Universitätskurs

Cybersicherheit in Smartphones

tech technologische universität

tech technologische universität

Universitätskurs
Cybersicherheit in Smartphones

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

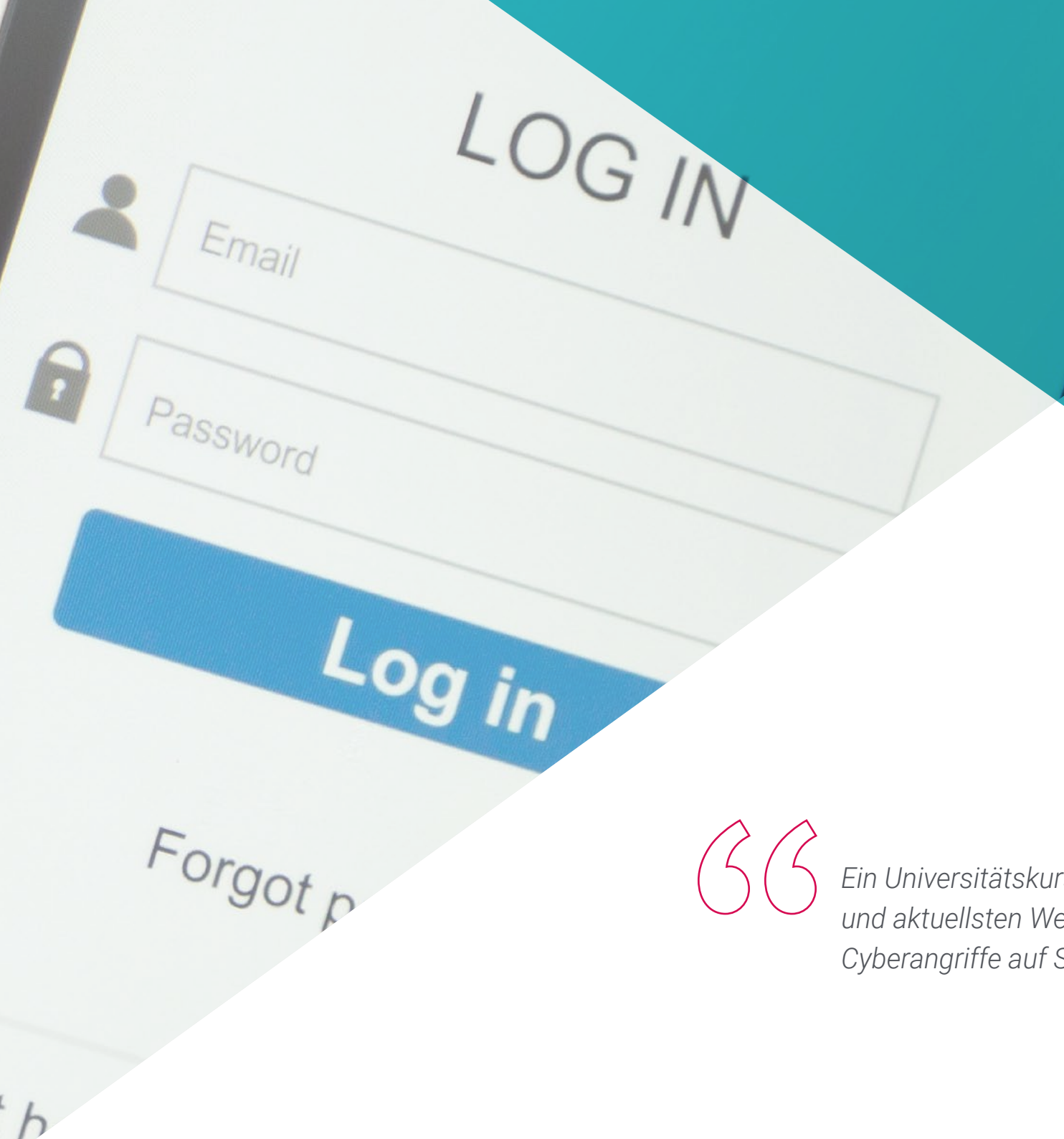
Internetzugang: www.techtitute.com/de/informatik/universitatskurs/cybersicherheit-smartphones

Index

01

Präsentation

Die Nutzung mobiler Geräte bringt für die Nutzer ein Risiko für den Schutz ihrer personenbezogenen Daten mit sich, das in einigen Fällen sehr hoch sein kann. Die zunehmende Intelligenz dieser Geräte, Telefone oder Tablets vergrößert auch die Angriffsfläche und eröffnet neue Schwachstellen, die zu Straftaten wie Identitätsdiebstahl, Raub oder Betrug führen können. Um dem entgegenzuwirken, muss der Cybersicherheitsexperte parallel zur Entstehung von Risiken arbeiten und kontinuierlich Schutzmaßnahmen entwickeln. Dieses Programm ist ein Instrument, das Fachleuten die neuesten Informationen auf diesem Gebiet vermittelt, damit sie effiziente und innovative Lösungen anbieten können.



Ein Universitätskurs, der Ihnen die innovativsten und aktuellsten Werkzeuge im Kampf gegen Cyberangriffe auf Smartphones an die Hand gibt"

Wir leben in einer Zeit, in der die Nutzung mobiler Geräte immer weiter zunimmt. Das Telefon ist längst nicht mehr nur ein Telefon, sondern ein kleiner Computer, der jederzeit im Internet surfen, Anwendungen aller Art ausführen, unsere Position auf einer Karte lokalisieren, Routen planen, Daten intern und extern speichern und vieles mehr kann. Wenn wir von diesen Geräten sprechen, meinen wir nicht nur Handys, sondern auch Tablets. Beides sind Geräte, die entwickelt wurden, um uns das Leben zu erleichtern. Dank ihnen können wir uns problemlos fortbewegen und haben jederzeit Zugang zum Internet und zu den immer beliebter werdenden Cloud-Diensten.

Wir dürfen nicht vergessen, dass dank all dieser „Intelligenz" die Angriffsfläche auf diese Geräte exponentiell von 0 auf 100 gestiegen ist und dass ihre massive Nutzung sie zu einem leichten Ziel gemacht hat. Mobile Geräte sind heute das Hauptziel von Angreifern, die in die Privatsphäre eindringen, Identitäten missbrauchen, Daten stehlen, sich ohne Zustimmung des Benutzers Zugang verschaffen und die Besitzer dieser Geräte für kriminelle Zwecke missbrauchen wollen.

Es ist daher unerlässlich und absolut notwendig, dass wir alle uns zur Verfügung stehenden Maßnahmen ergreifen, um unsere Privatsphäre zu schützen. Hundertprozentige Sicherheit gibt es nicht, aber wenn wir uns der Arten von Angriffen bewusst sind, denen wir ausgesetzt sind, und wenn wir über die notwendigen Informationen verfügen, um damit umzugehen, haben wir einen wichtigen Schritt getan und eine weitere Sicherheitsschicht für unsere Daten hinzugefügt.

Dieser **Universitätskurs in Cybersicherheit in Smartphones** enthält das vollständigste und aktuellste Programm auf dem Markt. Die hervorstechendsten Merkmale sind:

- Die Entwicklung praktischer Fälle, die von Experten in Cybersicherheit vorgestellt 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
- Theoretische Vorträge, Fragen an den Experten, Diskussionsforen zu kontroversen Themen und individuelle Reflexionsarbeit
- Die Verfügbarkeit des Zugangs zu Inhalten von jedem festen oder tragbaren Gerät mit Internetanschluss

Erwerben Sie das notwendige Wissen, um in nur wenigen Wochen ein effizientes mehrschichtiges Schutzsystem zu entwickeln"

Die Informationen, die der Profi braucht, um Schutzsysteme zu entwickeln, die die Sicherheit der Smartphone-Nutzung gewährleisten, in einem hochqualifizierten Programm”

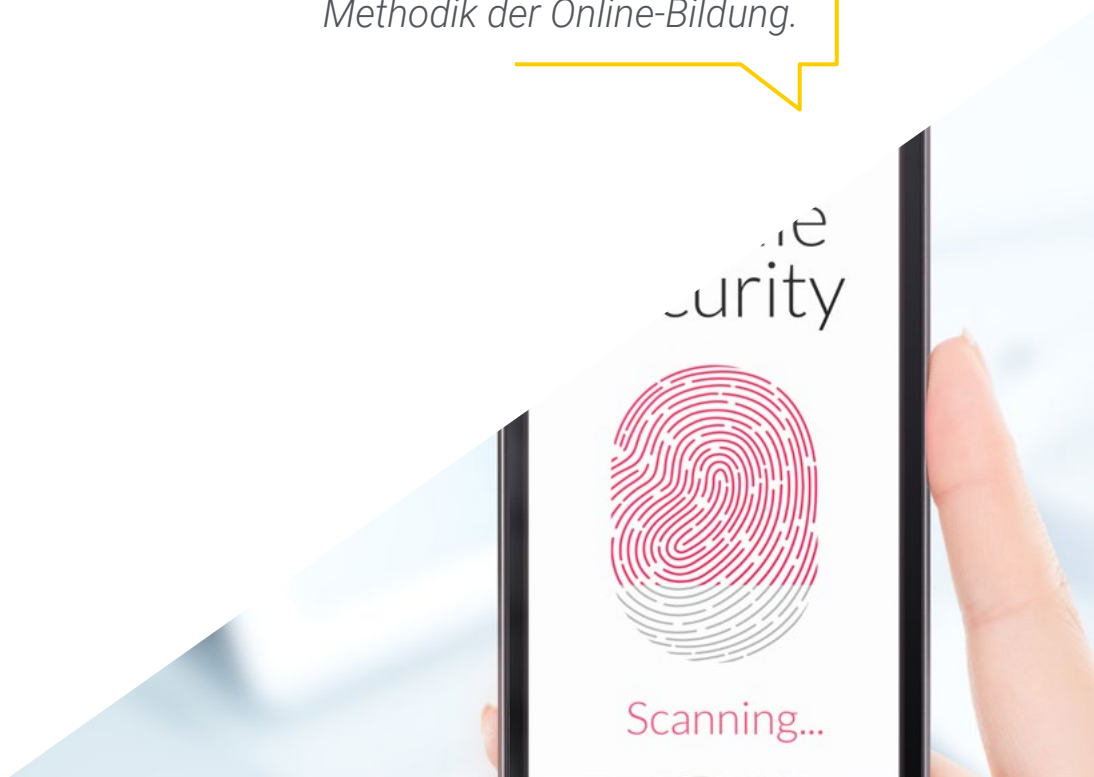
Studieren Sie in einem praxisorientierten Universitätskurs, der Ihre Fähigkeiten auf das Niveau eines Spezialisten hebt.

Ein hochqualifizierter Prozess, der so gestaltet ist, dass er überschaubar und flexibel ist, mit der interessantesten Methodik der Online-Bildung.

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 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.

Die Gestaltung 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. Zu diesem Zweck wird sie von einem innovativen interaktiven Videosystem unterstützt, das von renommierten Experten entwickelt wurde.



02

Ziele

Dieser Universitätskurs in Cybersicherheit in Smartphones vermittelt den Studenten die Fähigkeit, schnell und einfach in diesem Bereich zu arbeiten. Mit realistischen und hochinteressanten Zielen wurde dieser Studienprozess so gestaltet, dass die Studenten nach und nach die theoretischen und praktischen Kenntnisse erwerben, die sie benötigen, um mit Qualität zu intervenieren und übergreifende Kompetenzen zu entwickeln, die es ihnen ermöglichen, sich komplexen Situationen zu stellen, indem sie angepasste und präzise Antworten erarbeiten.

Setzen Sie Ihre Fähigkeiten in einem Bereich voller Beschäftigungsmöglichkeiten durch einen Prozess von außergewöhnlicher Lehrqualität ein"

Allgemeine Ziele

- Analysieren der wichtigsten aktuellen mobilen Plattformen, ihrer Funktionen und Nutzung
- Untersuchen der vorhandenen Schwachstellen und Bedrohungen sowie der wichtigsten Angriffsvektoren
- Bewerten der Risiken, die mit Schwachstellen innerhalb und außerhalb des Unternehmens verbunden sind
- Ermitteln von Tools und *Best Practice*-Richtlinien für die Sicherung mobiler Geräte

Mit Blick auf den Studenten implementiert dieser Universitätskurs die interessantesten Lernunterstützungssysteme, die heute verfügbar sind"

Spezifische Ziele

- Untersuchen der verschiedenen Angriffsvektoren, um zu vermeiden, ein leichtes Ziel zu werden
- Bestimmen der wichtigsten Angriffe und Arten von Malware, denen Benutzer mobiler Geräte ausgesetzt sind
- Analysieren der aktuellsten Geräte, um eine sicherere Konfiguration zu erstellen
- Festlegen der wichtigsten Schritte zur Durchführung eines Penetrationstests auf iOS- und Android-Plattformen
- Entwickeln von Fachwissen über die verschiedenen Schutz- und Sicherheitstools
- Etablieren von *Best Practices* bei der Programmierung für mobile Geräte

03

Kursleitung

Die Dozenten, die dieses Programm unterrichten, wurden aufgrund ihrer außergewöhnlichen Kompetenz in diesem Bereich ausgewählt. Sie verbinden technische und praktische Erfahrung mit Unterrichtserfahrung und bieten den Studenten erstklassige Unterstützung bei der Erreichung ihrer Ziele. Durch sie bietet das Programm die direkteste und unmittelbarste Sicht auf die realen Merkmale der Intervention in diesem Bereich und erreicht eine kontextuelle Vision von maximalem Interesse.

Fachkundige Dozenten für Cybersicherheit in Smartphones werden Sie durch jede Phase des Studiums begleiten und Ihnen einen möglichst realistischen Einblick in diese Arbeit geben"

Internationale Gastdirektorin

Dr. Frederic Lemieux ist international als innovativer Experte und inspirierende Führungspersönlichkeit in den Bereichen der **Intelligenz, der nationalen Sicherheit, der inneren Sicherheit, der Cybersicherheit** und der **disruptiven Technologien** anerkannt. Sein ständiges Engagement und seine wichtigen Beiträge zu Forschung und Bildung machen ihn zu einer zentralen Figur bei der Förderung der Sicherheit und des Verständnisses der heutigen neuen Technologien. Während seiner beruflichen Laufbahn hat er an mehreren renommierten Institutionen wie der **Universität von Montreal,** der **George Washington Universität** und der Universität von Georgetown zukunftsweisende akademische Programme konzipiert und geleitet.

Im Laufe seiner umfangreichen Erfahrung hat er mehrere Bücher von großer Bedeutung veröffentlicht, die sich alle mit **kriminalistischer Aufklärung, Polizeiarbeit, Cyber-Bedrohungen und internationaler Sicherheit** befassen. Er hat auch einen wichtigen Beitrag zum Bereich der Cybersicherheit geleistet, indem er zahlreiche Artikel in akademischen Zeitschriften veröffentlicht hat, die sich mit der Verbrechensbekämpfung bei großen Katastrophen, der Terrorismusbekämpfung, den Nachrichtendiensten und der polizeilichen Zusammenarbeit beschäftigen. Darüber hinaus war er Podiumsteilnehmer und Hauptredner bei verschiedenen nationalen und internationalen Konferenzen und hat sich als führender Wissenschaftler und Praktiker etabliert.

Dr. Lemieux hatte redaktionelle und bewertende Funktionen in verschiedenen akademischen, privaten und staatlichen Organisationen inne, was seinen Einfluss und sein Engagement für Spitzenleistungen in seinem Fachgebiet widerspiegelt. Im Rahmen seiner angesehenen akademischen Laufbahn war er Professor für Praxis und Fakultätsleiter der MPS-Programme für **Angewandte Intelligenz, Risikomanagement für Cybersicherheit, Technologiemanagement und Informationstechnologiemanagement** an der **Universität von Georgetown.**

Dr. Lemieux, Frederic

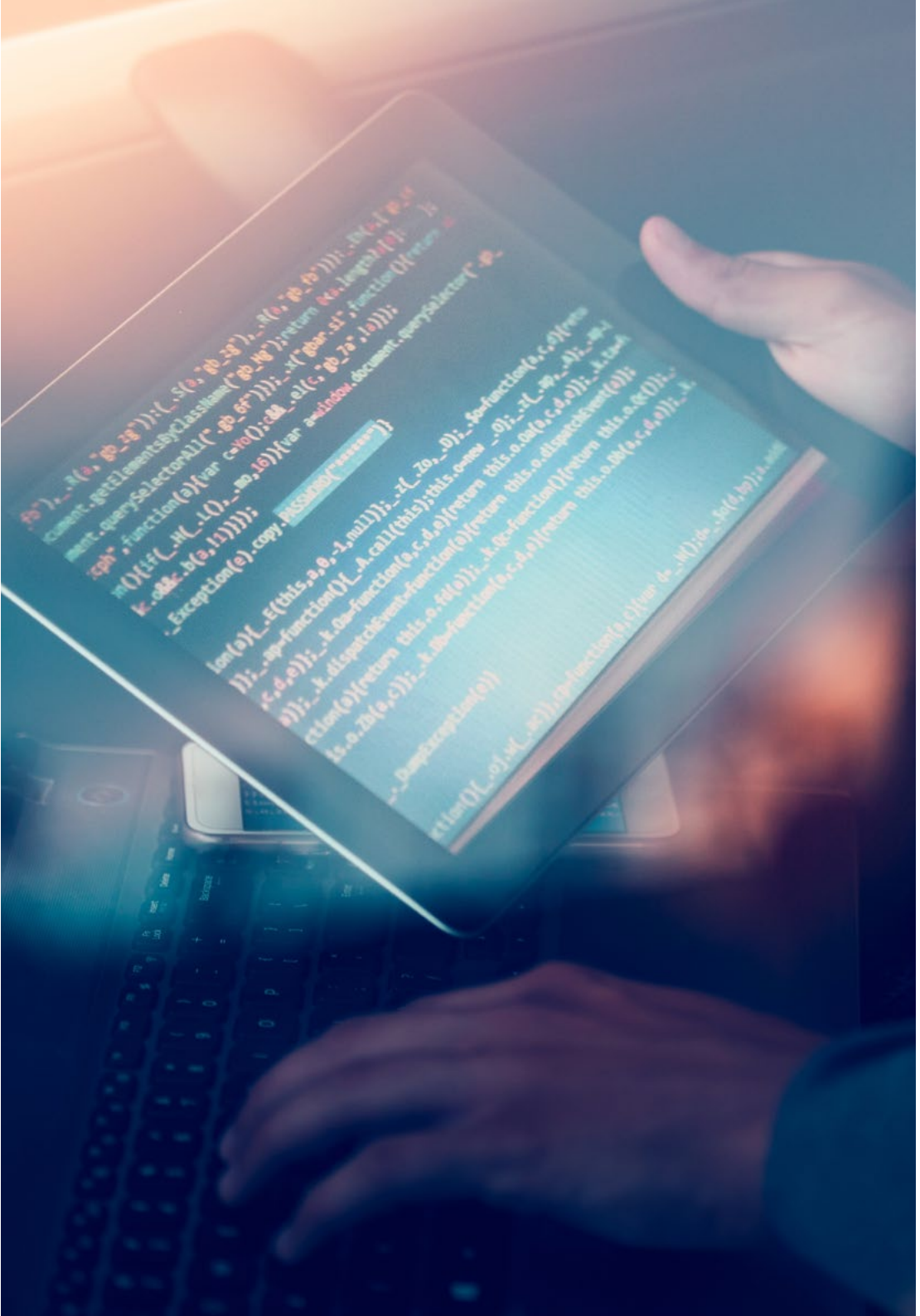
- Forscher im Bereich Intelligenz, Cybersicherheit und Disruptive Technologien an der Universität von Georgetown
- Direktor des Masterstudiengangs in Information Technology Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Technology Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Cybersecurity Risk Management an der Universität von Georgetown
- Direktor des Masterstudiengangs in Applied Intelligence an der Universität von Georgetown
- Professor für Praktika an der Universität von Georgetown
- Promotion in Kriminologie an der School of Criminology der Universität von Montreal
- Hochschulabschluss in Soziologie, Nebenfach Psychologie, Universität von Laval
- Mitglied von:
- New Program Roundtable Committee, Universität von Georgetown

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

Leitung

Fr. Fernández Sapena, Sonia

- Ausbilderin für Computersicherheit und *Ethical Hacking*, Nationales Referenzzentrum für IT und Telekommunikation in Getafe, Madrid
- Zertifizierte *E-Council*-Ausbilderin, Madrid
- 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*), Universität der Balearischen Inseln
- Informatik-Ingenieurin, Universität von Alcalá de Henares, Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes, Cas-Training, Madrid
- *Microsoft Azure Security Techonologies, E-Council*, Madrid



Professoren

Fr. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applikationsentwicklung bei B60, UK
- Analytikerin-Programmiererin für die Verwaltung, Koordination und Dokumentation einer virtualisierten Sicherheitsalarmumgebung bei einem Kunden
- Analytikerin-Programmiererin von Java-Anwendungen in Geldautomaten für Kunden
- *Software Development*-Expertin für die Validierung von Unterschriften und die Anwendung zur Dokumentenverwaltung beim Kunden
- Systemtechnikerin für die Migration von Geräten und für die Verwaltung, Wartung und Schulung von PDA-Mobilgeräten beim Kunden vor Ort
- Technisches Engineering von Computersystemen, Offene Universität von Katalonien
- Masterstudiengang in Computersicherheit und *Ethical Hacking,* Offizieller *EC-Council* und CompTIA von der Fachhochschule für neue Technologien CICE

Hr. Catalá Barba, José Francisco

- Mittleres Management im MINISDEF. Verschiedene Aufgaben und Verantwortlichkeiten innerhalb der GOE III, wie z.B. Verwaltung und Störungsmanagement des internen Netzwerks, Entwicklung von maßgeschneiderten Programmen für verschiedene Bereiche, Schulungen für Netzwerkbenutzer und Gruppenpersonal im Allgemeinen
- Elektroniker in der Ford-Fabrik in Almusafes, Valencia, Programmierung von Robotern, PLCs, Reparatur und Wartung
- Elektronik-Techniker
- Entwickler von Applikationen für mobile Geräte

04

Struktur und Inhalt

Im Laufe der verschiedenen Themen dieses Kurses wird der Student in der Lage sein, sich alle Kenntnisse anzueignen, die für die Entwicklung von Sicherheitssystemen in Smartphones erforderlich sind. Der Kurs wurde mit Blick auf den effizienten Erwerb von ergänzenden Lerninhalten strukturiert, die die Vertiefung und die Konsolidierung des Gelernten ermöglichen und die Studenten in die Lage versetzen, so schnell wie möglich zu intervenieren. Ein hochintensiver und qualitativ hochwertiger Kurs, der die Besten des Sektors fortbilden soll.

Alle Aspekte der Intervention im Bereich der Cybersicherheit in Smartphones werden auf strukturierte Weise in einem auf Effizienz ausgerichteten Studienansatz entwickelt"

Modul 1. Smartphone-Sicherheit

1.1. Die Welt der mobilen Geräte
- 1.1.1. Arten von mobilen Plattformen
- 1.1.2. IOS-Geräte
- 1.1.3. Android-Geräte

1.2. Verwaltung der mobilen Sicherheit
- 1.2.1. OWASP Projekt für mobile Sicherheit
  - 1.2.1.1. Top 10 Schwachstellen
- 1.2.2. Kommunikation, Netzwerke und Verbindungsarten

1.3. Das mobile Gerät in der Unternehmensumgebung
- 1.3.1. Risiken
- 1.3.2. Sicherheitsrichtlinien
- 1.3.3. Geräteüberwachung
- 1.3.4. Verwaltung mobiler Geräte (MDM)

1.4. Datenschutz und Datensicherheit
- 1.4.1. Zustände der Information
- 1.4.2. Datenschutz und Vertraulichkeit
  - 1.4.2.1. Zugriffsrechte
  - 1.4.2.2. Verschlüsselung
- 1.4.3. Sichere Speicherung von Daten
  - 1.4.3.1. Sicherer Speicher auf iOS
  - 1.4.3.2. Sicherer Speicher auf Android
- 1.4.4. Bewährte Praktiken bei der Applikationsentwicklung

1.5. Schwachstellen und Angriffsvektoren
- 1.5.1. Schwachstellen
- 1.5.2. Angriffsvektoren
  - 1.5.2.1. Malware
  - 1.5.2.2. Exfiltration von Daten
  - 1.5.2.3. Datenmanipulation

1.6. Wichtigste Bedrohungen
- 1.6.1. Ungezwungener Benutzer
- 1.6.2. Malware
  - 1.6.2.1. Arten von Malware
- 1.6.3. *Social Engineering*
- 1.6.4. Datenleck
- 1.6.5. Datendiebstahl
- 1.6.6. Ungesicherte WiFi-Netzwerke
- 1.6.7. Veraltete Software
- 1.6.8. Bösartige Anwendungen
- 1.6.9. Unsichere Passwörter
- 1.6.10. Schwache oder nicht vorhandene Sicherheitseinstellungen
- 1.6.11. Physischer Zugang
- 1.6.12. Verlust oder Diebstahl des Geräts
- 1.6.13. Impersonation (Integrität)
- 1.6.14. Schwache oder defekte Kryptographie
- 1.6.15. *Denial of Service* (DoS)

1.7. Große Angriffe
- 1.7.1. *Phishing*-Angriffe
- 1.7.2. Angriffe im Zusammenhang mit Kommunikationsmodi
- 1.7.3. *Smishing*-Angriffe
- 1.7.4. *Criptojacking*-Angriffe
- 1.7.5. *Man in The Middle*

1.8. *Hacking*
- 1.8.1. *Rooting* und *Jailbreaking*
- 1.8.2. Anatomie eines mobilen Angriffs
  - 1.8.2.1. Ausbreitung der Bedrohung
  - 1.8.2.2. Installation von Malware auf dem Gerät
  - 1.8.2.3. Persistenz
  - 1.8.2.4. Ausführen der *Payload* und Extrahieren der Informationen
- 1.8.3. Hacking auf iOS-Geräten: Mechanismen und Tools
- 1.8.4. Hacking auf Android-Geräten: Mechanismen und Tools

1.9. Penetrationstests
- 1.9.1. iOS *Pentesting*
- 1.9.2. Android *Pentesting*
- 1.9.3. Tools

1.10. Schutz und Sicherheit
- 1.10.1. Sicherheitseinstellungen
  - 1.10.1.1. Auf iOS-Geräten
  - 1.10.1.2. Auf Android-Geräten
- 1.10.2. Sicherheitsmaßnahmen
- 1.10.3. Schutz-Tools

Alle Analysen, Entwicklungen und Schutzinstrumente für Smartphones in einem hochinteressanten und aktuellen Studienplan”

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

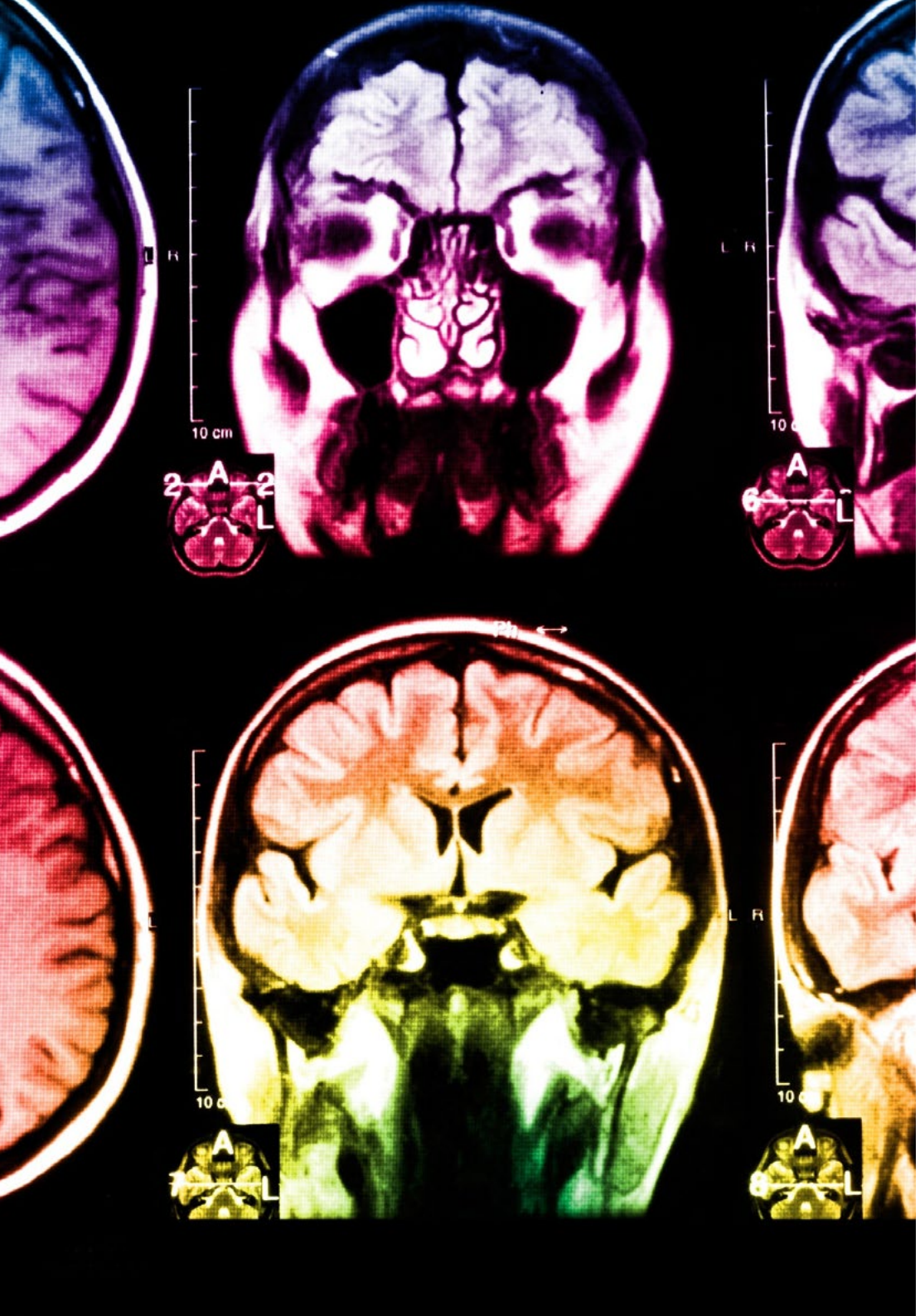
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

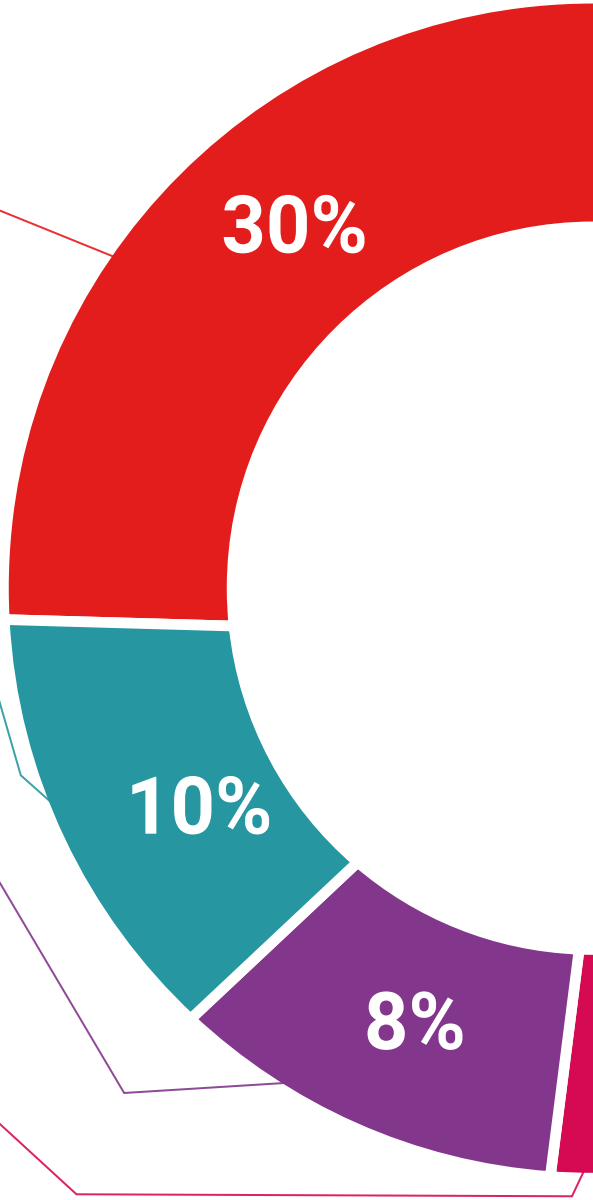
Das sogenannte Learning from an Expert baut Wissen und Gedächtnis auf und schafft Vertrauen für zukünftige schwierige Entscheidungen.

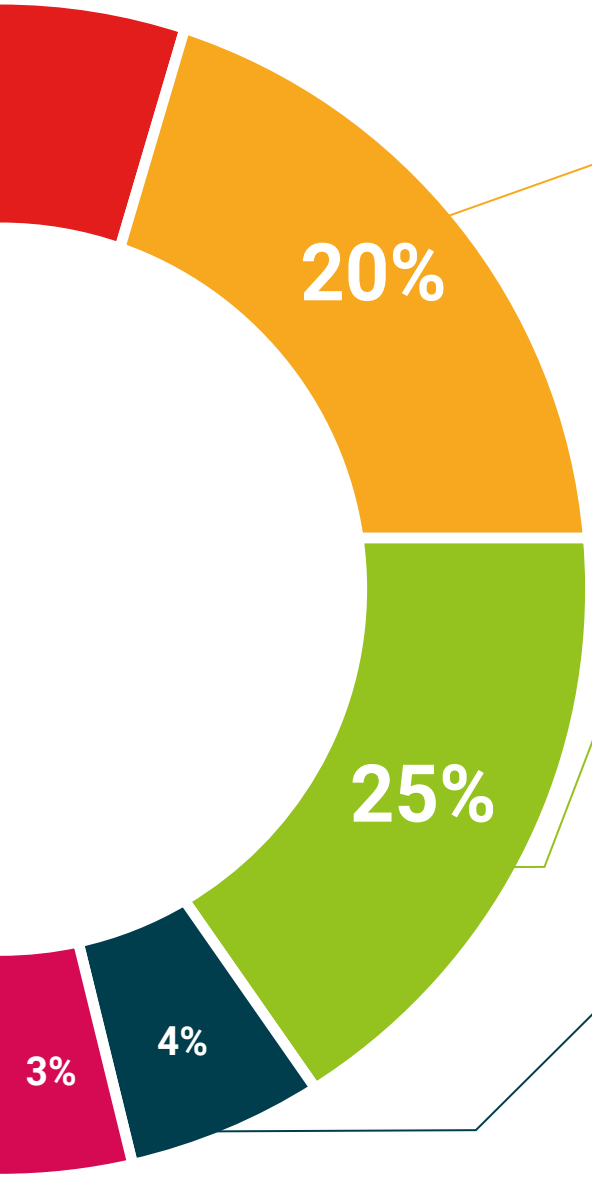
Fertigkeiten und Kompetenzen Praktiken

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 Universitätskurs in Cybersicherheit in Smartphones 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 **Universitätskurs in Cybersicherheit in Smartphones** 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: **Universitätskurs in Cybersicherheit in Smartphones**

Anzahl der offiziellen Arbeitsstunden: **150 Std.**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

UNIVERSITÄTSKURS

in

Cybersicherheit im Smartphones

Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 150 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

Universitätskurs
Cybersicherheit in Smartphones

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

Universitätskurs
Cybersicherheit in Smartphones

tech technologische universität