# Universitätsexperte

## Implementierung einer IT-Sicherheitspolitik

tech technologische universität

tech technologische universität

# Universitätsexperte

## Implementierung einer IT-Sicherheitspolitik

- 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-implementierung-it-sicherheitspolitik**

# Index

01

# Präsentation

Unternehmen konzentrieren sich auf die Computer- und Cloud-Sicherheit, um den Diebstahl oder Verlust wertvoller Daten zu verhindern, vernachlässigen jedoch andere Sicherheitsaspekte, die für ein Unternehmen ebenso wichtig sind, wie den Schutz der physischen Anlagen und der Umgebung. In diesem 100%igen Online-Kurs lernen IT-Fachkräfte, wie sie Systeme durch die Implementierung fortschrittlicher Sicherheitsmethoden absichern können, um die Zugangskontrolle und Autorisierung für jeden Benutzer zu gewährleisten. All dies mit qualitativ hochwertigen Inhalten, basierend auf Videozusammenfassungen, spezifischer Lektüre und Fallstudien, die es ermöglichen, sich in einem Bereich der Informatik zu spezialisieren, der hochqualifizierte Fachleute erfordert.

*Erfahren Sie mehr über die wichtigsten Identifizierungs- und Autorisierungstechnologien und implementieren Sie sicherere IT-Systeme mit diesem Universitätsexperten”*

Investitionen in IT-Sicherheit sind für Unternehmen und Institutionen unverzichtbar. Viele von ihnen konzentrieren sich jedoch auf mögliche Cyber-Angriffe von außen und vergessen dabei, eine angemessene physische und umgebungsbezogene Sicherheitspolitik zu entwickeln, um den Zugang zu IT-Systemen zu kontrollieren. Im Rahmen dieses Universitätsexperten werden IT-Experten die wichtigsten Aspekte erörtern, die bei der Umsetzung dieser nicht einfachen Aufgabe zu berücksichtigen sind.

Das Programm, das von professionellen IT-Sicherheitsexperten geleitet wird, behandelt die Überprüfung des Sicherheitsstatus eines IT-Systems durch CIS-Kontrollen, die Analyse aller bestehenden biometrischen Zugangskontrollsysteme, ihre Implementierung und das Risikomanagement. Ein weiterer Schwerpunkt ist die Implementierung von Kryptographie in Kommunikationsnetzwerken mit den gängigsten symmetrischen und asymmetrischen Protokollen.

Die Authentifizierung und Identifizierung wird ebenfalls einen wichtigen Platz in diesem Studiengang einnehmen, in dem die IT-Fachleute eine PKI entwickeln, ihre Struktur und die Nutzung dieser Infrastruktur zum Schutz des Netzes durch die Verwendung von digitalen Zertifikaten kennen lernen.

TECH bietet eine ausgezeichnete Möglichkeit, sich in einem Bereich zu spezialisieren, in dem Fachleute mit aktuellen und innovativen Kenntnissen im Bereich der IT-Sicherheit gesucht werden. Das 100%ige Online-Studienmodell ermöglicht es, das Studium mit anderen Bereichen des persönlichen Lebens zu verbinden, da die Studenten nur ein internetfähiges Gerät benötigen, um auf alle ihnen zur Verfügung gestellten hochwertigen Multimedia-Inhalte zugreifen zu können.

Dieser **Universitätsexperte in Implementierung einer IT-Sicherheitspolitik** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung von Fallstudien, die von Experten für Computersicherheit präsentiert werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt vermittelt alle für die berufliche Praxis unverzichtbaren technischen 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
- 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

*Bringen Sie Ihr Wissen über IT-Sicherheit bei Feuer und Erdbeben auf den neuesten Stand. Schreiben Sie sich für diesen Universitätsexperten ein"*

*Lernen Sie die neuesten Entwicklungen im Bereich der Fingerabdruck-, Gesichts-, Iris- und Netzhauterkennung als Computersicherheitsmaßnahmen kennen”*

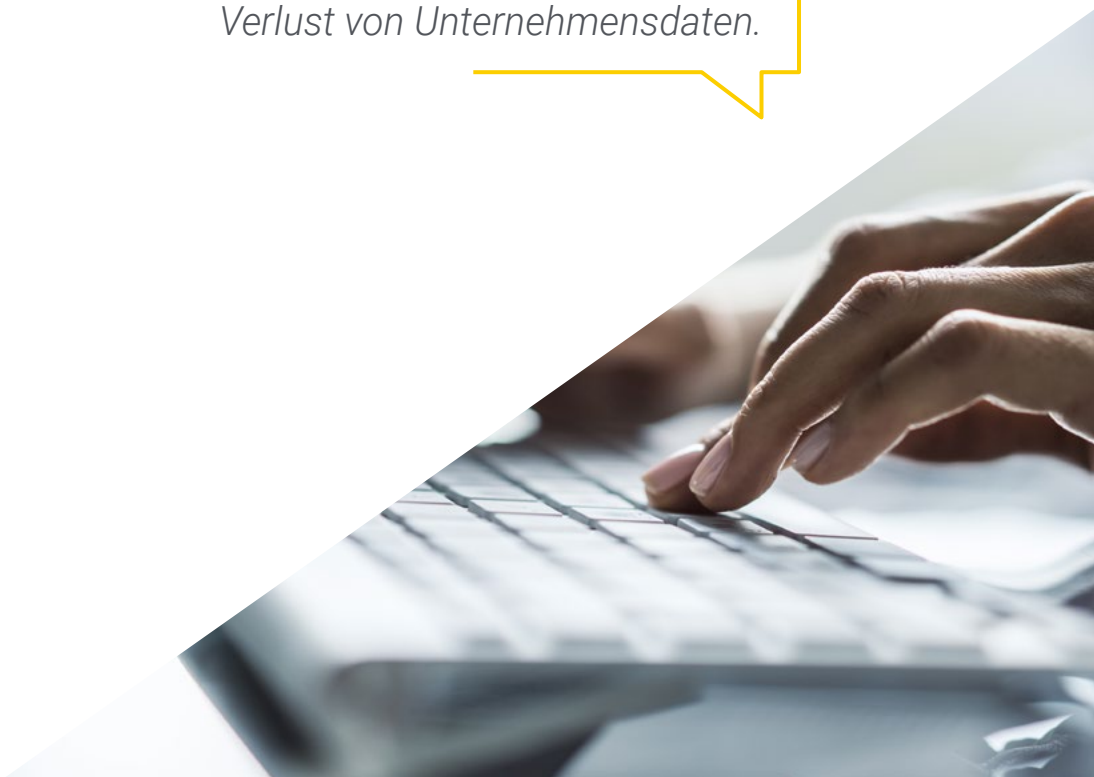
*Erfahren Sie mehr über sichere Kommunikationsprotokolle und wie Sie den Diebstahl wertvoller Daten verhindern können. Schreiben Sie sich jetzt ein.*

*Beherrschen Sie Secure Shell bis zur Perfektion und verhindern Sie den Verlust von Unternehmensdaten.*

Zu den Dozenten des Programms gehören Fachleute aus der Branche, die ihre Erfahrungen aus ihrer Arbeit in diese Weiterbildung einbringen, sowie anerkannte Spezialisten aus führenden Unternehmen 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 Studiengangs konzentriert sich auf problemorientiertes Lernen, bei dem die Fachkraft versuchen muss, die verschiedenen Situationen aus der beruflichen Praxis zu lösen, die während des akademischen Programms auftreten. Zu diesem Zweck wird sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.



02

# Ziele

Nach Abschluss dieses Universitätsexperten werden IT-Fachkräfte in der Lage sein, Sicherheitsrichtlinien in Soft- und Hardware zu implementieren oder Biometrie und biometrische Systeme zu untersuchen. Darüber hinaus werden die Studenten in der Lage sein, verschiedene Netzwerkverschlüsselungstechniken wie TLS, VPN oder SSH anzuwenden und die besten Systemüberwachungstools zu beherrschen, die derzeit auf dem Markt erhältlich sind. Das breite Spektrum an Ressourcen und Fallstudien bietet eine Lernerfahrung, die sehr nah an der Realität ist, mit der sie in ihrem Arbeitsumfeld konfrontiert werden.


*Spezialisieren Sie sich auf dem Gebiet der IT-Sicherheit mit Hilfe dieses Universitätsexperten. Schreiben Sie sich jetzt ein"*

## Allgemeine Ziele

- Vertiefen der wichtigsten Konzepte der Informationssicherheit
- Entwickeln der notwendigen Maßnahmen zur Gewährleistung guter Informationssicherheitspraktiken
- Entwickeln der verschiedenen Methoden zur Durchführung einer umfassenden Bedrohungsanalyse
- Installieren und Erlernen der verschiedenen Tools, die bei der Behandlung und Vorbeugung von Vorfällen eingesetzt werden

## Spezifische Ziele

### Modul 1. Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware

- Bestimmen, was Authentifizierung und Identifizierung sind
- Analysieren der verschiedenen existierenden Authentifizierungsmethoden und ihrer praktischen Umsetzung
- Implementieren der richtigen Zugriffskontrollpolitik für Software und Systeme
- Ermitteln der wichtigsten aktuellen Identifizierungstechnologien
- Generieren von Fachwissen über die verschiedenen Methoden, die für die Absicherung von Systemen existieren

### Modul 2. Implementierung von physischen und umweltbezogenen Sicherheitspolitiken im Unternehmen

- Analysieren der Begriffe sicherer Bereich und sicherer Umkreis
- Untersuchen der Biometrie und biometrischer Systeme
- Umsetzen der richtigen Sicherheitsrichtlinien für die physische Sicherheit
- Entwickeln der geltenden Vorschriften für sichere Bereiche von Computersystemen

### Modul 3. Richtlinien für sichere Kommunikation im Unternehmen

- Sichern eines Kommunikationsnetzwerks durch Partitionierung des Netzwerks
- Analysieren der verschiedenen Verschlüsselungsalgorithmen, die in Kommunikationsnetzwerken verwendet werden
- Implementieren verschiedener Verschlüsselungstechniken im Netzwerk wie TLS, VPN oder SSH

### Modul 4. Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme

- Entwickeln des Konzepts der Überwachung und Implementierung von Metriken
- Konfigurieren von Audit-Trails auf Systemen und Monitoring von Netzwerken
- Zusammenstellen der besten Systemüberwachungstools, die derzeit auf dem Markt sind

*Dieses Programm gibt Ihnen das nötige Rüstzeug, um Biometrie und biometrische Systeme in einem Unternehmen zu untersuchen”*

03

# Kursleitung

Dieser Universitätsexperte verfügt über Dozenten mit Erfahrung im Webmanagement und in der Sicherheit von Netzwerken und Dienstsystemen. Ihre umfassenden Kenntnisse in diesem Bereich der Informatik waren ausschlaggebend für ihre Wahl. Auf diese Weise haben die Studenten die Garantie, während des sechsmonatigen Kurses von einem Dozententeam betreut zu werden, das über die notwendige akademische Qualifikation und tägliche Praxis in der Anwendung von Sicherheitswerkzeugen, -systemen und -protokollen in Unternehmen verfügt. All dies mit dem Ziel, eine qualitativ hochwertige Weiterbildung anzubieten, die es dem IT-Spezialisten ermöglicht, in diesem Bereich voranzukommen.

*Ein Dozententeam mit umfassender Erfahrung im Bereich der Computersicherheit ist Ihre Garantie für einen erfolgreichen Lernprozess”*

## Leitung

### Fr. Fernández Sapena, Sonia

- Ausbilderin für Computersicherheit und Ethical Hacking am Nationalen Referenzzentrum von Getafe für Informatik und Telekommunikation von Madrid
- Zertifizierte E-Council-Ausbilderin
- Ausbilderin für die folgenden Zertifizierungen: EXIN Ethical Hacking Foundation und EXIN Cyber & IT Security Foundation, Madrid
- Von der CAM akkreditierte Fachausbilderin für die folgenden Berufszertifikate: IT-Sicherheit (IFCT0190), Verwaltung von Sprach- und Datennetzen (IFCM0310), Verwaltung von Abteilungsnetzen (IFCT0410), Alarmmanagement in Telekommunikationsnetzen (IFCM0410), Betreiber von Sprach- und Datennetzen (IFCM0110) und Verwaltung von Internetdiensten (IFCT0509)
- Externe Mitarbeit CSO/SSA (Chief Security Officer/Senior Security Architect)
- Computer- Ingenieurin an der Universität von Alcalá de Henares von Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes, Cas-Training
- Microsoft Azure Security Techonologies, E-Council

## Professoren

### Fr. López García, Rosa María

- Spezialistin für Management-Informationen
- Dozentin am Linux Professional Institute
- Mitarbeiterin der Hackerkademie Incibe
- Cybersecurity Talent Captain bei Teamciberhack
- Verwaltungs-, Buchhaltungs- und Finanzmanagerin bei Integra2Transportes
- Verwaltungsassistentin für den Einkauf von Ressourcen im Bildungszentrum Cardenal Marcelo Espínola
- Höhere Technikerin in Cybersicherheit und ethischem Hacking
- Mitglied von Ciberpatrulla

### Hr. Oropesiano Carrizosa, Francisco

- Computer-Ingenieur
- Mikroinformatiker, Netzwerktechniker und Sicherheitstechniker bei Cas-Training
- Entwickler für Webdienste, CMS, e-Commerce, UI und UX bei Fersa Reparaciones
- Manager für Webdienste, Inhalte, Mail und DNS bei Oropesia Web & Network
- Grafiker und Designer für Webanwendungen bei Xarxa Sakai Projectes
- Universitätskurs in Computersystemen an der Universität von Alcalá de Henares
- Masterstudiengang in DevOps: Docker and Kubernetes von Cyber Business Center
- Techniker für Netzwerke und Computersicherheit von der Universität der Balearischen Inseln
- Experte in Grafikdesign von der Polytechnischen Universität von Madrid

04

# Struktur und Inhalt

Das Dozententeam dieses Universitätsexperten hat einen Lehrplan entwickelt, der das gesamte Wissen über die praktische Umsetzung von Sicherheitsrichtlinien in Soft- und Hardware integriert und ein Modul der vertieften Behandlung von biometrischen Systemen und dem Schutz vor Umwelteinflüssen wie Feuer oder Erdbeben widmet. Darüber hinaus wird in diesem Studiengang besonderes Augenmerk auf Werkzeuge zur Systemüberwachung und auf kryptographische Algorithmen gelegt. Das *Relearning*-System, das auf der Wiederholung von Inhalten basiert, und die sehr praktischen Fallbeispiele ermöglichen es den Studenten, sich auf einfache Weise ein solides Wissen anzueignen.

*Passen Sie das Kurspensum Ihren Bedürfnissen an. Greifen Sie jederzeit und überall auf die Inhalte zu. Einfach anklicken und einschreiben”*

## **Modul 1.** Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware

1.1. Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware
  1.1.1. Implementierung von Identifizierung und Autorisierung
  1.1.2. Implementierung von Identifizierungstechniken
  1.1.3. Technische Maßnahmen zur Autorisierung
1.2. Identifizierungs- und Autorisierungstechniken
  1.2.1. Kennung und OTP
  1.2.2. USB-Token oder PKI-*Smartcard*
  1.2.3. Der Schlüssel „Vertrauliche Verteidigung"
  1.2.4. Aktive RFID
1.3. Sicherheitspolitiken für den Zugang zu Software und Systemen
  1.3.1. Implementierung von Politiken zur Zugriffskontrolle
  1.3.2. Umsetzung von Politiken für den Zugang zur Kommunikation
  1.3.3. Arten von Sicherheitstools für die Zugriffskontrolle
1.4. Verwaltung des Benutzerzugriffs
  1.4.1. Verwaltung von Zugriffsrechten
  1.4.2. Trennung von Rollen und Zugriffsfunktionen
  1.4.3. Implementierung von Zugriffsrechten in Systemen
1.5. Kontrolle des Zugriffs auf Systeme und Anwendungen
  1.5.1. Mindestzugriffsregel
  1.5.2. Sichere Anmeldetechnologien
  1.5.3. Passwort-Sicherheitsrichtlinien
1.6. Technologien für Identifikationssysteme
  1.6.1. Aktives Verzeichnis
  1.6.2. OTP
  1.6.3. PAP, CHAP
  1.6.4. KERBEROS, DIAMETER, NTLM
1.7. CIS-Kontrollen für Bastionierungssysteme
  1.7.1. Allgemeine CIS-Kontrollen
  1.7.2. Grundlegende CIS-Kontrollen
  1.7.3. Organisatorische CIS-Kontrollen
1.8. Operative Sicherheit
  1.8.1. Schutz vor bösartigem Code
  1.8.2. Sicherungskopien
  1.8.3. Aktivitätsprotokollierung und Überwachung
1.9. Management von technischen Schwachstellen
  1.9.1. Technische Schwachstellen
  1.9.2. Management von technischen Schwachstellen
  1.9.3. Einschränkungen bei der Software-Installation
1.10. Umsetzung der Sicherheitspraktiken
  1.10.1. Logische Schwachstellen
  1.10.2. Implementierung von Verteidigungsrichtlinien

## **Modul 2.** Implementierung von physischen und umweltbezogenen Sicherheitspolitiken im Unternehmen

2.1. Sichere Bereiche
  2.1.1. Physischer Sicherheitsbereich
  2.1.2. Arbeiten in Sicherheitsbereichen
  2.1.3. Sicherheit von Büros, Geschäftsräumen und Ressourcen
2.2. Physische Zugangskontrollen
  2.2.1. Richtlinien zur physischen Zugangskontrolle
  2.2.2. Physische Zugangskontrollsysteme
2.3. Schwachstellen beim physischen Zugang
  2.3.1. Die wichtigsten physischen Schwachstellen
  2.3.2. Umsetzung von Schutzmaßnahmen
2.4. Physiologische biometrische Systeme
  2.4.1. Fingerabdruck
  2.4.2. Gesichtserkennung
  2.4.3. Iris- und Retina-Erkennung
  2.4.4. Andere physiologische biometrische Systeme

2.5. Verhaltensbiometrische Systeme
  2.5.1. Erkennung von Unterschriften
  2.5.2. Erkennung von Schriftzeichen
  2.5.3. Spracherkennung
  2.5.4. Andere biometrische Verhaltenssysteme
2.6. Risikomanagement in der Biometrie
  2.6.1. Implementierung biometrischer Systeme
  2.6.2. Schwachstellen biometrischer Systeme
2.7. Implementierung von Richtlinien in Hosts
  2.7.1. Installation der Verkabelung, Bereitstellung und Sicherheit
  2.7.2. Platzierung der Geräte
  2.7.3. Verlassen der Geräte außerhalb des Gebäudes
  2.7.4. Unbeaufsichtigte Computerausrüstung und Sicherungspolitik beim Verlassen des Arbeitsplatzes
2.8. Umweltschutz
  2.8.1. Feuerschutzsysteme
  2.8.2. Schutzsysteme bei Erdbeben
  2.8.3. Erdbebenschutzsysteme
2.9. Sicherheit von Datenverarbeitungszentren
  2.9.1. Sicherheitstüren
  2.9.2. Videoüberwachungssysteme (CCTV)
  2.9.3. Sicherheitskontrolle
2.10. Internationale Vorschriften zur physischen Sicherheit
  2.10.1. IEC 62443-2-1 (europäisch)
  2.10.2. NERC CIP-005-5 (USA)
  2.10.3. NERC CIP-014-2 (USA)

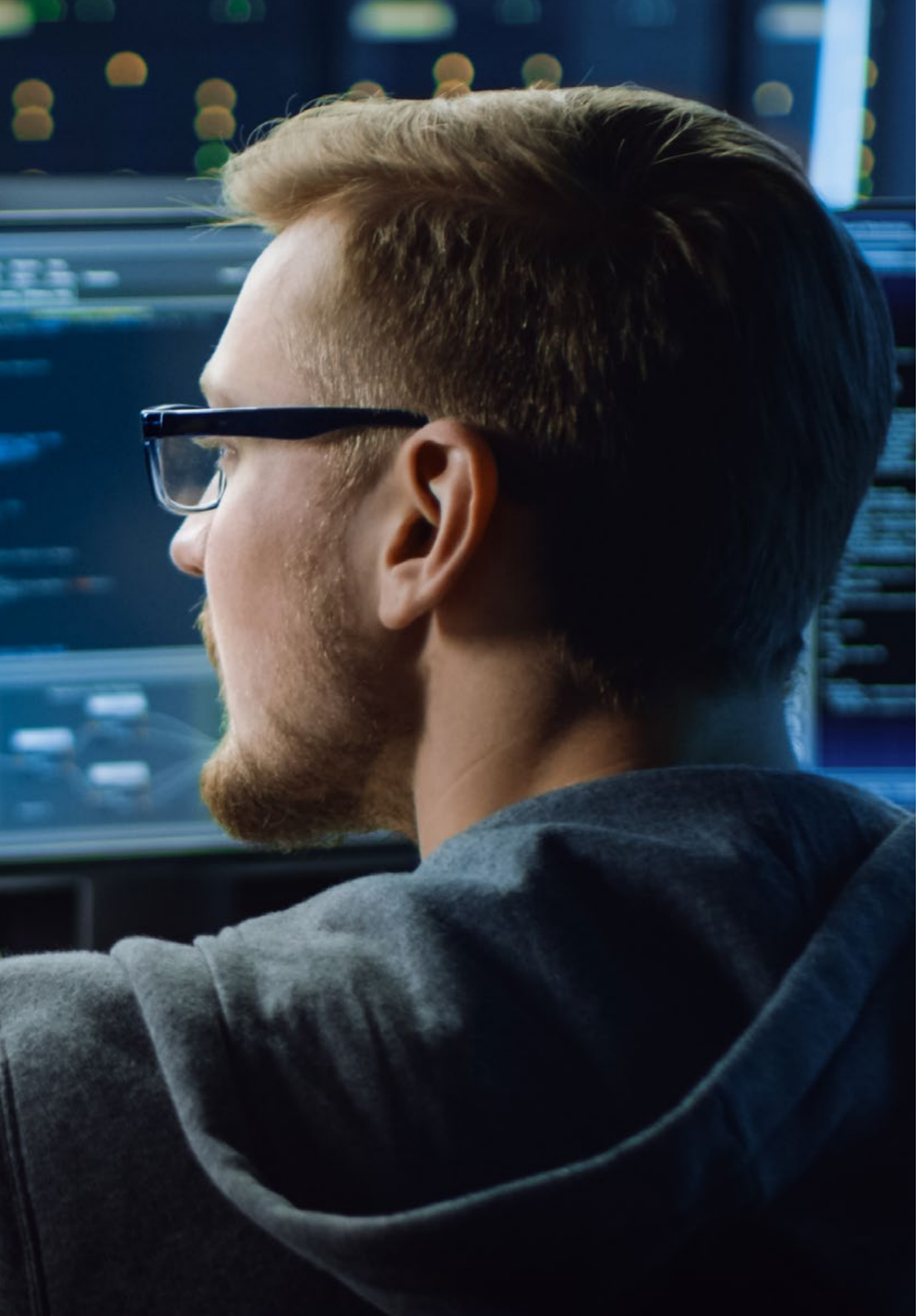
## **Modul 3.** Richtlinien für sichere Kommunikation im Unternehmen

3.1. Verwaltung der Netzwerksicherheit
  3.1.1. Netzwerkkontrolle und -überwachung
  3.1.2. Netzwerk-Trennung
  3.1.3. Netzwerk-Sicherheitssysteme
3.2. Sichere Kommunikationsprotokolle
  3.2.1. TCP/IP-Modell
  3.2.2. IPSEC-Protokoll
  3.2.3. TLS-Protokoll
3.3. TLS 1.3-Protokoll
  3.3.1. Phasen eines TLS 1.3-Prozesses
  3.3.2. *Handshake*-Protokoll
  3.3.3. Registrierungsprotokoll
  3.3.4. Unterschiede zu TLS 1.2
3.4. Kryptographische Algorithmen
  3.4.1. In der Kommunikation verwendete kryptographische Algorithmen
  3.4.2. *Cipher-Suites*
  3.4.3. Erlaubte kryptographische Algorithmen für TLS 1.3
3.5. *Digest*-Funktionen
  3.5.1. MD6
  3.5.2. SHA
3.6. PKI. Infrastruktur für den öffentlichen Schlüssel
  3.6.1. PKI und ihre Einrichtungen
  3.6.2. Digitales Zertifikat
  3.6.3. Arten von digitalen Zertifikaten
3.7. Tunnel- und Transportkommunikation
  3.7.1. Tunnel-Kommunikation
  3.7.2. Transport-Kommunikation
  3.7.3. Verschlüsselte Tunnel-Implementierung
3.8. SSH. *Secure Shell*
  3.8.1. SSH. Sichere Kapsel
  3.8.2. Betrieb von SSH
  3.8.3. SSH-Tools

3.9. Prüfung kryptographischer Systeme
  3.9.1. Prüfung der Integrität
  3.9.2. Testen von kryptographischen Systemen
3.10. Kryptografische Systeme
  3.10.1. Schwachstellen in kryptographischen Systemen
  3.10.2. Kryptografische Sicherheitsvorkehrungen

## **Modul 4.** Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme

4.1. Richtlinien für die Überwachung von Informationssystemen
  4.1.1. System-Überwachung
  4.1.2. Metriken
  4.1.3. Arten von Metriken
4.2. Auditing und Logging in Systemen
  4.2.1. Auditing und Logging in Windows
  4.2.2. Auditing und Logging in Linux
4.3. SNMP-Protokoll. *Simple Network Management Protocol*
  4.3.1. SNMP-Protokoll
  4.3.2. Betrieb von SNMP
  4.3.3. SNMP-Tools
4.4. Netzwerk-Überwachung
  4.4.1. Netzwerküberwachung in Kontrollsystemen
  4.4.2. Überwachungstools für Kontrollsysteme
4.5. Nagios. System zur Netzwerküberwachung
  4.5.1. Nagios
  4.5.2. Betrieb von Nagios
  4.5.3. Installation von Nagios
4.6. Zabbix. System zur Netzwerküberwachung
  4.6.1. Zabbix
  4.6.2. Betrieb von Zabbix
  4.6.3. Installation von Zabbix





4.7. Cacti. System zur Netzwerküberwachung
- 4.7.1. Cacti
- 4.7.2. Betrieb von Cacti
- 4.7.3. Installation von Cacti

4.8. Pandora. System zur Netzwerküberwachung
- 4.8.1. Pandora
- 4.8.2. Betrieb von Pandora
- 4.8.3. Installation von Pandora

4.9. SolarWinds. System zur Netzwerküberwachung
- 4.9.1. SolarWinds
- 4.9.2. Betrieb von SolarWinds
- 4.9.3. Installation von SolarWinds

4.10. Regelungen zur Überwachung
- 4.10.1. CIS-Kontrollen zur Audits und Registrierung
- 4.10.2. NIST 800-123 (USA)

*Die vom Dozententeam entwickelten interaktiven Zusammenfassungen und Fallstudien vermitteln Ihnen die Inhalte, die Sie benötigen, um Ihre Karriere zu fördern”*

05

# Methodik

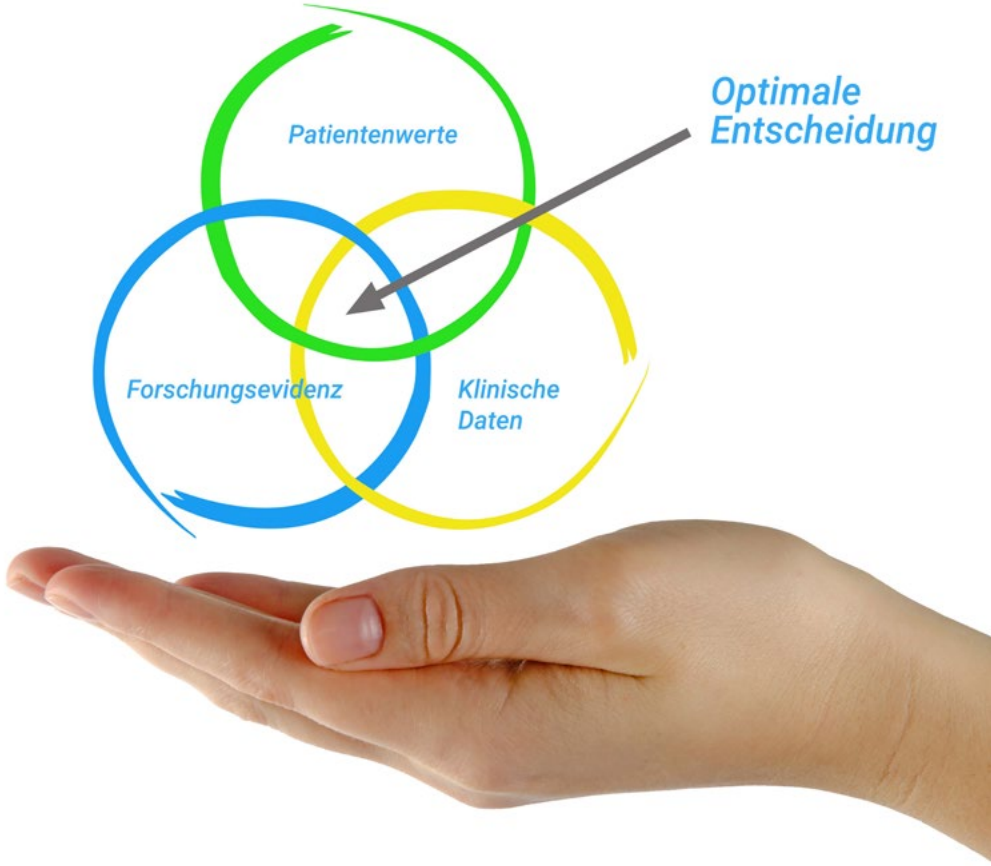
Dieses Fortbildungsprogramm bietet eine andere Art des Lernens. Unsere Methodik wird durch eine zyklische Lernmethode entwickelt: ***das Relearning***. Dieses Lehrsystem wird z. B. an den renommiertesten medizinischen Fakultäten der Welt angewandt und wird von wichtigen Publikationen wie dem ***New England 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

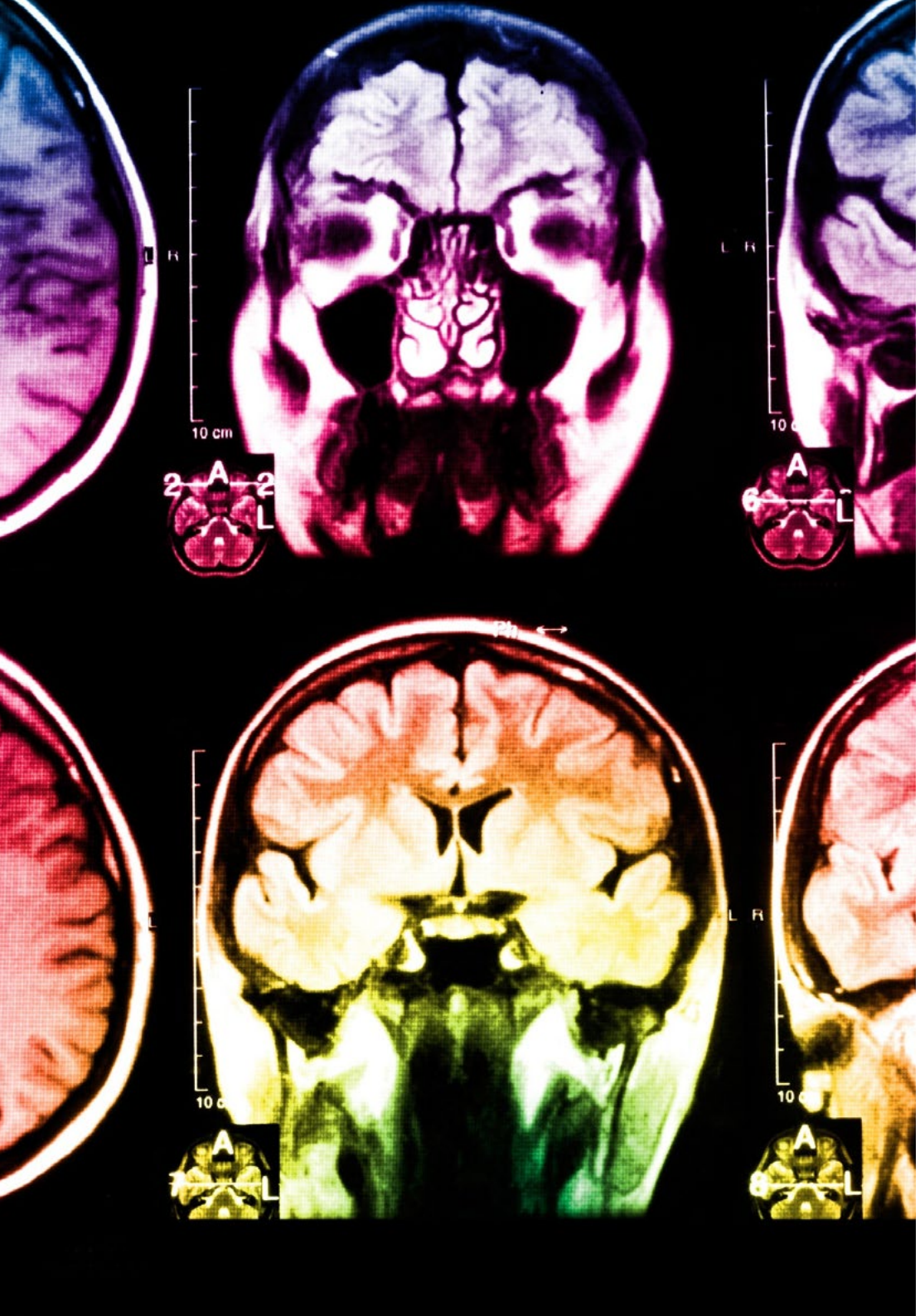
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

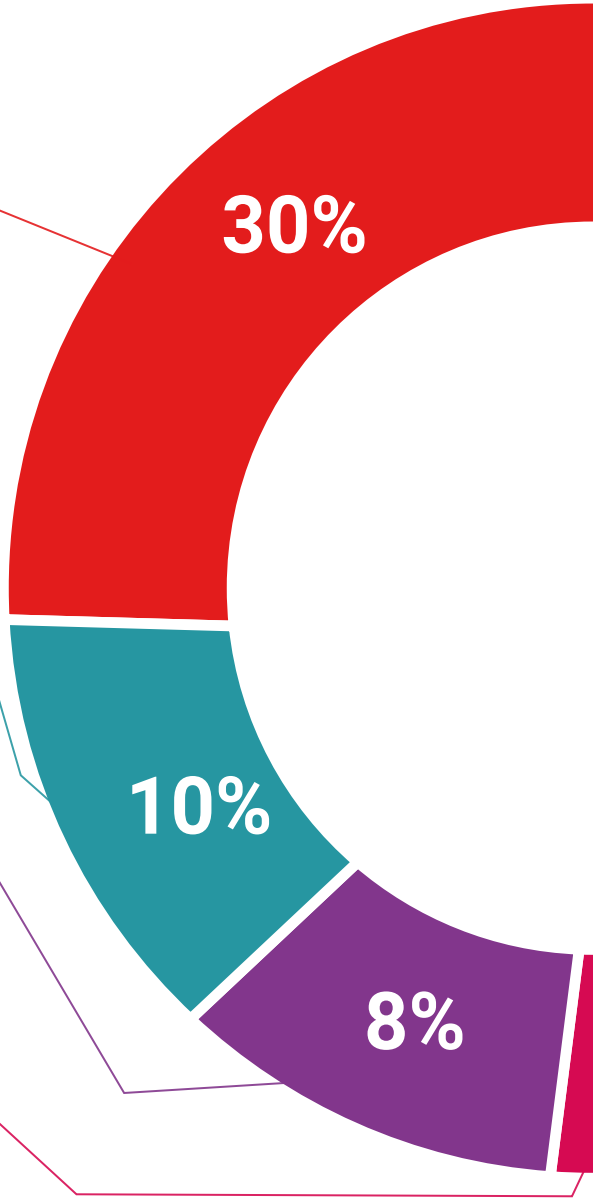
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

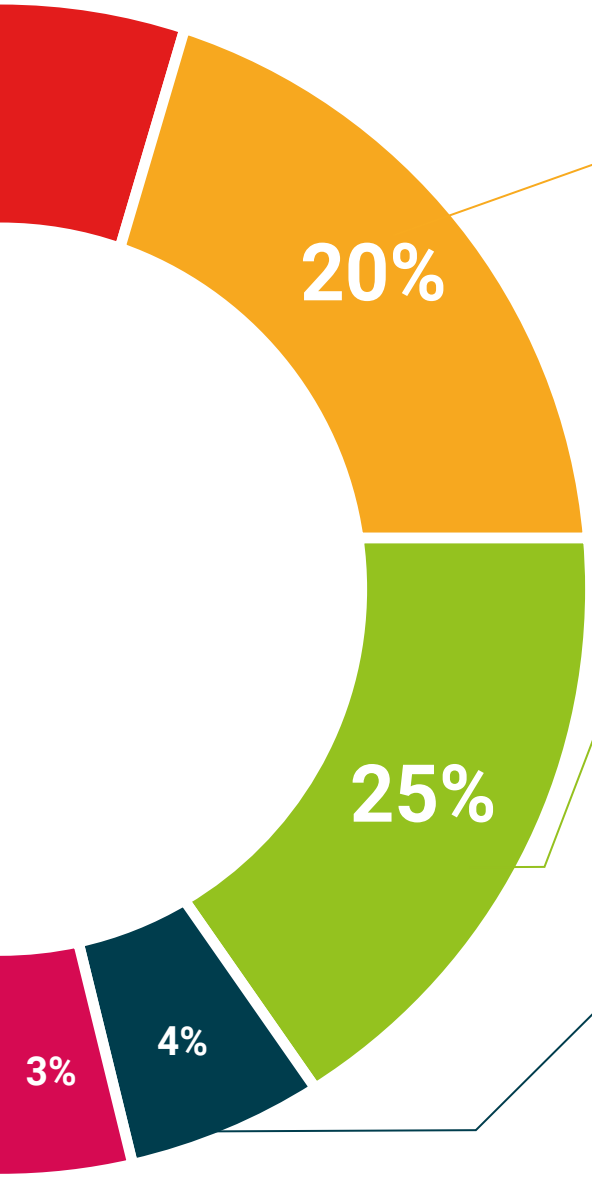
### Übungen für Fertigkeiten und Kompetenzen

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.

06

# Qualifizierung

Der Universitätsexperte in Implementierung einer IT-Sicherheitspolitik garantiert neben der präzisesten und aktuellsten Fortbildung 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 Implementierung einer IT-Sicherheitspolitik** 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 in Implementierung einer IT-Sicherheitspolitik**

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

Implementierung einer IT-Sicherheitspolitik

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
## Implementierung einer IT-Sicherheitspolitik

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

# Universitätsexperte

## Implementierung einer IT-Sicherheitspolitik

tech technologische universität