Universitätsexperte

IT-Sicherheit für Kommunikation

tech technologische universität

tech technologische universität

Universitätsexperte
IT-Sicherheit für Kommunikation

- Modalität: **online**
- Dauer: **6 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Internetzugang: www.techtitute.com/de/informatik/spezialisierung/spezialisierung-it-sicherheit-kommunikation

Index

01

Präsentation

Die unbefugte und missbräuchliche Nutzung von Netzen ist eines der Hauptprobleme, mit denen die Nutzer konfrontiert werden können. Die Durchführung von Maßnahmen zur IT-Sicherheit ist unerlässlich, da eine große Menge an privaten und vertraulichen Informationen über das Internet übertragen wird. Dieser Universitätsexperte bringt den Studenten den Bereich der IT-Sicherheit für Kommunikation mit einem aktualisierten und hochwertigen Programm näher. Es handelt sich um eine vollständige Vorbereitung, die darauf abzielt, Studenten für den Erfolg in ihrem Beruf zu qualifizieren.

Wenn Sie auf der Suche nach einer qualitativ hochwertigen Fortbildung sind, die Ihnen hilft, sich in einem der Bereiche mit den meisten beruflichen Möglichkeiten zu spezialisieren, ist dies Ihre beste Option"

Da sich die Telekommunikation als einer der sich am schnellsten entwickelnden Bereiche ständig weiterentwickelt, sind IT-Experten erforderlich, die sich an diese Veränderungen anpassen können und die neuen Instrumente und Techniken, die in diesem Bereich entstehen, aus erster Hand kennen.

In diesem Bereich muss die IT-Sicherheit zu den Aspekten gehören, denen die Unternehmen die größte Aufmerksamkeit schenken, da sich alle Informationen im Netz befinden und ein unkontrollierter Zugriff durch einen Benutzer zur Durchführung unerlaubter Aufgaben ein ernsthaftes Problem für die Organisation darstellen kann, sei es in finanzieller Hinsicht oder in Bezug auf den Ruf.

Der Universitätsexperte in IT-Sicherheit für Kommunikation deckt die gesamte Bandbreite der Themen in diesem Bereich ab. Das Studium hat einen klaren Vorteil gegenüber anderen Kursen, 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 Bildungsprogramms eine sorgfältige Auswahl der einzelnen Themen getroffen, um den Studenten ein möglichst umfassendes Studium zu ermöglichen das stets mit dem aktuellen Zeitgeschehen verbunden ist.

Dieses Programm richtet sich an diejenigen, die ein höheres Niveau an Kenntnissen im Bereich der IT-Sicherheit für Kommunikation erreichen wollen. Das Hauptziel besteht darin, die Studenten in die Lage zu versetzen, das im Rahmen dieses Universitätsexperte erworbene Wissen in der realen Welt anzuwenden, und zwar in einem Arbeitsumfeld, das die Bedingungen, denen sie in ihrer Zukunft begegnen könnten, auf strenge und realistische Weise wiedergibt.

Da es sich um einen 100% Online-Universitätsexperten handelt, sind die Studenten nicht an feste Zeiten oder die Notwendigkeit, sich an einen anderen Ort zu begeben, gebunden, sondern können zu jeder Tageszeit auf die Inhalte zugreifen und ihr Arbeits- oder Privatleben mit ihrem akademischen Leben in Einklang bringen.

Dieser **Universitätsexperte in IT-Sicherheit für Kommunikation** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten für T-Sicherheitvorgestellt 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
- Sein besonderer Schwerpunkt liegt auf innovativen Methoden der IT-Sicherheit für Kommunikation
- 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

Verpassen Sie nicht die Gelegenheit, diesen Universitätsexperten in IT-Sicherheit für Kommunikation bei uns zu erwerben. Es ist die perfekte Gelegenheit, um Ihre Karriere voranzutreiben"

Dieser Universitätsexperte ist die beste Investition, die Sie tätigen können, wenn Sie sich für ein Auffrischungsprogramm entscheiden, um Ihr Wissen über IT-Sicherheit für Kommunikation zu aktualisieren"

Diese Spezialisierung verfügt über das beste didaktische Material, das Ihnen ein kontextbezogenes Studium ermöglicht, das Ihr Lernen erleichtert.

Dieser Universitätsexperte der zu 100% online absolviert wird, wird Ihnen ermöglichen, Ihr Studium mit Ihrer beruflichen Tätigkeit zu verbinden. Sie entscheiden, wo und wann Sie lernen möchten.

Das Dozententeam setzt sich aus Fachleuten aus dem Bereich der Informatik zusammen der Telekommunikation, die ihre Berufserfahrung in diese Fortbildung einbringen, sowie aus anerkannten Experten von führenden Gesellschaften 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 Training ermöglicht, das auf reale Situationen ausgerichtet ist.

Das Konzept dieses Studiengangs 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 die Fachkraft von einem innovativen interaktiven Videosystem unterstützt, das von renommierten und erfahrenen Experten in IT-Sicherheit für Kommunikation entwickelt wurde.

02

Ziele

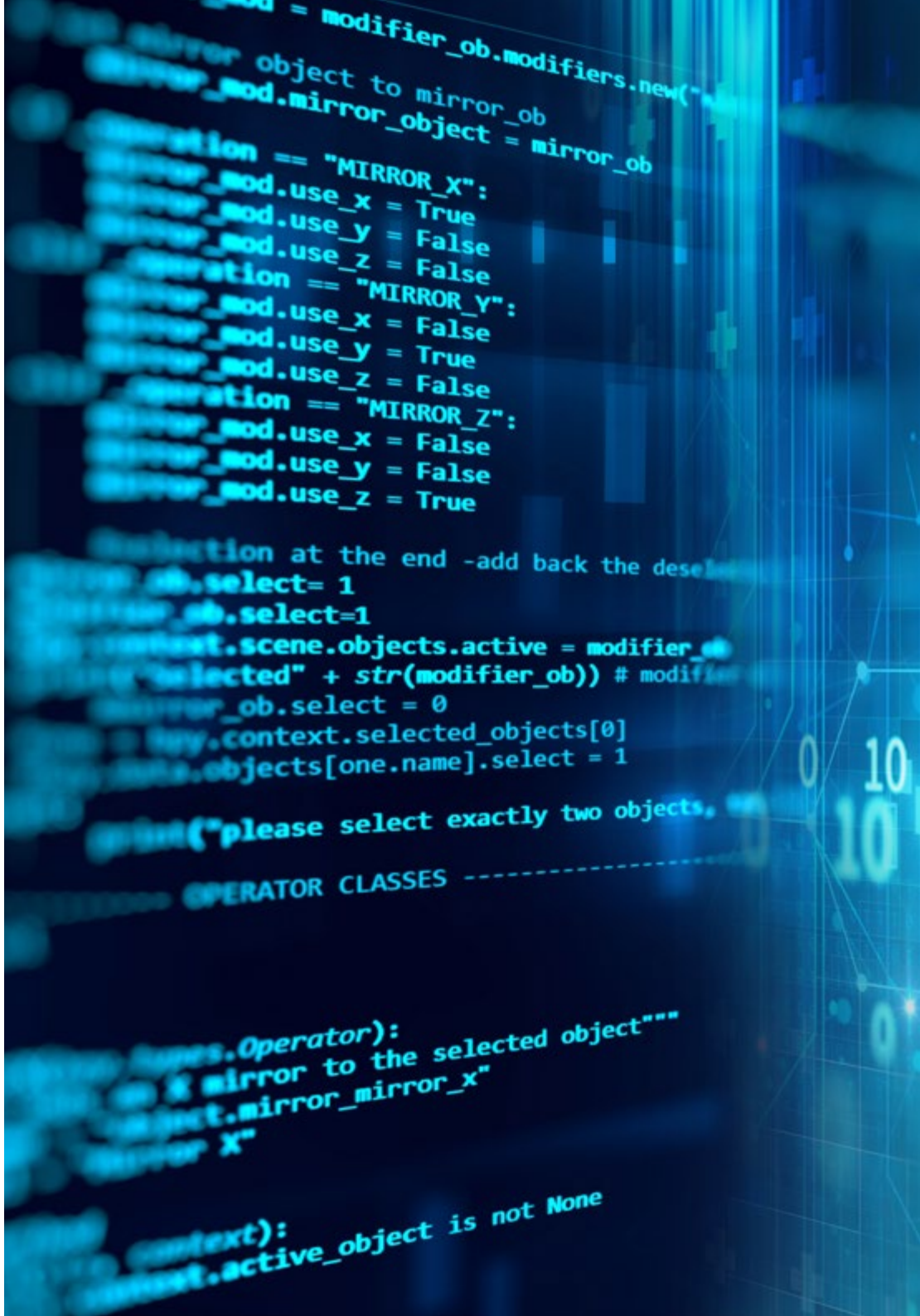
Der Universitätsexperte in IT-Sicherheit für Kommunikation zielt darauf ab, die Leistung von Fachleuten in diesem Bereich zu erleichtern, damit sie die wichtigsten neuen Entwicklungen in diesem Bereich erwerben und erlernen können.

Unser Ziel ist es, dass Sie die beste Fachkraft in Ihrem Bereich werden. Dafür haben wir die beste Methodik und den besten Inhalt"

Allgemeines Ziel

- Den Studenten in die Lage versetzen, sicher und mit hoher Qualität auf dem Gebiet der IT-Sicherheit für Kommunikation zu arbeiten

Erwerben Sie Ihre Fortbildung an der weltweit führenden privaten spanischsprachigen Online-Universität"



Spezifische Ziele

Modul 1. Sicherheit in Kommunikationssystemen und - netzen

- Kenntnis und Anwendung der Grundlagen der Programmierung in Telekommunikationsnetzen, -systemen und -diensten
- Beherrschung der Regeln und Vorschriften der Protokolle und Netze der internationalen Normungsorganisationen
- Verständnis der Konzepte der symmetrischen und asymmetrischen Kryptographie, der digitalen Signatur, der Hash-Funktionen und der Absicherung jeder Ebene einer Kommunikationsarchitektur
- Verständnis der verschiedenen Sicherheitsmechanismen und -protokolle, die auf der Zugangskontrolle basieren: Authentifizierung und Perimeterschutz
- Verständnis der Funktionsweise von technischen und menschlichen Bedrohungen für die Sicherheit von Telekommunikationsnetzen und -systemen
- Kategorisierung der verschiedenen Sicherheitsdienste für Netze und Systeme nach den zu schützenden Werten
- Anwendung von Netz- und Dienstmanagementsystemen auf Telekommunikationsnetze und -dienste für deren Konfiguration, Betrieb, Überwachung und Preisgestaltung
- Verwaltung der Sicherheit von Telekommunikationsnetzen und -diensten durch den Einsatz von Tunneln, Firewalls, Verschlüsselungs- und Authentifizierungsprotokollen sowie Mechanismen zum Schutz von Inhalten
- Verständnis und Anwendung der wichtigsten sicheren Programmiertechniken

Modul 2. Sicherheitsarchitekturen

- Verständnis für die Grundprinzipien der IT-Sicherheit
- Beherrschung von IT-Sicherheitsstandards und Zertifizierungsverfahren
- Analyse der organisatorischen und kryptographischen Grundlagen, auf denen die Sicherheitstechnologien beruhen
- Identifizierung der wichtigsten Bedrohungen und Schwachstellen der verschiedenen IKT-Elemente sowie deren Ursachen
- Gründliche Kenntnis der Netzsicherheitswerkzeuge und ihrer spezifischen Funktionen
- Anwendung der Technologien, aus denen sich eine IKT-Sicherheitsarchitektur zusammensetzt, in ihren verschiedenen Aspekten

Modul 3. Prüfung von Informationssystemen

- Beherrschung der wichtigsten Konzepte, Normen und Methoden der Systemprüfung
- Kenntnis der organisatorischen Elemente und des rechtlichen Rahmens von Audits
- Beschaffung eines Leitfadens für die Gestaltung neuer interner IT-Kontrollsysteme
- Verständnis und Identifizierung der Risiken, die durch technologische Entwicklungen entstehen
- Erkennung, wie verschiedene Informationssysteme die gewünschten Sicherheitsanforderungen erfüllen oder nicht erfüllen
- Durchführung eines Prozesses zur kontinuierlichen Verbesserung der Cybersicherheit

03

Struktur und Inhalt

Die Struktur der Inhalte wurde von den besten Fachleuten des Sektors der Computertechnik mit umfassender Erfahrung und anerkanntem Prestige in diesem Beruf entworfen.

Wir verfügen über das umfassendste und aktuellste wissenschaftliche Programm auf dem Markt. Wir streben nach Exzellenz und wollen, dass auch Sie sie erreichen“

Modul 1. Sicherheit in Kommunikationssystemen und -netzen

1.1. Ein Überblick über Sicherheit, Kryptographie und klassische Kryptoanalyse
- 1.1.1. IT-Sicherheit: Historische Perspektive
- 1.1.2. Aber was genau ist mit Sicherheit gemeint?
- 1.1.3. Geschichte der Kryptographie
- 1.1.4. Substitutions-Chiffren
- 1.1.5. Fallstudie: Die Enigma-Maschine

1.2. Symmetrische Kryptographie
- 1.2.1. Einführung und grundlegende Terminologie
- 1.2.2. Symmetrische Verschlüsselung
- 1.2.3. Betriebsarten
- 1.2.4. DES
- 1.2.5. Der neue AES-Standard
- 1.2.6. Stream-Verschlüsselung
- 1.2.7. Kryptoanalyse

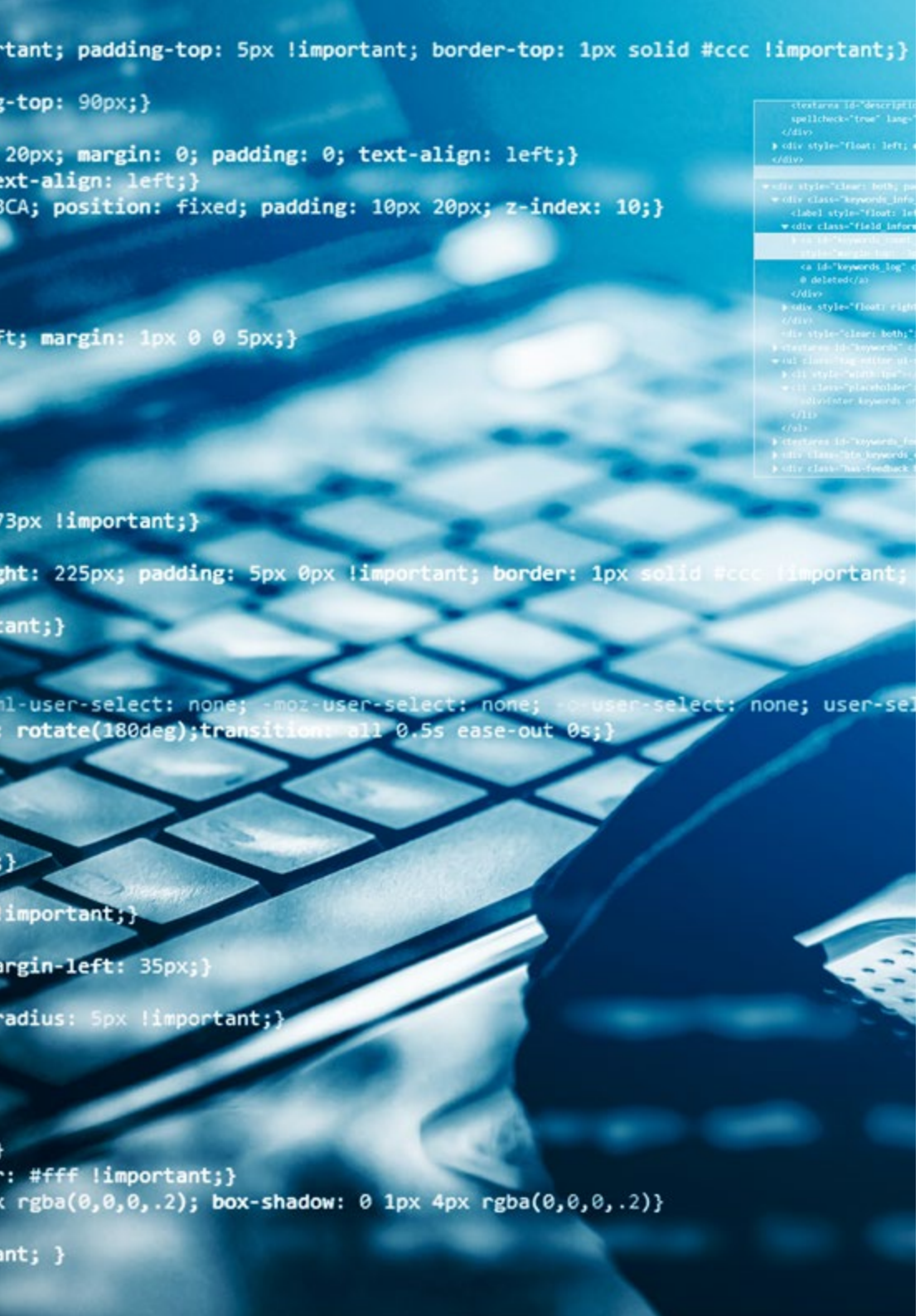
1.3. Asymmetrische Kryptographie
- 1.3.1. Die Ursprünge der Public Key Kryptographie
- 1.3.2. Grundlegende Konzepte und Bedienung
- 1.3.3. Der RSA-Algorithmus
- 1.3.4. Digitale Zertifikate
- 1.3.5. Speicherung und Verwaltung von Schlüsseln

1.4. Netzwerk-Angriffe
- 1.4.1. Bedrohungen und Angriffe aus dem Netzwerk
- 1.4.2. Aufzählung
- 1.4.3. Verkehrsüberwachung: *sniffers*
- 1.4.4. Denial-of-Service-Angriffe
- 1.4.5. ARP-Poisoning-Angriffe

1.5. Sicherheitsarchitekturen
- 1.5.1. Traditionelle Sicherheitsarchitekturen
- 1.5.2. *Secure Socket Layer*: SSL
- 1.5.3. SSH-Protokoll
- 1.5.4. Virtuelle private Netzwerke (VPNs)
- 1.5.5. Schutzmechanismen für externe Speicherlaufwerke
- 1.5.6. Hardware-Schutzmechanismen

1.6. Systemschutztechniken und Entwicklung von sicherem Code
- 1.6.1. Sicherheit bei Operationen
- 1.6.2. Ressourcen und Kontrollen
- 1.6.3. Überwachung
- 1.6.4. Systeme zur Erkennung von Eindringlingen
- 1.6.5. Host IDS
- 1.6.6. Netzwerk IDS
- 1.6.7. Signatur-basiertes IDS
- 1.6.8. Decoy Systeme
- 1.6.9. Grundlegende Sicherheitsprinzipien bei der Code-Entwicklung
- 1.6.10. Störungsmanagement
- 1.6.11. Staatsfeind Nummer 1: Der Buffer Overflow
- 1.6.12. Kryptographische Botschaften

1.7. Botnets und Spam
- 1.7.1. Ursprung des Problems
- 1.7.2. Prozess von Spam
- 1.7.3. Spam verschicken
- 1.7.4. Verfeinerung der Verteilerlisten
- 1.7.5. Methoden zum Schutz
- 1.7.6. Von Dritten angebotener Antispam-Service
- 1.7.7. Fallstudien
- 1.7.8. Exotischer Spam



1.8. Web Auditing und Angriffe
   1.8.1. Sammeln von Informationen
   1.8.2. Angriffs-Techniken
   1.8.3. Instrumente
1.9. Malware und bösartiger Code
   1.9.1. Was ist *Malware*?
   1.9.2. Arten von *Malware*
   1.9.3. Virus
   1.9.4. Kryptoviren
   1.9.5. Würmer
   1.9.6. *Adware*
   1.9.7. *Spyware*
   1.9.8. *Hoaxes*
   1.9.9. *Pishing*
   1.9.10. Trojaner
   1.9.11. Die *Malware*-Wirtschaft
   1.9.12. Mögliche Lösungen
1.10. Forensische Analyse
   1.10.1. Sammeln von Beweisen
   1.10.2. Analyse der Beweise
   1.10.3. Anti-Forensik-Techniken
   1.10.4. Praktische Fallstudie

Modul 2. Sicherheitsarchitekturen

2.1. Grundprinzipien der IT-Sicherheit
- 2.1.1. Was versteht man unter IT-Sicherheit?
- 2.1.2. Ziele der IT-Sicherheit
- 2.1.3. IT-Sicherheitsdienste
- 2.1.4. Folgen der mangelnden Sicherheit
- 2.1.5. Grundsatz der "Verteidigung in Sicherheit
- 2.1.6. Sicherheitspolitik, -pläne und -verfahren
  - 2.1.6.1. Verwaltung von Benutzerkonten
  - 2.1.6.2. Benutzeridentifizierung und -authentifizierung
  - 2.1.6.3. Autorisierung und logische Zugriffskontrolle
  - 2.1.6.4. Server-Überwachung
  - 2.1.6.5. Datenschutz
  - 2.1.6.6. Sicherheit von Remote-Verbindungen
- 2.1.7. Die Bedeutung des menschlichen Faktors

2.2. Standardisierung und Zertifizierung der IT-Sicherheit
- 2.2.1. Sicherheitsstandards
  - 2.2.1.1. Ziel der Standards
  - 2.2.1.2. Zuständige Stellen
- 2.2.2. Standards in den USA
  - 2.2.2.1. TCSEC
  - 2.2.2.2. Federal Criteria
  - 2.2.2.3. FISCAM
  - 2.2.2.4. NIST SP 800
- 2.2.3. Europäische Standards
  - 2.2.3.1. ITSEC
  - 2.2.3.2. ITSEM
  - 2.2.3.3. Europäische Agentur für Netz- und Informationssicherheit (ENISA)
- 2.2.4. Internationale Standards
- 2.2.5. Prozess der Zertifizierung

2.3. Bedrohungen für die IT-Sicherheit: Schwachstellen und *Malware*
- 2.3.1. Einführung
- 2.3.2. Schwachstellen der Systeme
  - 2.3.2.1. Sicherheitsvorfälle im Netz
  - 2.3.2.2. Ursachen für Schwachstellen in Informatiksystemen
  - 2.3.2.3. Arten von Schwachstellen
  - 2.3.2.4. Verantwortlichkeiten der Softwarehersteller
  - 2.3.2.5. Tools zur Schwachstellenbewertung
- 2.3.3. Bedrohungen der IT-Sicherheit
  - 2.3.3.1. Klassifizierung von Eindringlingen in das Netz
  - 2.3.3.2. Motivationen der Angreifer
  - 2.3.3.3. Phasen eines Angriffs
  - 2.3.3.4. Arten von Angriffen
- 2.3.4. Computerviren
  - 2.3.4.1. Allgemeine Merkmale
  - 2.3.4.2. Arten von Viren
  - 2.3.4.3. Schäden, die durch Viren verursacht werden
  - 2.3.4.4. Wie man Viren bekämpft

2.4. Cyber-Terrorismus und Reaktion auf Vorfälle
- 2.4.1. Einführung
- 2.4.2. Die Bedrohung durch Cyber-Terrorismus und Cyber-Kriegsführung
- 2.4.3. Folgen von Misserfolgen und Angriffen auf Unternehmen
- 2.4.4. Spionage in Computernetzen

2.5. Benutzeridentifizierung und biometrische Systeme
- 2.5.1. Einführung in die Benutzerauthentifizierung, -autorisierung und -registrierung
- 2.5.2. AAA-Sicherheitsmodell
- 2.5.3. Zugangskontrolle
- 2.5.4. Benutzeridentifikation
- 2.5.5. Überprüfung von Passwörtern
- 2.5.6. Authentifizierung mit digitalen Zertifikaten
- 2.5.7. Remote-Benutzeridentifikation

2.5.8. Einmalige Anmeldung
2.5.9. Passwort-Manager
2.5.10. Biometrische Systeme
2.5.10.1. Allgemeine Merkmale
2.5.10.2. Typen von biometrischen Systemen
2.5.10.3. Einführung von Systemen

2.6. Grundlagen der Kryptographie und kryptographische Protokolle
2.6.1. Einführung in die Kryptographie
2.6.1.1. Kryptographie, Kryptoanalyse und Kryptologie
2.6.1.2. Betrieb eines kryptografischen Systems
2.6.1.3. Geschichte der kryptografischen Systeme
2.6.2. Kryptoanalyse
2.6.3. Klassifizierung von kryptografischen Systemen
2.6.4. Symmetrische und asymmetrische kryptografische Systeme
2.6.5. Authentifizierung mit kryptografischen Systemen
2.6.6. Elektronische Unterschrift
2.6.6.1. Was ist eine elektronische Unterschrift?
2.6.6.2. Merkmale von elektronischen Unterschriften
2.6.6.3. Zertifizierungsstellen
2.6.6.4. Digitale Zertifikate
2.6.6.5. Vertrauenswürdige Systeme von Drittanbietern
2.6.6.6. Verwendung der elektronischen Unterschrift
2.6.6.7. Elektronischer Ausweis
2.6.6.8. Elektronische Rechnung

2.7. Tools für die Netzsicherheit
2.7.1. Das Problem der Sicherheit von Internetverbindungen
2.7.2. Sicherheit im externen Netz
2.7.3. Die Rolle von Proxyservern
2.7.4. Die Rolle von Firewalls
2.7.5. Authentifizierungsserver für Fernverbindungen
2.7.6. Analyse der Aktivitätsprotokolle
2.7.7. Systeme zur Erkennung von Eindringlingen
2.7.8. Köder

2.8. Sicherheit in virtuellen privaten und drahtlosen Netzen
2.8.1. Sicherheit in virtuellen privaten Netzen
2.8.1.1 Die Rolle von VPNs
2.8.1.2 Protokolle für VPNs
2.8.2. Traditionelle Sicherheit in drahtlosen Netzen
2.8.3. Mögliche Angriffe auf drahtlose Netzwerke
2.8.4. Das WEP-Protokoll
2.8.5. Standards für die Sicherheit drahtloser Netzwerke
2.8.6. Empfehlungen zur Verbesserung der Sicherheit

2.9. Sicherheit bei der Nutzung von Internetdiensten
2.9.1. Sicheres Surfen im Internet
2.9.1.1. Der www-Dienst
2.9.1.2. Sicherheitsprobleme in www
2.9.1.3. Sicherheitsempfehlungen
2.9.1.4. Schutz der Privatsphäre im Internet
2.9.2. E-Mail-Sicherheit
2.9.2.1. Merkmale von E-Mails
2.9.2.2. E-Mail-Sicherheitsprobleme
2.9.2.3. Empfehlungen zur E-Mail-Sicherheit
2.9.2.4. Erweiterte E-Mail-Dienste
2.9.2.5. Nutzung von E-Mail durch Mitarbeiter
2.9.3. SPAM
2.9.4. *Phising*

2.10. Kontrolle des Inhalts
2.10.1. Die Verbreitung von Inhalten über das Internet
2.10.2. Rechtliche Maßnahmen zur Bekämpfung illegaler Inhalte
2.10.3. Filterung, Katalogisierung und Sperrung von Inhalten
2.10.4. Schädigung von Image und Ruf

Modul 3. Wirtschaftsprüfung von Informationssystemen

3.1. Prüfung von Informationssystemen. Standards der guten Praxis
- 3.1.1. Einführung
- 3.1.2. Rechnungsprüfung und COBIT
- 3.1.3. Audit der IKT-Verwaltungssysteme
- 3.1.4. Zertifizierungen

3.2. Konzepte und Methoden der Systemprüfung
- 3.2.1. Einführung
- 3.2.2. Methoden der Systembewertung: quantitativ und qualitativ
- 3.2.3. IT-Audit-Methoden
- 3.2.4. Der Prüfungsplan

3.3. Der Prüfungsvertrag
- 3.3.1. Rechtlicher Charakter des Auftrags
- 3.3.2. Parteien eines Prüfungsauftrags
- 3.3.3. Gegenstand des Prüfungsvertrags
- 3.3.4. Der Prüfbericht

3.4. Organisatorische Elemente von Prüfungen
- 3.4.1. Einführung
- 3.4.2. Auftrag des Auditdienstes
- 3.4.3. Audit-Planung
- 3.4.4. SI-Audit-Methodik

3.5. Rechtlicher Rahmen für Audits
- 3.5.1. Schutz von personenbezogenen Daten
- 3.5.2. Rechtlicher Schutz von Software
- 3.5.3. Technologische Kriminalität
- 3.5.4. Vertragsabschluss, Unterschrift und elektronischer Ausweis

3.6. *Outsourcing* -Audit und Bezugsrahmen
- 3.6.1. Einführung
- 3.6.2. Grundlagen des *Outsourcing*
- 3.6.3. Prüfung von IT- *Outsourcing*
- 3.6.4. Referenzrahmen CMMI, ISO27001, ITIL

3.7. Sicherheitsaudit
- 3.7.1. Einführung
- 3.7.2. Physische und logische Sicherheit
- 3.7.3. Sicherheit in der Umgebung
- 3.7.4. Planung und Durchführung des Audits der physischen Sicherheit

3.8. Netzwerk- und Internet-Audits
- 3.8.1. Einführung
- 3.8.2. Schwachstellen im Netzwerk
- 3.8.3. Grundsätze und Rechte im Internet
- 3.8.4. Datenkontrolle und -verarbeitung

3.9. Prüfung von IT-Anwendungen und -Systemen
- 3.9.1. Einführung
- 3.9.2. Referenzmodelle
- 3.9.3. Bewertung der Qualität der Anwendungen
- 3.9.4. Audit der Organisation und Verwaltung des Bereichs Entwicklung und Instandhaltung

3.10. Prüfung der personenbezogenen Daten
- 3.10.1. Einführung
- 3.10.2. Gesetze und Vorschriften zum Datenschutz
- 3.10.3. Entwicklung des Audits
- 3.10.4. Verstöße und Sanktionen

Diese Spezialisierung wird es Ihnen ermöglichen, Ihre Karriere auf bequeme Weise voranzutreiben"

04

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

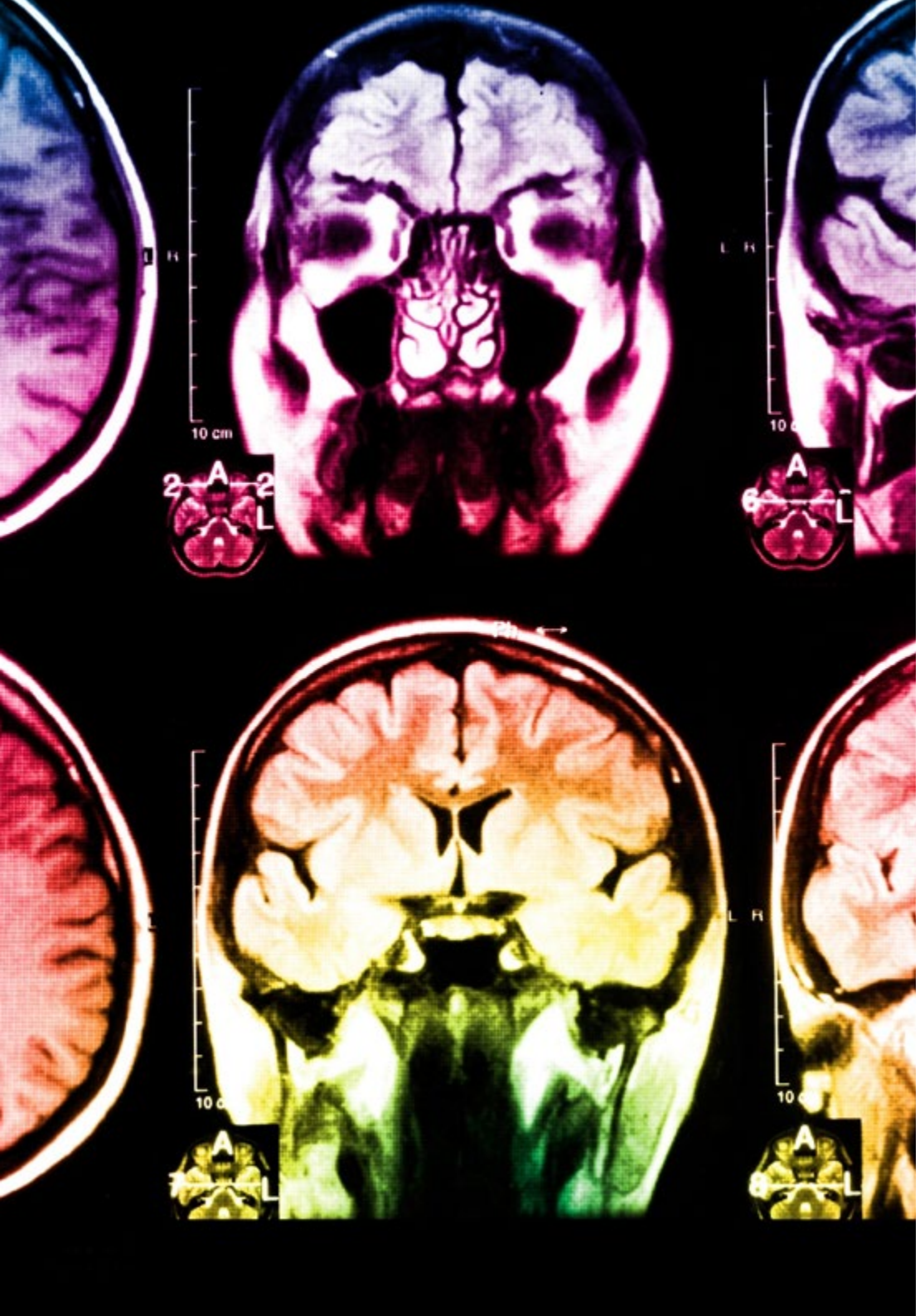
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

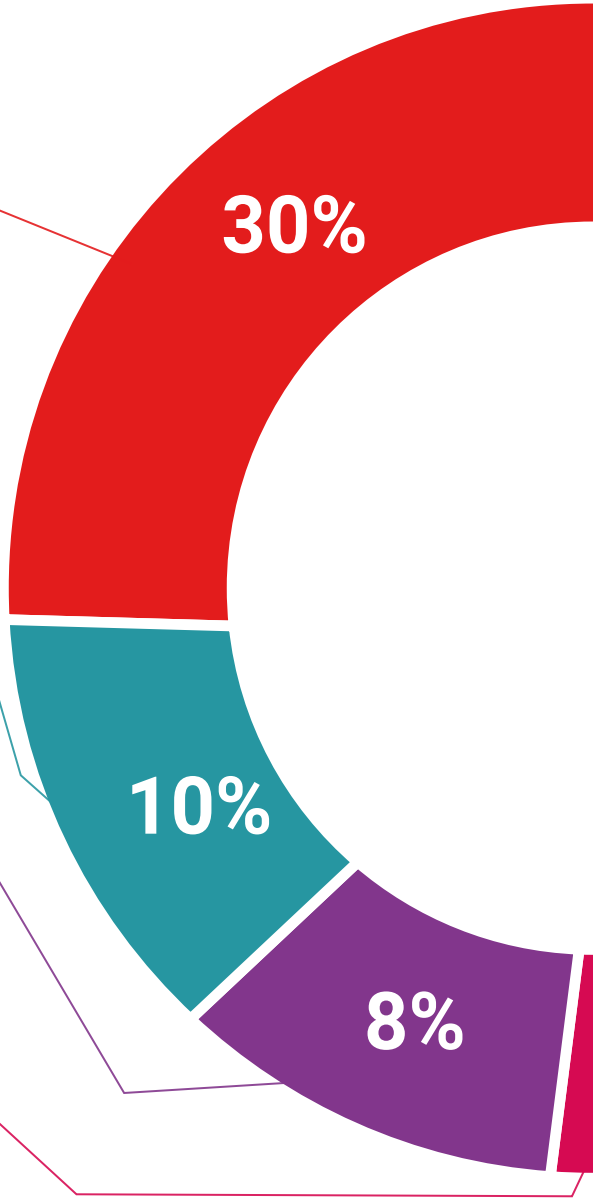
Das sogenannte Learning from an Expert baut Wissen und Gedächtnis auf und schafft Vertrauen für zukünftige schwierige Entscheidungen.

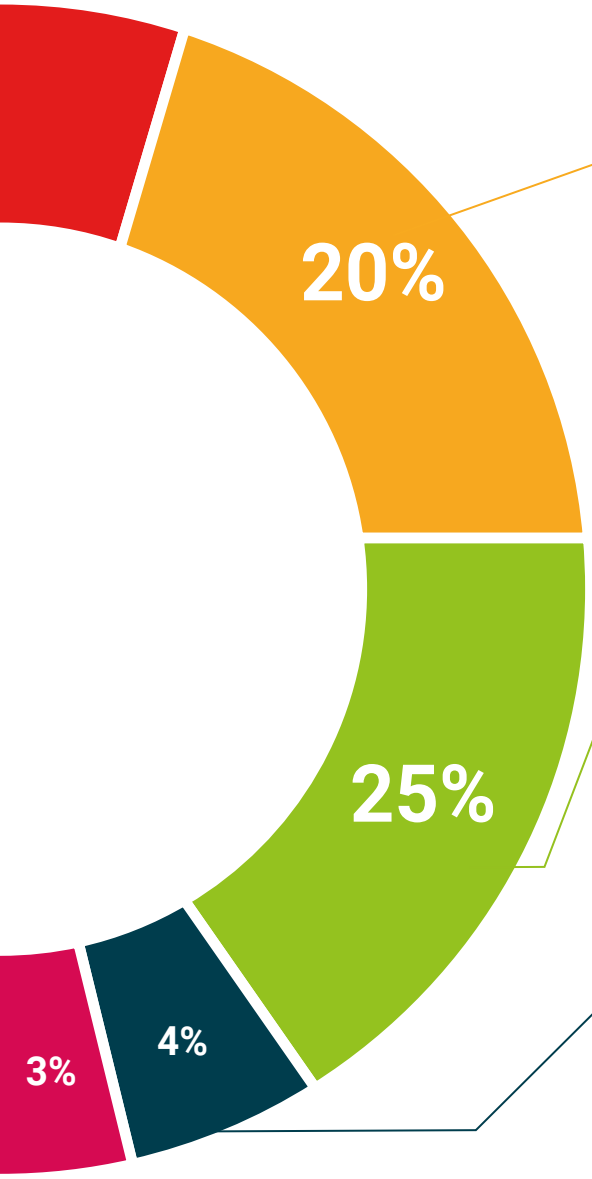
Fertigkeiten und Kompetenzen Praktiken

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.

05

Qualifizierung

Der Universitätsexperte in IT-Sicherheit für Kommunikation 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 **Universitätsexperte in IT-Sicherheit für Kommunikation** 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: **Universitätsexperte IT-Sicherheit für Kommunikation**

Anzahl der offiziellen Arbeitsstunden: **450 Std.**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

UNIVERSITÄTSEXPERTE

in

IT-Sicherheit für Kommunikation

Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 450 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

TECH ist eine private Hochschuleinrichtung, die seit dem 28. Juni 2018 vom Ministerium für öffentliche Bildung anerkannt ist.

Zum 17. Juni 2020

Tere Guevara Navarro
Rektorin

einzigartiger Code TECH: AFWOR23S techtitute.com/titel

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

tech technologische universität

Universitätsexperte
IT-Sicherheit für Kommunikation

- Modalität: **online**
- Dauer: **6 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Universitätsexperte

IT-Sicherheit für Kommunikation

tech technologische universität