Esperto Universitario
Sicurezza Informatica delle Comunicazioni

tech global university

tech global university

Esperto Universitario
Sicurezza Informatica delle Comunicazioni

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **18 ECTS**
- Orario: **a scelta**
- Esami: **online**

Accesso al sito web: www.techtitute.com/it/informatica/specializzazione/specializzazione-sicurezza-informatica-comunicazioni

Indice

01

Presentazione

L'uso non autorizzato e improprio delle reti è uno dei principali problemi che gli utenti devono affrontare. È essenziale quindi implementare azioni di sicurezza informatica, poiché una grande quantità di informazioni private e riservate si circola su internet. Questo Esperto Universitario offre agli studenti un'introduzione al campo della sicurezza informatica delle comunicazioni, con un programma aggiornato e di alta qualità. Si tratta di un percorso di studi completo che mira a preparare gli studenti ad ottenere il successo professionale.

Se cerchi una qualifica di qualità che ti consenta di specializzarti in uno dei settori con maggiori opportunità professionali, questa è la scelta migliore"

I progressi nel campo delle telecomunicazioni si susseguono incessantemente, in quanto si tratta di un'area in continua evoluzione, ed è pertanto necessaria la presenza di esperti informatici che si adattino a questi cambiamenti e conoscano in prima persona i nuovi strumenti e le nuove tecniche che emergono in questo settore.

In quest'ambito, la sicurezza informatica è uno degli aspetti a cui le aziende devono prestare la massima attenzione, poiché le loro informazioni si trovano in rete e un accesso imprevisto da parte di un utente per svolgere attività illecite può costituire un grave problema per l'organizzazione, sia dal punto di vista finanziario che della reputazione.

L'Esperto Universitario in Sicurezza Informatica delle Comunicazioni tratta la totalità delle tematiche che intervengono in questo campo. Il programma presenta un chiaro vantaggio rispetto ad altri che si concentrano su argomenti specifici, impedendo agli studenti di conoscere le interrelazioni con altre aree comprese nel campo multidisciplinare delle Telecomunicazioni. Il personale docente del programma ha selezionato attentamente ciascuna delle materie da svolgere durante questa preparazione, per offrire allo studente un'opportunità di studio il più completa possibile e legata in tutto e per tutto all'attualità.

Questo programma è rivolto a coloro che siano interessati ad acquisire un livello superiore di conoscenza nel campo della Sicurezza Informatica delle Comunicazioni. L'obiettivo principale è quello di preparare gli studenti ad applicare in modo rigoroso e realistico le conoscenze acquisite nel mondo del lavoro, in una realtà professionale che riproduce le condizioni che potrebbero incontrare nel prossimo futuro.

Trattandosi inoltre di un Esperto Universitario al 100% online, lo studente non è condizionato da orari fissi o dalla necessità di spostarsi in una sede fisica, ma può accedere ai contenuti in qualsiasi momento della giornata, conciliando il suo lavoro o la sua vita personale con quella accademica.

Questo **Esperto Universitario in Sicurezza Informatica delle Comunicazioni** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- Sviluppo di casi pratici presentati da esperti in sicurezza informatica
- 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 in sicurezza informatica delle comunicazioni
- Lezioni teoriche, domande all'esperto, forum di discussione su questioni controverse e compiti di riflessione individuale
- Contenuti disponibili da qualsiasi dispositivo fisso o mobile dotato di connessione a internet

Non perdere l'occasione di svolgere con noi questo Esperto Universitario in Sicurezza Informatica delle Comunicazioni. È l'occasione perfetta per crescere a livello professionale"

Questo Esperto Universitario è il miglior investimento che tu possa fare nella scelta di un programma di aggiornamento delle tue conoscenze in materia di Sicurezza Informatica delle Comunicazioni"

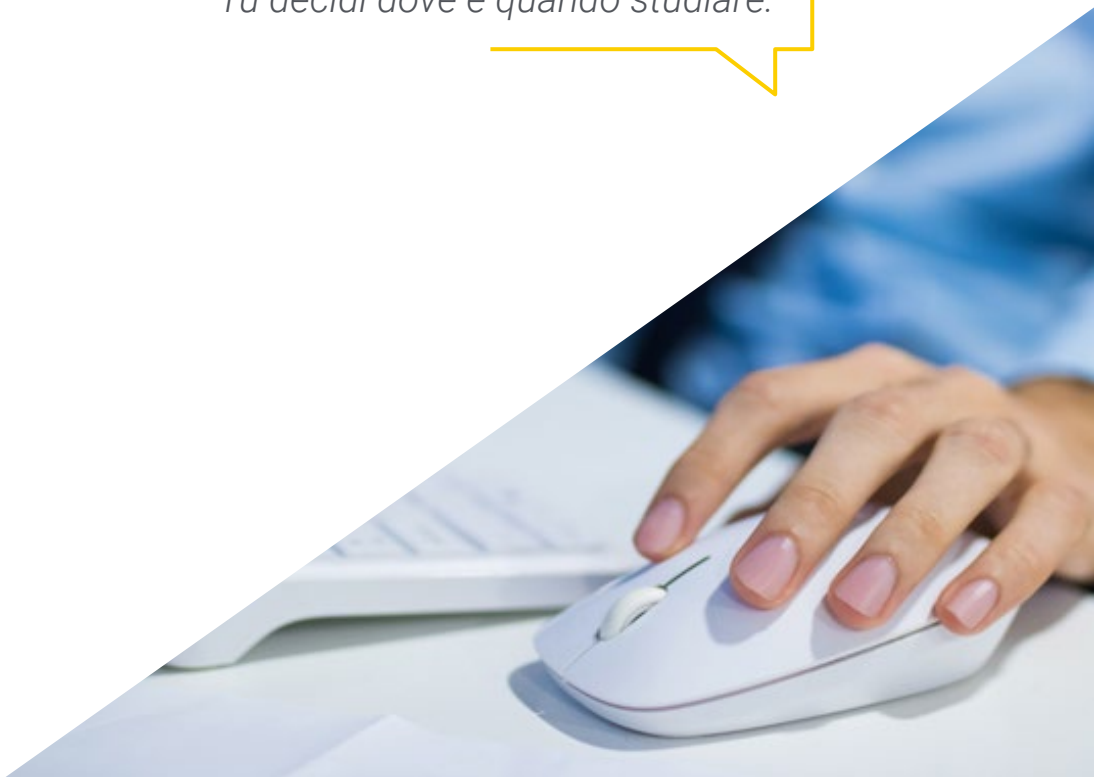
Questa specializzazione raccoglie i migliori materiali didattici, il che ti permetterà uno studio contestuale che faciliterà l'apprendimento.

Questo Esperto Universitario 100% online ti permetterà di conciliare gli studi con la tua attività professionale. Tu decidi dove e quando studiare.

Il personale docente del programma comprende rinomati professionisti in ambito informatico e delle telecomunicazioni, oltre a riconosciuti specialisti appartenenti a società e università prestigiose, 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 e con ampia esperienza nel campo della Sicurezza Informatica delle Comunicazioni.



02

Obiettivi

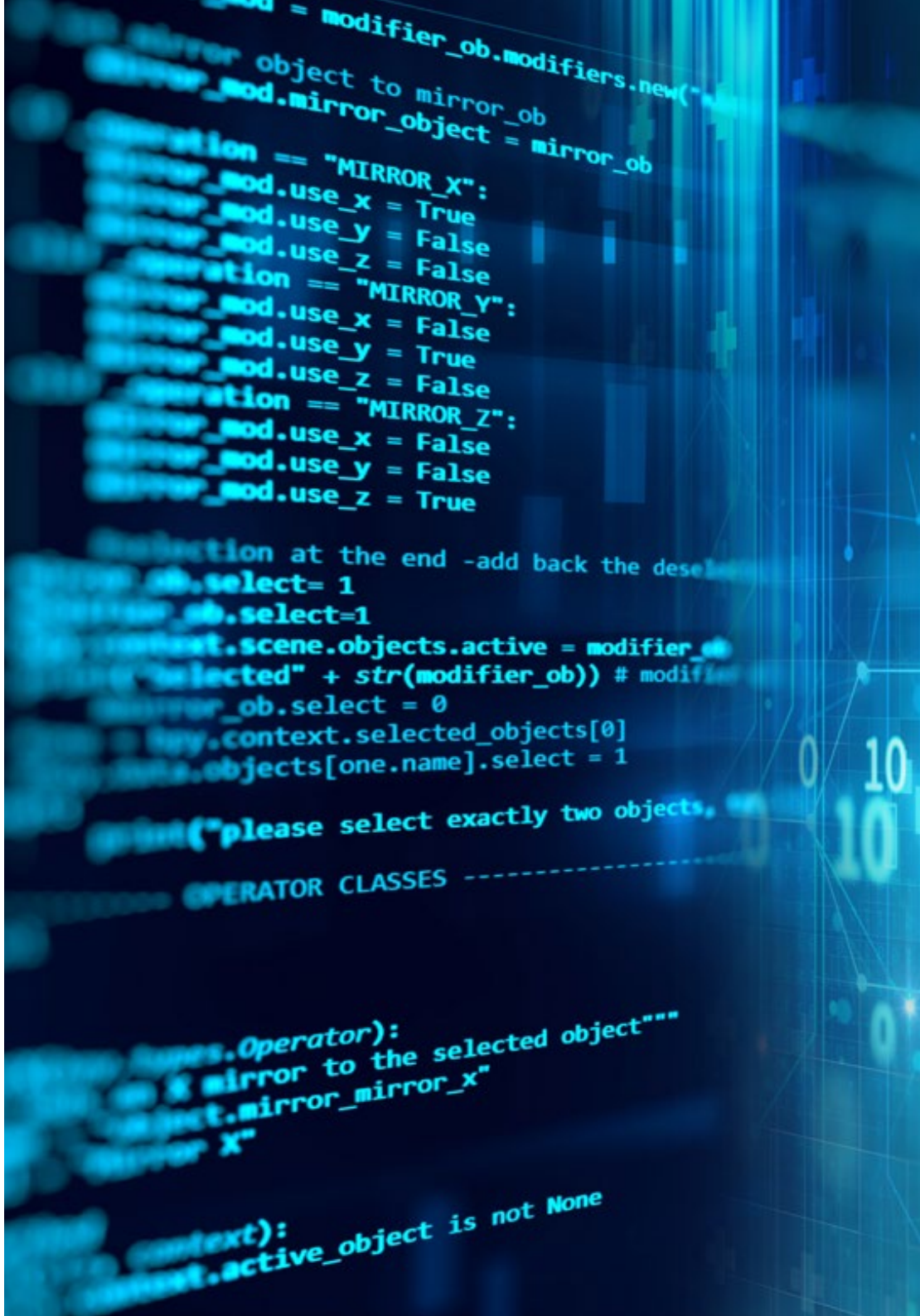
L'Esperto Universitario in Sicurezza Informatica delle Comunicazioni è orientato a facilitare la pratica del professionista in questo campo, affinché ne conosca le principali novità.

Il nostro obiettivo è trasformarti nel miglior professionista del settore. Per questo, disponiamo della metodologia e dei contenuti migliori"

Obiettivo generale

- Consentire allo studente di svolgere il proprio lavoro in totale sicurezza e con qualità nel campo della sicurezza informatica delle comunicazioni

Specializzati presso la principale università online privata nel mondo”



Obiettivi specifici

Modulo 1. Sicurezza dei sistemi e delle reti di comunicazione

- Conoscere e saper applicare i fondamenti della programmazione di reti, sistemi e servizi di telecomunicazione
- Padroneggiare gli standard e i regolamenti per i protocolli e le reti degli organismi internazionali di standardizzazione
- Comprendere i concetti di crittografia simmetrica e asimmetrica, firma digitale, funzioni hash e sicurezza ad ogni livello di un'architettura di comunicazione
- Comprendere i diversi meccanismi e protocolli di sicurezza basati sul controllo degli accessi: autenticazione e difesa perimetrale
- Comprendere il funzionamento delle minacce tecniche e umane alla sicurezza delle reti e dei sistemi di telecomunicazione
- Classificare in modo appropriato i diversi servizi di sicurezza per reti e sistemi in base agli asset che proteggono
- Applicare sistemi di gestione della rete e dei servizi per la configurazione, il funzionamento, il monitoraggio e l'addebito delle reti e dei servizi di telecomunicazione
- Saper gestire la sicurezza delle reti e dei servizi di telecomunicazione implementando tunneling, firewall, protocolli di crittografia e autenticazione e meccanismi di protezione dei contenuti
- Essere in grado di comprendere e applicare le principali tecniche di programmazione sicura

Modulo 2. Architetture di sicurezza

- Comprendere i principi di base della sicurezza informatica
- Padroneggiare gli standard di sicurezza informatica e i processi di certificazione
- Analizzare i fondamenti organizzativi e crittografici su cui si basano le tecnologie di sicurezza
- Identificare le principali minacce e vulnerabilità dei diversi elementi coinvolti nelle TIC e le loro cause
- Conoscere a fondo gli strumenti per la sicurezza delle reti e le loro funzioni specifiche
- Saper applicare le tecnologie che compongono un'architettura di sicurezza delle TIC da diverse prospettive

Modulo 3. Audit dei Sistemi Informativi

- Padroneggiare i principali concetti, standard e metodologie dell'audit dei sistemi
- Essere a conoscenza degli elementi organizzativi e del quadro giuridico degli audit
- Ottenere una guida di riferimento per la progettazione di nuovi sistemi di controllo interni informatici
- Comprendere e determinare i rischi connessi allo sviluppo tecnologico
- Rilevare il modo in cui i diversi sistemi informativi soddisfino o meno i requisiti di sicurezza desiderati
- Essere in grado di svolgere un processo di miglioramento continuo della sicurezza informatica

03

Struttura e contenuti

La struttura dei contenuti è stata ideata dai migliori specialisti dell'ingegneria delle telecomunicazioni, che vantano ampia esperienza e riconosciuto prestigio professionale.

Disponiamo del programma scientifico più completo e aggiornato del mercato. Puntiamo all'eccellenza e a fornirti gli strumenti affinché anche tu possa raggiungerla"

Modulo 1. Sicurezza dei sistemi e delle reti di comunicazione

1.1. Acquisire una prospettiva globale sulla sicurezza, la crittografia e la crittoanalisi classica
- 1.1.1. Sicurezza informatica: una prospettiva storica
- 1.1.2. Ma cosa si intende esattamente per sicurezza?
- 1.1.3. Storia della crittografia
- 1.1.4. Cifrario a sostituzione
- 1.1.5. Caso di studio: la macchina Enigma

1.2. Crittografia simmetrica
- 1.2.1. Introduzione e terminologia di base
- 1.2.2. Cifrario simmetrico
- 1.2.3. Modalità di funzionamento
- 1.2.4. DES
- 1.2.5. Il nuovo standard AES
- 1.2.6. Cifrario di flusso
- 1.2.7. Crittoanalisi

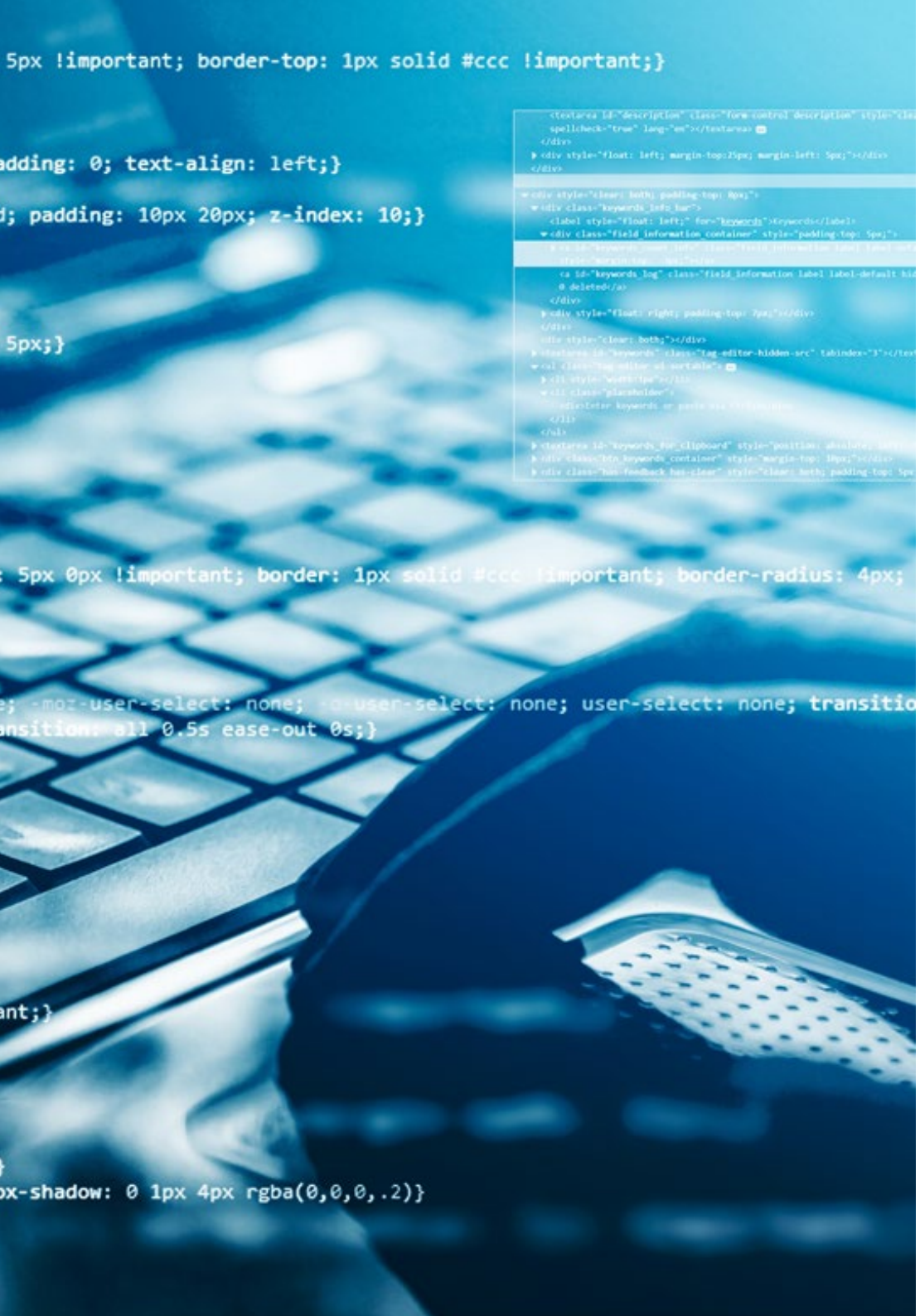
1.3. Crittografia asimmetrica
- 1.3.1. Origini della crittografia a chiave pubblica
- 1.3.2. Concetti di base e funzionamento
- 1.3.3. L'algoritmo RSA
- 1.3.4. Certificati digitali
- 1.3.5. Conservazione e gestione delle chiavi

1.4. Attacchi di rete
- 1.4.1. Minacce e attacchi alla rete
- 1.4.2. Enumerazione
- 1.4.3. Intercettazione del traffico: sniffers
- 1.4.4. Attacchi di negazione del servizio
- 1.4.5. Attacchi ARP poisoning

1.5. Architetture di sicurezza
- 1.5.1. Architettura di sicurezza tradizionale
- 1.5.2. Secure Socket Layer: SSL
- 1.5.3. Protocollo SSH
- 1.5.4. Reti private virtuali (VPN)
- 1.5.5. Meccanismi di protezione dell'unità di archiviazione esterna
- 1.5.6. Meccanismi di protezione hardware

1.6. Tecniche di protezione del sistema e sviluppo di codice sicuro
- 1.6.1. Sicurezza operativa
- 1.6.2. Risorse e controlli
- 1.6.3. Monitoraggio
- 1.6.4. Sistemi di rilevamento delle intrusioni
- 1.6.5. IDS di host
- 1.6.6. IDS di rete
- 1.6.7. IDS basati sulla firma
- 1.6.8. Sistemi di esche
- 1.6.9. Principi di sicurezza di base nello sviluppo del codice
- 1.6.10. Gestione dei guasti
- 1.6.11. Nemico pubblico numero 1: i buffer overflow
- 1.6.12. Inganni crittografici

1.7. Botnets e spam
- 1.7.1. Origine del problema
- 1.7.2. Processo dello spam
- 1.7.3. Invio di spam
- 1.7.4. Raffinare le mailing list
- 1.7.5. Tecniche di protezione
- 1.7.6. Servizio Antispam offerto da terzi
- 1.7.7. Casi di studio
- 1.7.8. Spam esotico



1.8. Audit e attacchi web
  1.8.1. Raccolta informazioni
  1.8.2. Tecniche di attacco
  1.8.3. Strumenti
1.9. Malware e codice maligno
  1.9.1. Che cos'è il malware?
  1.9.2. Tipi di Malware
  1.9.3. Virus
  1.9.4. Cryptovirus
  1.9.5. Worm
  1.9.6. Adware
  1.9.7. Spyware
  1.9.8. Hoaxes
  1.9.9. Pishing
  1.9.10. Troyan
  1.9.11. L'economia del malware
  1.9.12. Possibili soluzioni
1.10. Analisi forense
  1.10.1. Raccolta di evidenze
  1.10.2. Analisi delle evidenze
  1.10.3. Tecniche anti-forensi
  1.10.4. Caso di studio pratico

Modulo 2. Architetture di Sicurezza

2.1. Principi di base della sicurezza informatica
- 2.1.1. Cosa si intende per sicurezza informatica
- 2.1.2. Obiettivi della sicurezza informatica
- 2.1.3. Servizi di sicurezza informatica
- 2.1.4. Conseguenze della mancanza di sicurezza
- 2.1.5. Principio di "difesa di sicurezza"
- 2.1.6. Politiche, piani e procedure di sicurezza
  - 2.1.6.1. Gestione degli account degli utenti
  - 2.1.6.2. Identificazione e autenticazione degli utenti
  - 2.1.6.3. Autorizzazione e controllo logico degli accessi
  - 2.1.6.4. Monitoraggio dei server
  - 2.1.6.5. Protezione dei dati
  - 2.1.6.6. Sicurezza delle connessioni remote
- 2.1.7. L'importanza del fattore umano

2.2. Standardizzazione e certificazione della sicurezza informatica
- 2.2.1. Standard di sicurezza
  - 2.2.1.1. Propositi degli standard
  - 2.2.1.2. Organismi responsabili
- 2.2.2. Standard negli Stati Uniti
  - 2.2.2.1. TCSEC
  - 2.2.2.2. Federal Criteria
  - 2.2.2.3. FISCAM
  - 2.2.2.4. NIST SP 800
- 2.2.3. Standard europei
  - 2.2.3.1. ITSEC
  - 2.2.3.2. ITSEM
  - 2.2.3.3. Agenzia europea per la sicurezza delle informazioni e delle reti
- 2.2.4. Standard internazionali
- 2.2.5. Processo di certificazione

2.3. Minacce alla sicurezza informatica: vulnerabilità e malware
- 2.3.1. Introduzione
- 2.3.2. Vulnerabilità dei sistemi
  - 2.3.2.1. Problemi di sicurezza nelle reti
  - 2.3.2.2. Cause delle vulnerabilità dei sistemi informatici
  - 2.3.2.3. Tipi di vulnerabilità
  - 2.3.2.4. Responsabilità dei fabbricanti di software
  - 2.3.2.5. Strumenti per la valutazione delle vulnerabilità
- 2.3.3. Minacce della sicurezza informatica
  - 2.3.3.1. Classificazione degli intrusi in rete
  - 2.3.3.2. Le motivazioni degli aggressori
  - 2.3.3.3. Fasi di un attacco
  - 2.3.3.4. Tipi di attacchi
- 2.3.4. Virus informatici
  - 2.3.4.1. Caratteristiche generali
  - 2.3.4.2. Tipi di virus
  - 2.3.4.3. Danni causati dai virus
  - 2.3.4.4. Come combattere i virus

2.4. Cyberterrorismo e risposta agli incidenti
- 2.4.1. Introduzione
- 2.4.2. La minaccia del cyberterrorismo e delle guerre informatiche
- 2.4.3. Conseguenze di guasti e attacchi alle aziende
- 2.4.4. Spionaggio in rete sui computer

2.5. Identificazione degli utenti e sistemi biometrici
- 2.5.1. Introduzione all'autenticazione, autorizzazione e registrazione degli utenti
- 2.5.2. Modello di sicurezza AAA
- 2.5.3. Controlli di accesso
- 2.5.4. Identificazione degli utenti
- 2.5.5. Verifica delle password

2.5.6. Autenticazione con certificati digitali
2.5.7. Identificazione in remoto degli utenti
2.5.8. Inizio di sessione unico
2.5.9. Gestire le password
2.5.10. Sistemi biometrici
2.5.10.1. Caratteristiche generali
2.5.10.2. Tipi di sistemi biometrici
2.5.10.3. Implementazione dei sistemi

2.6. Fondamenti di crittografia e protocolli crittografici
2.6.1. Introduzione alla crittografia
2.6.1.1. Crittografia, crittoanalisi e crittologia
2.6.1.2. Funzionamento di un sistema crittografia
2.6.1.3. Storia dei sistemi crittografici
2.6.2. Crittoanalisi
2.6.3. Classificazione dei sistemi crittografici
2.6.4. Sistemi crittografici simmetrici e asimmetrici
2.6.5. Autenticazione con sistemi di crittografia
2.6.6. Firma elettronica
2.6.6.1. Che cos'è la firma elettronica
2.6.6.2. Caratteristiche della firma elettronica
2.6.6.3. Autorità di certificazione
2.6.6.4. Certificati digitali
2.6.6.5. Sistemi di terze parti di fiducia
2.6.6.6. Uso della firma elettronica
2.6.6.7. Documenti elettronici
2.6.6.8. Fatturazione elettronica

2.7. Strumenti per la sicurezza in rete
2.7.1. Il problema della sicurezza della connessione Internet
2.7.2. Sicurezza delle reti esterne
2.7.3. Il ruolo dei Server Proxy
2.7.4. Il ruolo dei firewall
2.7.5. Server di autenticazione per connessioni remote
2.7.6. L'analisi dei registri di attività
2.7.7. Sistemi di rilevamento delle intrusioni
2.7.8. Le esche

2.8. Sicurezza su reti private virtuali e wireless
2.8.1. Sicurezza di reti private virtuali
2.8.1.1 Il ruolo delle VPN
2.8.1.2 Protocolli VPN
2.8.2. Sicurezza tradizionale nelle reti wireless
2.8.3. Possibili attacchi alla rete wireless
2.8.4. Il protocollo WEP
2.8.5. Standard di sicurezza delle reti wireless
2.8.6. Raccomandazioni per rafforzare la sicurezza

2.9. Sicurezza nell'uso dei servizi Internet
2.9.1. Navigazione sicura sul web
2.9.1.1. Il servizio www
2.9.1.2. Problemi di sicurezza su www
2.9.1.3. Raccomandazioni di sicurezza
2.9.1.4. Protezione della privacy su Internet
2.9.2. Sicurezza nella posta elettronica
2.9.2.1. Caratteristiche della posta elettronica
2.9.2.2. Problemi di sicurezza delle email
2.9.2.3. Raccomandazioni di sicurezza per le e-mail
2.9.2.4. Servizi di posta elettronica avanzati
2.9.2.5. Utilizzo della posta elettronica da parte dei dipendenti
2.9.3. SPAM
2.9.4. Il phising

2.10. Controllo dei contenuti
2.10.1. La distribuzione di contenuti su Internet
2.10.2. Misure legali per combattere i contenuti illeciti
2.10.3. Filtraggio, catalogazione e blocco dei contenuti
2.10.4. Danni all'immagine e alla reputazione

Modulo 3. Audit dei Sistemi Informativi

3.1. Audit dei Sistemi Informativi. Regole di buone pratiche
- 3.1.1. Introduzione
- 3.1.2. Audit e COBIT
- 3.1.3. Audit dei Sistemi di Gestione nelle TIC
- 3.1.4. Certificazioni

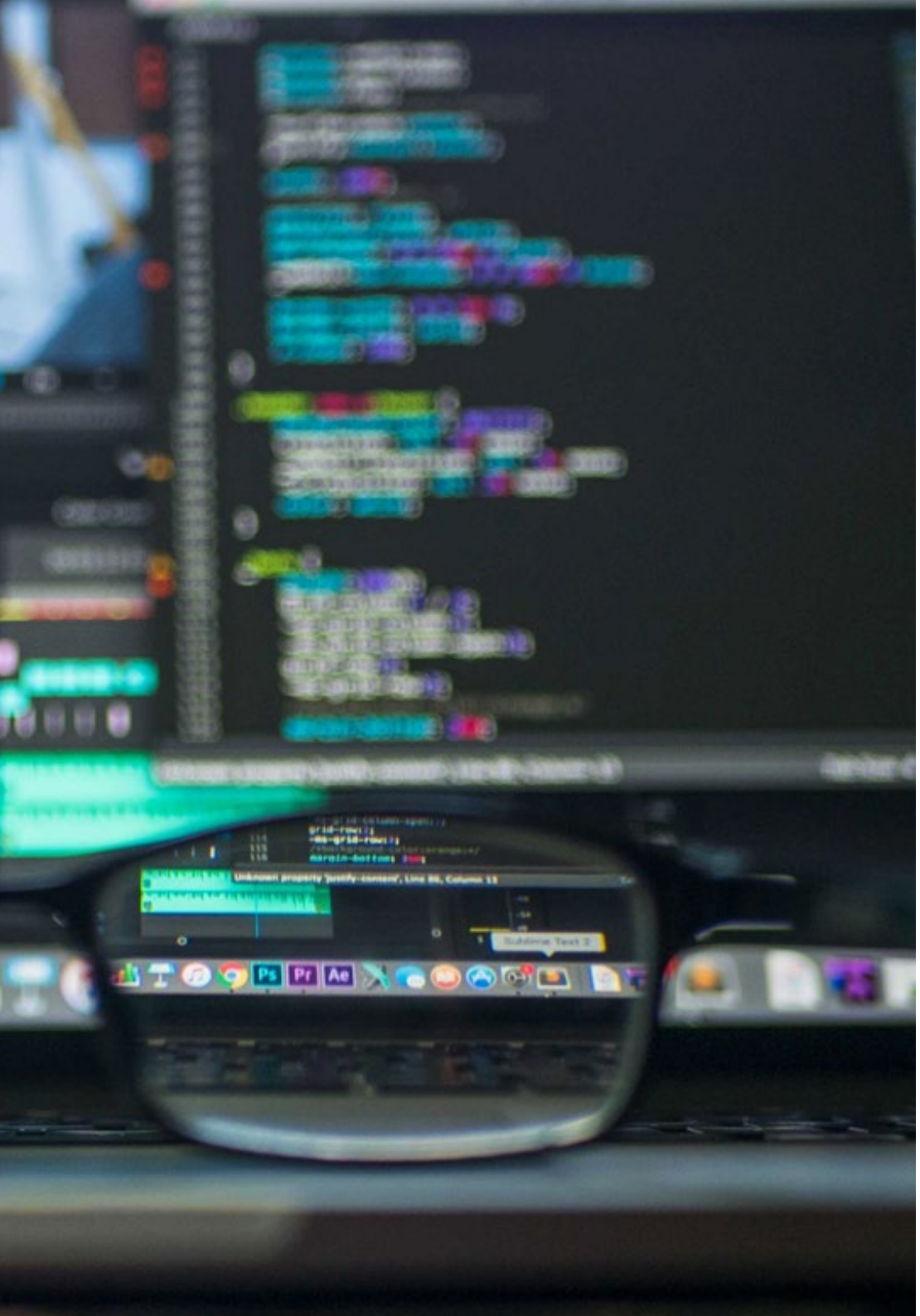
3.2. Concetti e metodologie dell'audit dei sistemi
- 3.2.1. Introduzione
- 3.2.2. Metodologie di valutazione dei sistemi: quantitative e qualitative
- 3.2.3. Metodologia di audit informatico
- 3.2.4. Il piano di audit

3.3. Contratto di audit
- 3.3.1. Natura giuridica del contratto
- 3.3.2. Parti un contratto di audit
- 3.3.3. Oggetto del contratto di audit
- 3.3.4. Il rapporto di audit

3.4. Elementi organizzativi degli audit
- 3.4.1. Introduzione
- 3.4.2. Missione della funzione di audit
- 3.4.3. Pianificazione dell'audit
- 3.4.4. Metodologia di una revisione dei SI

3.5. Quadro giuridico degli audit
- 3.5.1. Tutela dei dati personali
- 3.5.2. Tutela giuridica del software
- 3.5.3. Reati tecnologici
- 3.5.4. Contratto, firma e carta d'identità elettronica

3.6. Audit dell'Outsourcinge quadri di riferimento
- 3.6.1. Introduzione
- 3.6.2. Concetti di base dell'Outsourcing
- 3.6.3. Audit dell'Outsourcing di TI
- 3.6.4. Quadri di riferimento: CMMI, ISO27001, ITIL



3.7. Audit di sicurezza
- 3.7.1. Introduzione
- 3.7.2. Sicurezza fisica e logica
- 3.7.3. Sicurezza dell'ambiente
- 3.7.4. Pianificazione ed esecuzione dell'audit sulla sicurezza fisica

3.8. Revisioni di rete e internet
- 3.8.1. Introduzione
- 3.8.2. Vulnerabilità nelle reti
- 3.8.3. Principi e diritti su Internet
- 3.8.4. Controlli e trattamenti dei dati

3.9. Verifica di applicazioni e sistemi informatici
- 3.9.1. Introduzione
- 3.9.2. Modelli di riferimento
- 3.9.3. Valutazione della qualità delle applicazioni
- 3.9.4. Audit dell'organizzazione e gestione dell'area di sviluppo e manutenzione

3.10. Revisioni dei dati personali
- 3.10.1. Introduzione
- 3.10.2. Leggi e regolamenti sulla protezione dei dati
- 3.10.3. Sviluppo dell'audit
- 3.10.4. Infrazioni e sanzioni

Questa specializzazione ti permetterà di avanzare nella tua carriera in modo confortevole"

04

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

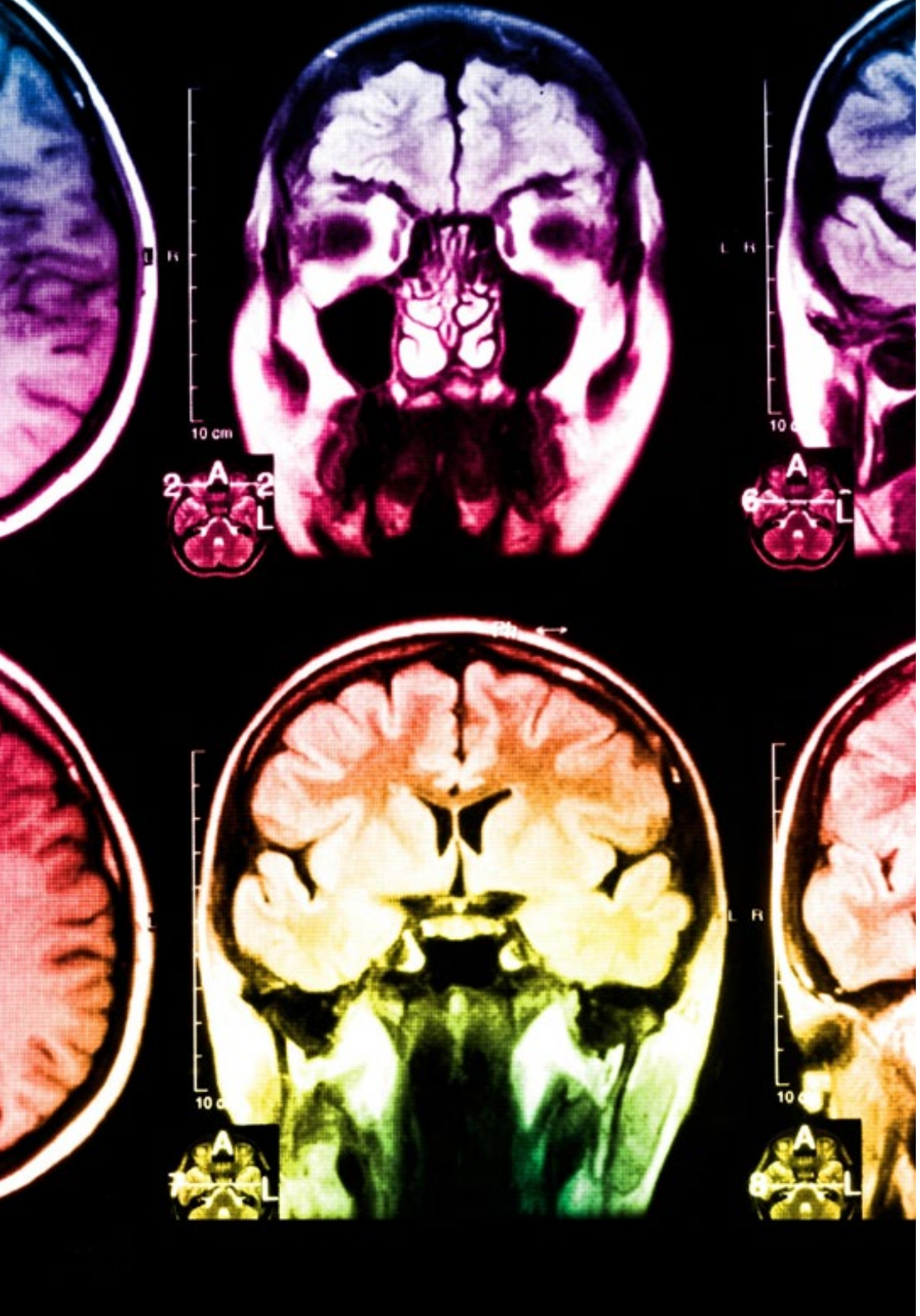
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

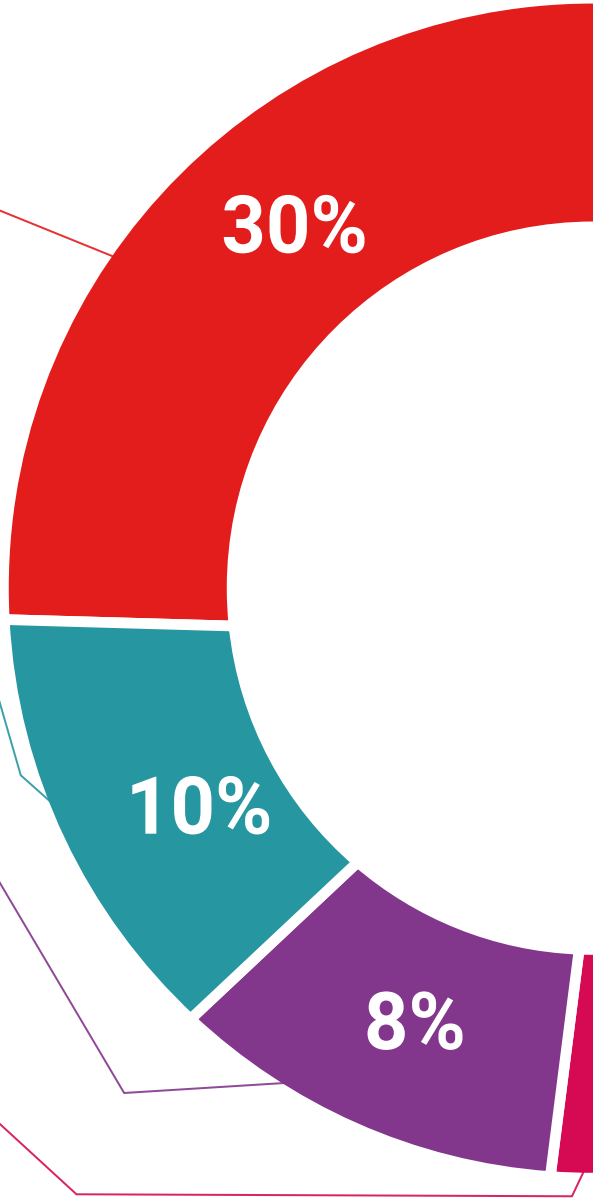
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

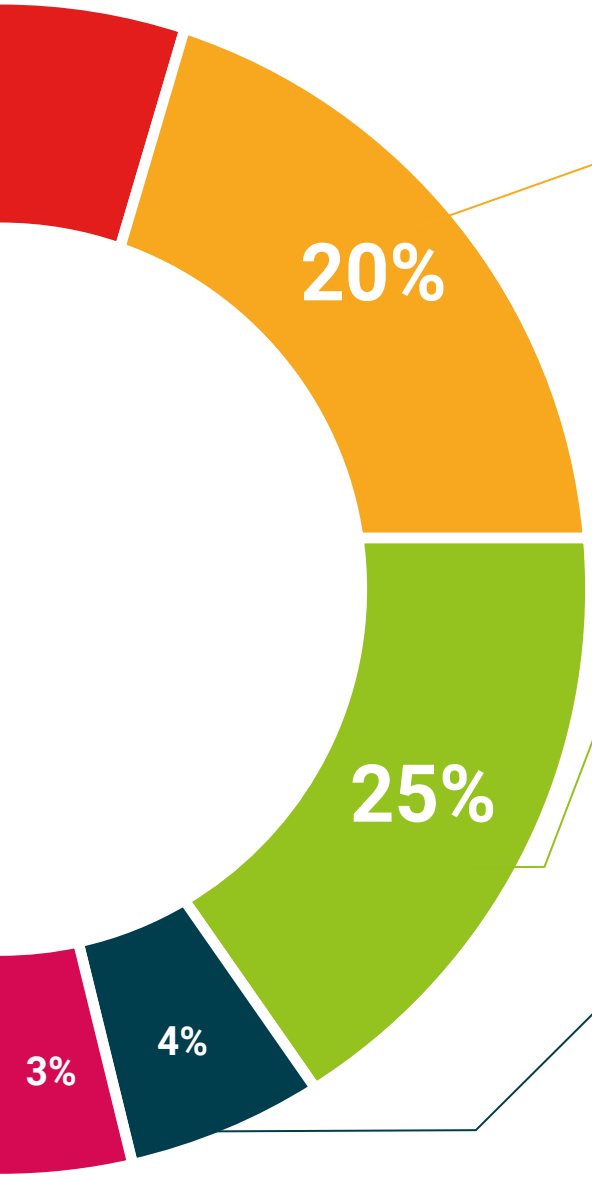
Pratiche di competenze e competenze

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.

05

Titolo

Il Esperto Universitario in Sicurezza Informatica delle Comunicazioni ti garantisce, oltre alla preparazione più rigorosa e aggiornata, l'accesso a una qualifica di Esperto Universitario rilasciata da TECH Global University.

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

Questo programma ti consentirà di ottenere il titolo di studio di **Esperto Universitario in Sicurezza Informatica delle Comunicazioni** rilasciato da **TECH Global University**, la più grande università digitale del mondo.

TECH Global University è un'Università Ufficiale Europea riconosciuta pubblicamente dal Governo di Andorra ***(bollettino ufficiale)***. Andorra fa parte dello Spazio Europeo dell'Istruzione Superiore (EHEA) dal 2003. L'EHEA è un'iniziativa promossa dall'Unione Europea che mira a organizzare il quadro formativo internazionale e ad armonizzare i sistemi di istruzione superiore dei Paesi membri di questo spazio. Il progetto promuove valori comuni, l'implementazione di strumenti congiunti e il rafforzamento dei meccanismi di garanzia della qualità per migliorare la collaborazione e la mobilità tra studenti, ricercatori e accademici.

Questo titolo privato di **TECH Global University** è un programma europeo di formazione continua e aggiornamento professionale che garantisce l'acquisizione di competenze nella propria area di conoscenza, conferendo allo studente che supera il programma un elevato valore curriculare.

Titolo: **Esperto Universitario in Sicurezza Informatica delle Comunicazioni**

Modalità: **online**

Durata: **6 mesi**

Accreditamento: **18 ECTS**


tech global university

Dott _____, con documento d'identità _____ ha superato con successo e ottenuto il titolo di:

Esperto Universitario in Sicurezza Informatica delle Comunicazioni

Si tratta di un titolo di studio privato corrispondente a 540 horas di durata equivalente a 18 ECTS, con data di inizio dd/mm/aaaa e data di fine dd/mm/aaaa.

TECH Global University è un'università riconosciuta ufficialmente dal Governo di Andorra il 31 de gennaio 2024, appartenente allo Spazio Europeo dell'Istruzione Superiore (EHEA).

In Andorra la Vella, 28 febbraio 2024

Dott. Pedro Navarro Illana
Rettore

código único TECH: AFWDR2SS techtitute.com/titulos

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

tech global university

Esperto Universitario
Sicurezza Informatica delle Comunicazioni

- Modalità: **online**
- Durata: **6 mesi**
- Titolo: **TECH Global University**
- Accreditamento: **18 ECTS**
- Orario: **a scelta**
- Esami: **online**

Esperto Universitario
Sicurezza Informatica delle Comunicazioni

tech global university