Universitätsexperte

Management von IT-Sicherheitsvorfällen

tech technologische universität

tech technologische universität

Universitätsexperte
Management von IT-Sicherheitsvorfällen

- 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-management-it-sicherheitsvorfallen

Index

01

Präsentation

Unternehmen sind sich bewusst, dass sie einer Vielzahl von Cyber-Angriffen ausgesetzt sind. Daher ist die Umsetzung von Sicherheitsrichtlinien heutzutage unerlässlich, um den Schutz sensibler Daten zu gewährleisten. In diesem Szenario müssen IT-Fachkräfte auf vorhersehbare Vorfälle im Unternehmen reagieren und präventive Maßnahmen ergreifen, um neue Angriffe zu verhindern. Dieser 100%ige Online-Studiengang vermittelt den Studenten alle notwendigen Werkzeuge für den Umgang mit IT-Sicherheit. Ein Team von Dozenten mit Fachkenntnissen in diesem Bereich und eine umfangreiche Bibliothek mit Multimedia-Ressourcen fördern das Studium und die Spezialisierung von Fachkräften in einem Bereich, der hohe Qualifikationen erfordert.

Sie werden darauf vorbereitet sein, mit jedem IT-Sicherheitsvorfall in einem Unternehmen umzugehen. Schreiben Sie sich für diesen Universitätsexperten ein"

Angesichts der großen Menge an sensiblen Daten, über die Unternehmen und Institutionen verfügen, wird IT-Sicherheit immer notwendiger. In vielen Fällen kommt es jedoch zu Verstößen und Zwischenfällen, die auf unsachgemäßes Verhalten des Personals oder mangelnde Kenntnisse in diesem technologischen Bereich zurückzuführen sind. Diese können manchmal zu Verlusten führen oder das Image eines Unternehmens ernsthaft schädigen.

Dieser Universitätsexperte bietet spezialisierte Kurse an, die die Analyse und das Management von Vorfällen ermöglichen, von ihrer Erkennung durch IDS/IPS-Systeme und ihrer anschließenden Behandlung in SIEM bis hin zum Prozess der Benachrichtigung und Eskalation an die zuständige Abteilung. Für diesen gesamten Prozess sind IT-Experten erforderlich, die sich mit nützlichen Werkzeugen zur Überwachung von Informationssystemen auskennen.

Dieses Programm, das einen sehr praktischen Ansatz verfolgt, versetzt die Studenten in eine Situation, in der sie mit einem *Ransomware*-Angriff konfrontiert werden, um ihre Kenntnisse in der Anwendung von Maßnahmen und Wiederherstellungsprotokollen zu perfektionieren.

Der 100%ige Online-Modus des Programms ermöglicht es den IT-Fachkräften, vom ersten Tag an von jedem internetfähigen Gerät aus auf hochwertige Multimedia-Inhalte zuzugreifen. TECH erleichtert somit das Lernen für Studenten, die ihr Berufs- und Privatleben mit einer Weiterbildung verbinden möchten, die für alle zugänglich ist.

Dieser **Universitätsexperte in Management von IT-Sicherheitsvorfällen** 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

Beherrschen Sie Netzwerküberwachungssoftware wie Nagios, Zabbix oder Pandora bis zur Perfektion und behalten Sie mit diesem Universitätsexperten Ihre Geräte im Auge"

Machen Sie einen Sprung nach vorn in Ihrer beruflichen Laufbahn. Spezialisieren Sie sich und geben Sie Antworten auf Computersicherheitsprobleme in Unternehmen und Institutionen. Schreiben Sie sich jetzt ein"

Erfahren Sie mehr über die Norm ISO 27035 und vermeiden Sie Sicherheitslücken, die Unternehmen gefährden könnten. Schreiben Sie sich für diese Qualifikation ein.

Beherrschen Sie die SNM-Protokolle und -Tools perfekt mit diesem Universitätsexperten.

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

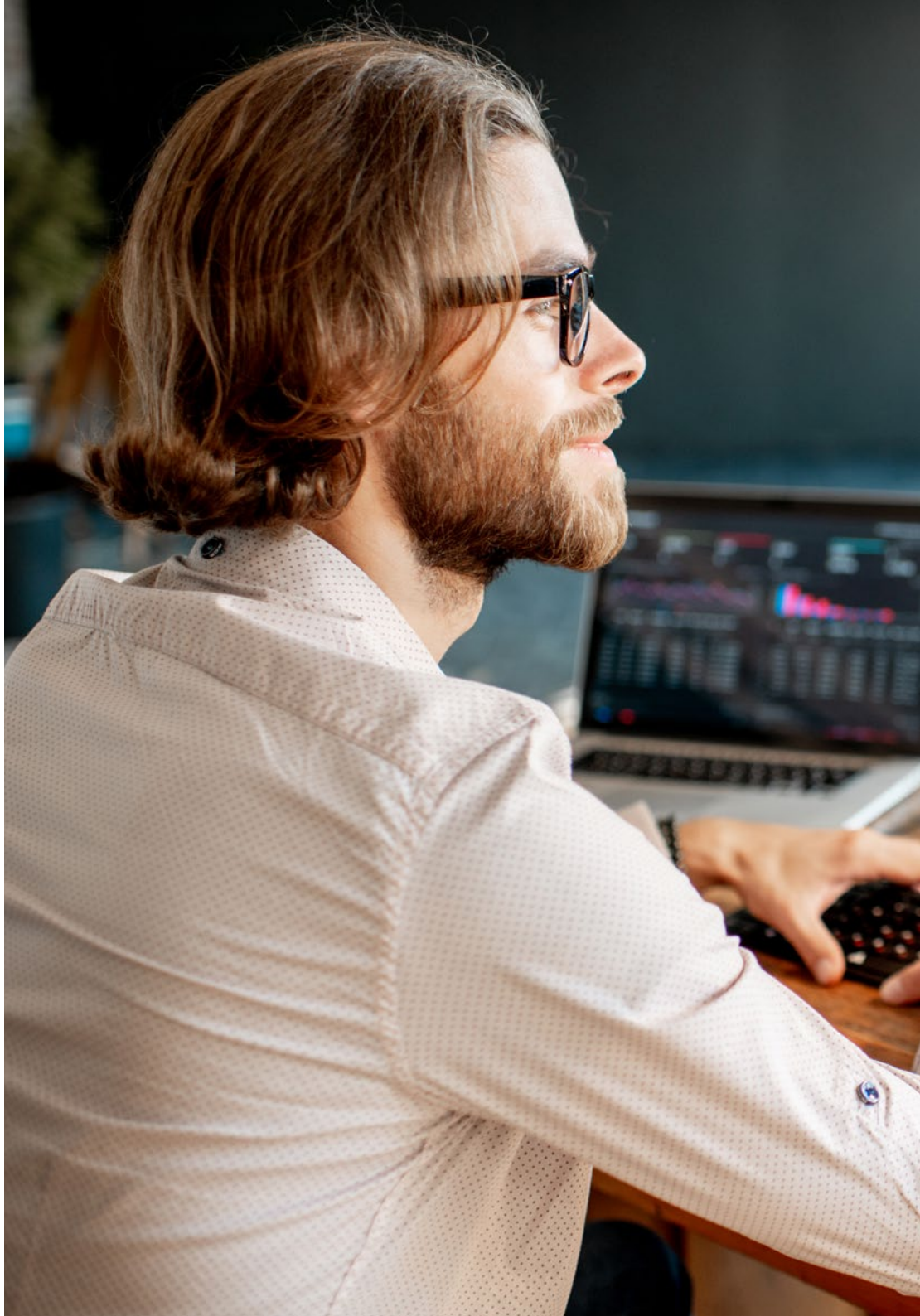
Während dieses sechsmonatigen Universitätsexperten vertiefen IT-Fachkräfte ihre Kenntnisse im Bereich der IT-Sicherheit, um wirksame Maßnahmen zur Gewährleistung guter Sicherheitspraktiken in Unternehmen zu entwickeln. Sie werden in der Lage sein, Systeme korrekt zu auditieren und Netzwerke mit den neuesten technologischen Mitteln zu überwachen. Am Ende des Kurses werden Sie in der Lage sein, einen perfekten Sicherheitsplan für den Katastrophenfall zu implementieren. Videozusammenfassungen zu jedem Thema und weiterführende Literatur helfen Ihnen, diese Ziele zu erreichen.

Entwickeln Sie den besten IT-Sicherheitsplan und werden Sie der Experte, den Unternehmen brauchen, um sich zu schützen"

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

Mit der didaktischen Methode von TECH erreichen Sie Ihre ehrgeizigsten Ziele schneller als Sie denken"



Spezifische Ziele

Modul 1. Richtlinien für das Management von Sicherheitsvorfällen

- Entwickeln von Fachwissen über den Umgang mit Vorfällen, die durch Computersicherheitsereignisse verursacht werden
- Festlegen der Arbeitsweise eines Teams zur Bearbeitung von Sicherheitsvorfällen
- Analysieren der verschiedenen Phasen des Managements von IT-Sicherheitsvorfällen
- Untersuchen von standardisierten Protokollen für den Umgang mit Sicherheitszwischenfällen

Modul 2. Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme

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

Modul 3. Praktische Sicherheitspolitiken für die Notfallwiederherstellung

- Generieren von Fachwissen über das Konzept der Kontinuität der Informationssicherheit
- Entwickeln eines *Business-Continuity*-Plans
- Analysieren eines IKT-Kontinuitätsplans
- Entwerfen eines Wiederherstellungsplans für den Katastrophenfall

03

Kursleitung

TECH bietet den Studenten eine qualitativ hochwertige Weiterbildung, die an die neuesten Entwicklungen des Sektors, in diesem Fall der Cybersicherheit, angepasst ist. In diesem Universitätsexperten erhalten IT-Fachleute Zugang zu einem breiten Wissensspektrum, das von einem Dozententeam vermittelt wird, das über umfangreiche Erfahrungen im Bereich der Cybersicherheit verfügt und in diesem Sektor tätig ist. Die Studenten profitieren somit von einer Fortbildung, die der Realität sehr nahe kommt, mit der die Fachleute tagtäglich angesichts von Cyber-Angriffen konfrontiert sind.

Sicherheitsexperten aus dem öffentlichen und privaten Sektor geben Ihnen die Werkzeuge an die Hand, mit denen Sie Ihre berufliche Karriere in diesem Bereich vorantreiben können"

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

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

Hr. Ortega López, Florencio

- Sicherheitsberater (Identitätsmanagement) bei der SIA-Gruppe
- IKT- und Sicherheitsberater als Freiberufler
- Ausbilder in der IT-Branche
- Hochschulabschluss in technischem Wirtschaftsingenieurwesen an der Universität von Alcalá de Henares
- Masterstudiengang für Lehrkräfte von der UNIR
- MBA in Unternehmensführung und Verwaltung vom IDE-CESEM
- Masterstudiengang in Management der Informationstechnologie vom IDE-CESEM
- Certified Information Security Management (CISM) von ISACA

04

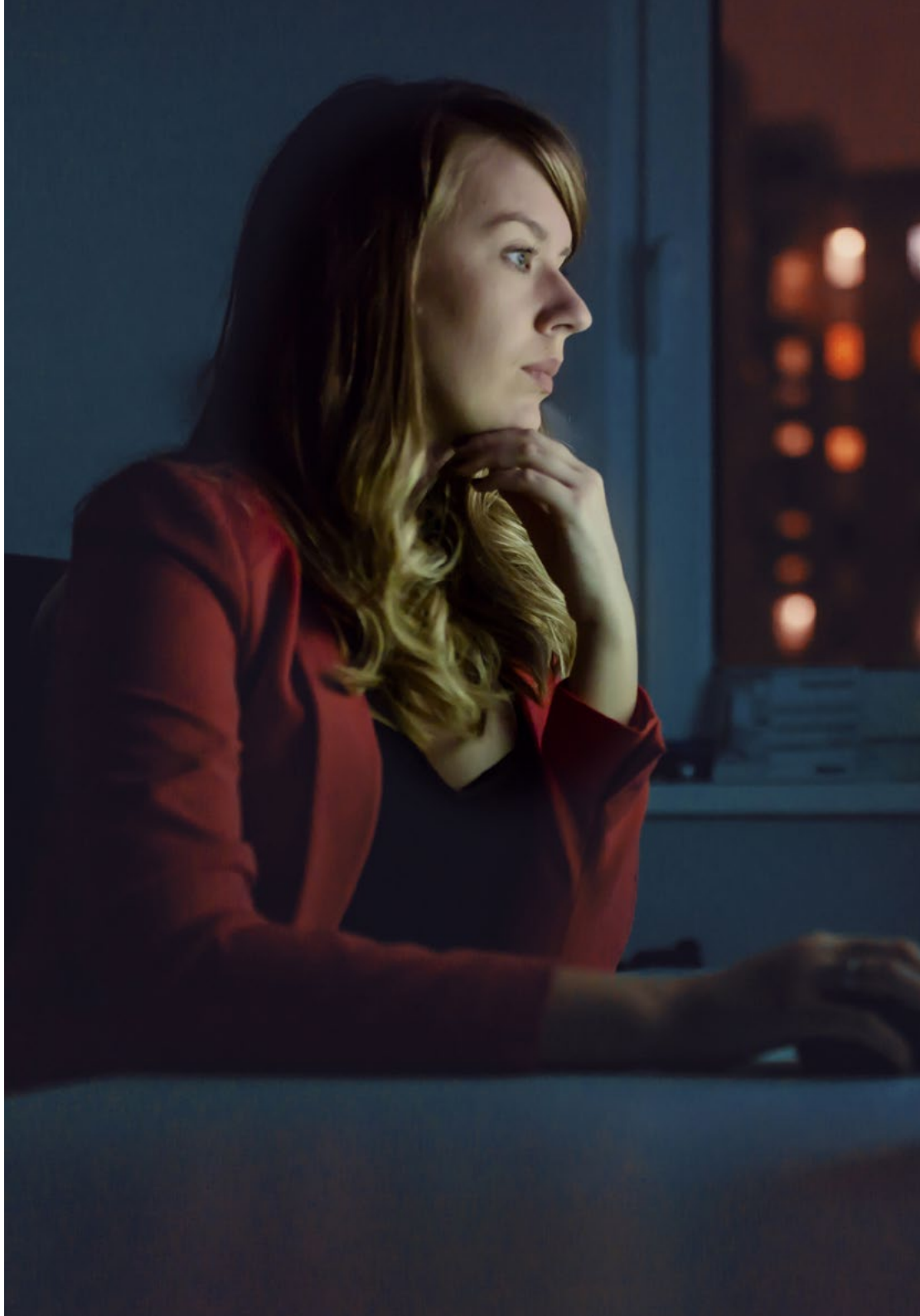
Struktur und Inhalt

Der Lehrplan dieses Universitätsexperten wurde so konzipiert, dass er in seinen drei Modulen die wichtigsten Aspekte des Managements von IT-Sicherheitsvorfällen abdeckt. So lernen die Studenten etwas über Management-Richtlinien, Erkennungs- und Präventionssysteme und beschäftigen sich im Laufe des Programms mit Sicherheitswerkzeugen, Protokollen und Audits. Praktische Sicherheitsnotfallhilfe wird ebenfalls eine wichtige Rolle in diesem Programm spielen. Die Fallstudien und das *Relearning*-System, das auf der Wiederholung von Inhalten basiert, werden es den Studenten erleichtern und beschleunigen, sich das gesamte Wissen dieses Programms anzueignen.

Das breite Spektrum an Multimedia-Ressourcen bereichert diesen Lehrplan, der von Experten auf dem Gebiet der Computersicherheit entwickelt wurde"

Modul 1. Richtlinien für das Management von Sicherheitsvorfällen

1.1. Richtlinien und Verbesserungen für das Management von Sicherheitsvorfällen in der Informationssicherheit
  1.1.1. Management von Zwischenfällen
  1.1.2. Verantwortlichkeiten und Verfahren
  1.1.3. Event-Benachrichtigung
1.2. Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS)
  1.2.1. Daten zur Systemleistung
  1.2.2. Arten von Intrusion Detection Systemen
  1.2.3. Kriterien für den Standort von IDS/IPS
1.3. Reaktion auf Sicherheitsvorfälle
  1.3.1. Verfahren zum Sammeln von Informationen
  1.3.2. Verfahren zur Überprüfung der Intrusion
  1.3.3. CERT-Gremien
1.4. Benachrichtigung über einen Einbruchsversuch und Managementprozess
  1.4.1. Verantwortlichkeiten im Benachrichtigungsprozess
  1.4.2. Klassifizierung von Vorfällen
  1.4.3. Lösung und Wiederherstellungsprozess
1.5. Forensische Analyse als Sicherheitspolitik
  1.5.1. Volatile und nichtvolatile Beweise
  1.5.2. Analyse und Sammlung von elektronischen Beweismitteln
    1.5.2.1. Analyse von elektronischen Beweismitteln
    1.5.2.2. Sammlung von elektronischen Beweismitteln
1.6. Werkzeuge für *Intrusion Detection und Prevention* Systeme (IDS/IPS)
  1.6.1. Snort
  1.6.2. Suricata
  1.6.3. SolarWinds
1.7. Tools zur Zentralisierung von Ereignissen
  1.7.1. SIM
  1.7.2. SEM
  1.7.3. SIEM



1.8. CCN-STIC Sicherheitsleitfaden 817
- 1.8.1. Management von Cybervorfällen
- 1.8.2. Metriken und Indikatoren

1.9. NIST SP800-61
- 1.9.1. Fähigkeit zur Reaktion auf Computer-Sicherheitsvorfälle
- 1.9.2. Umgang mit einem Vorfall
- 1.9.3. Koordinierung und Informationsaustausch

1.10. ISO 27035-Norm
- 1.10.1. ISO 27035-Norm. Grundsätze des Vorfallsmanagements
- 1.10.2. Richtlinien für die Entwicklung eines Vorfallsmanagementplans
- 1.10.3. Richtlinien für die Reaktion auf Vorfälle

Modul 2. Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme

2.1. Richtlinien für die Überwachung von Informationssystemen
- 2.1.1. System-Überwachung
- 2.1.2. Metriken
- 2.1.3. Arten von Metriken

2.2. Auditing und Logging in Systemen
- 2.2.1. Auditing und *Logging* in Windows
- 2.2.2. Auditing und *Logging* in Linux

2.3. SNMP-Protokoll. *Simple Network Management Protocol*
- 2.3.1. SNMP-Protokoll
- 2.3.2. Betrieb von SNMP
- 2.3.3. SNMP-Tools

2.4. Netzwerk-Überwachung
- 2.4.1. Netzwerküberwachung in Kontrollsystemen
- 2.4.2. Überwachungstools für Kontrollsysteme

2.5. Nagios. System zur Netzwerküberwachung
- 2.5.1. Nagios
- 2.5.2. Betrieb von Nagios
- 2.5.3. Installation von Nagios

2.6. Zabbix. System zur Netzwerküberwachung
- 2.6.1. Zabbix
- 2.6.2. Betrieb von Zabbix
- 2.6.3. Installation von Zabbix

2.7. Cacti. System zur Netzwerküberwachung
- 2.7.1. Cacti
- 2.7.2. Betrieb von Cacti
- 2.7.3. Installation von Cacti

2.8. Pandora. System zur Netzwerküberwachung
- 2.8.1. Pandora
- 2.8.2. Betrieb von Pandora
- 2.8.3. Installation von Pandora

2.9. SolarWinds. System zur Netzwerküberwachung
- 2.9.1. SolarWinds
- 2.9.2. Betrieb von SolarWinds
- 2.9.3. Installation von SolarWinds

2.10. Regelungen zur Überwachung
- 2.10.1. CIS-Kontrollen zur Prüfung und Registrierung
- 2.10.2. NIST 800-123 (USA)

Modul 3. Praktische Sicherheitspolitiken für die Notfallwiederherstellung

3.1. DRP. *Disaster-Recovery-Plan*
- 3.1.1. Zweck eines DRP
- 3.1.2. Vorteile eines DRP
- 3.1.3. Konsequenzen, wenn Sie keinen DRP haben oder diesen nicht auf dem neuesten Stand halten

3.2. Leitfaden für die Definition eines DRP (*Disaster Recovery Plan*)
- 3.2.1. Umfang und Ziele
- 3.2.2. Entwurf der Wiederherstellungsstrategie
- 3.2.3. Zuweisung von Rollen und Verantwortlichkeiten
- 3.2.4. Inventarisierung von Hardware, Software und Diensten
- 3.2.5. Toleranz für Ausfallzeiten und Datenverluste
- 3.2.6. Festlegen der spezifischen Arten von DRPs, die erforderlich sind
- 3.2.7. Umsetzung eines Plans zur Fortbildung, Sensibilisierung und Kommunikation

3.3. Umfang und Ziele eines DRP (*Disaster Recovery Plan*)
- 3.3.1. Sicherstellung der Reaktionsfähigkeit
- 3.3.2. Technologische Komponenten
- 3.3.3. Umfang der Kontinuitätspolitik

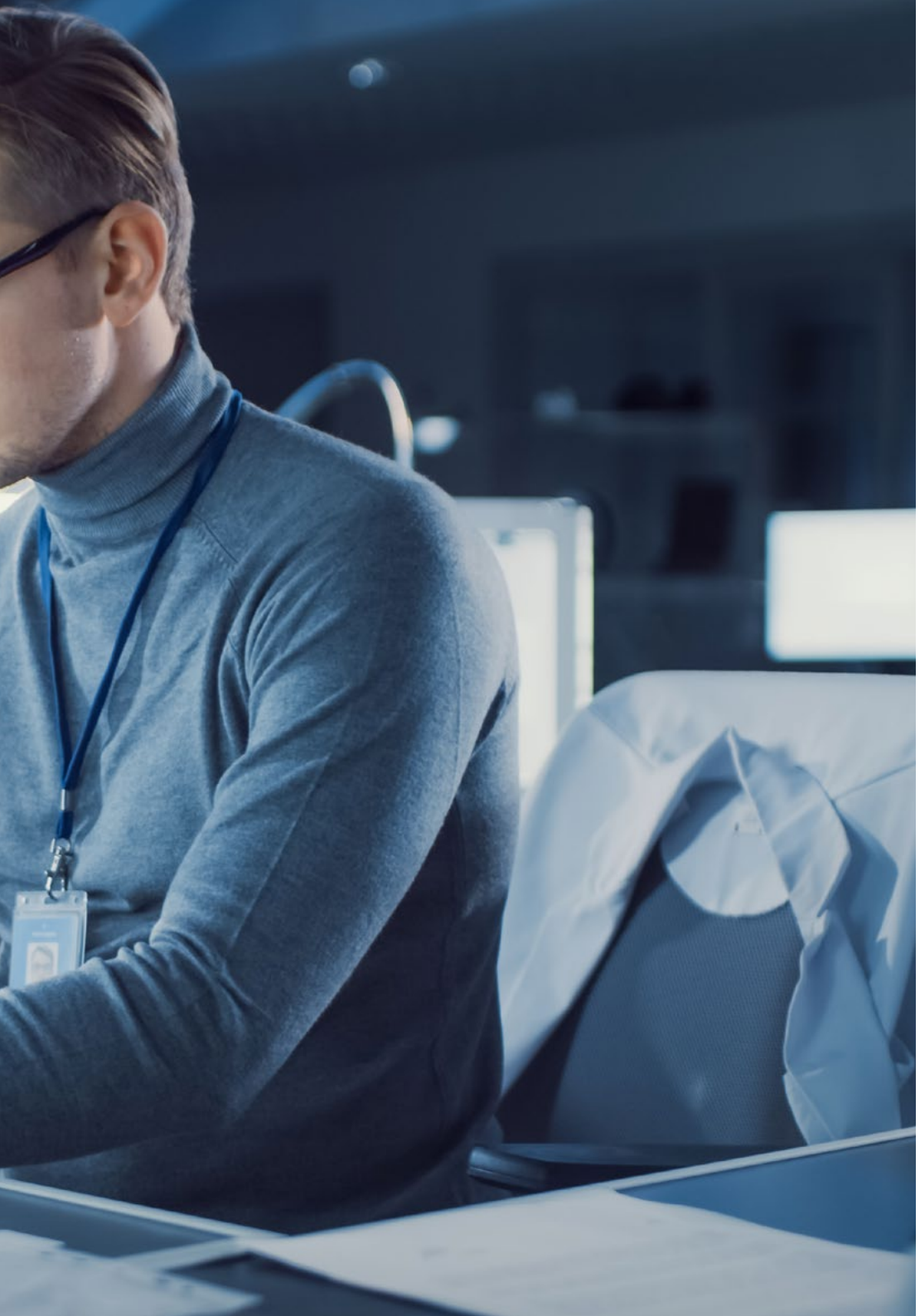
3.4. Entwurf einer DRP-Strategie (*Disaster Recovery*)
- 3.4.1. Disaster-Recovery-Strategie
- 3.4.2. Budget
- 3.4.3. Personelle und materielle Ressourcen
- 3.4.4. Gefährdete Managementpositionen
- 3.4.5. Technologie
- 3.4.6. Daten

3.5. Kontinuität der Informationsprozesse
- 3.5.1. Planung der Kontinuität
- 3.5.2. Implementierung der Kontinuität
- 3.5.3. Überprüfung der Kontinuitätsbewertung

3.6. Umfang eines BCP (*Business Continuity Plan*)
- 3.6.1. Bestimmung der kritischsten Prozesse
- 3.6.2. Asset-basierter Ansatz
- 3.6.3. Prozessorientierter Ansatz

3.7. Implementierung von gesicherten Geschäftsprozessen
- 3.7.1. Vorrangige Aktivitäten (PA)
- 3.7.2. Ideale Wiederherstellungszeiten (IRT)
- 3.7.3. Überlebensstrategien

3.8. Analyse der Organisation
- 3.8.1. Sammeln von Informationen
- 3.8.2. Analyse der geschäftlichen Auswirkungen (BIA)
- 3.8.3. Organisatorische Risikoanalyse



3.9. Reaktion auf Notfälle
  3.9.1. Krisenplan
  3.9.2. Wiederherstellungspläne für das Betriebsumfeld
  3.9.3. Verfahren für technische Arbeiten oder Zwischenfälle
3.10. Internationale Norm ISO 27031 BCP
  3.10.1. Ziele
  3.10.2. Begriffe und Definitionen
  3.10.3. Operation

Das Relearning-System und die 100%ige Online-Modalität werden Ihre Verbündeten sein, um Ihnen ein sehr nützliches Studium in Ihrem Berufsfeld zu ermöglichen"

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

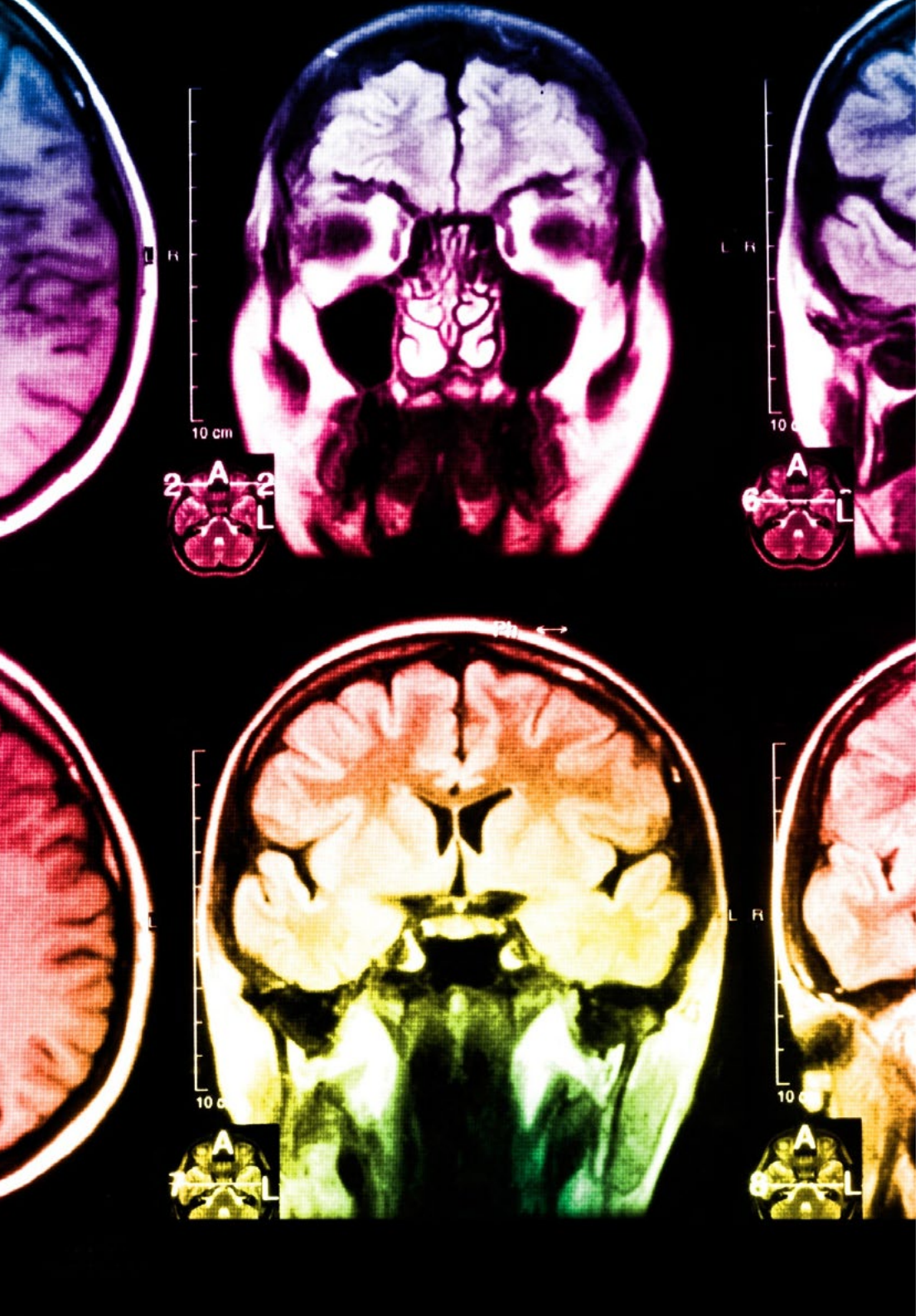
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

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.

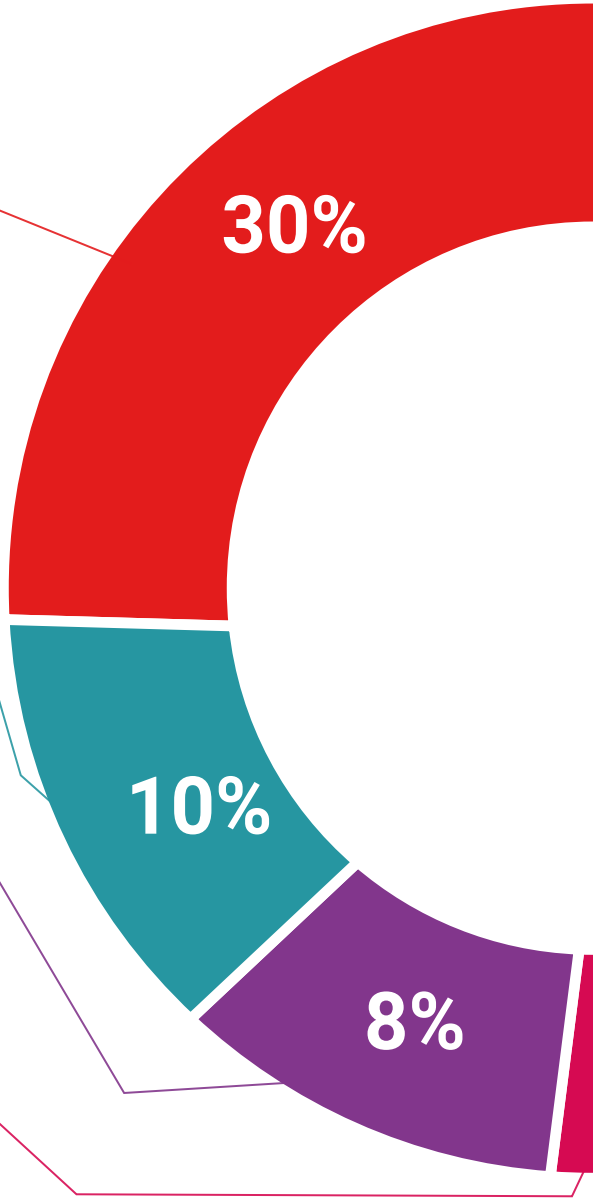
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

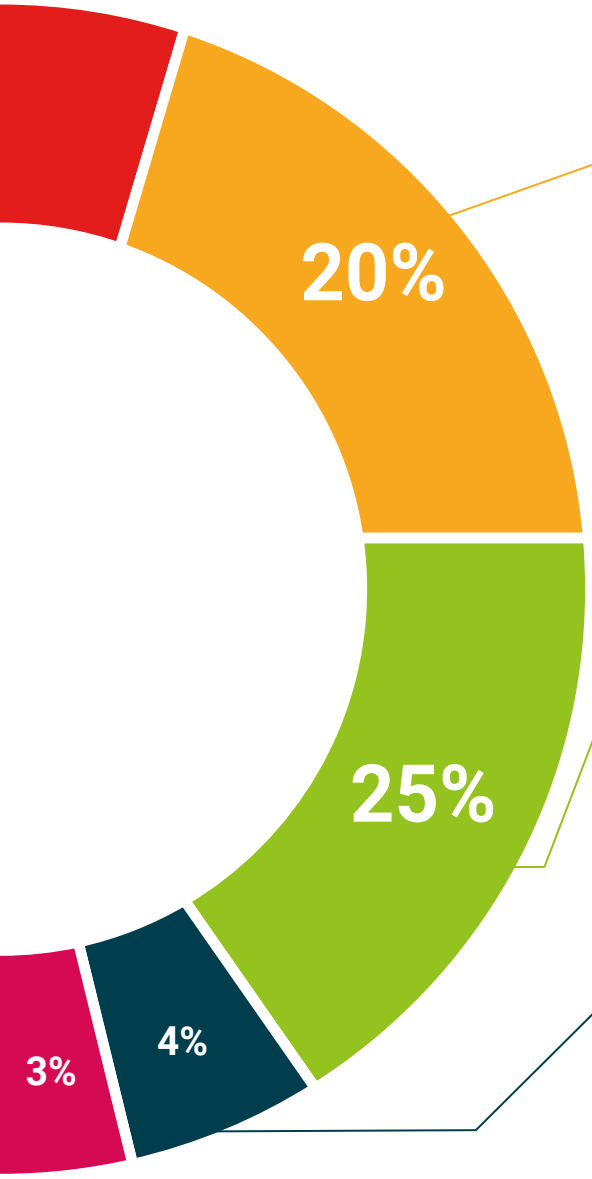
Übungen für Fertigkeiten und Kompetenzen

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 Management von IT-Sicherheitsvorfällen 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 Management von IT-Sicherheitsvorfällen** 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 Management von IT-Sicherheitsvorfällen**

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

Management von IT-Sicherheitsvorfällen

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
Management von IT-Sicherheitsvorfällen

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

Universitätsexperte

Management von IT-Sicherheitsvorfällen

tech technologische universität