Esperto Universitario
Misure di Difesa della Sicurezza Informatica

tech università tecnologica

tech università tecnologica

Esperto Universitario

Misure di Difesa della Sicurezza Informatica

- 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-misure-difesa-sicurezza-informatica

Indice

01
Presentazione
Pag. 4

02
Obiettivi
Pag. 8

03
Direzione del corso
Pag. 12

04
Struttura e contenuti
Pag. 16

05
Metodologia
pag. 22

06
Titolo
pag. 30

01

Presentazione

I settori finanziario, commerciale e turistico hanno subito un aumento degli attacchi di ingegneria sociale che compromettono le informazioni sensibili e preziose delle organizzazioni stesse e dei loro clienti. Gli attacchi informatici continuano a essere un problema per le aziende, motivo per cui negli ultimi anni è aumentato il numero di posti di lavoro creati per garantire la sicurezza informatica. Questo programma offre ai professionisti dell'informatica una specializzazione nel campo dell'adozione di misure di difesa informatica di fronte a qualsiasi attacco. Un personale docente esperto del settore insegna questa qualifica in modalità 100% online, consentendo di acquisire un apprendimento attuale e completo grazie agli ampi contenuti multimediali.

Dai la migliore risposta alla sicurezza informatica e impedisci alle aziende di cadere nell'ingegneria sociale con questo Esperto Universitario"

L'implementazione di politiche di sicurezza informatica ha un costo per le aziende, ma queste sono disposte a pagarlo a causa delle elevate perdite che subiscono quando i loro sistemi vengono violati, compromettendo il loro corretto funzionamento e la fornitura di servizi ai loro clienti. I professionisti dell'informatica svolgono un ruolo fondamentale in questo scenario.

L'Esperto Universitario offre agli studenti un apprendimento approfondito delle misure di difesa della sicurezza informatica, che si basano sull'analisi delle minacce e sulla loro corretta classificazione per capire dove un'azienda è più o meno vulnerabile. Il personale docente specializzato in questa materia fornirà gli strumenti essenziali per effettuare un'analisi informatica forense. Verrà dimostrato il rilevamento degli incidenti attraverso i sistemi IDS/IPS e il loro trattamento nel SIEM fino al processo di notifica e di escalation.

Per essere all'avanguardia nella difesa della sicurezza, i professionisti informatici svilupperanno, in questa qualifica, tecniche per mitigare i denial of service, il *Session Hacking* e gli attacchi alle applicazioni web. Tutto questo viene insegnato al 100% online, permettendo agli studenti di combinare il loro lavoro professionale con un programma che offre contenuti multimediali innovativi. È sufficiente un dispositivo con connessione a Internet per accedere a un piano di studi che può essere seguito al proprio ritmo.

Questo **Esperto Universitario in Misure di Difesa della Sicurezza Informatica** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- Sviluppo di casi di studio pratici presentati da esperti in campo della Sicurezza Informatica
- Contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni tecniche e pratiche sulle discipline essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- Enfasi speciale sulle metodologie innovative
- Lezioni teoriche, domande all'esperto, forum di discussione su temi controversi e lavoro di riflessione individuale
- Possibilità di accedere ai contenuti da qualsiasi dispositivo fisso o portatile provvisto di connessione a internet

Implementa efficacemente le politiche di sicurezza contro il Session Hijacking, l'hacking dei server Web o delle piattaforme mobili, grazie a questo Esperto Universitario"

Controlla lo standard ISO 27035 e soddisfa i requisiti per una corretta gestione degli incidenti. Iscriviti a questo Esperto Universitario"

Fai crescere la tua carriera professionale con un programma che ti permetterà di approfondire l'analisi e il controllo delle minacce informatiche.

Sei a un solo clic di distanza dall'iscrizione a un Esperto Universitario che ti aprirà ulteriori opportunità di carriera.

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

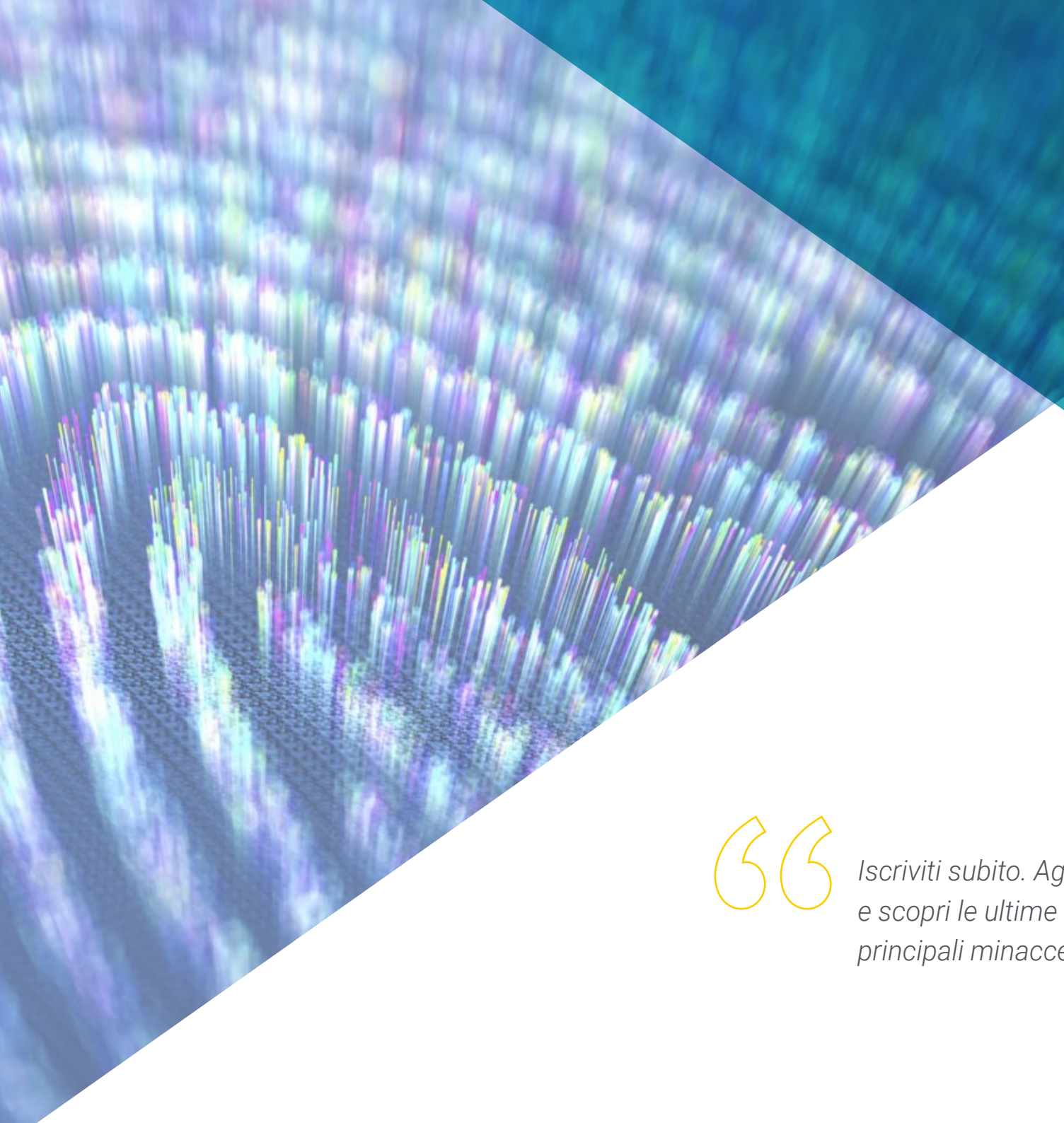
I contenuti multimediali, sviluppati in base alle ultime tecnologie educative, forniranno al professionista un apprendimento coinvolgente e localizzato, ovvero inserito in un contesto reale.

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

02

Obiettivi

Questo Esperto Universitario offre una preparazione il cui obiettivo è quello di consentire ai professionisti informatici di ottenere una qualifica specializzata nel campo della sicurezza. Nel corso di questo programma miglioreranno le competenze degli studenti nell'analisi delle minacce, confrontando le diverse metodologie di gestione che permetteranno loro di scegliere quella più adatta all'incidente. Saranno inoltre addestrati a implementare tecnicamente le misure per mitigare le principali minacce ricevute dall'azienda. Gli informatici otterranno così una qualifica che consentirà loro di progredire nel mondo del lavoro.



Iscriviti subito. Aggiorna le tue conoscenze e scopri le ultime tecniche per prevenire le principali minacce informatiche per un'azienda”

Obiettivi generali

- Approfondire la comprensione dei concetti chiave della sicurezza informatica
- Sviluppare le misure necessarie per garantire buone pratiche di sicurezza delle informazioni
- Sviluppare le diverse metodologie per condurre un'analisi completa delle minacce
- Installare e conoscere i diversi strumenti utilizzati nel trattamento e nella prevenzione degli incidenti

Accedi a una qualifica che ti fornirà le strategie più recenti ed efficaci per gestire qualsiasi attacco informatico"

Obiettivi specifici

Modulo 1. Politiche di Sicurezza per l'Analisi delle Minacce dei Sistemi Informatici

- Analizzare il significato delle minacce
- Determinare le fasi della gestione preventiva delle minacce
- Comparazione di diverse metodologie di gestione delle minacce

Modulo 2. Politiche di Gestione degli Incidenti di Sicurezza

- Sviluppare competenze su come gestire gli incidenti causati da eventi di sicurezza informatica
- Determinare il funzionamento di un team di gestione degli incidenti di sicurezza
- Analizzare le diverse fasi della gestione degli eventi di sicurezza informatica
- Esaminare i protocolli standardizzati per la gestione degli incidenti di sicurezza

Modulo 3. Implementazione Pratica delle Politiche di Sicurezza contro gli Attacchi

- Determinare i diversi attacchi effettivi al sistema informativo
- Valutare le diverse politiche di sicurezza per mitigare gli attacchi
- Implementare tecnicamente le misure per mitigare le principali minacce

03

Direzione del corso

TECH seleziona con cura l'intero personale docente che impartisce i vari corsi di specializzazione. Questo Esperto Universitario dispone di un professionista altamente qualificato nel campo della sicurezza informatica. La sua esperienza come responsabile della sicurezza in questo settore in enti pubblici e privati garantisce agli studenti una conoscenza approfondita che fornisce un grande valore al professionista che desidera conoscere in prima persona le principali misure adottate in questo campo, a fronte delle principali minacce subite. I casi pratici presentati sono simili a situazioni reali che gli studenti devono affrontare nel loro ambiente di lavoro, e quindi li faranno crescere professionalmente.

Un personale docente esperto in sicurezza informatica metterà a tua disposizione tutte le sue conoscenze per aiutarti a progredire nella tua carriera professionale"

Direzione

Dott.ssa Fernández Sapena, Sonia

- Formatrice in Sicurezza Informatica e Hacking Etico presso il Centro di Riferimento Nazionale per l'Informatica e le Telecomunicazioni di Getafe, Madrid
- Istruttrice certificata E-Council
- Formatrice nelle seguenti certificazioni: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation. Madri
- Formatrice esperta accreditata dal CAM per i seguenti certificati di professionalità: Sicurezza Informatica (IFCT0190), Gestione di Reti di Voce e dati (IFCM0310), Amministrazione di Reti dipartimentali (IFCT0410), Gestione degli Allarmi nelle reti di telecomunicazione (IFCM0410), Operatore di Reti di voce e dati (IFCM0110) e Amministrazione di servizi internet (IFCT0509)
- Colaboratrice esterna CSO/SSA (Chief Security Officer/Senior Security Architect) presso l'Università delle Isole Baleari
- Laurea in Ingegneria Informatica presso l'Università di Alcalá de Henares a Madrid
- Master in DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Personale docente

Dott.ssa López García, Rosa María

- Specialista in Informazioni Gestionali
- Docente presso l'Istituto Professionale Linux
- Collaboratrice di Incibe Hacker Academy
- Direttrice del Talento di Cybersecurity presso il Teamciberhack
- Responsabile amministratrice, contabile e finanziaria presso Integra2Transportes
- Assistente amministrativa per l'acquisto di risorse presso il Centro Educativo Cardenal Marcelo Espínola
- Tecnico Superiore in Cybersecurity ed Ethical Hacking
- Membro di Ciberpatrulla

Dott. Oropesiano Carrizosa, Francisco

- Ingegnere informatico
- Tecnico di Microcomputing, Networking e Sicurezza presso Cas-Training
- Sviluppatore di servizi web, CMS, e-commerce, UI e UX presso Fersa Reparaciones
- Responsabile servizi web, contenuti, posta e DNS presso Oropesia Web & Network
- Progettista di applicazioni grafiche e web presso Xarxa Sakai Projectes
- Diploma in Informatica di Sistema presso l'Università di Alcalá de Henares
- Master in DevOps: Docker e Kubernetes por Cyber Business Center
- Tecnico di Rete e Sicurezza Informatica presso l'Università delle Isole Baleari
- Esperto in Disegno Grafico presso l'Università Politecnica di Madrid

04

Struttura e contenuti

Il personale docente di questo Esperto Universitario ha sviluppato un piano di studio che approfondisce ciascuna delle fasi di sviluppo di un piano di sicurezza per affrontare le minacce ai sistemi informatici. Vengono approfonditi l'auditing delle minacce, la categorizzazione, la gestione degli incidenti e gli strumenti più recenti per il rilevamento delle minacce. Tratta anche i problemi sollevati dall'ingegneria sociale nelle aziende che ne sono colpite. Tutto questo, con materiale multimediale aggiornato che facilita la comprensione dei contenuti e con il sistema *Relearning*, che permette di acquisire solide conoscenze.

Accedi a un apprendimento online al 100%, flessibile e autogestito. Coniuga la tua vita personale con un insegnamento di qualità. Iscriviti adesso"

Modulo 1. Politiche di Sicurezza per l'Analisi delle Minacce dei Sistemi Informatici

1.1. Gestione delle minacce nelle politiche di sicurezza
- 1.1.1. Gestione del rischio
- 1.1.2. Rischio per la sicurezza
- 1.1.3. Metodologie di gestione delle minacce
- 1.1.4. Implementazione delle metodologie

1.2. Fasi della gestione delle minacce
- 1.2.1. Identificazione
- 1.2.2. Analisi
- 1.2.3. Localizzazione
- 1.2.4. Misure di salvaguardia

1.3. Sistemi di audit per la localizzazione delle minacce
- 1.3.1. Classificazione e flusso di informazioni
- 1.3.2. Analisi dei processi vulnerabili

1.4. Classificazione del rischio
- 1.4.1. Tipi di rischio
- 1.4.2. Calcolo della probabilità di rischio
- 1.4.3. Rischio residuo

1.5. Trattamento del rischio
- 1.5.1. Attuazione delle misure di salvaguardia
- 1.5.2. Trasferimento o assunzione

1.6. Controllo del rischio
- 1.6.1. Processo continuo di gestione del rischio
- 1.6.2. Implementazione di metriche di sicurezza
- 1.6.3. Modello strategico delle metriche di sicurezza delle informazioni

1.7. Metodologie pratiche per l'analisi e il controllo delle minacce
- 1.7.1. Catalogo delle minacce
- 1.7.2. Catalogo delle misure di controllo
- 1.7.3. Catalogo delle misure di sicurezza

1.8. Norma ISO 27005
- 1.8.1. Identificazione del rischio
- 1.8.2. Analisi del rischio
- 1.8.3. Valutazione del rischio

1.9. Matrice dei rischi, degli impatti e delle minacce
  1.9.1. Dati, sistemi e personale
  1.9.2. Probabilità di minaccia
  1.9.3. Entità del danno
1.10. Progettazione di fasi e processi nell'analisi dei pericoli
  1.10.1. Identificazione degli elementi critici dell'organizzazione
  1.10.2. Determinazione delle minacce e degli impatti
  1.10.3. Analisi degli impatti e dei rischi
  1.10.4. Metodologie

Modulo 2. Politiche di Gestione degli Incidenti di Sicurezza

2.1. Politiche e miglioramenti per la gestione degli incidenti di sicurezza delle informazioni
  2.1.1. Gestione degli imprevisti
  2.1.2. Responsabilità e procedure
  2.1.3. Notifica dell'evento
2.2. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
  2.2.1. Dati di funzionamento del sistema
  2.2.2. Tipi di sistemi di rilevamento delle intrusioni
  2.2.3. Criteri di posizionamento degli IDS/IPS
2.3. Risposta agli incidenti di sicurezza
  2.3.1. Procedura di raccolta delle informazioni
  2.3.2. Processo di verifica dell'intrusione
  2.3.3. Organi del CERT
2.4. Processo di notifica e gestione dei tentativi di intrusione
  2.4.1. Responsabilità nel processo di notifica
  2.4.2. Classificazione degli incidenti
  2.4.3. Processo di risoluzione e recupero
2.5. L'analisi forense come politica di sicurezza
  2.5.1. Prove volatili e non volatili
  2.5.2. Analisi e raccolta di prove elettroniche
    2.5.2.1. Analisi delle prove elettroniche
    2.5.2.2. Raccolta di prove elettroniche

2.6. Strumenti di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 2.6.1. Snort
- 2.6.2. Suricata
- 2.6.3. SolarWinds

2.7. Strumenti di centralizzazione degli eventi
- 2.7.1. SIM
- 2.7.2. SEM
- 2.7.3. SIEM

2.8. Guida alla sicurezza CCN-STIC
- 2.8.1. Gestione degli incidenti informatici
- 2.8.2. Metriche e Indicatori

2.9. NIST SP800-61
- 2.9.1. Capacità di risposta agli incidenti di sicurezza informatica
- 2.9.2. Gestione degli incidenti
- 2.9.3. Coordinamento e condivisione delle informazioni

2.10. Norma ISO 27035
- 2.10.1. Norma ISO 27035. Principi di gestione degli incidenti
- 2.10.2. Linee guida per lo sviluppo di un piano di gestione degli incidenti
- 2.10.3. Linee guida per le operazioni di risposta agli incidenti

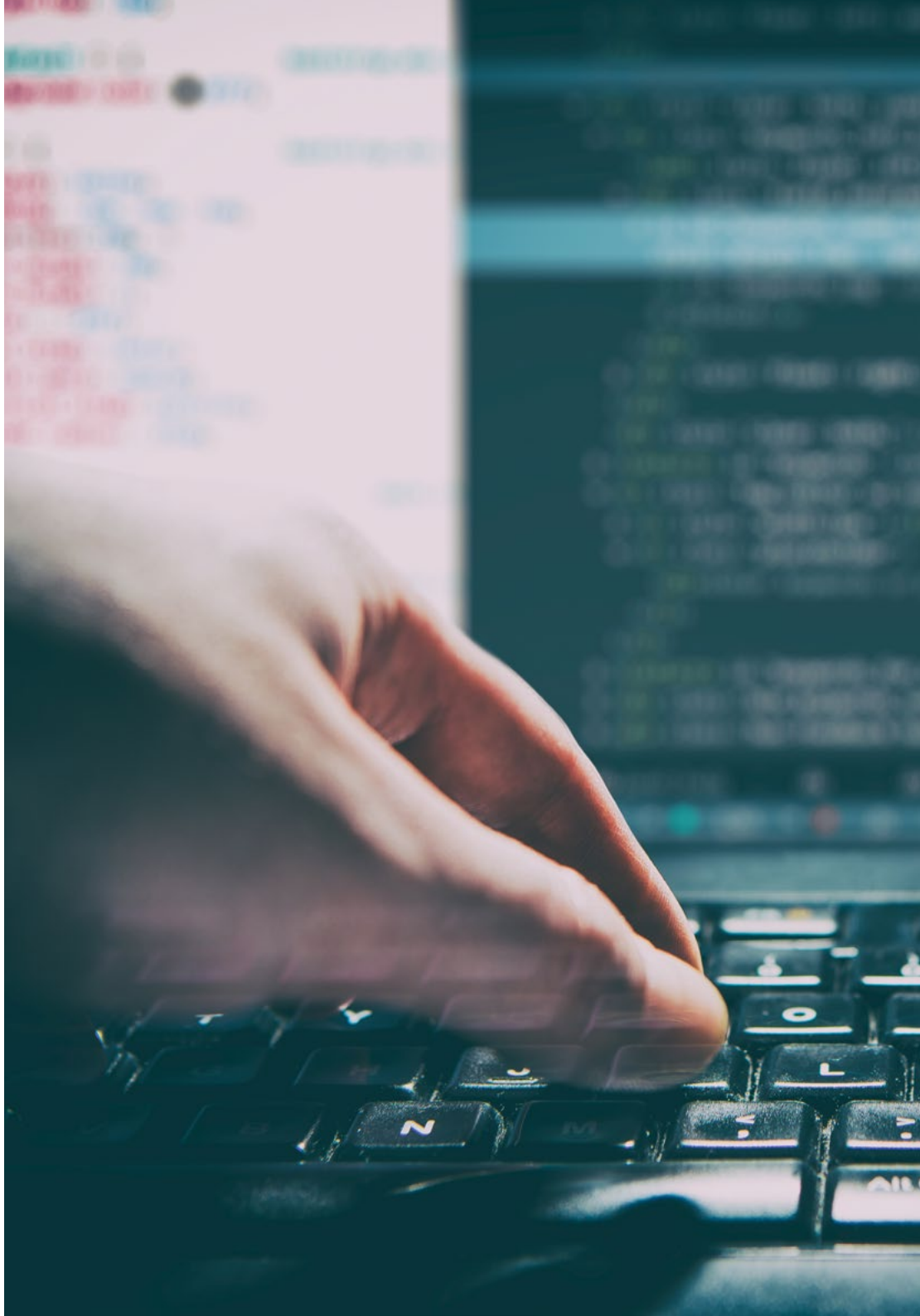
Modulo 3. Implementazione Pratica delle Politiche di Sicurezza contro gli Attacchi

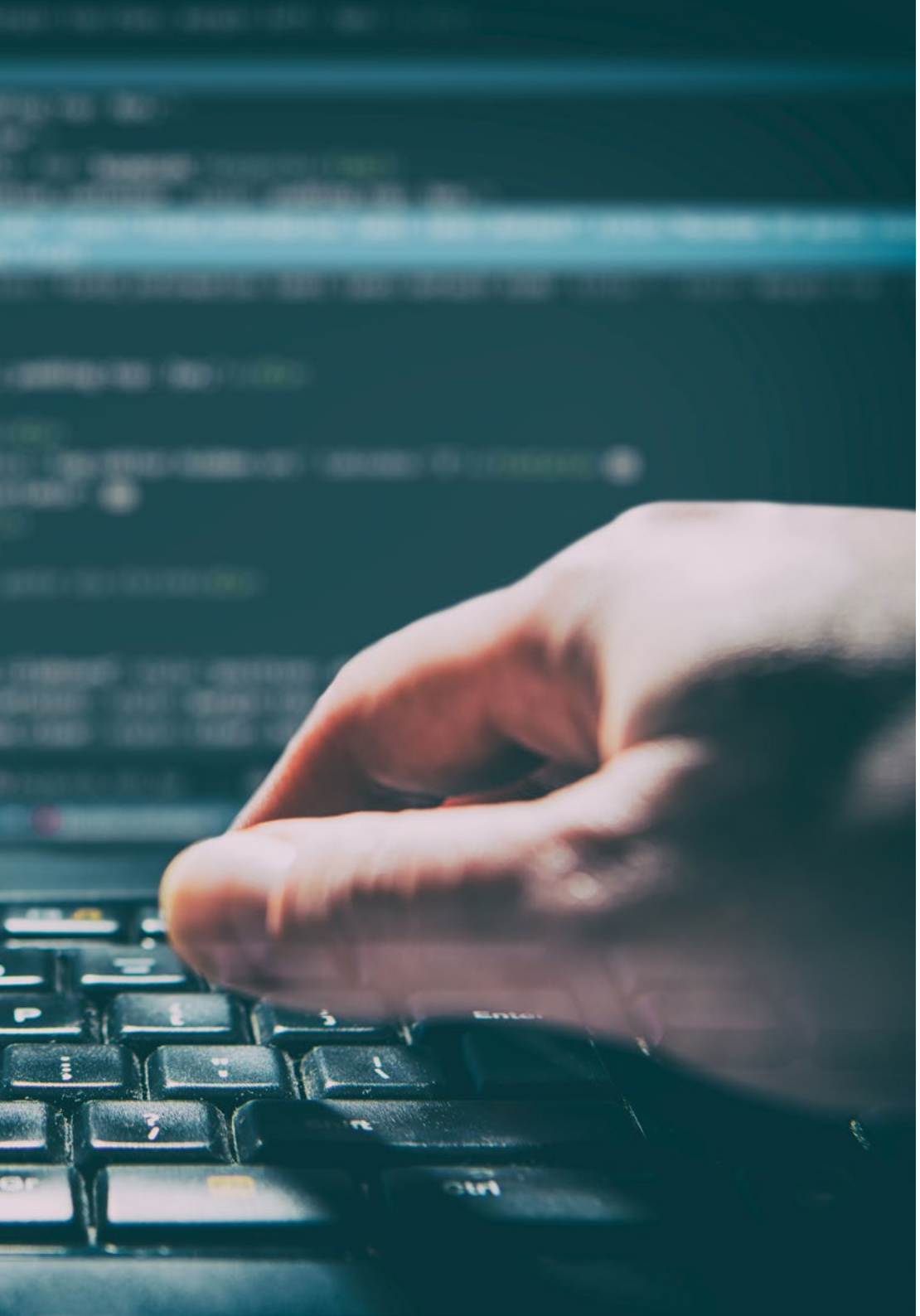
3.1. *System Hacking*
- 3.1.1. Rischi e vulnerabilità
- 3.1.2. Contromisure

3.2. DoS nei servizi
- 3.2.1. Rischi e vulnerabilità
- 3.2.2. Contromisure

3.3. *Session Hijacking*
- 3.3.1. Il processo di Hijacking
- 3.3.2. Contromisure al *Hijacking*

3.4. Evasione di IDS *Firewalls and Honeypots*
- 3.4.1. Tecniche di elusione
- 3.4.2. Implementazione di contromisure





3.5. *Hacking Web Servers*
- 3.5.1. Attacchi ai server web
- 3.5.2. Implementazione delle misure di difesa

3.6. *Hacking Web Applications*
- 3.6.1. Attacchi alle applicazioni web
- 3.6.2. Implementazione delle misure di difesa

3.7. *Hacking Wireless Networks*
- 3.7.1. Vulnerabilità nelle reti wifi
- 3.7.2. Implementazione delle misure di difesa

3.8. *Hacking Mobile Platforms*
- 3.8.1. Vulnerabilità delle piattaforme mobili
- 3.8.2. Implementazione di contromisure

3.9. *Ramsonware*
- 3.9.1. Vulnerabilità che causano *Ramsonware*
- 3.9.2. Implementazione di contromisure

3.10. Ingegneria sociale
- 3.10.1. Tipi di ingegneria sociale
- 3.10.2. Contromisure per l'ingegneria sociale

I casi di studio e i contenuti multimediali sono gli strumenti più potenti di questo Esperto Universitario. Scarica questi strumenti fin dal primo giorno e progredisci nella tua carriera professionale"

05

Metodologia

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

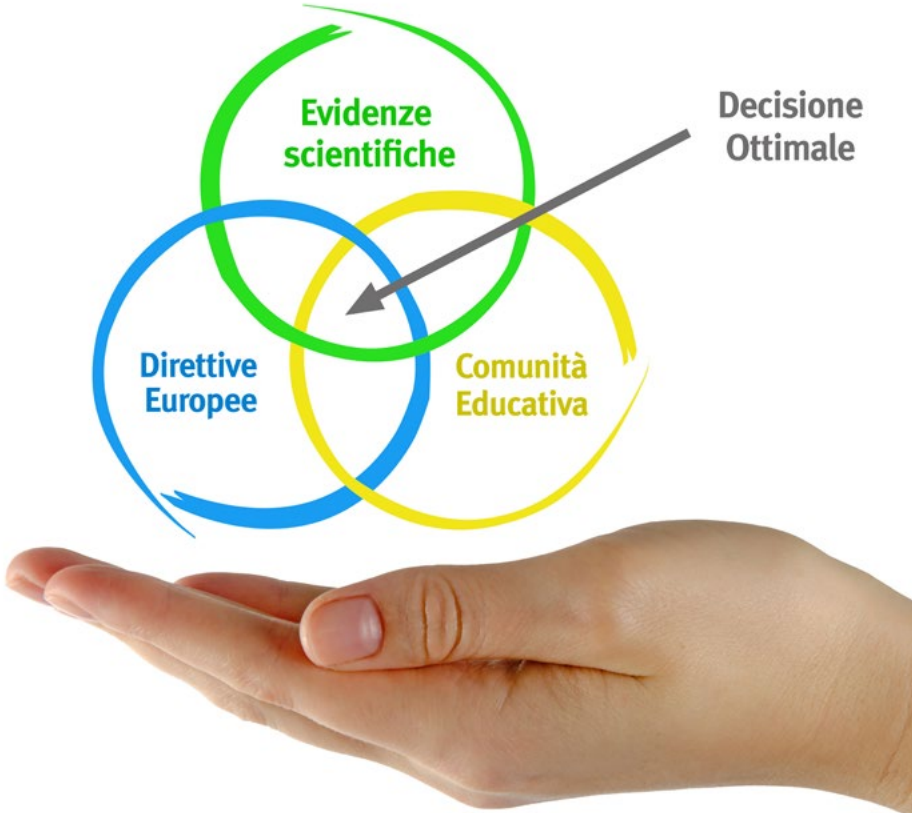
Questo sistema di insegnamento viene applicato nelle più prestigiose facoltà di medicina del mondo ed è considerato uno dei più efficaci da importanti pubblicazioni come il ***New England Journal of Medicine.***

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

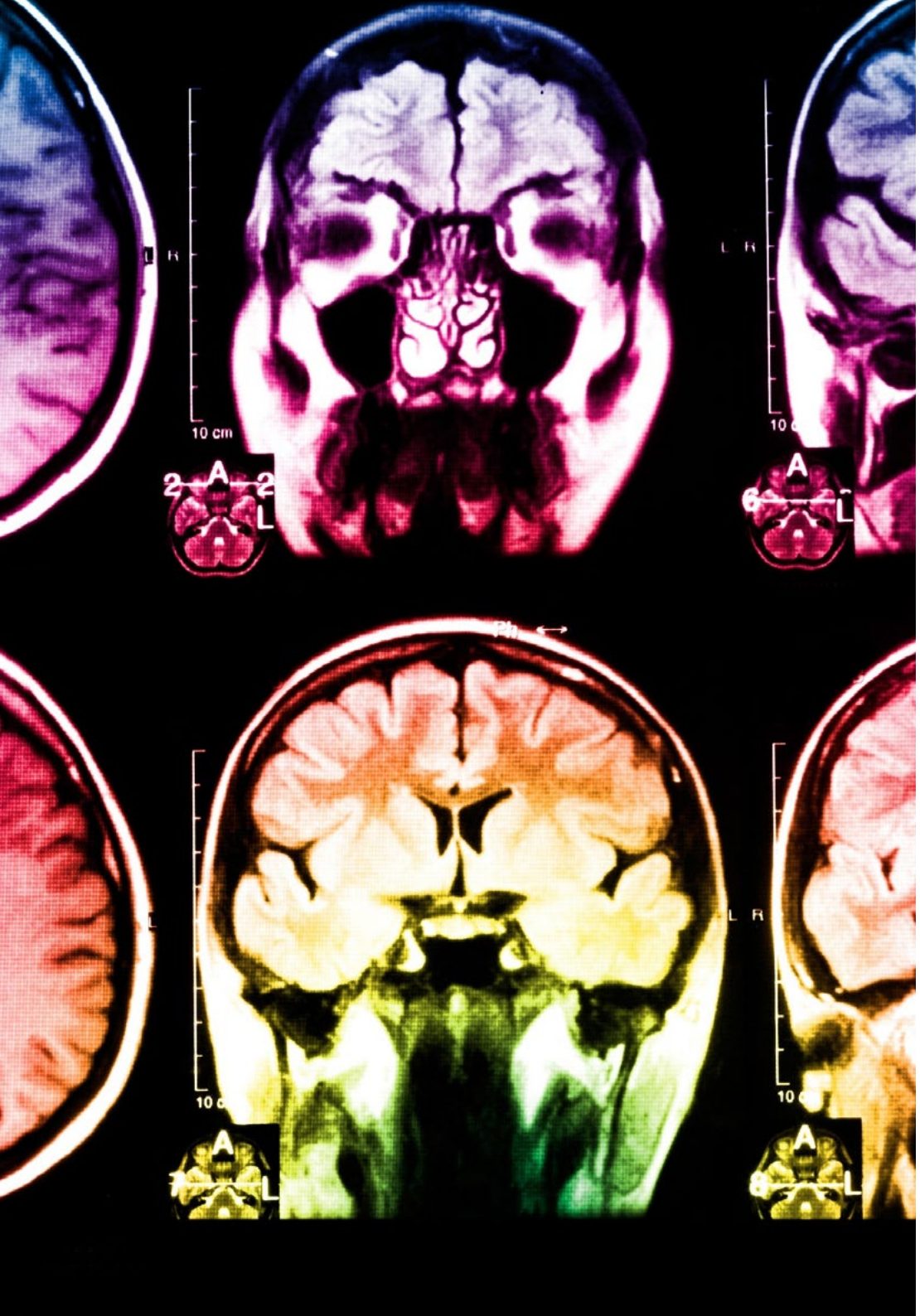
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

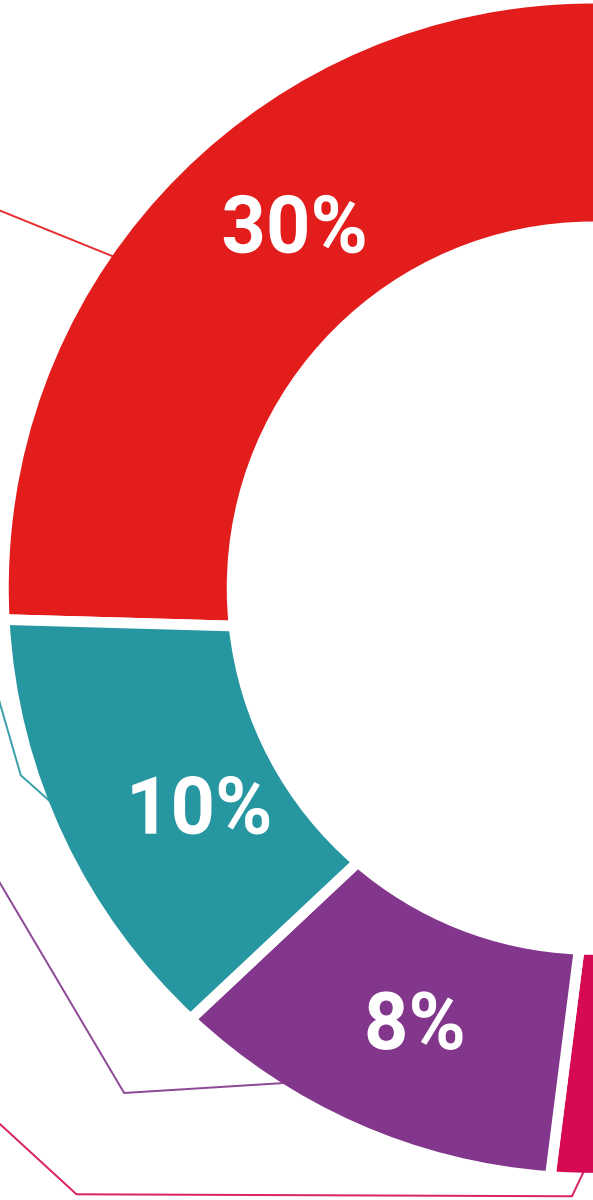
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

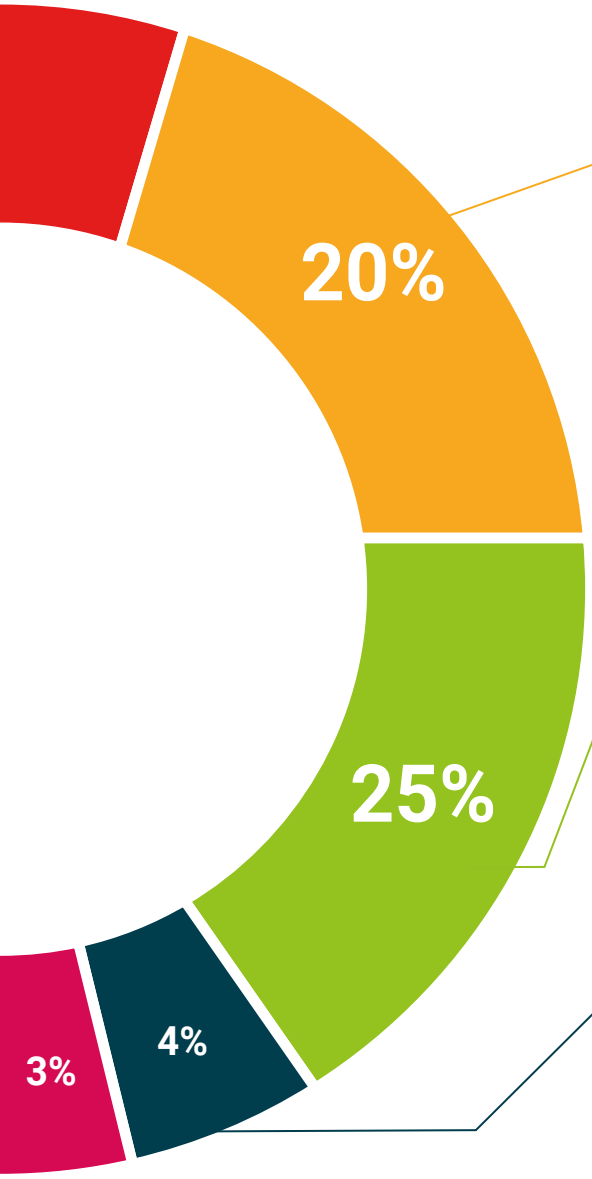
Pratiche di competenze e competenze

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 Misure di Difesa della Sicurezza Informatica garantisce, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di 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 Misure di Difesa della Sicurezza Informatica** 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 Misure di Difesa della Sicurezza Informatica**
Nº 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

Misure di Difesa della Sicurezza Informatica

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

*Apostille dell'Aia. 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

Misure di Difesa della Sicurezza Informatica

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

Esperto Universitario

Misure di Difesa della Sicurezza Informatica

tech università tecnologica