Executive Master

Verwaltung der Cybersicherheitspolitik im Unternehmen

MVCU

tech technologische universität

tech technologische universität

Executive Master

Verwaltung der Cybersicherheitspolitik im Unternehmen

- Modalität: online
- Dauer: **12 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**
- Gerichtet an: **Hochschulabsolventen, die zuvor einen der Studiengänge in den Bereichen Sozial- und Rechtswissenschaften, Verwaltung und Business Administration abgeschlossen haben.**

Internetzugang: **www.techtitute.com/de/wirtschaftsschule/masterstudiengang/verwaltung-cybersicherheitspolitik-unternehmen**

Index

01

Willkommen

Schätzungen zufolge gehen die Verluste durch Cyber-Angriffe heute in die Millionen und weit darüber hinaus. Die Gefahr von Cyber-Angriffen ist so groß, dass sogar Staaten von Cyber-Vorfällen betroffen sein können. Dies macht deutlich, wie wichtig es ist, über Führungskräfte zu verfügen, die sich auf das Management von Cybersicherheitsrichtlinien spezialisiert haben und über die erforderlichen Kenntnisse in Bezug auf Organisation, Umsetzung und Überwachungsinstrumente verfügen, um alle Cybersicherheitsbemühungen zu koordinieren. Das Programm bereitet Manager darauf vor, unsicheren Szenarien mit Selbstvertrauen und fortgeschrittenem Wissen zu begegnen und bietet hochwertige Lösungen im Bereich der Informationssicherheit. Umfassende theoretische Inhalte, die auf realen Praxisfällen basieren, vermitteln Ihnen eine moderne und umfassende Perspektive auf alle Funktionen, die ein Cybersicherheitsmanager erfüllen muss. Und das alles in einem 100%igen Online-Format, ohne Präsenzveranstaltungen und vorgegebene Stundenpläne, mit völliger Flexibilität.

Executive Master in Verwaltung der Cybersicherheitspolitik im Unternehmen.
TECH Technologische Universität

Bringen Sie einen unschätzbaren Wert in Ihre Cybersicherheitspolitik ein, indem Sie alle Nuancen kennen, von den Sicherheitssystemen selbst bis zu den Praktiken der Bedrohungsanalyse, die Ihnen den Schlüssel zu einer vorteilhaften Positionierung in Ihrem Unternehmen liefern"

02

Warum an der TECH studieren?

TECH ist die weltweit größte 100%ige Online Business School. Es handelt sich um eine Elite-Business School mit einem Modell, das höchsten akademischen Ansprüchen genügt. Ein leistungsstarkes internationales Zentrum für die intensive Fortbildung von Führungskräften.

TECH ist eine Universität an der Spitze der Technologie, die dem Studenten alle Ressourcen zur Verfügung stellt, um ihm zu helfen, geschäftlich erfolgreich zu sein"

Bei TECH Technologische Universität

Innovation

Die Universität bietet ein Online-Lernmodell an, das modernste Bildungstechnologie mit höchster pädagogischer Genauigkeit verbindet. Eine einzigartige Methode mit höchster internationaler Anerkennung, die dem Studenten die Schlüssel für seine Entwicklung in einer Welt des ständigen Wandels liefert, in der Innovation der wesentliche Einsatz eines jeden Unternehmers sein muss.

"Die Erfolgsgeschichte von Microsoft Europa" für die Einbeziehung des neuen interaktiven Multivideosystems in unsere Programme.

Maximalforderung

Das Zulassungskriterium von TECH ist nicht wirtschaftlich. Sie brauchen keine große Investitionen zu tätigen, um bei TECH zu studieren. Um jedoch einen Abschluss bei TECH zu erlangen, werden die Grenzen der Intelligenz und der Kapazität des Studenten getestet. Die akademischen Standards von TECH sind sehr hoch...

95% | **der Studenten von TECH schließen ihr Studium erfolgreich ab**

Networking

Fachleute aus der ganzen Welt nehmen an der TECH teil, so dass der Student ein großes Netzwerk von Kontakten knüpfen kann, die für seine Zukunft nützlich sein werden.

+100.000
jährlich spezialisierte Manager

+200
verschiedene Nationalitäten

Empowerment

Der Student wird Hand in Hand mit den besten Unternehmen und Fachleuten von großem Prestige und Einfluss wachsen. TECH hat strategische Allianzen und ein wertvolles Netz von Kontakten zu den wichtigsten Wirtschaftsakteuren auf den 7 Kontinenten aufgebaut.

+500 | **Partnerschaften mit den besten Unternehmen**

Talent

Dieses Programm ist ein einzigartiger Vorschlag, um die Talente des Studenten in der Geschäftswelt zu fördern. Eine Gelegenheit für ihn, seine Anliegen und seine Geschäftsvision vorzutragen.

TECH hilft dem Studenten, sein Talent am Ende dieses Programms der Welt zu zeigen.

Multikultureller Kontext

Ein Studium bei TECH bietet dem Studenten eine einzigartige Erfahrung. Er wird in einem multikulturellen Kontext studieren. In einem Programm mit einer globalen Vision, dank derer er die Arbeitsweise in verschiedenen Teilen der Welt kennenlernen und die neuesten Informationen sammeln kann, die am besten zu seiner Geschäftsidee passen.

Unsere Studenten kommen aus mehr als 200 Ländern.

Mit den Besten lernen

Das Lehrteam von TECH erklärt im Unterricht, was sie in ihren Unternehmen zum Erfolg geführt hat, und zwar in einem realen, lebendigen und dynamischen Kontext. Lehrkräfte, die sich voll und ganz dafür einsetzen, eine hochwertige Spezialisierung zu bieten, die es dem Studenten ermöglicht, in seiner Karriere voranzukommen und sich in der Geschäftswelt zu profilieren.

Lehrkräfte aus 20 verschiedenen Ländern.

Bei TECH werden Sie Zugang zu den präzisesten und aktuellsten Fallstudien im akademischen Bereich haben"

TECH strebt nach Exzellenz und hat zu diesem Zweck eine Reihe von Merkmalen, die sie zu einer einzigartigen Universität machen:

Analyse

TECH erforscht die kritische Seite des Studenten, seine Fähigkeit, Dinge zu hinterfragen, seine Problemlösungsfähigkeiten und seine zwischenmenschlichen Fähigkeiten.

Akademische Spitzenleistung

TECH bietet dem Studenten die beste Online-Lernmethodik. Die Universität kombiniert die *Relearning*-Methode (die international am besten bewertete Lernmethode für Aufbaustudien) mit der Fallstudie. Tradition und Avantgarde in einem schwierigen Gleichgewicht und im Rahmen einer anspruchsvollen akademischen Laufbahn.

Skaleneffekt

TECH ist die größte Online-Universität der Welt. Sie verfügt über ein Portfolio von mehr als 10.000 Hochschulabschlüssen. Und in der neuen Wirtschaft gilt: **Volumen + Technologie = disruptiver Preis**. Damit stellt TECH sicher, dass das Studium nicht so kostspielig ist wie an anderen Universitäten.

03

Warum unser Programm?

Die Teilnahme am TECH-Programm bedeutet eine Vervielfachung der Chancen auf beruflichen Erfolg im Bereich der höheren Unternehmensführung.

Es ist eine Herausforderung, die Anstrengung und Hingabe erfordert, aber die Tür zu einer vielversprechenden Zukunft öffnet. Der Student wird von den besten Lehrkräften und mit den flexibelsten und innovativsten Lehrmethoden unterrichtet.

Wir verfügen über das renommierteste Dozententeam und den umfassendsten Lehrplan auf dem Markt, so dass wir Ihnen eine Fortbildung auf höchstem akademischen Niveau bieten können"

Dieses Programm bietet eine Vielzahl von beruflichen und persönlichen Vorteilen, darunter die Folgenden:

01 Einen deutlichen Schub für die Karriere des Studenten

Mit einem Studium bei TECH wird der Student seine Zukunft selbst in die Hand nehmen und sein volles Potenzial entfalten können. Durch die Teilnahme an diesem Programm wird er die notwendigen Kompetenzen erwerben, um in kurzer Zeit eine positive Veränderung in seiner Karriere zu erreichen.

70% der Teilnehmer dieser Spezialisierung erreichen in weniger als 2 Jahren eine positive Veränderung in ihrer Karriere.

02 Entwicklung einer strategischen und globalen Vision des Unternehmens

TECH bietet einen detaillierten Überblick über das allgemeine Management, um zu verstehen, wie sich jede Entscheidung auf die verschiedenen Funktionsbereiche des Unternehmens auswirkt.

Die globale Vision des Unternehmens von TECH wird Ihre strategische Vision verbessern.

03 Konsolidierung des Studenten in der Unternehmensführung

Ein Studium an der TECH öffnet die Türen zu einem beruflichen Panorama von großer Bedeutung, so dass der Student sich als hochrangiger Manager mit einer umfassenden Vision des internationalen Umfelds positionieren kann.

Sie werden mehr als 100 reale Fälle aus dem Bereich der Unternehmensführung bearbeiten.

04 Übernahme neuer Verantwortung

Während des Programms werden die neuesten Trends, Entwicklungen und Strategien vorgestellt, damit der Student seine berufliche Tätigkeit in einem sich verändernden Umfeld ausüben kann.

45% der Studenten werden intern befördert.

05

Zugang zu einem leistungsfähigen Netzwerk von Kontakten

TECH vernetzt seine Studenten, um ihre Chancen zu maximieren. Studenten mit den gleichen Sorgen und dem Wunsch zu wachsen. So wird es möglich sein, Partner, Kunden oder Lieferanten zu teilen.

Sie werden ein Netz von Kontakten finden, das für Ihre berufliche Entwicklung unerlässlich ist.

06

Rigorose Entwicklung von Unternehmensprojekten

Der Student wird eine tiefgreifende strategische Vision erlangen, die ihm helfen wird, sein eigenes Projekt unter Berücksichtigung der verschiedenen Bereiche des Unternehmens zu entwickeln.

20% unserer Studenten entwickeln ihre eigene Geschäftsidee.

07

Verbesserung von *Soft Skills* und Führungsqualitäten

TECH hilft dem Studenten, sein erworbenes Wissen anzuwenden und weiterzuentwickeln und seine zwischenmenschlichen Fähigkeiten zu verbessern, um eine Führungspersönlichkeit zu werden, die etwas bewirkt.

Verbessern Sie Ihre Kommunikations- und Führungsfähigkeiten und geben Sie Ihrer Karriere einen neuen Impuls.

08

Teil einer exklusiven Gemeinschaft sein

Der Student wird Teil einer Gemeinschaft von Elite-Managern, großen Unternehmen, renommierten Institutionen und qualifizierten Professoren der renommiertesten Universitäten der Welt sein: die Gemeinschaft der TECH Technologischen Universität.

Wir bieten Ihnen die Möglichkeit, sich mit einem Team von international anerkannten Dozenten zu spezialisieren.

04

Ziele

Da die Cybersicherheit ein entscheidender Aspekt für die Entwicklung jedes modernen Unternehmens ist, konnte das Ziel dieses Programms nur darin bestehen, die bestmögliche Weiterbildung im Bereich der Verwaltung der Cybersicherheitspolitik anzubieten. Zu diesem Zweck hat eine Gruppe von IT-Experten umfangreiches didaktisches Material zusammengestellt, das sich ausschließlich auf die Verbesserung der Fähigkeiten, Kompetenzen und Fertigkeiten von Managern konzentriert.

Die Cybersicherheit der eigenen Organisation zu managen und die Besonderheiten der effektivsten Cybersicherheitsrichtlinien zu kennen"

TECH macht sich die Ziele ihrer Studenten zu eigen. Gemeinsam arbeiten sie daran, diese zu erreichen.

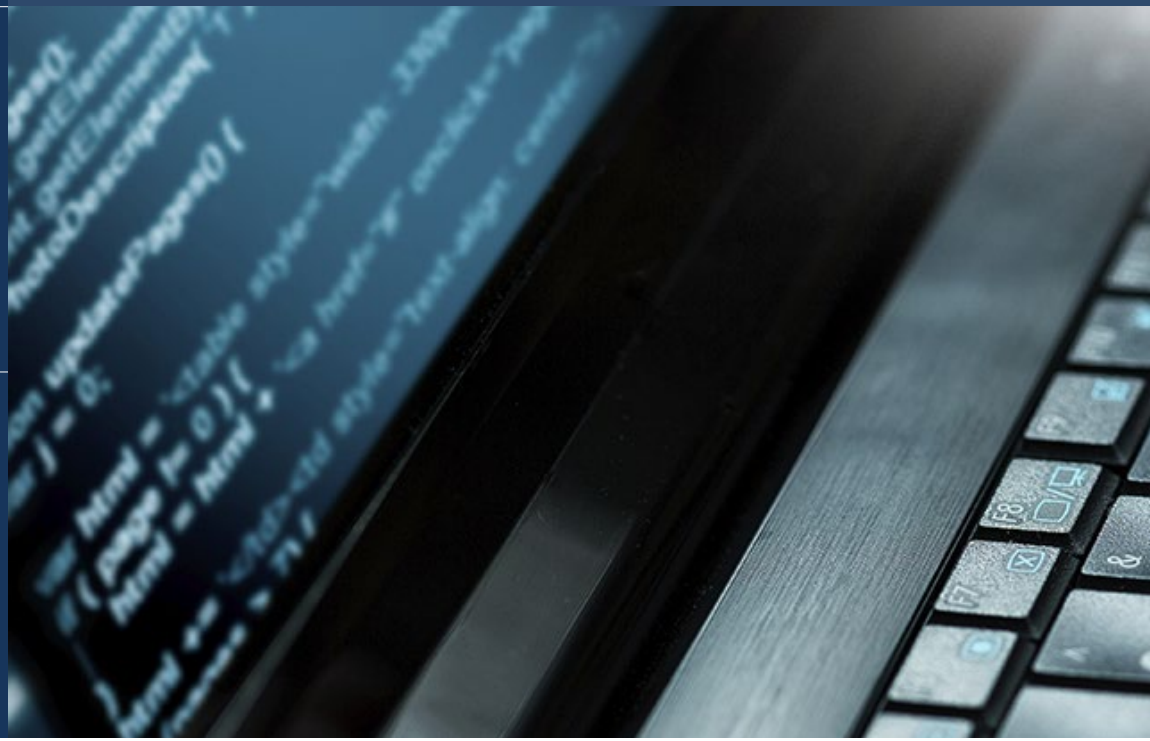
Der **Executive Master in Verwaltung der Cybersicherheitspolitik im Unternehmen** wird den Studenten zu Folgendem befähigen:

01 Vertiefen der Schlüsselkonzepte der Informationssicherheit

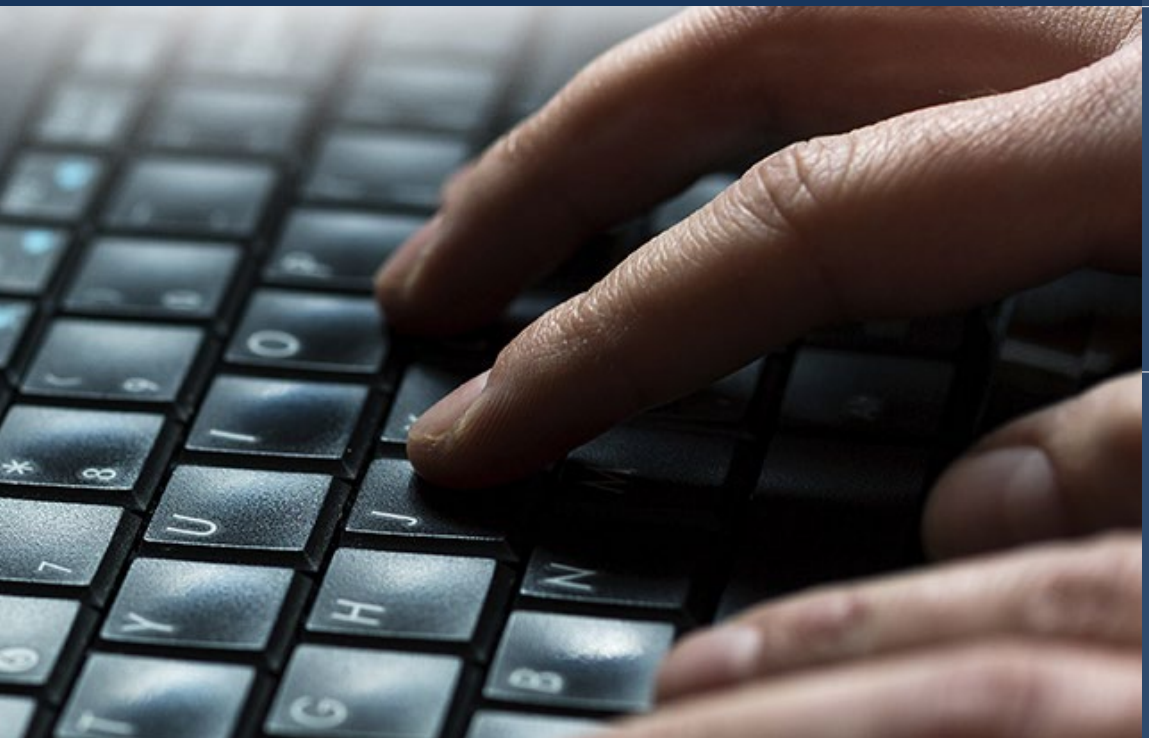
02 Analysieren der Vorschriften und Standards, die derzeit für ISMS gelten

03 Implementieren eines ISMS im Unternehmen

04 Bestimmen, welche Abteilungen die Implementierung des Sicherheitsmanagementsystems abdecken soll



05 Entwickeln der notwendigen Maßnahmen zur Gewährleistung guter Informationssicherheitspraktiken



06 Bestimmen, was Authentifizierung und Identifizierung sind

07 Analysieren der verschiedenen existierenden Authentifizierungsmethoden und ihrer praktischen Umsetzung

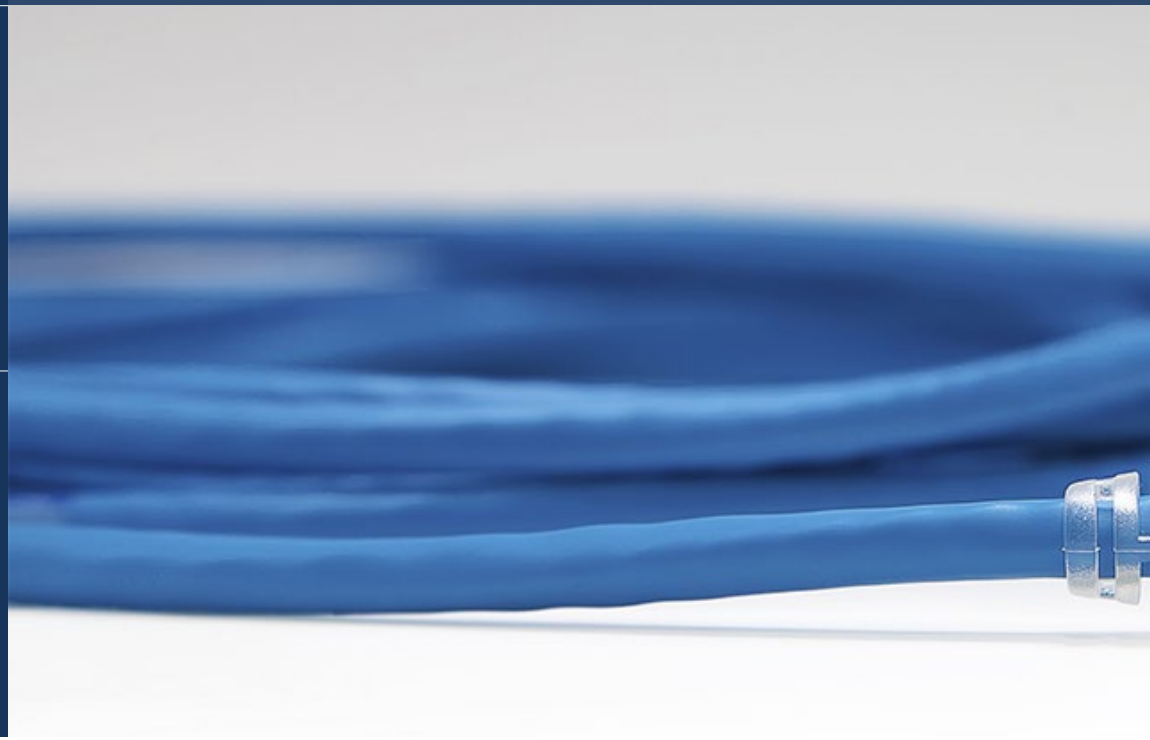
08 Implementieren der richtigen Zugriffskontrollpolitik für Software und Systeme

09 Entwickeln von Fachwissen über den Umgang mit Vorfällen, die durch Computersicherheitsereignisse verursacht werden

10 Analysieren der Begriffe sicherer Bereich und sicherer Umkreis

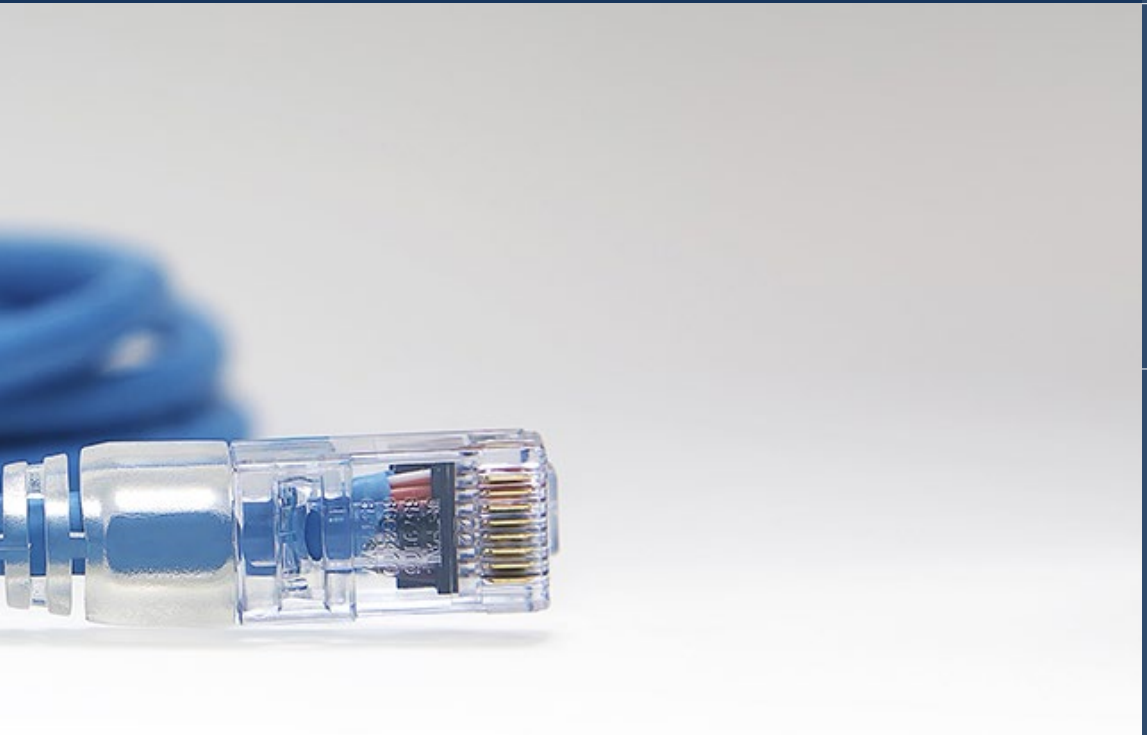
11 Analysieren der verschiedenen Verschlüsselungsalgorithmen, die in Kommunikationsnetzwerken verwendet werden

12 Bestimmen der verschiedenen realen Angriffe auf unser Informationssystem



13 Bewerten der verschiedenen Sicherheitsmaßnahmen zur Eindämmung von Angriffen

14 Entwickeln des Konzepts der Überwachung und Implementierung von Metriken



15 Generieren von Fachwissen über das Konzept der Kontinuität der Informationssicherheit

16 Bestimmen, was Kryptographie ist und welche Arten von Kryptographie es gibt

05

Kompetenzen

Die ordnungsgemäße Verwaltung von Cybersicherheitsrichtlinien erfordert nicht nur ausgezeichnete IT- und Technologiekenntnisse und -fähigkeiten, sondern auch ein hohes Maß an Organisationstalent. Aus diesem Grund bietet dieses Programm nicht nur ein nützliches Nachschlagewerk für das IT-Sicherheitsmanagement, sondern stärkt auch die Führungs- und Managementfähigkeiten des Managers.

Sie entwickeln die notwendigen Fähigkeiten, um sich als Experte für Cybersicherheitspolitik zu profilieren, was Ihnen den Vorteil verschafft bei der Besetzung wichtiger Führungspositionen"

01 Bestimmen der Einbindung eines ISMS in die interne Organisation des Unternehmens sowie dessen Status

02 Festlegen der Sicherheitsrichtlinien im Unternehmen

03 Bestimmen, welche Maßnahmen wir bei Lieferanten und bei der Wartung von Informationssystemen umsetzen müssen

04 Generieren von Fachwissen über die Kontrolle von Bedrohungen

05 Bestimmen der Phasen des präventiven Bedrohungsmanagements

06 Entwickeln von Methoden für die Analyse von Computerbedrohungen

07 Klassifizieren von Bedrohungen nach Auswirkungen und Schweregrad

08 Entwickeln einer eigenen Methodik für die präventive Analyse und Überwachung von Bedrohungen

09 Implementieren einer korrekten Zugriffskontrollpolitik für Netzwerke und Dienste

10 Analysieren der Bedeutung einer korrekten Handhabung von Sicherheitsvorfällen

11 Zusammenstellen der verschiedenen biometrischen Systeme, die es gibt

12 Untersuchen der Biometrie und biometrischer Systeme

13 Implementieren der richtigen physischen Sicherheitsrichtlinien und Zugangskontrollsysteme in Datenverarbeitungszentren

14 Implementieren eines sicheren Netzwerks

15 Untersuchen der Schwachstellen von mobilen und IoT-Plattformen und wie man sie vermeidet

16 Erkennen der Arten von *Social Engineering* und lernen, wie man sie entschärfen kann

17 Analysieren des Konzepts der Überwachung und der Implementierung von Metriken

18 Bestimmen des Bedarfs an Kontinuität der Informationssicherheit

06

Struktur und Inhalt

TECH hat dieses Programm auf der Grundlage der *Relearning*-Methode strukturiert, was bedeutet, dass der Manager keine langen Studienzeiten aufwenden muss, um sich das gesamte angebotene Wissen anzueignen. Die wichtigsten Begriffe und Konzepte im Bereich der Cybersicherheitspolitik werden auf natürliche und sich wiederholende Weise während des gesamten Programms vermittelt, was zu einem viel progressiveren Lernprozess führt.

Sie können das virtuelle Klassenzimmer 24 Stunden am Tag betreten und so das Lerntempo an Ihre eigenen Interessen anpassen"

Lehrplan

Der Executive Master in Verwaltung der Cybersicherheitspolitik im Unternehmen der TECH Technologischen Universität ist ein intensiver Studiengang, der die Studenten auf die anspruchsvollsten Bereiche der Cybersicherheit im Unternehmen vorbereitet.

Der Inhalt des Executive Masters in Verwaltung der Cybersicherheitspolitik im Unternehmen ist darauf ausgerichtet, die Entwicklung von Managementfähigkeiten zu fördern, die es ermöglichen, in unsicheren Umgebungen fundierte Entscheidungen zu treffen.

Dieser Executive Master befasst sich eingehend mit der digitalen Welt, der Sicherheit in diesem Umfeld und der Umsetzung des elektronischen Geschäftsverkehrs in Unternehmen und zielt darauf ab, Fachleute weiterzubilden, die das Management der Cybersicherheitspolitik in Unternehmen aus einer strategischen, internationalen und innovativen Perspektive verstehen.

Dieser Executive Master erstreckt sich über 12 Monate und ist in 10 Module unterteilt:

Modul 1	Informationssicherheits-Managementsystem (ISMS)
Modul 2	Organisatorische Aspekte der Informationssicherheitspolitik
Modul 3	Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen
Modul 4	Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware
Modul 5	Richtlinien für das Management von Sicherheitsvorfällen
Modul 6	Implementierung von physischen und ökologischen Sicherheitspolitiken im Unternehmen
Modul 7	Richtlinien für sichere Kommunikation im Unternehmen
Modul 8	Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen
Modul 9	Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme
Modul 10	Praktische Sicherheitspolitiken für die Notfallwiederherstellung

Wo, wann und wie wird unterrichtet?

TECH bietet die Möglichkeit, diesen Executive Master in Verwaltung der Cybersicherheitspolitik im Unternehmen vollständig online zu absolvieren. Während der 12-monatigen Spezialisierung wird der Student jederzeit auf alle Inhalte dieses Programms zugreifen können, was ihm die Möglichkeit gibt, seine Studienzeit selbst zu verwalten.

Eine einzigartige, wichtige und entscheidende Bildungserfahrung, um Ihre berufliche Entwicklung voranzutreiben und den endgültigen Sprung zu schaffen.

Modul 1. Informationssicherheits-Managementsystem (ISMS)

1.1. Informationssicherheit. Schlüsselaspekte

1.1.1. Informationssicherheit
- 1.1.1.1. Vertraulichkeit
- 1.1.1.2. Integrität
- 1.1.1.3. Verfügbarkeit
- 1.1.1.4. Maßnahmen zur Informationssicherheit

1.2. Managementsystem für die Informationssicherheit

1.2.1. Modelle für das Management der Informationssicherheit
1.2.2. Dokumente für die Implementierung eines ISMS
1.2.3. ISMS-Stufen und Kontrollen

1.3. Internationale Normen und Standards

1.3.1. Internationale Normen zur Informationssicherheit
1.3.2. Ursprung und Entwicklung des Standards
1.3.3. Internationale Standards für das Management der Informationssicherheit
1.3.4. Andere Referenzstandards

1.4. ISO/IEC 27000-Normen

1.4.1. Zweck und Anwendungsbereich
1.4.2. Aufbau der Norm
1.4.3. Zertifizierung
1.4.4. Phasen der Akkreditierung
1.4.5. Vorteile der ISO/IEC 27.000-Normen

1.5. Entwurf und Implementierung eines allgemeinen Informationssicherheitssystems

1.5.1. Phasen der Implementierung eines allgemeinen Informationssicherheitssystems
1.5.2. *Business Continuity Plan*

1.6. Phase I: Diagnose

1.6.1. Vorläufige Diagnose
1.6.2. Identifizierung der Ebene der Schichtung
1.6.3. Grad der Einhaltung von Standards/Normen

1.7. Phase II: Vorbereitung

1.7.1. Organisatorischer Kontext
1.7.2. Analyse der geltenden Sicherheitsvorschriften
1.7.3. Umfang des gesamten Informationssicherheitssystems
1.7.4. Allgemeine Richtlinien für das Informationssicherheitssystem
1.7.5. Zielsetzungen des allgemeinen Informationssicherheitssystems

1.8. Phase III: Planung

1.8.1. Klassifizierung der Vermögenswerte
1.8.2. Risikobewertung
1.8.3. Identifizierung von Bedrohungen und Risiken

1.9. Phase IV: Umsetzung und Überwachung

1.9.1. Analyse der Ergebnisse
1.9.2. Zuweisung von Verantwortlichkeiten
1.9.3. Zeitplan für den Aktionsplan
1.9.4. Überwachung und Audits

1.10. Sicherheitsrichtlinien für das Incident Management

1.10.1. Phasen
1.10.2. Kategorisierung von Vorfällen
1.10.3. Verfahren für Zwischenfälle und Zwischenfallmanagement

Modul 2. Organisatorische Aspekte der Informationssicherheitspolitik

2.1. Interne Organisation
2.1.1. Zuweisung von Verantwortlichkeiten
2.1.2. Trennung der Aufgaben
2.1.3. Kontakte mit Behörden
2.1.4. Informationssicherheit in der Projektverwaltung

2.2. Vermögensverwaltung
2.2.1. Verantwortung für Vermögenswerte
2.2.2. Klassifizierung der Informationen
2.2.3. Handhabung von Speichermedien

2.3. Sicherheitspolitiken in Geschäftsprozessen
2.3.1. Analyse der anfälligen Geschäftsprozesse
2.3.2. Analyse der Auswirkungen auf das Geschäft
2.3.3. Einstufung der Prozesse in Bezug auf die geschäftlichen Auswirkungen

2.4. Sicherheitspolitiken in Verbindung mit dem Personalwesen
2.4.1. Vor der Einstellung
2.4.2. Während der Rekrutierung
2.4.3. Beendigung oder Wechsel der Stelle

2.5. Sicherheitsrichtlinien auf Managementebene
2.5.1. Managementrichtlinien zur Informationssicherheit
2.5.2. BIA - Analyse der Auswirkungen
2.5.3. Wiederherstellungsplan als Sicherheitspolitik

2.6. Anschaffung und Wartung von Informationssystemen
2.6.1. Anforderungen an die Sicherheit von Informationssystemen
2.6.2. Entwicklung und Unterstützung der Datensicherheit
2.6.3. Testdaten

2.7. Sicherheit bei Lieferanten
2.7.1. IT-Sicherheit mit Zulieferern
2.7.2. Management der Bereitstellung des Dienstes mit Garantie
2.7.3. Sicherheit der Lieferkette

2.8. Operative Sicherheit
2.8.1. Operative Verantwortlichkeiten
2.8.2. Schutz vor bösartigem Code
2.8.3. Sicherheitskopien
2.8.4. Aktivitätsprotokolle und Überwachung

2.9. Sicherheitsmanagement und Vorschriften
2.9.1. Einhaltung der gesetzlichen Vorschriften
2.9.2. Überprüfung der Informationssicherheit

2.10. Sicherheit im *Business Continuity Management*
2.10.1. Kontinuität der Informationssicherheit
2.10.2. Redundanzen

Modul 3. Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen

3.1. Bedrohungsmanagement in Sicherheitsrichtlinien
3.1.1. Das Risikomanagement
3.1.2. Das Sicherheitsrisiko
3.1.3. Methodologien im Bedrohungsmanagement
3.1.4. Implementierung von Methoden

3.2. Phasen des Managements von Bedrohungen
3.2.1. Identifizierung
3.2.2. Analyse
3.2.3. Lokalisation
3.2.4. Schutzmaßnahmen

3.3. Auditsysteme zur Lokalisierung von Bedrohungen
3.3.1. Klassifizierung und Informationsfluss
3.3.2. Analyse der anfälligen Prozesse

3.4. Risikoklassifizierung
3.4.1. Arten von Risiko
3.4.2. Berechnung der Gefahrenwahrscheinlichkeit
3.4.3. Residuales Risiko

3.5. Risikobehandlung
3.5.1. Umsetzung von Schutzmaßnahmen
3.5.2. Übertragung oder Übernahme

3.6. Risikokontrolle
3.6.1. Kontinuierlicher Risikomanagementprozess
3.6.2. Implementierung von Sicherheitsmetriken
3.6.3. Strategisches Modell der Metriken für die Informationssicherheit

3.7. Praktische Methoden für die Analyse und Kontrolle von Bedrohungen
3.7.1. Katalog der Bedrohungen
3.7.2. Katalog der Kontrollmaßnahmen
3.7.3. Katalog der Sicherheitsvorkehrungen

3.8. ISO 27005-Norm
3.8.1. Identifizierung von Risiken
3.8.2. Risikoanalyse
3.8.3. Risikobewertung

3.9. Matrix der Risiken, Auswirkungen und Bedrohungen
3.9.1. Daten, Systeme und Personal
3.9.2. Wahrscheinlichkeit der Bedrohung
3.9.3. Ausmaß des Schadens

3.10. Gestaltung von Phasen und Prozessen in der Gefahrenanalyse
3.10.1. Identifizierung der kritischen Elemente der Organisation
3.10.2. Bestimmung der Bedrohungen und Auswirkungen
3.10.3. Analyse der Auswirkungen und Risiken
3.10.4. Methoden

Modul 4. Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware

4.1. Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware
4.1.1. Implementierung von Identifizierung und Autorisierung
4.1.2. Implementierung von Identifizierungstechniken
4.1.3. Technische Maßnahmen zur Autorisierung

4.2. Identifizierungs- und Autorisierungstechniken
4.2.1. Kennung und OTP
4.2.2. USB-Token oder PKI-*Smartcard*
4.2.3. Der Schlüssel "Vertrauliche Verteidigung"
4.2.4. Aktive RFID

4.3. Sicherheitspolitiken für den Zugang zu Software und Systemen
4.3.1. Implementierung von Politiken zur Zugriffskontrolle
4.3.2. Umsetzung von Politiken für den Zugang zur Kommunikation
4.3.3. Arten von Sicherheitstools für die Zugriffskontrolle

4.4. Verwaltung des Benutzerzugriffs
4.4.1. Verwaltung von Zugriffsrechten
4.4.2. Trennung von Rollen und Zugriffsfunktionen
4.4.3. Implementierung von Zugriffsrechten in Systemen

4.5. Kontrolle des Zugriffs auf Systeme und Anwendungen
4.5.1. Mindestzugriffsregel
4.5.2. Sichere Anmeldetechnologien
4.5.3. Passwort-Sicherheitsrichtlinien

4.6. Technologien für Identifikationssysteme
4.6.1. Aktives Verzeichnis
4.6.2. OTP
4.6.3. PAP, CHAP
4.6.4. KERBEROS, DIAMETER, NTLM

4.7. CIS-Kontrollen für Bastionierungssysteme
4.7.1. Allgemeine CIS-Kontrollen
4.7.2. Grundlegende CIS-Kontrollen
4.7.3. Organisatorische CIS-Kontrollen

4.8. Operative Sicherheit
4.8.1. Schutz vor bösartigem Code
4.8.2. Sicherungskopien
4.8.3. Aktivitätsprotokollierung und Überwachung

4.9. Management von technischen Schwachstellen
4.9.1. Technische Schwachstellen
4.9.2. Management von technischen Schwachstellen
4.9.3. Einschränkungen bei der Software-Installation

4.10. Umsetzung der Sicherheitspraktiken
4.10.1. Logische Schwachstellen
4.10.2. Implementierung von Verteidigungsrichtlinien

Modul 5. Richtlinien für das Management von Sicherheitsvorfällen

5.1. Richtlinien und Verbesserungen für das Management von Sicherheitsvorfällen in der Informationssicherheit
5.1.1. Management von Zwischenfällen
5.1.2. Verantwortlichkeiten und Verfahren
5.1.3. Event-Benachrichtigung

5.2. Systeme zur Erkennung und Verhinderung von Angriffen (IDS/IPS)
5.2.1. Daten zur Systemleistung
5.2.2. Arten von *Intrusion Detection Systems*
5.2.3. Kriterien für den Standort von IDS/IPS

5.3. Reaktion auf Sicherheitsvorfälle
5.3.1. Verfahren zum Sammeln von Informationen
5.3.2. Verfahren zur Überprüfung der Intrusion
5.3.3. CERT-Gremien

5.4. Benachrichtigung über einen Angriffsversuch und Managementprozess
5.4.1. Verantwortlichkeiten im Benachrichtigungsprozess
5.4.2. Klassifizierung von Vorfällen
5.4.3. Lösung und Wiederherstellungsprozess

5.5. Forensische Analyse als Sicherheitspolitik
5.5.1. Volatile und nichtvolatile Beweise
5.5.2. Analyse und Sammlung von elektronischen Beweismitteln
5.5.2.1. Analyse von elektronischen Beweismitteln
5.5.2.2. Sammlung von elektronischen Beweismitteln

5.6. Tools für die Erkennung und Verhinderung von Angriffen (IDS/IPS)
5.6.1. Snort
5.6.2. Suricata
5.6.3. Solar-Winds

5.7. Tools zur Zentralisierung von Ereignissen
5.7.1. SIM
5.7.2. SEM
5.7.3. SIEM

5.8. CCN-STIC Sicherheitsleitfaden 817
5.8.1. CCN-STIC Sicherheitsleitfaden 817
5.8.2. Management von Cybervorfällen
5.8.3. Metriken und Indikatoren

5.9. NIST SP800-61
5.9.1. Fähigkeit zur Reaktion auf Computer-Sicherheitsvorfälle
5.9.2. Umgang mit einem Vorfall
5.9.3. Koordinierung und Informationsaustausch

5.10. ISO 27035-Norm
5.10.1. ISO 27035-Norm. Grundsätze des Vorfallsmanagements
5.10.2. Richtlinien für die Entwicklung eines Vorfallsmanagementplans
5.10.3. Richtlinien für die Reaktion auf Vorfälle

Modul 6. Implementierung von physischen und ökologischen Sicherheitspolitiken im Unternehmen

6.1. Sichere Bereiche
6.1.1. Physischer Sicherheitsbereich
6.1.2. Arbeiten in Sicherheitsbereichen
6.1.3. Sicherheit von Büros, Geschäftsräumen und Ressourcen

6.2. Physische Zugangskontrollen
6.2.1. Richtlinien zur physischen Zugangskontrolle
6.2.2. Physische Zugangskontrollsysteme

6.3. Schwachstellen beim physischen Zugang
6.3.1. Die wichtigsten physischen Schwachstellen
6.3.2. Umsetzung von Schutzmaßnahmen

6.4. Physiologische biometrische Systeme
6.4.1. Fingerabdruck
6.4.2. Gesichtserkennung
6.4.3. Iris- und Retina-Erkennung
6.4.4. Andere physiologische biometrische Systeme

6.5. Verhaltensbiometrische Systeme
6.5.1. Erkennung von Unterschriften
6.5.2. Erkennung von Schriftzeichen
6.5.3. Spracherkennung
6.5.4. Andere biometrische Verhaltenssysteme

6.6. Risikomanagement in der Biometrie
6.6.1. Implementierung biometrischer Systeme
6.6.2. Schwachstellen biometrischer Systeme

6.7. Implementierung von Richtlinien in Hosts
6.7.1. Installation der Verkabelung, Bereitstellung und Sicherheit
6.7.2. Platzierung der Geräte
6.7.3. Verlassen der Geräte außerhalb des Gebäudes
6.7.4. Unbeaufsichtigte Computerausrüstung und Sicherungspolitik beim Verlassen des Arbeitsplatzes

6.8. Umweltschutz
6.8.1. Feuerschutzsysteme
6.8.2. Schutzsysteme bei Erschütterungen
6.8.3. Erdbebenschutzsysteme

6.9. Sicherheit von Datenverarbeitungszentren
6.9.1. Sicherheitstüren
6.9.2. Videoüberwachungssysteme (CCTV)
6.9.3. Sicherheitskontrolle

6.10. Internationale Vorschriften zur physischen Sicherheit
6.10.1. IEC 62443-2-1 (europäisch)
6.10.2. NERC CIP-005-5 (USA)
6.10.3. NERC CIP-014-2 (USA)

Modul 7. Richtlinien für sichere Kommunikation im Unternehmen

7.1. Verwaltung der Netzwerksicherheit
7.1.1. Netzwerkkontrolle und -überwachung
7.1.2. Netzwerk-Trennung
7.1.3. Netzwerk-Sicherheitssysteme

7.2. Sichere Kommunikationsprotokolle
7.2.1. TCP/IP-Modell
7.2.2. IPSEC-Protokoll
7.2.3. TLS-Protokoll

7.3. TLS 1.3 Protokoll
7.3.1. Phasen eines TLS1.3-Prozesses
7.3.2. *Handshake*-Protokoll
7.3.3. Registrierungsprotokoll
7.3.4. Unterschiede zu TLS 1.2

7.4. Kryptographische Algorithmen
7.4.1. In der Kommunikation verwendete kryptographische Algorithmen
7.4.2. *Cipher-Suites*
7.4.3. Erlaubte kryptographische Algorithmen für TLS 1.3

7.5. Digest-Funktionen
7.5.1. Digest-Funktionen
7.5.2. MD6
7.5.3. SHA

7.6. PKI. Infrastruktur für den öffentlichen Schlüssel
7.6.1. PKI und ihre Einrichtungen
7.6.2. Digitales Zertifikat
7.6.3. Arten von digitalen Zertifikaten

7.7. Tunnel- und Transportkommunikation
7.7.1. Tunnel-Kommunikation
7.7.2. Transport-Kommunikation
7.7.3. Verschlüsselte Tunnel-Implementierung

7.8. SSH. *Secure Shell*
7.8.1. SSH. Sichere Kapsel
7.8.2. Betrieb von SSH
7.8.3. SSH-Tools

7.9. Prüfung kryptographischer Systeme
7.9.1. Prüfung der Integrität
7.9.2. Testen von kryptographischen Systemen

7.10. Kryptografische Systeme
7.10.1. Schwachstellen in kryptographischen Systemen
7.10.2. Kryptografische Sicherheitsvorkehrungen

Modul 8. Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen

8.1. *System Hacking*
8.1.1. Risiken und Schwachstellen
8.1.2. Gegenmaßnahmen

8.2. DoS in Dienstleistungen
8.2.1. Risiken und Schwachstellen
8.2.2. Gegenmaßnahmen

8.3. *Session Hijacking*
8.3.1. Der *Hijacking*-Prozess
8.3.2. Gegenmaßnahmen zum *Hijacking*

8.4. Umgehung von IDS, Firewalls und Honeypots
8.4.1. Umgehungstechniken
8.4.2. Implementierung von Gegenmaßnahmen

8.5. *Hacking Web Servers*
8.5.1. Angriffe auf Webserver
8.5.2. Implementierung von Abwehrmaßnahmen

8.6. *Hacking Web Applications*
8.6.1. Angriffe auf Webanwendungen
8.6.2. Implementierung von Verteidigungsmaßnahmen

8.7. *Hacking Wireless Networks*
8.7.1. Schwachstellen im Wifi-Netzwerk
8.7.2. Implementierung von Verteidigungsmaßnahmen

8.8. *Hacking Mobile Platforms*
8.8.1. Schwachstellen von mobilen Plattformen
8.8.2. Implementierung von Gegenmaßnahmen

8.9. *Ramsonware*
8.9.1. Schwachstellen, die *Ramsonware* verursachen
8.9.2. Implementierung von Gegenmaßnahmen

8.10. *Social Engineering*
8.10.1. Arten von *Social Engineering*
8.10.2. Gegenmaßnahmen für *Social Engineering*

Modul 9. Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme

9.1. Richtlinien für die Überwachung von Informationssystemen
9.1.1. System-Überwachung
9.1.2. Metriken
9.1.3. Arten von Metriken

9.2. Auditing und Logging in Systemen
9.2.1. Auditing und Logging in Systemen
9.2.2. Auditing und Logging in Windows
9.2.3. Auditing und Logging in Linux

9.3. SNMP-Protokoll. *Simple Network Management Protocol*
9.3.1. SNMP-Protokoll
9.3.2. SNMP-Betrieb
9.3.3. SNMP-Tools

9.4. Netzwerk-Überwachung
9.4.1. Netzwerküberwachung in Kontrollsystemen
9.4.2. Überwachungstools für Kontrollsysteme

9.5. Nagios. System zur Netzwerküberwachung
9.5.1. Nagios
9.5.2. Betrieb von Nagios
9.5.3. Installieren von Nagios

9.6. Zabbix. System zur Netzwerküberwachung
9.6.1. Zabbix
9.6.2. Betrieb von Zabbix
9.6.3. Installieren von Zabbix

9.7. Cacti. System zur Netzwerküberwachung
9.7.1. Cacti
9.7.2. Betrieb von Cacti
9.7.3. Installation von Cacti

9.8. Pandora. System zur Netzwerküberwachung
9.8.1. Pandora
9.8.2. Betrieb von Pandora
9.8.3. Installation von Pandora

9.9. SolarWinds. System zur Netzwerküberwachung
9.9.1. SolarWinds
9.9.2. Betrieb von SolarWinds
9.9.3. Installation von SolarWinds

9.10. Regelungen zur Überwachung
9.10.1. CIS-Kontrollen zur Prüfung und Registrierung
9.10.2. NIST 800-123 (USA)

Modul 10. Praktische Sicherheitspolitiken für die Notfallwiederherstellung

10.1. DRP. *Disaster Recovery Plan*
10.1.1. Zweck eines DRP
10.1.2. Vorteile eines DRP
10.1.3. Konsequenzen, wenn Sie keinen DRP haben und diesen nicht auf dem neuesten Stand halten

10.2. Leitfaden für die Definition eines DRP (*Disaster Recovery Plan*)
10.2.1. Umfang und Ziele
10.2.2. Entwurf der Wiederherstellungsstrategie
10.2.3. Zuweisung von Rollen und Verantwortlichkeiten
10.2.4. Inventarisierung von Hardware, Software und Diensten
10.2.5. Toleranz für Ausfallzeiten und Datenverluste
10.2.6. Festlegen der spezifischen Arten von DRP, die erforderlich sind
10.2.7. Umsetzung eines Plans zur Fortbildung, Sensibilisierung und Kommunikation

10.3. Umfang und Ziele eines DRP (*Disaster Recovery Plan*)
10.3.1. Sicherstellung der Reaktionsfähigkeit
10.3.2. Technologische Komponenten
10.3.3. Umfang der Kontinuitätspolitik

10.4. Entwurf einer DRP-Strategie (*Disaster Recovery*)
10.4.1. Disaster-Recovery-Strategie
10.4.2. Budget
10.4.3. Personelle und materielle Ressourcen
10.4.4. Gefährdete Managementpositionen
10.4.5. Technologie
10.4.6. Daten

10.5. Kontinuität der Informationsprozesse
10.5.1. Planung der Kontinuität
10.5.2. Implementierung der Kontinuität
10.5.3. Überprüfung der Kontinuitätsbewertung

10.6. Umfang eines BCP (*Business Continuity Plan*)
10.6.1. Bestimmung der kritischsten Prozesse
10.6.2. Asset-basierter Ansatz
10.6.3. Prozessorientierter Ansatz

10.7. Implementierung von gesicherten Geschäftsprozessen
10.7.1. Vorrangige Aktivitäten (PA)
10.7.2. Ideale Wiederherstellungszeiten (IRT)
10.7.3. Überlebensstrategien

10.8. Analyse der Organisation
10.8.1. Sammeln von Informationen
10.8.2. Analyse der geschäftlichen Auswirkungen (BIA)
10.8.3. Organisatorische Risikoanalyse

10.9. Reaktion auf Eventualitäten
10.9.1. Krisenplan
10.9.2. Wiederherstellungspläne für das Betriebsumfeld
10.9.3. Verfahren für technische Arbeiten oder Zwischenfälle

10.10. Internationale Norm ISO 27031 BCP
10.10.1. Ziele
10.10.2. Begriffe und Definitionen
10.10.3. Operation


main.cpp

07

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"

Die TECH Business School verwendet die Fallstudie, um alle Inhalte zu kontextualisieren.

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"

Dieses Programm bereitet Sie darauf vor, geschäftliche Herausforderungen in einem unsicheren Umfeld zu meistern und Ihr Unternehmen erfolgreich zu machen.

Unser Programm bereitet Sie darauf vor, sich neuen Herausforderungen in einem unsicheren Umfeld zu stellen und in Ihrer Karriere erfolgreich zu sein.

Eine innovative und andersartige Lernmethode

Dieses TECH-Programm ist eine intensive Spezialisierung, die von Grund auf neu geschaffen wurde, um Managern Herausforderungen und Geschäftsentscheidungen auf höchstem Niveau zu bieten, sowohl auf nationaler als auch auf internationaler Ebene. 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 geschäftliche Realität berücksichtigt wird.

> *Sie werden durch gemeinschaftliche Aktivitäten und reale Fälle lernen, komplexe Situationen in realen Geschäftsumgebungen zu lösen"*

Die Fallmethode ist das am weitesten verbreitete Lernsystem an den besten Business Schools 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 werden wir bei der Fallmethode konfrontiert, einer handlungsorientierten Lernmethode. Während des gesamten Programms werden die Studenten mit mehreren realen Fällen konfrontiert. Sie müssen ihr gesamtes Wissen integrieren, recherchieren, argumentieren und ihre Ideen und Entscheidungen verteidigen.

Relearning Methodology

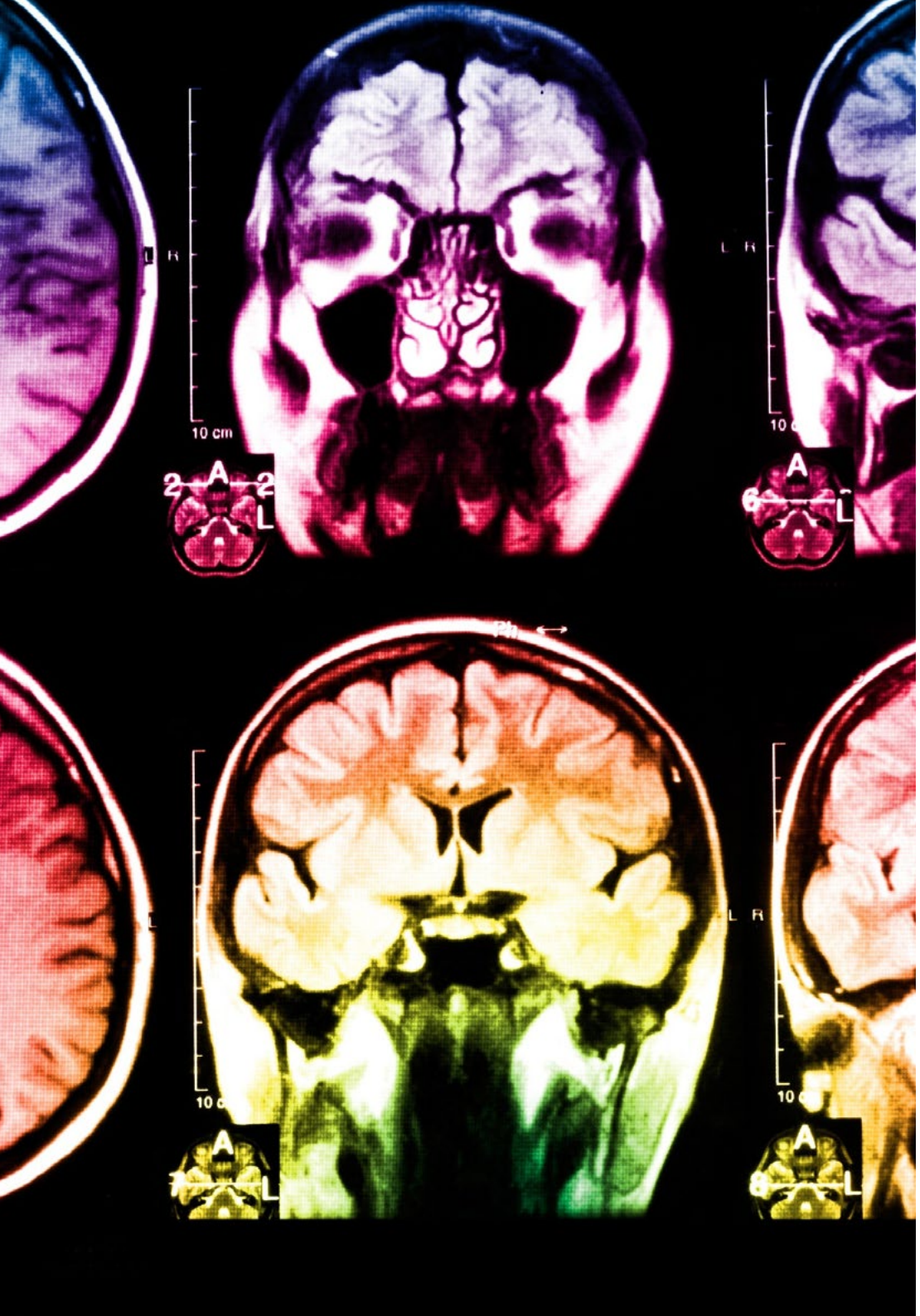
TECH kombiniert die Methodik der Fallstudien effektiv mit einem 100%igen Online-Lernsystem, das auf Wiederholung basiert und in jeder Lektion verschiedene didaktische Elemente kombiniert.

Wir ergänzen die Fallstudie mit der besten 100%igen Online-Lehrmethode: Relearning.

Unser Online-System ermöglicht es Ihnen, Ihre Zeit und Ihr Lerntempo zu organisieren und an Ihren Zeitplan anzupassen. Sie können die Inhalte von jedem festen oder mobilen Gerät mit Internetanschluss abrufen.

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 Wirtschaftshochschule ist die einzige spanischsprachige Schule, 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 kombinieren wir jedes dieser Elemente konzentrisch. 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.

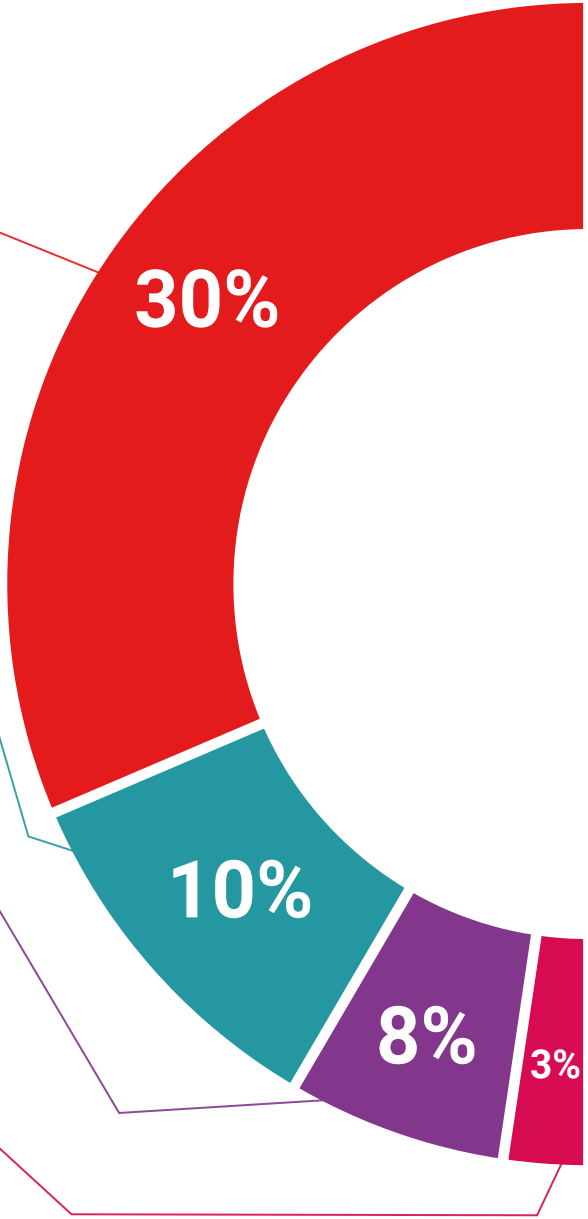
Das sogenannte Learning from an Expert festigt das Wissen und das Gedächtnis und schafft Vertrauen für zukünftige schwierige Entscheidungen.

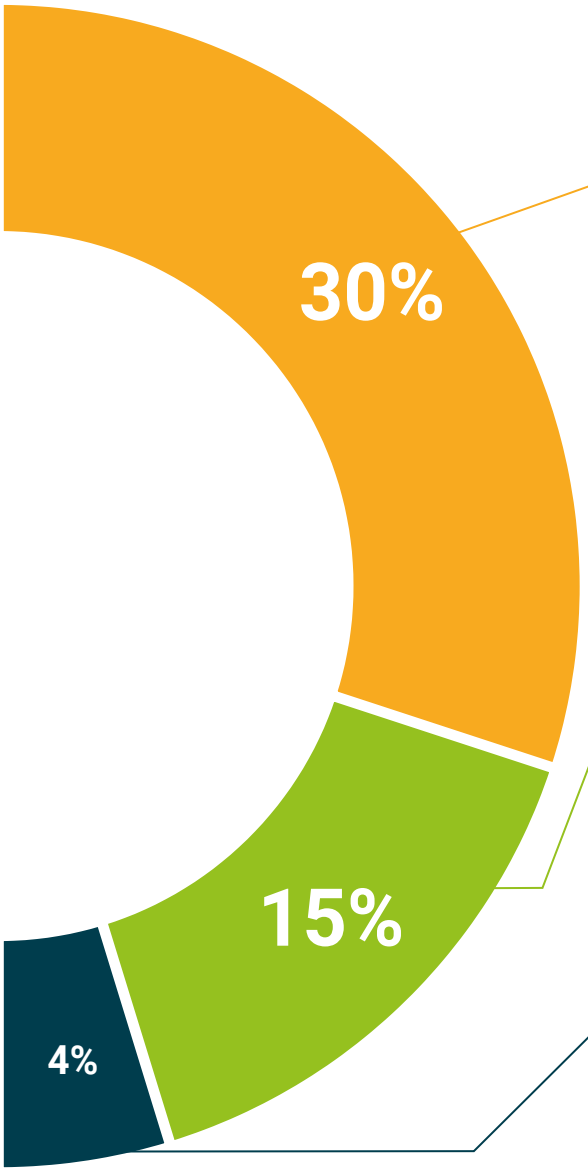
Übungen zu Managementfähigkeiten

Sie werden Aktivitäten durchführen, um spezifische Managementfähigkeiten in jedem Fachbereich zu entwickeln. Übungen und Aktivitäten zum Erwerb und zur Entwicklung der Fähigkeiten und Fertigkeiten, die ein leitender Angestellter 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. Fälle, die von den besten Experten in Senior Management der internationalen Szene präsentiert, analysiert und betreut werden.

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.

08

Profil unserer Studenten

Der Executive Master richtet sich an Hochschulabsolventen, die zuvor einen Abschluss in einem der folgenden Bereiche erworben haben: Sozial- und Rechtswissenschaften, Verwaltung und Wirtschaft.

Die Vielfalt der Teilnehmer mit unterschiedlichen akademischen Profilen und mehreren Nationalitäten macht den multidisziplinären Ansatz dieses Programms aus.

Der Executive Master steht auch Berufstätigen mit zwei Jahren Berufserfahrung im Bereich des *Cybersecurity Policy Management* offen, selbst wenn sie einen Hochschulabschluss in einem beliebigen Bereich haben.

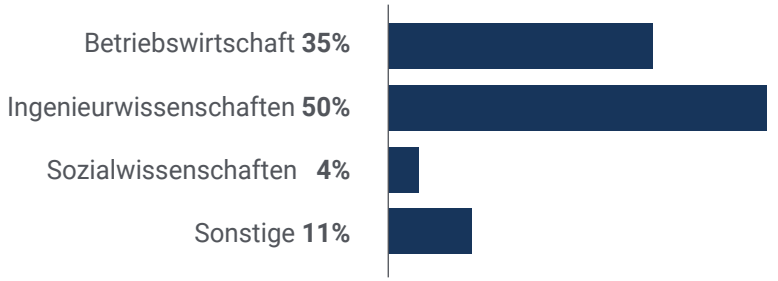
Wenn Sie Ihre berufliche Karriere mit qualitativ hochwertigem Wissen auf der Grundlage der aktuellsten Realität der Cybersicherheit vorantreiben möchten, schreiben Sie sich jetzt für dieses Programm ein"

Durchschnittliches Alter

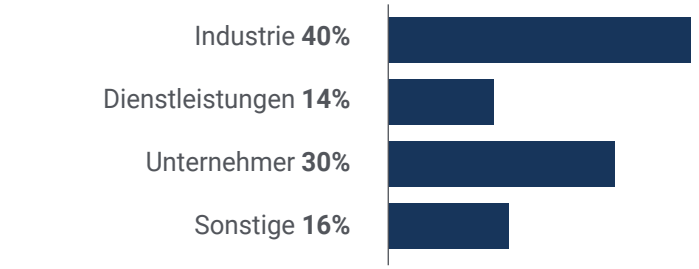
Zwischen **35** und **45** Jahren

Jahre der Erfahrung

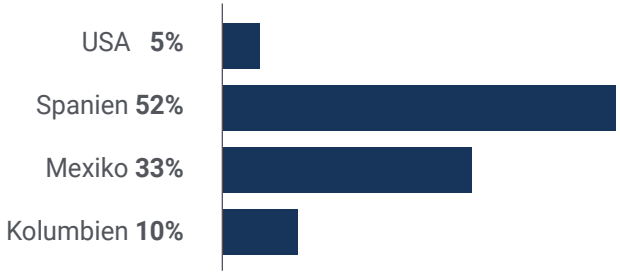
Ausbildung



Akademisches Profil



Geografische Verteilung



Gabriel Gutiérrez Gómez

Leiter der Abteilung Cybersicherheit

"Nachdem wir in unserem Unternehmen einen schweren Cyberangriff erlitten hatten, legten wir mehr Wert auf den Schutz unserer Datenbanken und widmeten eine kleine Abteilung diesem Thema. Dank dieses Programms war ich in der Lage, diese Bemühungen zu leiten und die Cybersicherheitspolitik zu entwerfen und umzusetzen, die wir heute noch anwenden"

09

Kursleitung

Um die höchstmögliche Qualität aller didaktischen Inhalte zu erreichen, hat TECH eine Gruppe von Dozenten ausgewählt, die Experten in den verschiedenen Bereichen der Cybersicherheit sind. So hat der Manager Zugang zu einem Lehrplan, der von Fachleuten mit umfassender Erfahrung im Management von Cybersicherheitsmaßnahmen verfasst wurde, die mit ihrer ausgeprägten praktischen Vision für jedes der behandelten Themen zur gesamten Theorie beigetragen haben.

Sie werden von einem Dozententeam unterstützt, das über Erfahrungen in der Unternehmensführung und im komplexen IT-Sicherheitsmanagement verfügt und sich mit Themen wie der Wartung von Informationssystemen, forensischen Analysen und Hijacking beschäftigt"

Leitung

Fr. Fernández Sapena, Sonia

- Ausbilderin für Computersicherheit und Ethical Hacking am Nationalen Referenzzentrum von Getafe für Informatik und Telekommunikation, 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, Madrid
- Masterstudiengang in DevOps: Docker und Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies E-Council

Professoren

Hr. Solana Villarias, Fabián

- Berater für Informationstechnologie
- Entwickler und Administrator von Umfragediensten bei Investigación, Planificación y Desarrollo, SA
- Spezialist für Finanzmärkte und IT-Systempflege bei Iberia Financial Software
- Webentwickler und Spezialist für Barrierefreiheit bei Indra
- Hochschulabschluss in Systemtechnik an der Universität von Wales/CESINE
- Universitätskurs in technischem Ingenieurwesen in *Computer Systems Engineering* an der Universität von Wales/CESINE

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

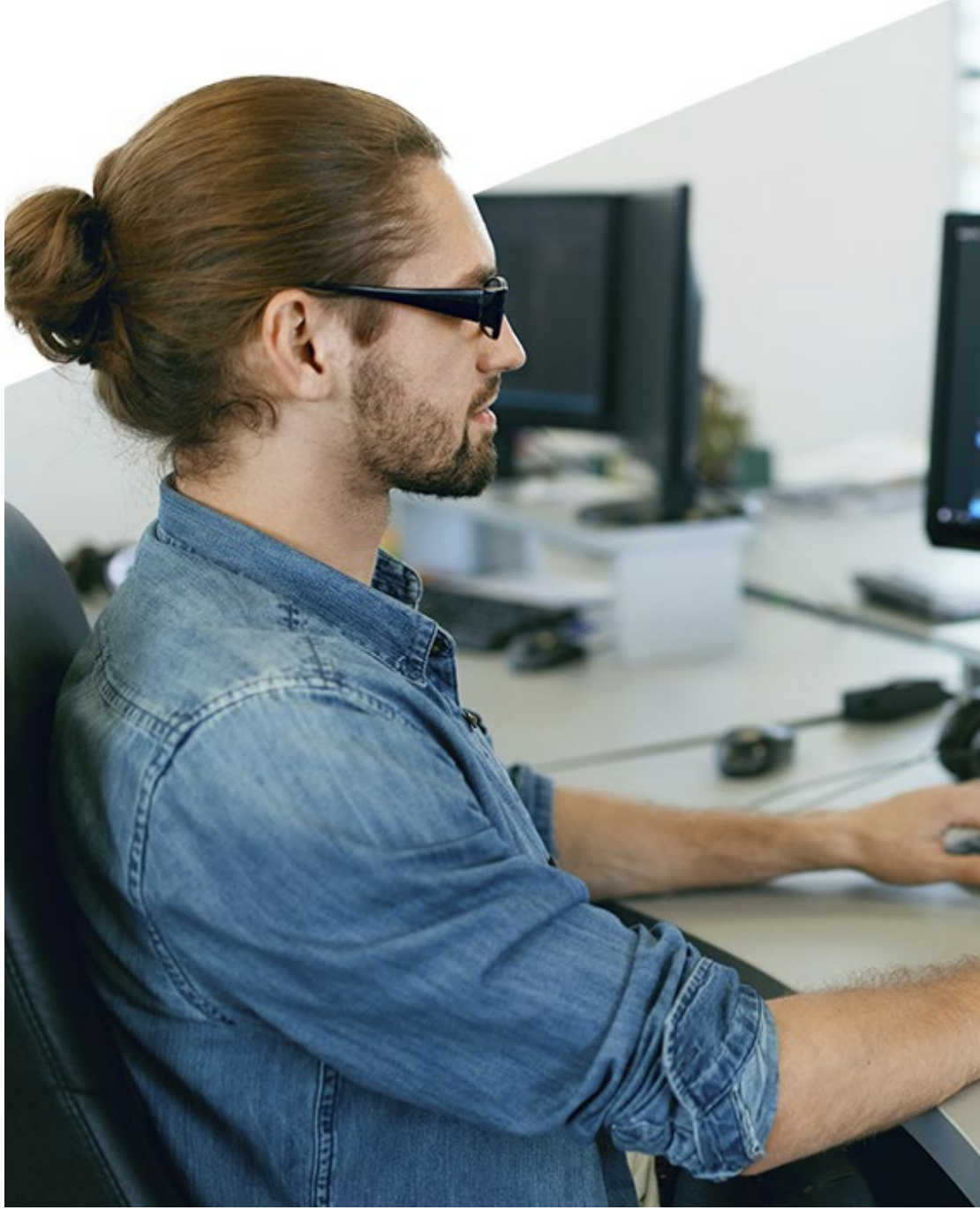
- Computer-Ingenieur
- Mikroinformatiker, Netzwerktechniker und Sicherheitstechniker bei Cas-Training
- Entwickler für Webdienste, CMS, E-Commerce, UI und UX bei Fersa Reparaciones
- Manager für Webdienste, Inhalte, Mail und DNS bei Oropesia Web & Network
- Grafiker und Designer für Webanwendungen bei 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

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

Hr. Peralta Alonso, Jon

- Senior Consultant - Datenschutz und Cybersicherheit, Altia
- Rechtsanwalt/Rechtsbeistand, Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Rechtsberater/Praktikant, Professionelles Büro: Oscar Padura
- Hochschulabschluss in Jura, Öffentliche Universität des Baskenlandes
- Masterstudiengang in Datenschutzbeauftragter, EIS Innovative School
- Masterstudiengang in Rechtswissenschaften, Öffentliche Universität des Baskenlandes
- Masterstudiengang in Zivilprozessrecht, Internationale Universität Isabel I de Castilla
- Dozent im Masterstudiengang für Datenschutz, Cybersicherheit und IKT-Recht



TECH hat das Dozententeam für dieses Programm sorgfältig ausgewählt, damit Sie von den besten Spezialisten von heute lernen können"

10

Auswirkung auf Ihre Karriere

TECH ist sich der Anstrengungen bewusst, die Manager auf sich nehmen müssen, um ein Studium mit diesen Merkmalen zu absolvieren. Daher legt TECH besonderen Wert darauf, dass alle angebotenen Inhalte und Lehrmaterialien den höchsten Qualitätsstandards entsprechen. Die Multimedia-Bibliothek, zu der sie Zugang haben, ist eine außergewöhnliche Referenz im Bereich der Cybersicherheit und kann sogar vollständig heruntergeladen werden, um sie nach Abschluss des Studiums weiter zu verwenden.

Sie erhalten den wirtschaftlichen und beruflichen Vorsprung, den Sie anstreben, dank der kontinuierlichen Unterstützung durch ein Team von Dozenten und Experten, die sich dafür einsetzen, Sie an die Spitze der Cybersicherheit zu bringen"

Schreiben Sie sich jetzt für diesen Executive Master ein und warten Sie nicht länger, um Ihr Umfeld positiv zu verändern.

Sind Sie bereit, den Sprung zu wagen? Es erwartet Sie eine hervorragende berufliche Weiterentwicklung.

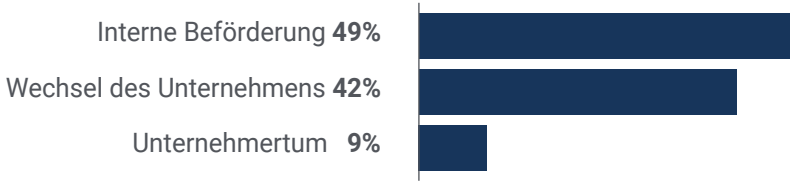
Der Executive Master in Verwaltung der Cybersicherheitspolitik im Unternehmen der TECH ist ein intensives Programm, das den Studenten auf die Herausforderungen und Geschäftsentscheidungen im Bereich Cybersecurity vorbereitet. Sein Hauptziel ist es, seine persönliche und berufliche Entwicklung zu fördern und ihm dabei zu helfen, erfolgreich zu sein.

Wenn der Student sich verbessern, eine positive Veränderung auf beruflicher Ebene herbeiführen und sich mit den Besten vernetzen möchte, ist dieses Programm genau das Richtige für ihn.

Dank der pädagogischen Methodik von TECH werden Sie in kürzerer Zeit, als Sie denken, die von Ihnen angestrebte berufliche Verbesserung erreichen.

Zeitpunkt des Wandels

Art des Wandels



Gehaltsverbesserung

Der Abschluss dieses Programms bedeutet für unsere Studenten eine Gehaltserhöhung von mehr als **25,22%**

11

Vorteile für Ihr Unternehmen

Der Executive Master in Verwaltung der Cybersicherheitspolitik im Unternehmen trägt dazu bei, die Talente der Organisation durch die Fortbildung von hochrangigen Führungskräften auf ihr maximales Potenzial zu bringen.

Die Teilnahme an diesem Executive Master ist eine einmalige Gelegenheit, ein leistungsfähiges Kontaktnetz zu knüpfen, um künftige Geschäftspartner, Kunden oder Lieferanten zu finden.

Cyber-Bedrohungen sind eine der größten Schwachstellen, denen Unternehmen aller Art und Größe ausgesetzt sind. Spezialisieren Sie sich auf den Bereich mit den größten Zukunftsaussichten"

Die Entwicklung und Bindung von Talenten in Unternehmen ist die beste langfristige Investition.

01

Wachsendes Talent und intellektuelles Kapital

Die Fachkraft wird neue Konzepte, Strategien und Perspektiven in das Unternehmen einbringen, die relevante Veränderungen bewirken können.

02

Bindung von Führungskräften mit hohem Potenzial und Vermeidung der Abwanderung von Fachkräften

Dieses Programm stärkt die Verbindung zwischen dem Unternehmen und der Fachkraft und eröffnet neue Wege für die berufliche Entwicklung innerhalb des Unternehmens.

03

Aufbau von Akteuren des Wandels

Die Fachkraft wird in der Lage sein, in unsicheren und krisenhaften Zeiten Entscheidungen zu treffen und der Organisation zu helfen, Hindernisse zu überwinden.

04

Verbesserte Möglichkeiten zur internationalen Expansion

Dank dieses Programms wird das Unternehmen mit den wichtigsten Märkten der Weltwirtschaft in Kontakt kommen.

05

Entwicklung eigener Projekte

Die Fachkraft kann an einem realen Projekt arbeiten oder neue Projekte im Bereich FuE oder *Business Development* ihres Unternehmens entwickeln.

06

Gesteigerte Wettbewerbsfähigkeit

Dieses Programm wird die Fachkräfte mit den Fähigkeiten ausstatten, neue Herausforderungen anzunehmen und so das Unternehmen voranzubringen.

12

Qualifizierung

Der Executive Master in Verwaltung der Cybersicherheitspolitik im Unternehmen 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 **Executive Master in Verwaltung der Cybersicherheitspolitik im Unternehmen** 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: **Executive Master in Verwaltung der Cybersicherheitspolitik im Unternehmen**

Anzahl der offiziellen Arbeitsstunden: **1.500 Std.**


tech technologische universität

Verleiht dieses

DIPLOM

an

Herr/Frau _____, mit Ausweis-Nr. _____

Für den erfolgreichen Abschluss und die Akkreditierung des Programms

PRIVATER MASTERSTUDIENGANG

in

Verwaltung der Cybersicherheitspolitik im Unternehmen

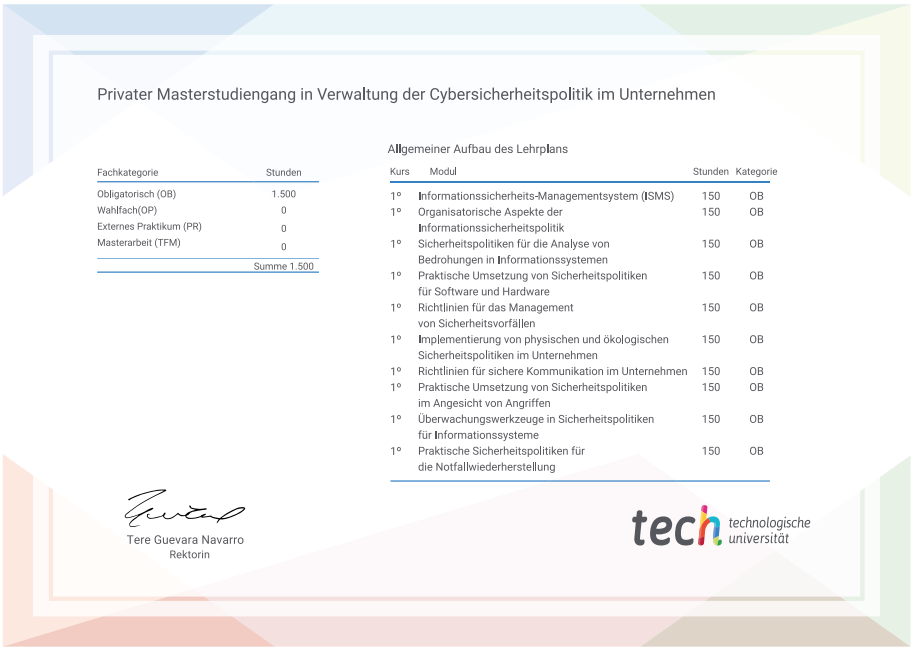
Es handelt sich um einen von dieser Universität verliehenen Abschluss, mit einer Dauer von 1.500 Stunden, mit Anfangsdatum tt/mm/jjjj und Enddatum tt/mm/jjjj.

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


Privater Masterstudiengang in Verwaltung der Cybersicherheitspolitik im Unternehmen

Fachkategorie	Stunden
Obligatorisch (OB)	1.500
Wahlfach(OP)	0
Externes Praktikum (PR)	0
Masterarbeit (TFM)	0
	Summe 1.500

Allgemeiner Aufbau des Lehrplans

Kurs	Modul	Stunden	Kategorie
1°	Informationssicherheits-Managementsystem (ISMS)	150	OB
1°	Organisatorische Aspekte der Informationssicherheitspolitik	150	OB
1°	Sicherheitspolitiken für die Analyse von Bedrohungen in Informationssystemen	150	OB
1°	Praktische Umsetzung von Sicherheitspolitiken für Software und Hardware	150	OB
1°	Richtlinien für das Management von Sicherheitsvorfällen	150	OB
1°	Implementierung von physischen und ökologischen Sicherheitspolitiken im Unternehmen	150	OB
1°	Richtlinien für sichere Kommunikation im Unternehmen	150	OB
1°	Praktische Umsetzung von Sicherheitspolitiken im Angesicht von Angriffen	150	OB
1°	Überwachungswerkzeuge in Sicherheitspolitiken für Informationssysteme	150	OB
1°	Praktische Sicherheitspolitiken für die Notfallwiederherstellung	150	OB

Tere Guevara Navarro
Rektorin

tech technologische universität

*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

Executive Master

Verwaltung der Cybersicherheitspolitik im Unternehmen

- **Modalität: online**
- Dauer: **12 Monate**
- Qualifizierung: **TECH Technologische Universität**
- Aufwand: **16 Std./Woche**
- Zeitplan: **in Ihrem eigenen Tempo**
- Prüfungen: **online**

Executive Master

Verwaltung der Cybersicherheitspolitik im Unternehmen

tech technologische universität