Universitätsexperte

Verwaltung der Sicherheit der Informationstechnologie

tech technologische universität

tech technologische universität

Universitätsexperte
Verwaltung der Sicherheit der Informationstechnologie

- 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-verwaltung-sicherheit-informationstechnologie

Index

01

Präsentation

Die Integration von Informationstechnologien in vielen Unternehmen hat einen Nebeneffekt: Die Risiken für die IT-Sicherheit sind gestiegen. Unternehmen müssen sich jetzt über verschiedene Angriffe und Schwachstellen im Klaren sein, die ihr ordnungsgemäßes Funktionieren und ihre Dienste beeinträchtigen können. Es ist daher unerlässlich, einen Spezialisten im Unternehmen zu haben, der für das Sicherheitsmanagement dieser Technologien verantwortlich ist. Dieses Programm bietet Fachleuten die Möglichkeit, die fortschrittlichsten IT-Schutzmethoden in diesem Bereich kennenzulernen, da sie sich mit Aspekten wie Risikobewertung auf der Grundlage von Geschäftsparametern, Identitäts- und Zugriffsmanagement oder Intrusionstests befassen werden.

Immer mehr Unternehmen benötigen Spezialisten für das IT-Sicherheitsmanagement. Dieses Programm ermöglicht es Ihnen, sich beruflich weiterzuentwickeln und Themen wie die Planung der Geschäftskontinuität im Zusammenhang mit der Sicherheit zu vertiefen"

Es ist eine Tatsache: Es gibt kaum noch Unternehmen, die in ihren internen Prozessen keine digitalen und IT-Tools einsetzen. Tätigkeiten und Abläufe wie die Identifizierung von Mitarbeitern, Logistiksysteme oder der Kontakt mit Lieferanten und Kunden werden heute hauptsächlich über die Informationstechnologie abgewickelt. Diese Technologien müssen jedoch ordnungsgemäß konzipiert und überwacht werden, da sie ausgenutzt werden können, um an Daten zu gelangen oder sich Zugang zu sensiblen Bereichen des Unternehmens zu verschaffen.

Aus diesem Grund ist der Spezialist für Sicherheitsadministration eine zunehmend gefragte Position, die nicht von jedem IT-Spezialisten besetzt werden kann. Es ist ein hochaktuelles Wissen erforderlich, das die neuesten Entwicklungen im Bereich der Cybersicherheit berücksichtigt. Daher wurde dieser Universitätsexperte so konzipiert, dass er Fachleuten die neuesten Fortschritte in diesem Bereich bietet und sich mit Themen wie Sicherheitsaudits, Sicherheit von Endgeräten oder der wirksamsten Reaktion auf verschiedene Vorfälle befasst.

Auch dieses Programm wurde in einem 100%igen Online-Format entwickelt, das sich an die Lebensumstände der Berufstätigen anpasst und es ihnen ermöglicht, zu studieren, wann, wo und wie sie wollen. Es wird auch über einen renommierten Lehrkörper auf dem Gebiet der Cybersicherheit verfügt, der durch zahlreiche Multimedia-Ressourcen unterstützt wird, um den Lernprozess bequem, schnell und effektiv zu gestalten.

Dieser **Universitätsexperte in Verwaltung der Sicherheit der Informationstechnologie** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung praktischer Fälle, die von Experten der Informatik und Cybersicherheit vorgestellt werden
- Der anschauliche, schematische und äußerst praxisnahe Inhalt soll wissenschaftliche und praktische Informationen zu den für die berufliche Praxis wesentlichen Disziplinen vermitteln
- Die praktischen Übungen, bei denen der Selbstbewertungsprozess zur Verbesserung des Lernens durchgeführt werden kann
- Ihr besonderer Schwerpunkt liegt auf innovativen Methoden
- Theoretische Vorträge, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugriffs auf die Inhalte von jedem festen oder tragbaren Gerät mit Internetanschluss

Dieses Programm ermöglicht es Ihnen, Aspekte wie den Lebenszyklus eines Plans zur Aufrechterhaltung des Geschäftsbetriebs oder das Schwachstellenmanagement zu vertiefen"

TECH stellt Ihnen die besten Multimedia-Ressourcen zur Verfügung: Fallstudien, theoretisch-praktische Aktivitäten, Videos, interaktive Zusammenfassungen, usw. Alles, um den Lernprozess agil zu gestalten und jede Minute, die Sie investieren, optimal zu nutzen"

Sie werden in der Lage sein, auf alle Arten von Bedrohungen der Cybersicherheit angemessen zu reagieren. Schreiben Sie sich ein und werden Sie ein echter Spezialist.

Lernen Sie in Ihrem eigenen Tempo, ohne Unterbrechungen oder starre Zeitpläne: Die Lehrmethode von TECH ist so bequem.

Zu den Dozenten des Programms gehören Fachleute aus der Branche, die ihre Erfahrungen in diese Fortbildung einbringen, sowie anerkannte Spezialisten 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. Zu diesem Zweck wird sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.

02

Ziele

In Anbetracht der zunehmenden Komplexität des Bereichs der Cybersicherheit besteht das Hauptziel dieses Universitätsexperten in Verwaltung der Sicherheit der Informationstechnologie darin, den Fachleuten die wichtigsten Entwicklungen in diesem Bereich näher zu bringen. Auf diese Weise werden Sie zu einem großen Spezialisten auf diesem Gebiet, der in der Lage ist, den Bereich der Cybersicherheit in Unternehmen aller Branchen zu verwalten und zu leiten.

TECH hilft Ihnen, Ihre Ziele zu erreichen, denn mit diesem Programm können Sie sich auf wichtige berufliche Positionen in den wichtigsten nationalen und internationalen Unternehmen bewerben"

Allgemeine Ziele

- Entwicklung eines Informationssicherheits-Managementsystems (ISMS)
- Identifizierung der Schlüsselelemente, aus denen ein ISMS besteht
- Bewertung der verschiedenen Sicherheitsarchitekturmodelle, um das für das Unternehmen am besten geeignete Modell zu ermitteln
- Identifizierung der regulatorischen Rahmenbedingungen für die Anwendung und deren Rechtsgrundlagen
- Analyse der organisatorischen und funktionalen Struktur eines Informationssicherheitsbereichs (das Büro des CISO)
- Erstellung eines Audit-Programms, das den Selbstbewertungsbedarf der Organisation in Bezug auf die Cybersicherheit abdeckt
- Entwicklung eines Programms zum Scannen und Überwachen von Schwachstellen und eines Plans zur Reaktion auf Cyber-Sicherheitsvorfälle
- Bestimmung der grundlegenden Elemente eines Business Continuity Plan (BCP) auf der Grundlage der ISO-22301-Leitlinien
- Prüfung der Risiken, die sich aus dem Fehlen eines Business Continuity Plan (BCP) ergeben
- Analyse der Erfolgskriterien eines BCP und seiner Integration in das allgemeine Risikomanagement eines Unternehmens
- Festlegung der Implementierungsphasen eines Business Continuity Plan

Spezifische Ziele

Modul 1. Architekturen und Modelle für die Informationssicherheit

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

Modul 2. IT-Sicherheitsmanagement

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

Modul 3. Business Continuity Plan in Verbindung mit Sicherheit

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

Sie werden der führende IT-Sicherheitsspezialist in Ihrem Umfeld sein. Warten Sie nicht länger: Schreiben Sie sich jetzt ein"

03

Kursleitung

Die weltweit führenden Spezialisten für die Verwaltung der IT-Sicherheit zur Verfügung zu haben, ist eine große Chance für die Fachleute. Und genau das bietet dieser Universitätsexperte, dessen Lehrkörper aus renommierten Ingenieuren und Informatikern besteht, die den Studenten die fortschrittlichsten Techniken und Verfahren vermitteln, um die angemessene interne Sicherheit eines Unternehmens zu gewährleisten.

Sie werden mit den führenden Spezialisten im Bereich der Cybersicherheit in Kontakt kommen, die Ihnen das nötige Rüstzeug mit auf den Weg geben, um in diesem Bereich auf höchstem Niveau zu arbeiten"

Leitung

Hr. Olalla Bonal, Martín

- Technischer Kundenspezialist Blockchain bei IBM
- *Blockchain* Architekt
- Infrastruktur Architekt im Bankwesen
- Projektleitung und Implementierung von Lösungen
- Techniker für digitale Elektronik
- Dozent: *Hyperledger Fabric*-Schulung für Unternehmen
- Dozent: Geschäftsorientierte *Blockchain*-Schulungen für Unternehmen

Professoren

Hr. Gozalo Fernández, Juan Luis

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

Hr. Embid Ruiz, Mario

- Jurist, Experte für ICT und Datenschutzrecht
- Juristische Leitung von Branddocs, SL, einem Technologieunternehmen, das vertrauenswürdige Lösungen anbietet
- Hochschulabschluss in Jura und Betriebswirtschaftslehre an der Universität Rey Juan Carlos, Madrid
- Masterstudiengang in Neue Technologien, Internet und audiovisuelles Recht vom Zentrum für universitäre Studien Villanueva und Cremades & Calvo Sotelo

Hr. Rodrigo Estébanez, Juan Manuel

- Gründung von ISMET TECH S.L
- Hochschulabschluss in Ingenieurwesen an der Universität Valladolid
- Masterstudiengang in Integrierten Managementsystemen von CFE-CEU
- ISO 27001 Lead Auditor (IMQ)
- ISO 27001 Lead Implementor (IMQ)
- NATO Standards HPS

04

Struktur und Inhalt

Der Lehrplan dieses Universitätsexperten in Verwaltung der Sicherheit der Informationstechnologie ist in 3 Module gegliedert, die in 450 Lernstunden erarbeitet werden. Während dieser Zeit wird sich die Fachkraft mit relevanten Aspekten dieses Sektors befassen, z. B. mit der forensischen Analyse, mit Modellen der Informationssicherheit, mit dem in diesem Bereich geltenden Rechtsrahmen oder mit der Gestaltung von Regeln für die Netzsicherheit, neben vielen anderen Themen.

Ihnen steht der vollständigste Lehrplan zur Verfügung, der mit didaktischen Mitteln präsentiert wird, auf die Sie 24 Stunden am Tag zugreifen können"

Modul 1. Architekturen und Modelle für die Informationssicherheit

1.1. Architektur der Informationssicherheit
- 1.1.1. ISMS / ISDP
- 1.1.2. Strategische Ausrichtung
- 1.1.3. Risikomanagement
- 1.1.4. Leistungsmessung

1.2. Modelle der Informationssicherheit
- 1.2.1. Richtlinienbasierte Sicherheitsmodelle
- 1.2.2. Basierend auf Schutz-Tools
- 1.2.3. Teambasiert

1.3. Sicherheitsmodell. Wichtige Komponenten
- 1.3.1. Identifizierung von Risiken
- 1.3.2. Definition von Kontrollen
- 1.3.3. Kontinuierliche Bewertung des Risikoniveaus
- 1.3.4. Sensibilisierungsplan für Mitarbeiter, Lieferanten, Partner usw.

1.4. Prozess der Risikoverwaltung
- 1.4.1. Identifizierung von Vermögenswerten
- 1.4.2. Identifizierung von Bedrohungen
- 1.4.3. Risikobewertung
- 1.4.4. Priorisierung der Kontrollen
- 1.4.5. Neubeurteilung und Restrisiko

1.5. Geschäftsprozesse und Informationssicherheit
- 1.5.1. Geschäftsprozesse
- 1.5.2. Risikobewertung auf der Grundlage geschäftlicher Parameter
- 1.5.3. Analyse der Auswirkungen auf das Geschäft
- 1.5.4. Geschäftsbetrieb und Informationssicherheit

1.6. Prozess zur kontinuierlichen Verbesserung
- 1.6.1. Der Deming-Zyklus
  - 1.6.1.1. Planung
  - 1.6.1.2. Machen
  - 1.6.1.3. Prüfen
  - 1.6.1.4. Agieren

1.7. Sicherheitsarchitekturen
- 1.7.1. Auswahl und Homogenisierung von Technologien
- 1.7.2. Identitätsmanagement. Authentifizierung
- 1.7.3. Zugriffsverwaltung. Autorisierung
- 1.7.4. Sicherheit der Netzwerkinfrastruktur
- 1.7.5. Verschlüsselungstechnologien und -lösungen
- 1.7.6. Sicherheit der Endgeräte (EDR)

1.8. Der rechtliche Rahmen
- 1.8.1. Regulatorischer Rahmen
- 1.8.2. Zertifizierungen
- 1.8.3. Gesetzgebung

1.9. Der ISO 27001-Standard
- 1.9.1. Implementierung
- 1.9.2. Zertifizierung
- 1.9.3. Audits und Penetrationstests
- 1.9.4. Laufendes Risikomanagement
- 1.9.5. Klassifizierung der Informationen

1.10. Gesetzgebung zum Datenschutz. RGPD (GDPR)
- 1.10.1. Anwendungsbereich der Allgemeinen Datenschutzverordnung (GDPR)
- 1.10.2. Persönliche Daten
- 1.10.3. Rollen bei der Verarbeitung von personenbezogenen Daten
- 1.10.4. ARCO-Rechte
- 1.10.5. Der DSB. Funktionen

Modul 2. IT-Sicherheitsmanagement

2.1. Sicherheitsmanagement
- 2.1.1. Sicherheitsmaßnahmen
- 2.1.2. Rechtliche und regulatorische Aspekte
- 2.1.3. Geschäftliche Freigabe
- 2.1.4. Risikomanagement
- 2.1.5. Identitäts- und Zugriffsmanagement

2.2. Struktur des Sicherheitsbereichs. Das Büro des CISO
- 2.2.1. Organisatorische Struktur. Position des CISO in der Struktur
- 2.2.2. Verteidigungslinien
- 2.2.3. Organigramm des Büros des CISO
- 2.2.4. Haushaltsführung

2.3. Sicherheitsmanagement
- 2.3.1. Sicherheitsausschuss
- 2.3.2. Ausschuss für Risikoüberwachung
- 2.3.3. Prüfungsausschuss
- 2.3.4. Krisenausschuss

2.4. Security Governance. Funktionen
- 2.4.1. Politiken und Standards
- 2.4.2. Masterplan Sicherheit
- 2.4.3. Dashboards
- 2.4.4. Sensibilisierung und Schulung
- 2.4.5. Sicherheit der Lieferkette

2.5. Sicherheitsmaßnahmen
- 2.5.1. Identitäts- und Zugriffsmanagement
- 2.5.2. Konfiguration von Netzwerksicherheitsregeln. Firewalls
- 2.5.3. Verwaltung der IDS/IPS-Plattform
- 2.5.4. Scannen auf Schwachstellen

2.6. Cybersecurity-Rahmenwerk. NIST CSF
- 2.6.1. NIST-Methodik
  - 2.6.1.1. Identifizieren
  - 2.6.1.2. Schützen
  - 2.6.1.3. Erkennen
  - 2.6.1.4. Reagieren
  - 2.6.1.5. Zurückgewinnen

2.7. Sicherheitsoperationszentrum (SOC). Funktionen
- 2.7.1. Schutz. *Red Team, Pentesting, Threat Intelligence*
- 2.7.2. Erkennung. SIEM, *user behavior analytics, fraud prevention*
- 2.7.3. Antwort

2.8. Sicherheitsaudits
- 2.8.1. Penetrationstests
- 2.8.2. Übungen des *Red Team*
- 2.8.3. Quellcode-Prüfungen. Sichere Entwicklung
- 2.8.4. Komponentensicherheit (*software supply chain*)
- 2.8.5. Forensische Analyse

2.9. Reaktion auf Vorfälle
- 2.9.1. Vorbereitung
- 2.9.2. Erkennung, Analyse und Berichterstattung
- 2.9.3. Eindämmung, Ausrottung und Wiederherstellung
- 2.9.4. Aktivitäten nach dem Vorfall
  - 2.9.4.1. Aufbewahrung von Beweisen
  - 2.9.4.2. Forensische Analyse
  - 2.9.4.3. Lücken-Management
- 2.9.5. Offizielle Leitfäden für das Management von Cybervorfällen

2.10. Management von Schwachstellen
- 2.10.1. Scannen auf Schwachstellen
- 2.10.2. Bewertung der Anfälligkeit
- 2.10.3. Verstärkung des Systems
- 2.10.4. Zero-Day-Sicherheitslücken. *Zero-Day*

Modul 3. Business Continuity Plan in Verbindung mit Sicherheit

3.1. Business Continuity Plan
- 3.1.1. Pläne für die Geschäftskontinuität (BCP)
- 3.1.2. Plan für die Geschäftskontinuität (BCP). Schlüsselaspekte
- 3.1.3. Business Continuity Plan (BCP) für die Unternehmensbewertung

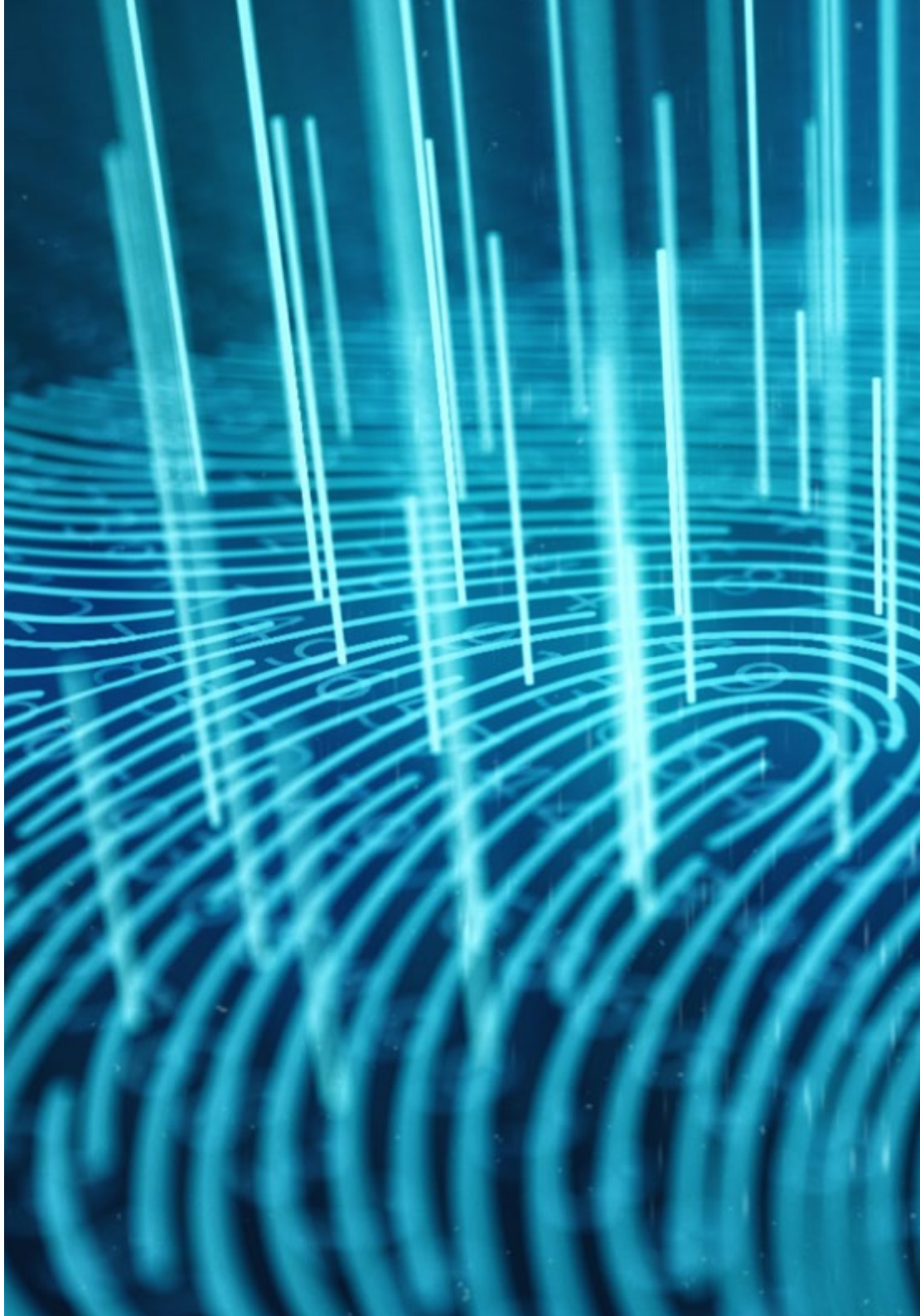
3.2. Metriken in einem Business Continuity Plan (BCP)
- 3.2.1. *Recovery Time Objective* (RTO) und *Recovery Point Objective* (RPO)
- 3.2.2. Maximal verträgliche Zeit (MTD)
- 3.2.3. Mindestanforderungen für die Wiederherstellung (ROL)
- 3.2.4. Wiederherstellungspunkt-Ziel (RPO)

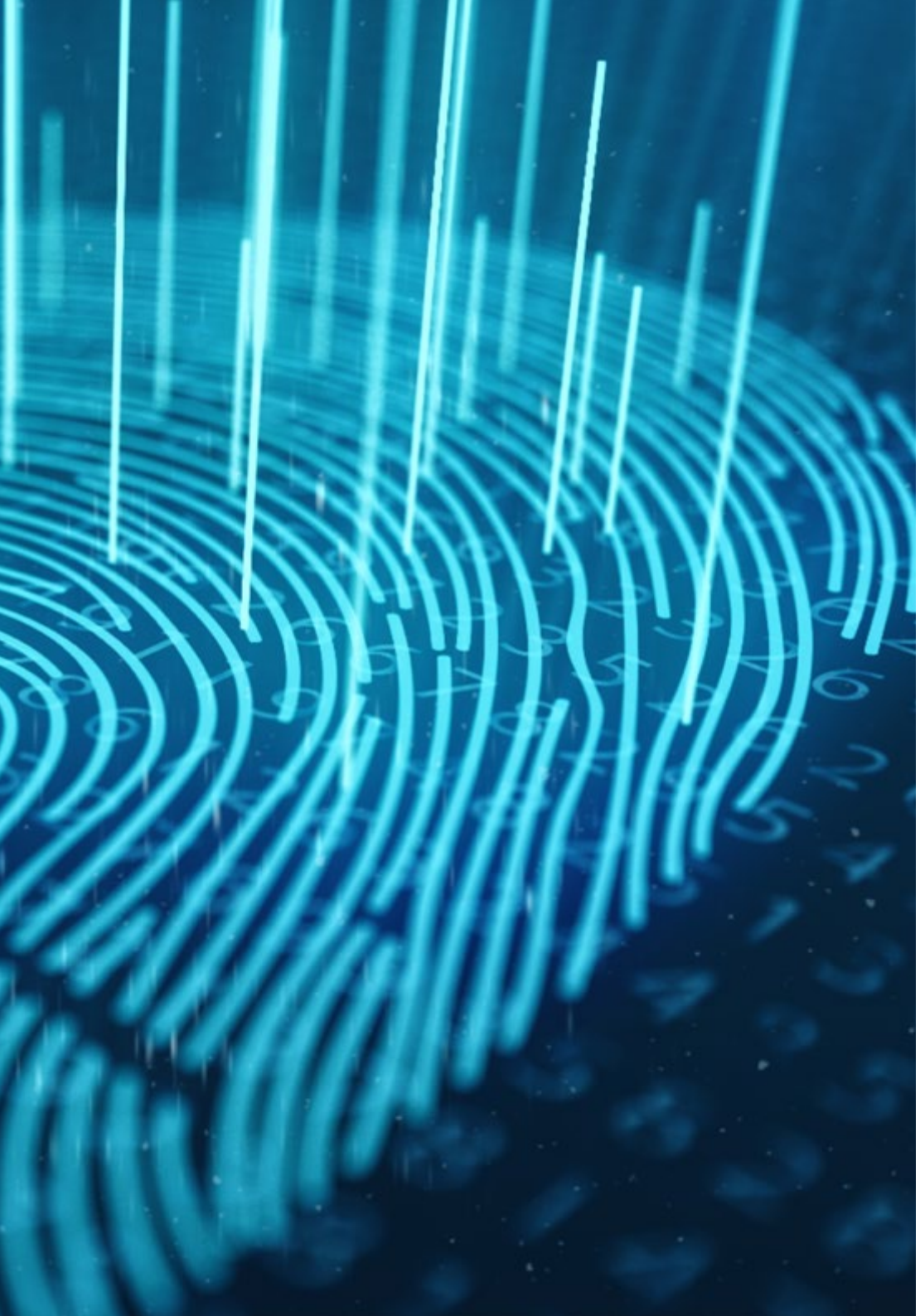
3.3. Kontinuitätsprojekte. Typologie
- 3.3.1. Plan für die Geschäftskontinuität (BCP)
- 3.3.2. IKT-Kontinuitätsplan (ICTCP)
- 3.3.3. Plan zur Wiederherstellung im Katastrophenfall (DRP)

3.4. Risikomanagement im Zusammenhang mit dem BCP
- 3.4.1. Analyse der Auswirkungen auf das Geschäft
- 3.4.2. Vorteile der Implementierung eines BCP
- 3.4.3. Risikobasiertes Denken

3.5. Lebenszyklus eines Business Continuity Plans
- 3.5.1. Phase 1: Analyse der Organisation
- 3.5.2. Phase 2: Festlegung der Kontinuitätsstrategie
- 3.5.3. Phase 3: Reaktion auf Notfälle
- 3.5.4. Phase 4: Tests, Wartung und Überprüfung

3.6. Phase der Organisationsanalyse eines BCP
- 3.6.1. Identifizierung der Prozesse, die in den Geltungsbereich des BCP fallen
- 3.6.2. Identifizierung von kritischen Geschäftsbereichen
- 3.6.3. Identifizierung von Abhängigkeiten zwischen Bereichen und Prozessen
- 3.6.4. Bestimmung der geeigneten MTD
- 3.6.5. Liefergegenstände. Erstellung eines Plans





3.7. Phase der Festlegung der Kontinuitätsstrategie in einer BCP
  3.7.1. Rollen in der Phase der Strategiebestimmung
  3.7.2. Aufgaben in der Phase der Strategiefestlegung
  3.7.3. Liefergegenstände
3.8. Phase der Notfallmaßnahmen eines BCP
  3.8.1. Rollen in der Reaktionsphase
  3.8.2. Aufgaben in dieser Phase
  3.8.3. Liefergegenstände
3.9. Test-, Wartungs- und Überarbeitungsphase eines BCP
  3.9.1. Rollen in der Test-, Wartungs- und Überprüfungsphase
  3.9.2. Aufgaben in der Test-, Wartungs- und Überprüfungsphase
  3.9.3. Liefergegenstände
3.10. ISO-Normen im Zusammenhang mit Business Continuity Plans (BCP)
  3.10.1. ISO 22301:2019
  3.10.2. ISO 22313:2020
  3.10.3. Andere verwandte ISO- und internationale Normen

Dieses Programm ermöglicht es Ihnen, sich mit Themen wie der Identifizierung von Abhängigkeiten zwischen Bereichen und Prozessen zu befassen, ein grundlegender Aspekt für die Schaffung einer korrekten Cybersicherheit"

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 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

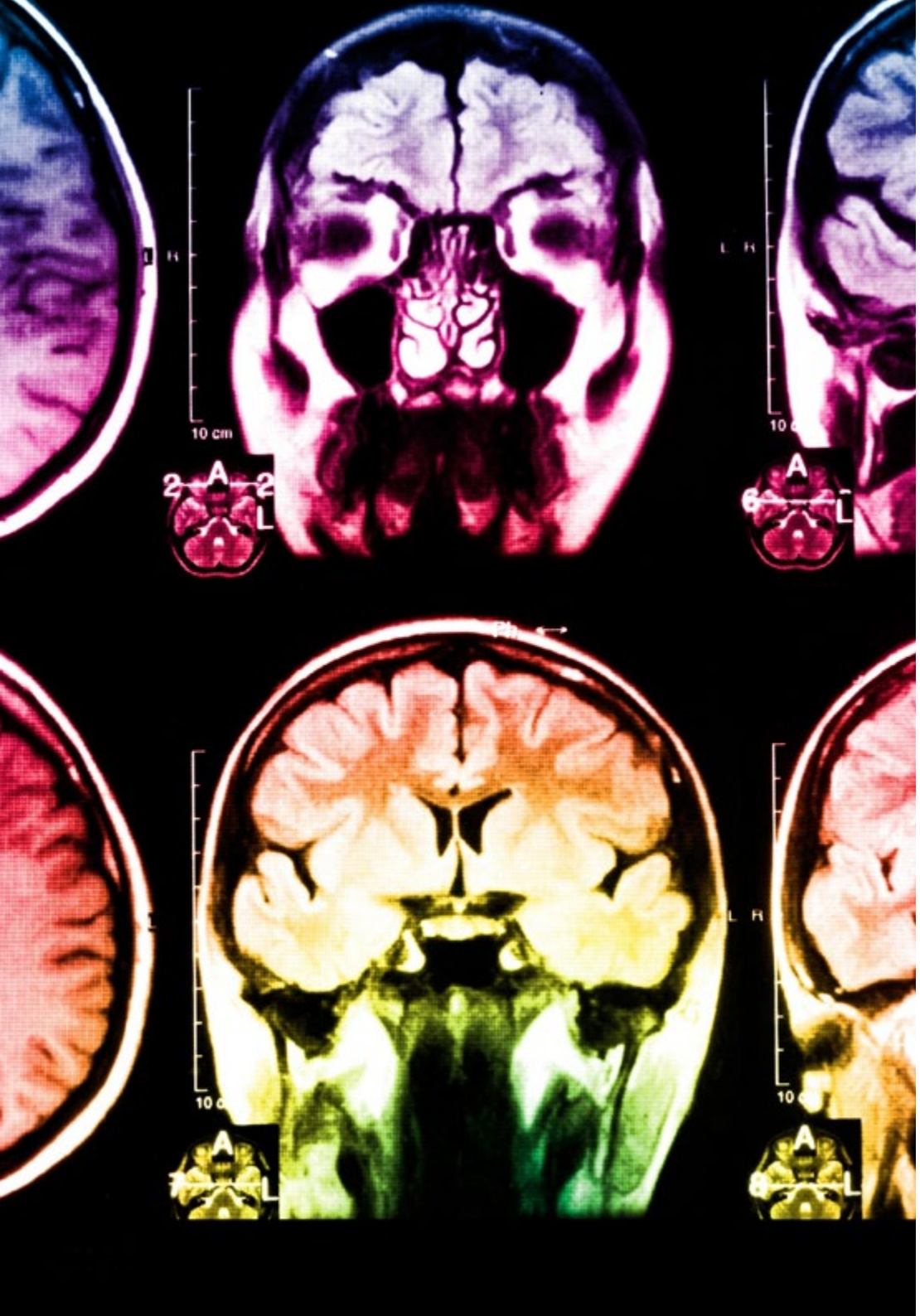
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

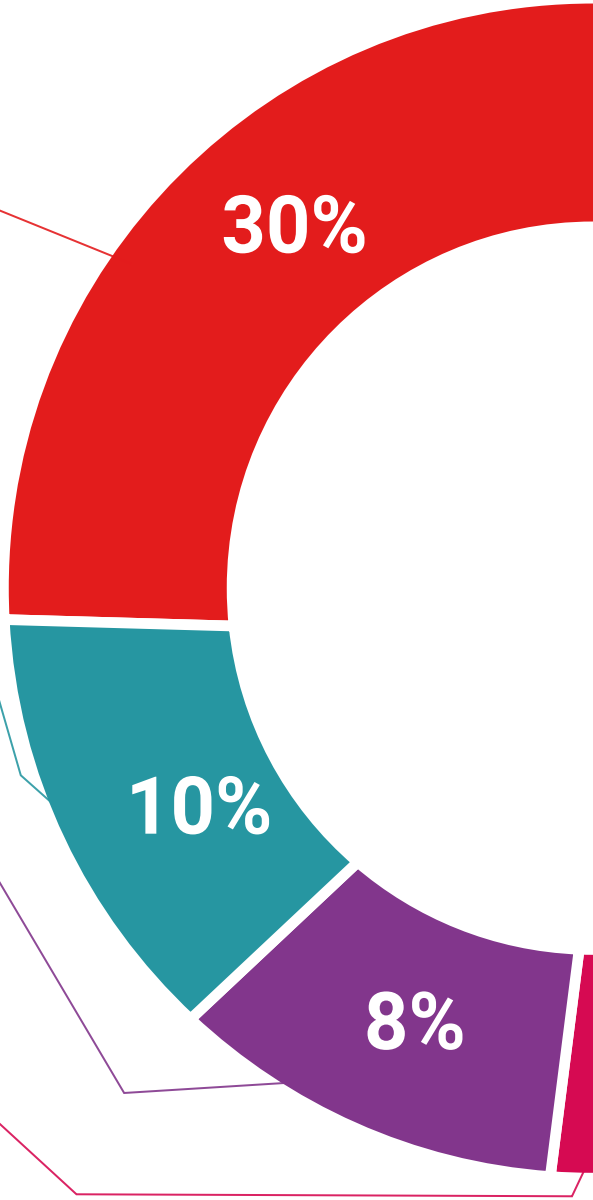
Das sogenannte Learning from an Expert baut Wissen und Gedächtnis auf und schafft Vertrauen für zukünftige schwierige Entscheidungen.

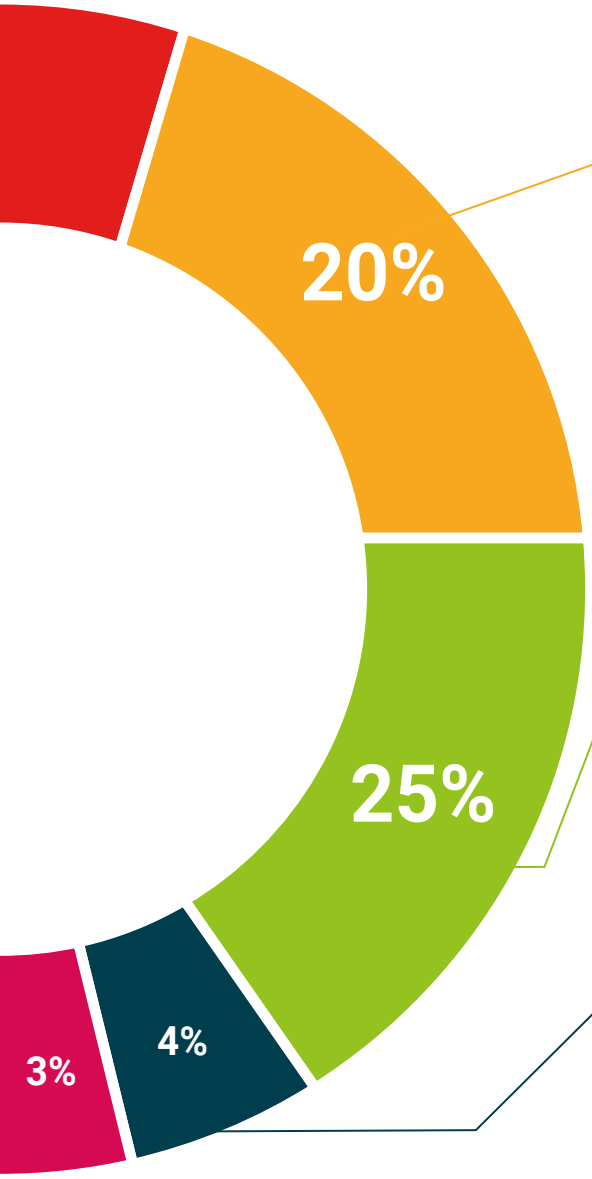
Fertigkeiten und Kompetenzen Praktiken

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.

06

Qualifizierung

Der Universitätsexperte in Verwaltung der Sicherheit der Informationstechnologie 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 Verwaltung der Sicherheit der Informationstechnologie** 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 Verwaltung der Sicherheit der Informationstechnologie**

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

Verwaltung der Sicherheit der Informationstechnologie

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
Verwaltung der Sicherheit der Informationstechnologie

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

Universitätsexperte

Verwaltung der Sicherheit der Informationstechnologie

tech technologische universität