Esperto Universitario

Amministrazione della Sicurezza nelle Tecnologie di Informazione

tech università tecnologica

tech università tecnologica

Esperto Universitario
Amministrazione della Sicurezza nelle Tecnologie di Informazione

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Università Tecnologica**
- Dedizione: **16 ore/settimana**
- Orario: **a scelta**
- Esami: **online**

Accesso al sito web: www.techtitute.com/it/informatica/specializzazione/specializzazione-amministrazione-sicurezza-tecnologie-informazione

Indice

01

Presentazione

L'integrazione delle tecnologie informatiche in molte aziende ha avuto un effetto collaterale: i rischi per la sicurezza informatica sono aumentati. Ora le aziende devono stare attente ai vari attacchi che possono compromettere il loro corretto funzionamento e i loro servizi. È quindi essenziale avere in azienda uno specialista responsabile della gestione della sicurezza di queste tecnologie. Questo programma offre ai professionisti l'opportunità di conoscere i metodi di protezione informatica più avanzati in questo settore, approfondendo aspetti quali la valutazione del rischio in base a parametri aziendali, la gestione delle identità e degli accessi o i test di intrusione.

Sempre più aziende hanno bisogno di specialisti nella gestione della sicurezza informatica. Questo programma ti permetterà di progredire a livello professionale, approfondendo temi come la pianificazione della continuità operativa legata alla sicurezza"

È un dato di fatto che non esiste quasi più alcuna azienda che non utilizzi strumenti digitali e informatici nei propri processi interni. Attività e operazioni come l'identificazione dei dipendenti, i sistemi logistici o i contatti con i fornitori e i clienti sono oggi realizzati principalmente attraverso le tecnologie dell'informazione. Tuttavia, queste tecnologie devono essere oggetto di una progettazione e di un monitoraggio adeguati, poiché possono essere sfruttate per ottenere dati o per violare l'accesso ad aspetti sensibili dell'azienda.

Per questo motivo, lo specialista in amministrazione della sicurezza è un profilo sempre più ricercato e non può essere rivestito da uno specialista IT qualsiasi. Richiede infatti una conoscenza altamente aggiornata che tenga conto degli ultimi sviluppi in materia di cybersecurity. Pertanto, questo Esperto Universitario è stato ideato per offrire ai professionisti i più recenti progressi in questo settore, approfondendo argomenti quali gli audit di sicurezza, la sicurezza dei dispositivi terminali o la risposta più efficace a diversi incidenti.

Questo programma è sviluppato in un formato 100% online che si adatta agli impegni del professionista, consentendogli di studiare quando, dove e come vuole. Possiede inoltre un personale docente di grande prestigio nel campo della cybersecurity, che si avvale di numerose risorse multimediali per rendere il processo di apprendimento confortevole, veloce ed efficace.

Puesto **Esperto Universitario in Amministrazione della Sicurezza nelle Tecnologie di Informazione** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- Sviluppo di casi pratici presentati da esperti in Informatica e Cybersecurity
- Contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni scientifiche e pratiche sulle discipline essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- Speciale enfasi sulle metodologie innovative
- Lezioni teoriche, domande all'esperto e/o al tutore, forum di discussione su questioni controverse e compiti di riflessione individuale
- Disponibilità di accesso ai contenuti da qualsiasi dispositivo fisso o portatile con una connessione internet

Questo programma ti permetterà di approfondire aspetti come il ciclo di vita di un piano di continuità operativa o la gestione delle vulnerabilità"

TECH mette a disposizione le migliori risorse multimediali: casi di studio, attività teorico-pratiche, video, riassunti interattivi, ecc. Tutto ciò per rendere il processo di apprendimento agile e per sfruttarne al meglio ogni minuto"

Sarai in grado di affrontare in modo appropriato tutti i tipi di minacce legate alla cybersecurity. Iscriviti e diventa un ottimo specialista.

Studia al tuo ritmo, senza interruzioni e orari rigidi: il metodo di insegnamento di TECH offre il massimo della comodità.

Il personale docente del programma comprende rinomati specialisti che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

I contenuti multimediali, sviluppati in base alle ultime tecnologie educative, forniranno al professionista un apprendimento coinvolgente e localizzato, ovvero inserito in un contesto reale.

La creazione di questo programma è incentrata sull'Apprendimento Basato su Problemi, mediante il quale lo specialista deve cercare di risolvere le diverse situazioni che gli si presentano durante il corso. Lo studente potrà usufruire di un innovativo sistema di video interattivi creati da esperti di rinomata fama.

02

Obiettivi

Tenendo conto della crescente complessità del campo della cybersecurity, l'obiettivo principale di questo Esperto Universitario in Amministrazione della Sicurezza nelle Tecnologie di Informazione è quello di far conoscere al professionista gli sviluppi più importanti in questo campo. In questo modo, potrà diventare un grande specialista del settore, in grado di lavorare gestendo e dirigendo l'area della cybersecurity di aziende di ogni settore.

TECH ti aiuta a raggiungere i tuoi obiettivi grazie a questo programma, grazie al quale potrai aspirare a importanti posizioni professionali nelle principali aziende a livello nazionale e internazionale"

Obiettivi generali

- Sviluppare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
- Identificare gli elementi chiave che compongono un SGSI
- Valutare diversi modelli di organizzazione della sicurezza per stabilire il modello più appropriato per l'azienda
- Identificare i quadri normativi applicabili e le relative basi normative
- Analizzare la struttura organizzativa e funzionale di un'area di sicurezza informatica (l'ufficio del CISO)
- Stabilire un programma di verifica che soddisfi le esigenze di autovalutazione della sicurezza informatica all'interno dell'organizzazione
- Sviluppare un programma di analisi e monitoraggio dei punti di vulnerabilità e un piano di risposta agli incidenti di cybersecurity
- Determinare gli elementi di base di un Piano di Continuità Operativa (PCO) utilizzando come base la guida ISO-22301
- Esaminare i rischi derivanti dall'assenza di un Piano di Continuità Operativa
- Analizzare i criteri di successo di un PCO e la sua integrazione in una gestione globale del rischio aziendale
- Concretizzare le fasi di implementazione di un piano di continuità operativa

Obiettivi specifici

Modulo 1. Strutture e modelli per la sicurezza delle informazioni

- Allineare il Master Plan per la sicurezza agli obiettivi strategici dell'organizzazione
- Stabilire un quadro di gestione costante dei rischi come parte integrante del Master Plan sulla sicurezza
- Stabilire gli indicatori appropriati per il monitoraggio della messa in atto del SGSI
- Stabilire una strategia di sicurezza basata sulle policy
- Analizzare gli obiettivi e le procedure associate al piano di sensibilizzazione dei dipendenti, dei fornitori e dei partner
- Identificare, all'interno del quadro normativo, i regolamenti, le certificazioni e le leggi applicabili a ciascuna organizzazione
- Definire gli elementi fondamentali richiesti dallo standard ISO 27001:2013
- Implementare un modello di gestione della privacy in linea con il regolamento europeo GDPR/RGPD

Modulo 2. Gestione della sicurezza IT

- Identificare le diverse componenti che un'area di sicurezza informatica può presentare
- Sviluppare un modello di sicurezza basato su tre linee di difesa
- Presentare i diversi comitati periodici e straordinari in cui è coinvolta l'area della cybersecurity
- Definire gli strumenti tecnologici che integrano le funzioni principali del team operativo di sicurezza (SOC)
- Valutare le misure di controllo dei punti di vulnerabilità appropriate per ogni scenario
- Sviluppare un quadro operativo per la sicurezza basato sul NIST CSF
- Specificare l'ambito dei diversi tipi di verifiche (*Red Team*, Pentesting, Bug Bounty, ecc.)
- Proporre le attività da svolgere dopo un incidente che coinvolge la sicurezza
- Creare un centro di comando per la sicurezza delle informazioni che comprenda tutti i soggetti interessati (autorità, clienti, fornitori, ecc.)

Modulo 3. Piano di continuità operativa associato alla sicurezza

- Presentare gli elementi chiave di ciascuna fase e analizzare le caratteristiche del Piano di Continuità Operativa (PCO)
- Giustificare la necessità di un Piano di Continuità Operativa
- Stabilire le mappe di successo e di rischio per ogni fase del Piano di Continuità Operativa
- Specificare come viene stabilito un piano d'azione per la realizzazione del PCO
- Valutare la completezza di un Piano di Continuità Operativa (PCO)
- Sviluppare l'implementazione di un Piano di Continuità Operativa

Sarai uno dei più grandi specialisti della sicurezza informatica nel tuo settore. Non esitare: iscriviti subito"

03

Direzione del corso

Avere a disposizione i maggiori specialisti mondiali in amministrazione della sicurezza nel campo delle tecnologie dell'informazione è una grande opportunità per il professionista. Questo è precisamente ciò che offre il presente Esperto Universitario, il quale possiede un personale docente composto da prestigiosi ingegneri e informatici che forniranno allo studente le tecniche e le procedure più avanzate per garantire l'adeguata sicurezza interna di un'azienda.

Entrerai in contatto con i principali specialisti di cybersecurity, che ti forniranno tutti gli elementi chiave per lavorare ai massimi livelli in questo settore"

Direzione

Dott. Olalla Bonal, Martín

- Client Technical Specialist Blockchain in IBM
- Architetto *Blockchain*
- Architetto di Infrastrutture nel Settore Bancario
- Gestione di progetti e implementazione di soluzioni
- Tecnico di Elettronica Digitale
- Docente: Training *Hyperledger Fabric* per le aziende
- Docente: Training *Blockchain* per il settore business delle aziende

Personale docentet

Dott. Gozalo Fernández, Juan Luis

- Ingegnere informatico
- Docente Associato di DevOps e Blockchain presso l'UNIR
- Ex-direttore Blockchain DevOps presso Alastria
- Responsabile per lo Sviluppo dell'Applicazione Mobile di Tinkerlink presso Cronos Telecom
- Direttore IT del Banco Santander
- Direttore della Tecnologia di Gestione dei Servizi IT presso Barclays Bank Spagna
- Laurea in Ingegneria Informatica presso l'Università Nazionale di Educazione a Distanza (UNED)

Dott. Embid Ruiz, Mario

- Avvocato specializzato in diritto delle tecnologie dell'informazione e della comunicazione e in protezione dei dati personali
- Responsabile legale di Branddocs, SL, una società di soluzioni tecnologiche di fiducia
- Master in Giurisprudenza e Amministrazione per le Imprese conseguito presso l'Università Rey Juan Carlos
- Master in Nuove tecnologie, Internet e Diritto audiovisivo presso il Centro di Studi Universitari Villanueva e Cremades & Calvo Sotelo

Dott. Rodrigo Estébanez, Juan Manuel

- Fondatore di ISMET TECH S.L
- Laurea in Ingegneria presso l'Università di Valladolid
- Master in Sistemi di Gestione Integrata di CFE-CEU
- ISO 27001 Lead Auditor (IMQ)
- ISO 27001 Lead Auditor (IMQ)
- NATO Standards HPS (OTAN)

04

Struttura e contenuti

Il piano di studi di questo Esperto Universitario in Amministrazione della Sicurezza nelle Tecnologie di Informazione è stato strutturato su 3 moduli che si svolgono durante 450 ore di apprendimento. Durante questo periodo, il professionista approfondirà aspetti rilevanti di questo settore come l'analisi forense, i modelli di sicurezza informatica, il quadro normativo applicabile o la configurazione delle regole di sicurezza della rete, oltre a molte altre questioni.

Avrai a disposizione il programma più completo, presentato attraverso risorse didattiche a cui potrai accedere 24 ore su 24"

Modulo 1. Strutture e modelli per la sicurezza delle informazioni

1.1. Struttura di sicurezza delle informazioni
- 1.1.1. SGSI / PSS
- 1.1.2. Allineamento strategico
- 1.1.3. Gestione del rischio
- 1.1.4. Misurazione della performance

1.2. Modelli di sicurezza delle informazioni
- 1.2.1. In base alle politiche di sicurezza
- 1.2.2. In base agli strumenti di protezione
- 1.2.3. In base alle apparecchiature di lavoro

1.3. Modello di sicurezza. Componenti chiave
- 1.3.1. Identificazione dei rischi
- 1.3.2. Definizione dei controlli
- 1.3.3. Valutazione continua dei livelli di rischio
- 1.3.4. Piano di sensibilizzazione per dipendenti, fornitori, partner, ecc.

1.4. Processo di gestione dei rischi
- 1.4.1. Identificazione delle risorse
- 1.4.2. Identificazione delle minacce
- 1.4.3. Valutazione dei rischi
- 1.4.4. Priorità dei controlli
- 1.4.5. Rivalutazione e rischio residuo

1.5. Processi operativi e sicurezza delle informazioni
- 1.5.1. Processi aziendali
- 1.5.2. Valutazione del rischio in base ai parametri aziendali
- 1.5.3. Analisi dell'impatto aziendale
- 1.5.4. Operazioni aziendali e sicurezza delle informazioni

1.6. Processo di miglioramento continuo
- 1.6.1. Il ciclo di Deming
  - 1.6.1.1. Pianificare
  - 1.6.1.2. Fare
  - 1.6.1.3. Verificare
  - 1.6.1.4. Agire

1.7. Architetture di sicurezza
- 1.7.1. Selezione e omogeneizzazione delle tecnologie
- 1.7.2. Gestione dell'identità. Autenticazione
- 1.7.3. Gestione degli accessi. Autorizzazione
- 1.7.4. Sicurezza dell'infrastruttura di rete
- 1.7.5. Tecnologie e soluzioni di crittografia
- 1.7.6. Sicurezza delle apparecchiature terminali (EDR)

1.8. Quadro normativo
- 1.8.1. Regolamenti settoriali
- 1.8.2. Certificazioni
- 1.8.3. Legislazione

1.9. Standard ISO 27001
- 1.9.1. Implementazione
- 1.9.2. Certificazione
- 1.9.3. Verifiche e penetration test
- 1.9.4. Gestione continua del rischio
- 1.9.5. Classificazione delle informazioni

1.10. Legislazione sulla privacy. RGPD (GDPR)
- 1.10.1. Ambito di applicazione del Regolamento generale sulla protezione dei dati (RGPD)
- 1.10.2. Dati personali
- 1.10.3. Ruoli nel trattamento dei dati personali
- 1.10.4. Diritti ARCO
- 1.10.5. Il DPO. Funzioni

Modulo 2. Gestione della sicurezza IT

2.1. Gestione della sicurezza
- 2.1.1. Operazioni di sicurezza
- 2.1.2. Aspetti giuridici e normativi
- 2.1.3. Abilitazione all'esercizio dell'attività
- 2.1.4. Gestione dei rischi
- 2.1.5. Gestione dell'identità e degli accessi

2.2. Struttura dell'area di sicurezza. L'ufficio del CISO
- 2.2.1. Struttura organizzativa. Posizione del CISO nella struttura
- 2.2.2. Linee di difesa
- 2.2.3. Organigramma dell'ufficio del CISO
- 2.2.4. Gestione del bilancio

2.3. Governance della sicurezza
- 2.3.1. Comitato per la sicurezza
- 2.3.2. Comitato per il monitoraggio dei rischi
- 2.3.3. Comitato per il controllo
- 2.3.4. Comitato per le crisi

2.4. Governance della sicurezza. Funzioni
- 2.4.1. Politiche e standard
- 2.4.2. Piano generale di sicurezza
- 2.4.3. Quadro di controllo
- 2.4.4. Sensibilizzazione e corsi di aggiornamento
- 2.4.5. Sicurezza nella supply chain

2.5. Operazioni di sicurezza
- 2.5.1. Gestione dell'identità e degli accessi
- 2.5.2. Configurazione delle regole di sicurezza della rete. Firewall
- 2.5.3. Gestione di piattaforme IDS/IPS
- 2.5.4. Analisi dei punti deboli

2.6. Quadro di riferimento per la cybersecurity. NIST CSF
- 2.6.1. Metodologia NIST
  - 2.6.1.1. Identificare
  - 2.6.1.2. Proteggere
  - 2.6.1.3. Rilevare
  - 2.6.1.4. Rispondere
  - 2.6.1.5. Recuperare

2.7. Centro Operativo di Sicurezza (SOC). Funzioni
- 2.7.1. Protezione. *Red Team, penetration test, threat intelligence*
- 2.7.2. Rilevamento. SIEM, *user behavior analytics, fraud prevention*
- 2.7.3. Risposta

2.8. Verifiche di sicurezza
- 2.8.1. Penetration test
- 2.8.2. Esercizi di *Red Team*
- 2.8.3. Verifiche del codice sorgente. Sviluppo sicuro
- 2.8.4. Sicurezza dei componenti (*software supply chain*)
- 2.8.5. Analisi forense

2.9. Risposta agli incidenti
- 2.9.1. Preparazione
- 2.9.2. Rilevamento, analisi e reporting
- 2.9.3. Contenimento, eliminazione e recupero
- 2.9.4. Attività in seguito all'incidente
  - 2.9.4.1. Conservazione delle prove
  - 2.9.4.2. Analisi forense
  - 2.9.4.3. Gestire una violazione dei dati
- 2.9.5. Guide ufficiali per la gestione degli incidenti informatici

2.10. Gestione delle vulnerabilità
- 2.10.1. Analisi dei punti deboli
- 2.10.2. Valutazione della vulnerabilità
- 2.10.3. Base di sistema
- 2.10.4. Vulnerabilità 0-day. *Zero-day*

Modulo 3. Piano di continuità operativa associato alla sicurezza

3.1. Piano di Continuità Operativa
- 3.1.1. I piani di Continuità Operativa (PCO)
- 3.1.2. Piano di Continuità Operativa (PCO). Aspetti chiave
- 3.1.3. Piano di Continuità Operativa (PCO) per la valutazione dell'azienda

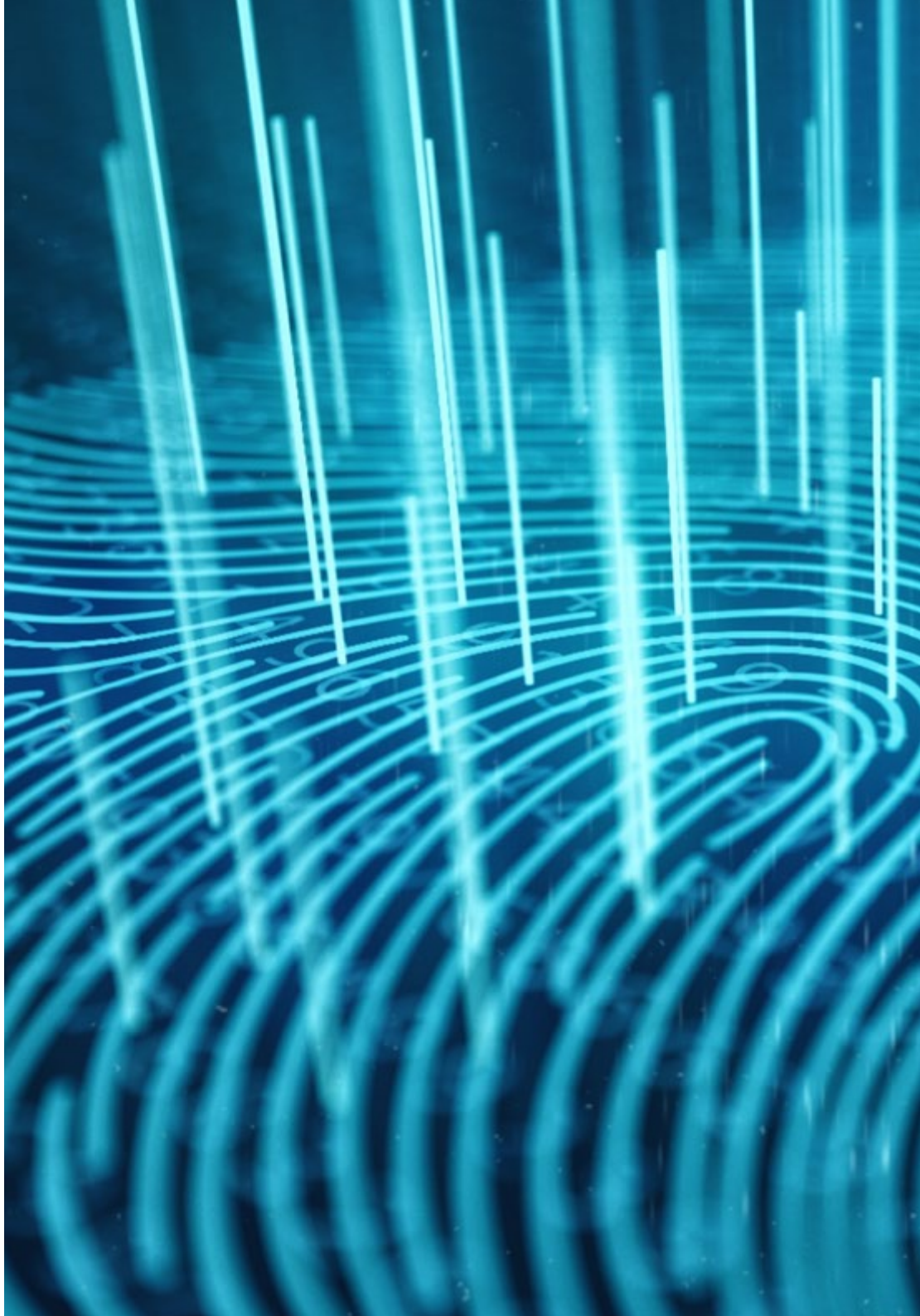
3.2. Parametri in un Piano di Continuità Operativa (PCO)
- 3.2.1. *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO)
- 3.2.2. Tempo massimo tollerabile (MTD)
- 3.2.3. Livelli minimi di recupero (ROL)
- 3.2.4. Obiettivo del punto di recupero (RPO)

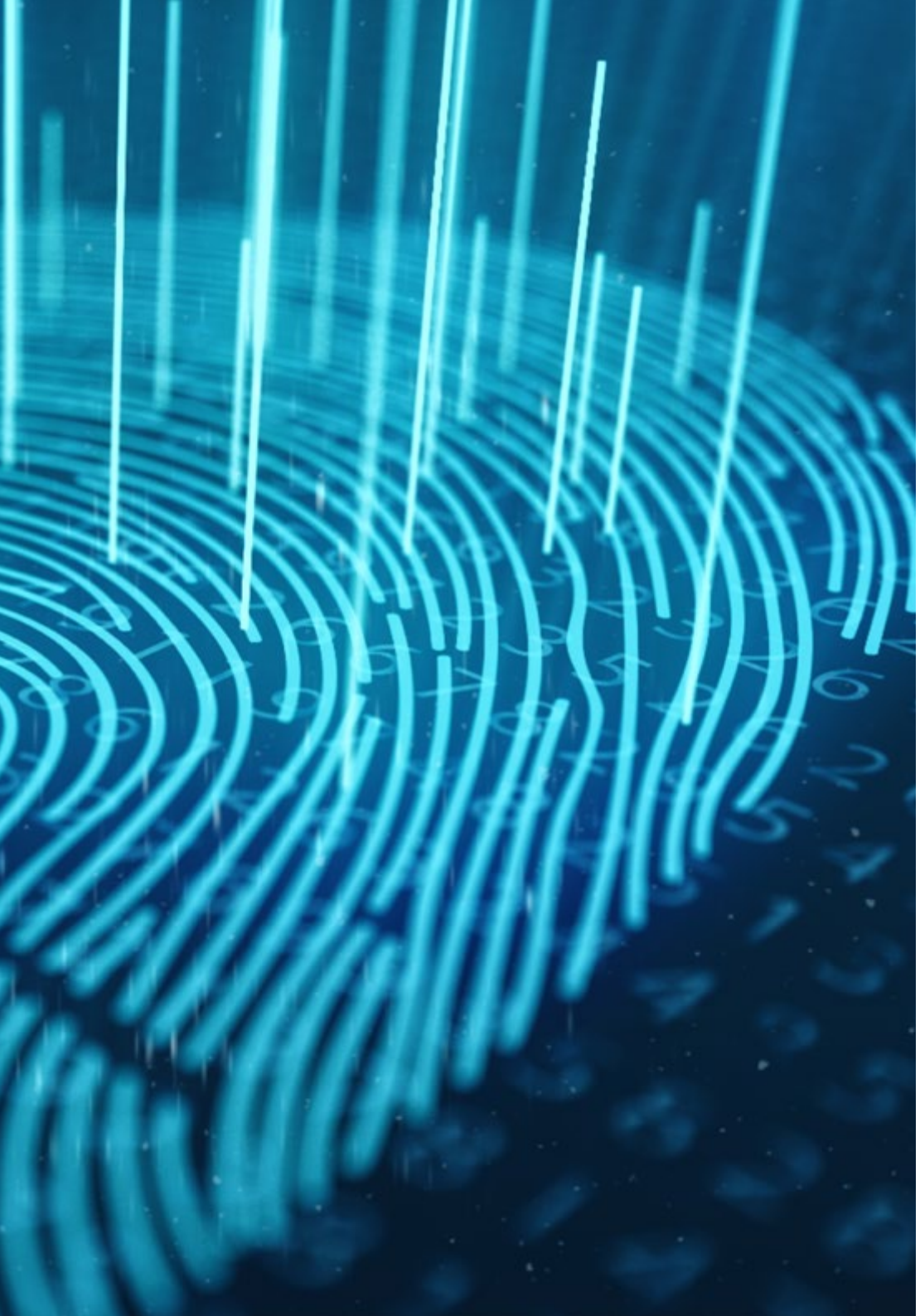
3.3. Progetti di continuità. Tipologia
- 3.3.1. Piano di Continuità Operativa (PCO)
- 3.3.2. Piano di continuità ICT
- 3.3.3. Piano di ripristino in caso di disastro (DRP)

3.4. Gestione dei rischi connessi al PCO
- 3.4.1. Analisi dell'impatto aziendale
- 3.4.2. Vantaggi dell'implementazione di un PCO
- 3.4.3. Mentalità basata sul rischio

3.5. Ciclo di vita di un piano di continuità operativa
- 3.5.1. Fase 1: analisi dell'organizzazione
- 3.5.2. Fase 2: determinazione della strategia di continuità
- 3.5.3. Fase 3: risposta alla contingenza
- 3.5.4. Fase 4: test, manutenzione e revisione

3.6. Fase di analisi organizzativa di un PCO
- 3.6.1. Identificazione dei processi che rientrano nell'ambito di applicazione del PCO
- 3.6.2. Identificazione delle aree aziendali critiche
- 3.6.3. Identificazione delle dipendenze tra aree e processi
- 3.6.4. Determinazione del MTD appropriato
- 3.6.5. Prodotti. Creazione di un piano





3.7. Fase di determinazione della strategia di continuità in un PCO
- 3.7.1. Ruoli nella fase di determinazione della strategia
- 3.7.2. Compiti nella fase di determinazione della strategia
- 3.7.3. Consegna

3.8. Fase di risposta alla contingenza di un PCO
- 3.8.1. Ruoli nella fase di risposta
- 3.8.2. Compiti di questa fase
- 3.8.3. Consegna

3.9. Fase di test, manutenzione e revisione di un PCO
- 3.9.1. Ruoli nella fase di test, manutenzione e revisione
- 3.9.2. Lavori nella fase di test, manutenzione e revisione
- 3.9.3. Consegna

3.10. Standard ISO associati ai piani di Continuità Operativa (PCO)
- 3.10.1. ISO 22301:2019
- 3.10.2. ISO 22313:2020
- 3.10.3. Altri standard ISO e internazionali correlati

Questo programma ti permetterà di approfondire argomenti come l'identificazione dei rapporti tra aree e processi, un aspetto fondamentale per stabilire una corretta cybersecurity"

05

Metodologia

Questo programma ti offre un modo differente di imparare. La nostra metodologia si sviluppa in una modalità di apprendimento ciclico: ***il Relearning***.

Questo sistema di insegnamento viene applicato nelle più prestigiose facoltà di medicina del mondo ed è considerato uno dei più efficaci da importanti pubblicazioni come il ***New England Journal of Medicine.***

Scopri il Relearning, un sistema che abbandona l'apprendimento lineare convenzionale, per guidarti attraverso dei sistemi di insegnamento ciclici: una modalità di apprendimento che ha dimostrato la sua enorme efficacia, soprattutto nelle materie che richiedono la memorizzazione"

Caso di Studio per contestualizzare tutti i contenuti

Il nostro programma offre un metodo rivoluzionario per sviluppare le abilità e le conoscenze. Il nostro obiettivo è quello di rafforzare le competenze in un contesto mutevole, competitivo e altamente esigente.

Con TECH potrai sperimentare un modo di imparare che sta scuotendo le fondamenta delle università tradizionali in tutto il mondo"

Avrai accesso a un sistema di apprendimento basato sulla ripetizione, con un insegnamento naturale e progressivo durante tutto il programma.

Imparerai, attraverso attività collaborative e casi reali, la risoluzione di situazioni complesse in ambienti aziendali reali.

Un metodo di apprendimento innovativo e differente

Questo programma di TECH consiste in un insegnamento intensivo, creato ex novo, che propone le sfide e le decisioni più impegnative in questo campo, sia a livello nazionale che internazionale. Grazie a questa metodologia, la crescita personale e professionale viene potenziata, effettuando un passo decisivo verso il successo. Il metodo casistico, la tecnica che sta alla base di questi contenuti, garantisce il rispetto della realtà economica, sociale e professionale più attuali.

> *Il nostro programma ti prepara ad affrontare nuove sfide in ambienti incerti e a raggiungere il successo nella tua carriera"*

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori Scuole di Informatica del mondo da quando esistono. Sviluppato nel 1912 affinché gli studenti di Diritto non imparassero la legge solo sulla base del contenuto teorico, il metodo casistico consisteva nel presentare loro situazioni reali e complesse per prendere decisioni informate e giudizi di valore su come risolverle. Nel 1924 fu stabilito come metodo di insegnamento standard ad Harvard.

Cosa dovrebbe fare un professionista per affrontare una determinata situazione? Questa è la domanda con cui ti confrontiamo nel metodo dei casi, un metodo di apprendimento orientato all'azione. Durante il corso, gli studenti si confronteranno con diversi casi di vita reale. Dovranno integrare tutte le loro conoscenze, effettuare ricerche, argomentare e difendere le proprie idee e decisioni.

Metodologia Relearning

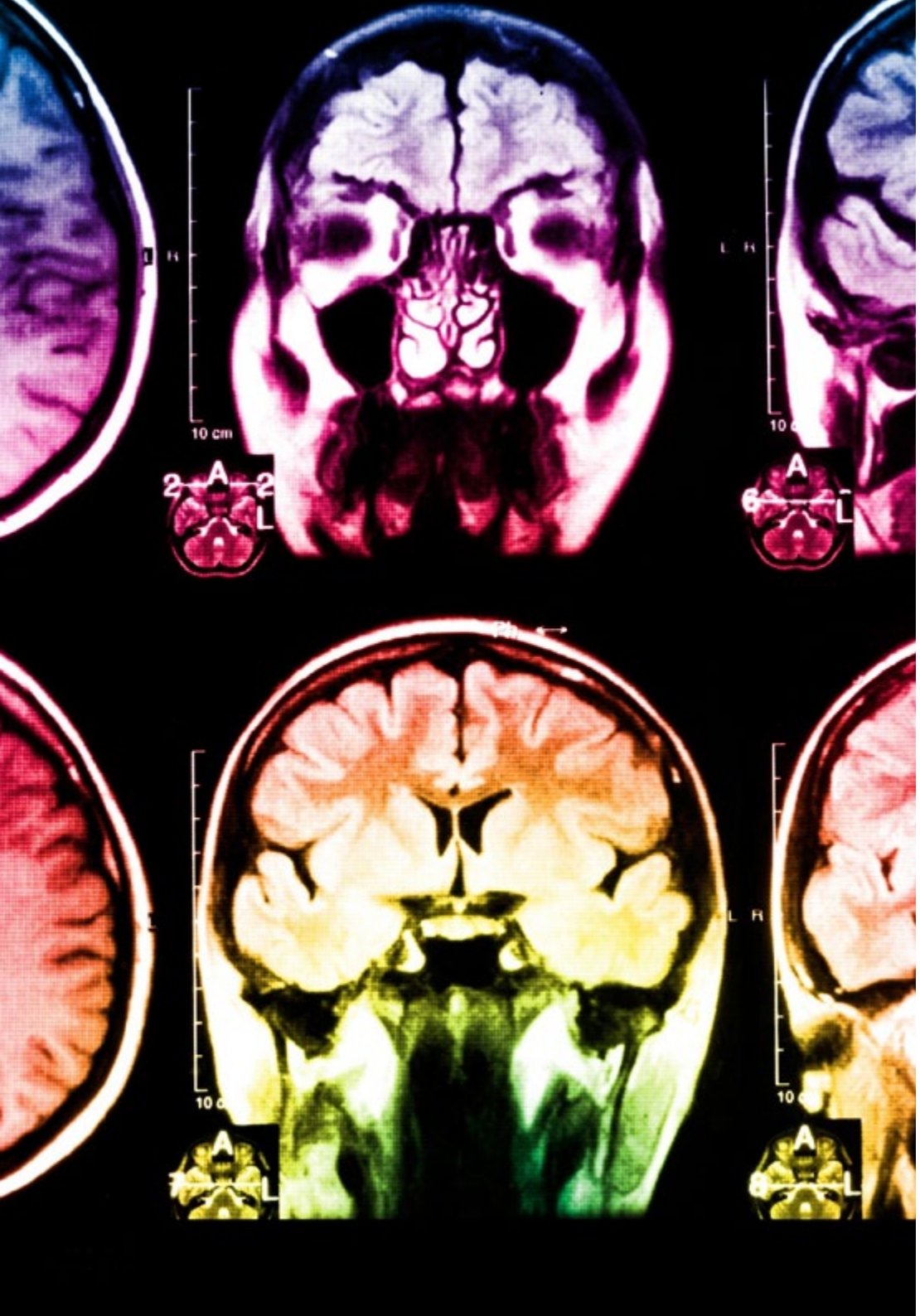
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

Potenziamo il Caso di Studio con il miglior metodo di insegnamento 100% online: il Relearning.

Nel 2019 abbiamo ottenuto i migliori risultati di apprendimento di tutte le università online del mondo.

In TECH imparerai con una metodologia all'avanguardia progettata per formare i manager del futuro. Questo metodo, all'avanguardia della pedagogia mondiale, si chiama Relearning.

La nostra università è l'unica autorizzata a utilizzare questo metodo di successo. Nel 2019, siamo riusciti a migliorare il livello di soddisfazione generale dei nostri studenti (qualità dell'insegnamento, qualità dei materiali, struttura del corso, obiettivi...) rispetto agli indicatori della migliore università online.



Nel nostro programma, l'apprendimento non è un processo lineare, ma avviene in una spirale (impariamo, disimpariamo, dimentichiamo e re-impariamo). Pertanto, combiniamo ciascuno di questi elementi in modo concentrico. Questa metodologia ha formato più di 650.000 laureati con un successo senza precedenti in campi diversi come la biochimica, la genetica, la chirurgia, il diritto internazionale, le competenze manageriali, le scienze sportive, la filosofia, il diritto, l'ingegneria, il giornalismo, la storia, i mercati e gli strumenti finanziari. Tutto questo in un ambiente molto esigente, con un corpo di studenti universitari con un alto profilo socio-economico e un'età media di 43,5 anni.

Il Relearning ti permetterà di apprendere con meno sforzo e più performance, impegnandoti maggiormente nella tua specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando le opinioni: un'equazione diretta al successo.

Dalle ultime evidenze scientifiche nel campo delle neuroscienze, non solo sappiamo come organizzare le informazioni, le idee, le immagini e i ricordi, ma sappiamo che il luogo e il contesto in cui abbiamo imparato qualcosa è fondamentale per la nostra capacità di ricordarlo e immagazzinarlo nell'ippocampo, per conservarlo nella nostra memoria a lungo termine.

In questo modo, e in quello che si chiama Neurocognitive Context-dependent E-learning, i diversi elementi del nostro programma sono collegati al contesto in cui il partecipante sviluppa la sua pratica professionale.

Questo programma offre i migliori materiali didattici, preparati appositamente per i professionisti:

Materiale di studio

Tutti i contenuti didattici sono creati appositamente per il corso dagli specialisti che lo impartiranno, per fare in modo che lo sviluppo didattico sia davvero specifico e concreto.

Questi contenuti sono poi applicati al formato audiovisivo che supporterà la modalità di lavoro online di TECH. Tutto questo, con le ultime tecniche che offrono componenti di alta qualità in ognuno dei materiali che vengono messi a disposizione dello studente.

Master class

Esistono evidenze scientifiche sull'utilità dell'osservazione di esperti terzi.

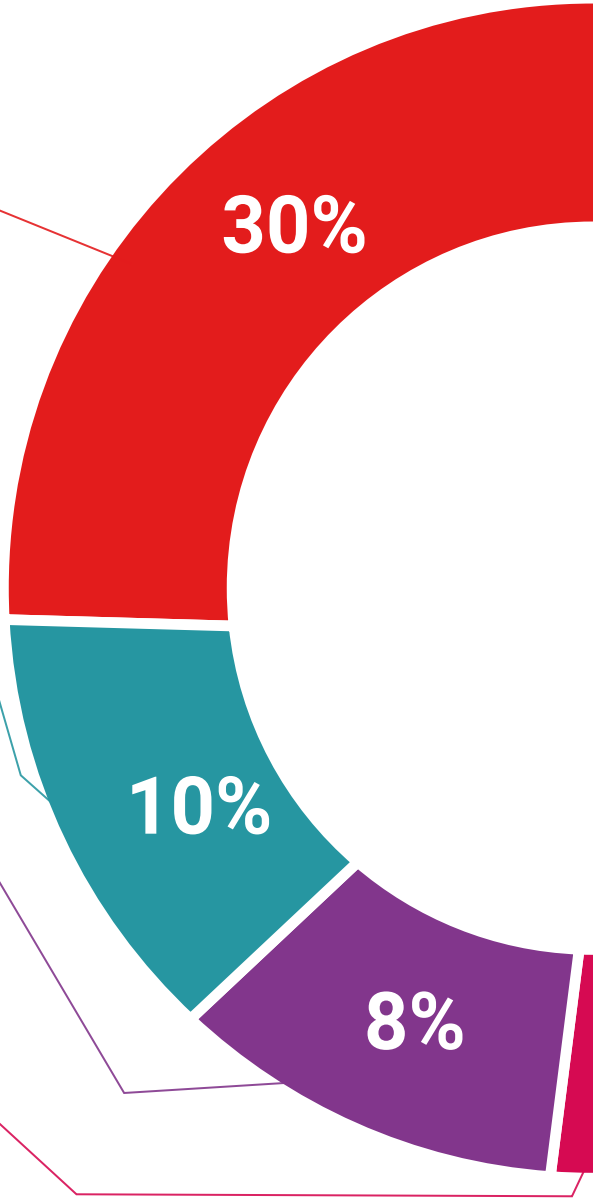
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

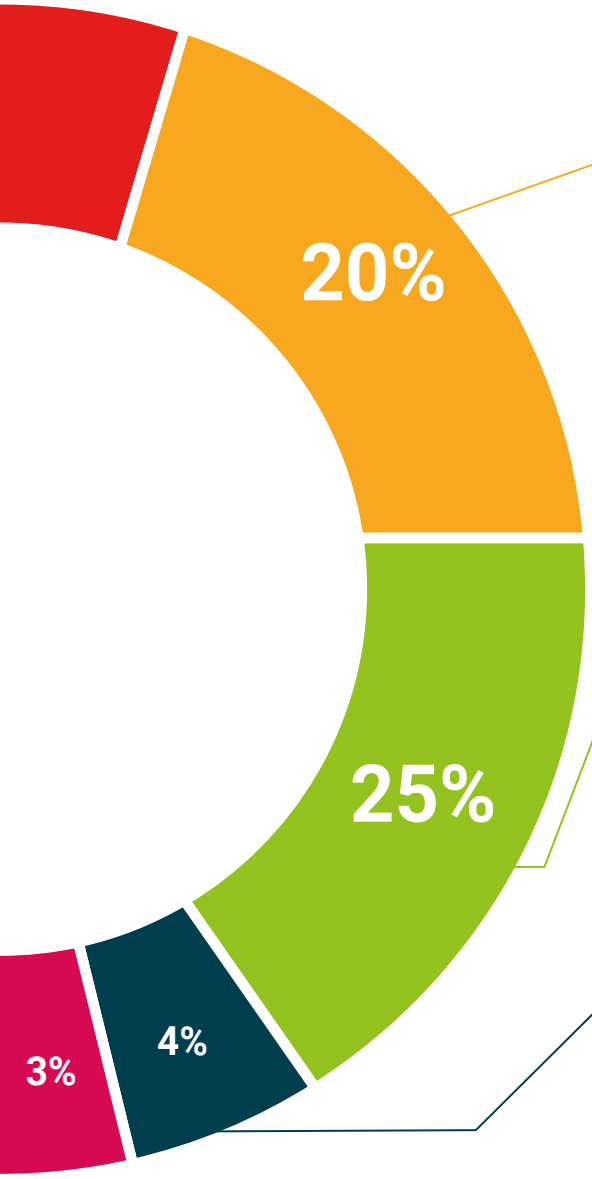
Pratiche di competenze e competenze

Svolgerai attività per sviluppare competenze e capacità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve sviluppare nel quadro della globalizzazione in cui viviamo.

Letture complementari

Articoli recenti, documenti di consenso e linee guida internazionali, tra gli altri. Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua specializzazione.





Casi di Studio

Completerai una selezione dei migliori casi di studio scelti appositamente per questo corso. Casi presentati, analizzati e monitorati dai migliori specialisti del panorama internazionale.

Riepiloghi interattivi

Il team di TECH presenta i contenuti in modo accattivante e dinamico in pillole multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

Questo esclusivo sistema di specializzazione per la presentazione di contenuti multimediali è stato premiato da Microsoft come "Caso di successo in Europa".

Testing & Retesting

Valutiamo e rivalutiamo periodicamente le tue conoscenze durante tutto il programma con attività ed esercizi di valutazione e autovalutazione, affinché tu possa verificare come raggiungi progressivamente i tuoi obiettivi.

06

Titolo

L'Esperto Universitario in Amministrazione della Sicurezza nelle Tecnologie di Informazione ti garantisce, oltre alla preparazione più rigorosa e aggiornata, l'accesso a una qualifica di Esperto Universitario rilasciata da TECH Università Tecnologica.

Porta a termine questo programma e ricevi la tua qualifica universitaria senza spostamenti o fastidiose formalità”

Questo **Esperto Universitario in Amministrazione della Sicurezza nelle Tecnologie di Informazione** possiede il programma più completo e aggiornato del mercato.

Dopo aver superato la valutazione, lo studente riceverà mediante lettera certificata* con ricevuta di ritorno, la sua corrispondente qualifica di **Esperto Universitario** rilasciata da **TECH Università Tecnologica.**

Il titolo rilasciato da **TECH Università Tecnologica** esprime la qualifica ottenuta nell'Esperto Universitario, e riunisce tutti i requisiti comunemente richiesti da borse di lavoro, concorsi e commissioni di valutazione di carriere professionali.

Titolo: **Esperto Universitario in Amministrazione della Sicurezza nelle Tecnologie di Informazione**

Ore Ufficiali: **450 o.**


tech università tecnologica

Conferisce il presente

DIPLOMA

a

Dott./Dott.ssa _____, con documento d'identità nº_____

Per aver completato con esito positivo e accreditato il programma di

ESPERTO UNIVERSITARIO

in

Amministrazione della Sicurezza nelle Tecnologie di Informazione

Si tratta di un titolo rilasciato da questa Università ed equivalente a 450 ore, con data di inizio gg/mm/aaaa e con data di fine gg/mm/aaaa.

TECH è un Istituto Privato di Istruzione Superiore riconosciuto dal Ministero della Pubblica Istruzione a partire dal 28 giugno 2018.

In data 7 Giugno 2020

Tere Guevara Navarro
Rettrice

codice unico TECH: AFWORD23S techtitute.com/titulos

*Se lo studente dovesse richiedere che il suo diploma cartaceo sia provvisto di Apostille dell'Aia, TECH EDUCATION effettuerà le gestioni opportune per ottenerla pagando un costo aggiuntivo.

tech università tecnologica

Esperto Universitario
Amministrazione della Sicurezza nelle Tecnologie di Informazione

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Università Tecnologica**
- Dedizione: **16 ore/settimana**
- Orario: **a scelta**
- Esami: **online**

Esperto Universitario

Amministrazione della Sicurezza nelle Tecnologie di Informazione

tech università tecnologica