildung auch den Zugang zu einem von der TECH Global University ausgestellten Diplom.

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

Mit diesem Programm erwerben Sie den von **TECH Global University**, der größten digitalen Universität der Welt, bestätigten eigenen Titel **Weiterbildender Masterstudiengang in Telematik.**

TECH Global University ist eine offizielle europäische Universität, die von der Regierung von Andorra (***Amtsblatt***) öffentlich anerkannt ist. Andorra ist seit 2003 Teil des Europäischen Hochschulraums (EHR). Der EHR ist eine von der Europäischen Union geförderte Initiative, die darauf abzielt, den internationalen Ausbildungsrahmen zu organisieren und die Hochschulsysteme der Mitgliedsländer dieses Raums zu vereinheitlichen. Das Projekt fördert gemeinsame Werte, die Einführung gemeinsamer Instrumente und die Stärkung der Mechanismen zur Qualitätssicherung, um die Zusammenarbeit und Mobilität von Studenten, Forschern und Akademikern zu verbessern.

Dieser eigene Abschluss der **TECH Global University** ist ein europäisches Programm zur kontinuierlichen Weiterbildung und beruflichen Fortbildung, das den Erwerb von Kompetenzen in seinem Wissensgebiet garantiert und dem Lebenslauf des Studenten, der das Programm absolviert, einen hohen Mehrwert verleiht.

Titel: **Weiterbildender Masterstudiengang in Telematik**

Modalität: **online**

Dauer: **12 Monate**

Akkreditierung: **60 ECTS**


tech global university

Hr./Fr. _____, mit der Ausweis-Nr. _____ hat erfolgreich bestanden und den folgenden Abschluss erworben:

Weiterbildender Masterstudiengang in Telematik

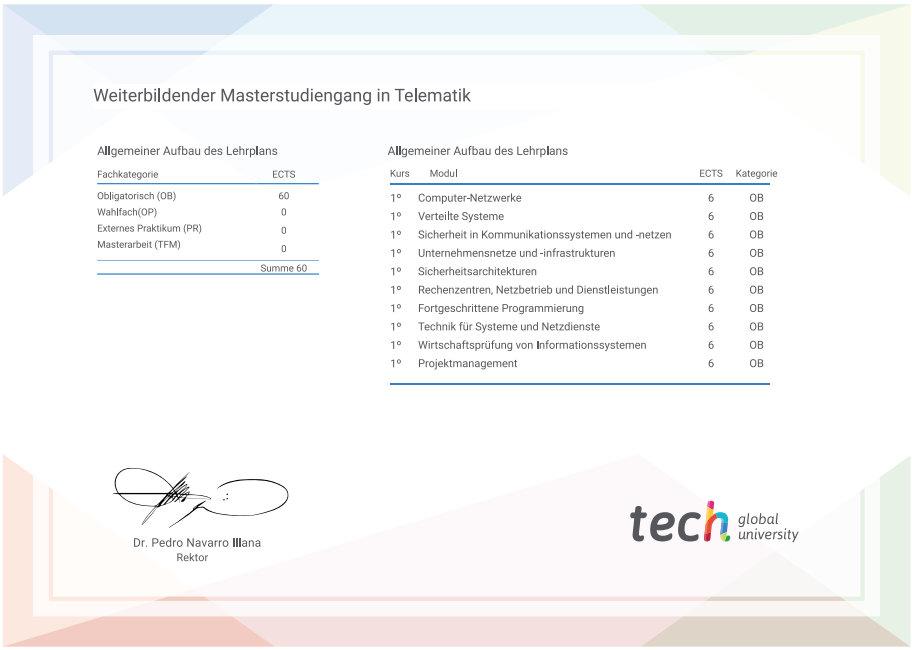
Es handelt sich um einen eigenen Abschluss mit einer Dauer von 1.800 Stunden, was 60 ECTS entspricht, mit Anfangsdatum am dd/mm/aaaa und Enddatum am dd/mm/aaaa.

TECH Global University ist eine von der Regierung Andorras am 31. Januar 2024 offiziell anerkannte Universität, die dem Europäischen Hochschulraum (EHR) angehört.

Andorra la Vella, den 28. Februar 2024

Dr. Pedro Navarro Illana
Rektor

einzigartiger Code TECH: AFWOR23S techtitute.com/titel


Weiterbildender Masterstudiengang in Telematik

Allgemeiner Aufbau des Lehrplans

Fachkategorie	ECTS
Obligatorisch (OB)	60
Wahlfach(OP)	0
Externes Praktikum (PR)	0
Masterarbeit (TFM)	0
	Summe 60

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	ECTS	Kategorie
1°	Computer-Netzwerke	6	OB
1°	Verteilte Systeme	6	OB
1°	Sicherheit in Kommunikationssystemen und -netzen	6	OB
1°	Unternehmensnetze und -infrastrukturen	6	OB
1°	Sicherheitsarchitekturen	6	OB
1°	Rechenzentren, Netzbetrieb und Dienstleistungen	6	OB
1°	Fortgeschrittene Programmierung	6	OB
1°	Technik für Systeme und Netzdienste	6	OB
1°	Wirtschaftsprüfung von Informationssystemen	6	OB
1°	Projektmanagement	6	OB

Dr. Pedro Navarro Illana
Rektor

tech global university

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

tech global university

Weiterbildender Masterstudiengang

Telematik

- Modalität: **online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Global University**
- Akkreditierung: **60 ECTS**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Weiterbildender Masterstudiengang
Telematik

tech global university