Esperto Universitario

Implementazione delle Politiche di Sicurezza Informatica

tech global university

tech global university

Esperto Universitario

Implementazione delle Politiche di Sicurezza Informatica

- 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-implementazione-politiche-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

Le aziende si concentrano sulla sicurezza dei computer e del cloud per prevenire il furto o la perdita di dati preziosi, ma trascurano altri aspetti della sicurezza che sono altrettanto importanti in un'azienda, come la protezione delle attrezzature fisiche e ambientali. In questo corso 100% online, i professionisti dell'informatica approfondiranno la protezione dei sistemi con l'implementazione di metodi di sicurezza avanzati per mantenere il controllo degli accessi e l'autorizzazione per ogni utente. Il tutto, con contenuti di qualità basati su video riassuntivi, letture specifiche e casi di studio che permetteranno di specializzarsi in un settore dell'IT che necessita di professionisti altamente qualificati.

Scopri le principali tecnologie di identificazione e autorizzazione e implementa sistemi informatici più sicuri con questo Esperto Universitario"

Investire nella sicurezza informatica è essenziale per le aziende e le istituzioni, tuttavia molte di esse si concentrano sui possibili attacchi informatici esterni e dimenticano di sviluppare una corretta politica di sicurezza fisica e ambientale per controllare l'accesso ai sistemi informatici. In questo Esperto Universitario, lo studente approfondirà i principali aspetti da tenere in considerazione per mettere in pratica questo compito, che non è affatto semplice.

Il programma, tenuto da esperti professionisti della sicurezza informatica, approfondisce come verificare lo stato di sicurezza di un sistema informatico attraverso i controlli CIS, analizzando tutti i sistemi di controllo degli accessi biometrici esistenti, la loro implementazione e la gestione dei rischi. Si affronta anche l'implementazione della crittografia nelle reti di comunicazione con i protocolli attuali più diffusi, sia simmetrici che asimmetrici.

L'autenticazione e l'identificazione avranno un posto importante in questa qualifica, dove i professionisti informatici svilupperanno una PKI, impareranno a conoscere la sua struttura e l'uso di questa infrastruttura per proteggere la rete attraverso l'uso di Certificati Digitali.

Si tratta di un'eccellente opportunità offerta da TECH per specializzarsi in un settore che richiede professionisti con conoscenze aggiornate e innovative nel campo della sicurezza informatica. Il modello di insegnamento 100% online permette di combinare l'apprendimento con altri ambiti della vita personale, in quanto gli studenti hanno bisogno solo di un dispositivo con una connessione a Internet per accedere a tutti i contenuti multimediali di qualità a loro disposizione.

Questo **Esperto Universitario in Implementazione delle Politiche di 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.
- Contenuti disponibili da qualsiasi dispositivo fisso o portatile provvisto di connessione a internet

Aggiorna le tue conoscenze sulla sicurezza informatica in caso di incendi e terremoti. Iscriviti a questo Esperto Universitario"

Scopri gli ultimi sviluppi nel riconoscimento delle impronte digitali, del volto, dell'iride e della retina come misure di sicurezza informatica"

Approfondisci i protocolli di comunicazione sicuri e previeni il furto di dati di alto valore. Iscriviti subito in TECH.

Gestisci perfettamente lo strumento Secure Shell e impedisci la fuga di informazioni aziendali.

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

Al termine di questo Esperto Universitario gli studenti saranno in grado di implementare politiche di sicurezza nel software e nell'hardware o di esaminare la biometria e i sistemi biometrici. Gli studenti saranno in grado di applicare varie tecniche di crittografia di rete come TLS, VPN o SSH e di controllare i migliori strumenti di monitoraggio del sistema attualmente disponibili sul mercato. L'ampia gamma di risorse e casi di studio fornirà un'esperienza di apprendimento molto vicina alla realtà che dovranno affrontare nel loro ambiente di lavoro.

Raggiungi una specializzazione nel campo della sicurezza informatica grazie a questo Esperto Universitario. Iscriviti ora"

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

Obiettivi specifici

Modulo 1. Implementazione pratica delle politiche di sicurezza software e hardware

- Determinare cosa sono l'autenticazione e l'identificazione
- Analizzare i diversi metodi di autenticazione esistenti e la loro implementazione pratica
- Implementare la corretta politica di controllo degli accessi per software e sistemi
- Stabilire le principali tecnologie di identificazione attuali
- Generare una conoscenza specialistica delle diverse metodologie esistenti per il bastioning dei sistemi

Modulo 2. Implementare le politiche di sicurezza fisica e ambientale in azienda

- Analizzare i termini area sicura e perimetro sicuro
- Esaminare la biometria e i sistemi biometrici
- Implementare le corrette politiche di sicurezza per la sicurezza fisica
- Sviluppare le normative vigenti sulle aree sicure dei sistemi informatici

Modulo 3. Politiche di Comunicazione Sicura in Azienda

- Proteggere una rete di comunicazione suddividendola in partizioni
- Analizzare i diversi algoritmi di crittografia utilizzati nelle reti di comunicazione
- Implementare varie tecniche di crittografia nella rete, come TLS, VPN o SSH

Modulo 4. Strumenti di monitoraggio nelle Politiche di Sicurezza dei Sistemi Informativi

- Sviluppare il concetto di monitoraggio e l'implementazione di metriche
- Configurare le tracce di audit sui sistemi e monitorare le reti
- Compilare i migliori strumenti di monitoraggio dei sistemi attualmente presenti sul mercato

Questo programma ti fornirà gli strumenti necessari per esaminare la biometria e i sistemi biometrici in un'azienda"

03

Direzione del corso

Questo Esperto Universitario dispone di un personale docente con esperienza nella gestione del web e nella sicurezza delle reti e dei sistemi di servizio. La sua vasta conoscenza di questo settore dell'informatica è stata la base della scelta. Gli studenti hanno la garanzia di essere guidati, durante i sei mesi di questo corso, da docenti che hanno la necessaria preparazione accademica e la pratica quotidiana nell'applicazione di strumenti, sistemi e protocolli di sicurezza nelle aziende. Con l'obiettivo finale di fornire un apprendimento di qualità, che permetta ai professionisti dell'informatica di progredire in questo settore.

Un personale docente con una vasta esperienza nel campo della sicurezza informatica sarà la tua garanzia di successo in questo processo di apprendimento"

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)
- Collaboratrice 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 questa Esperto Universitario ha sviluppato un programma di studi che integra tutte le conoscenze sull'implementazione pratica delle politiche di sicurezza nel software e nell'hardware, dedicando uno dei suoi moduli a trattare in modo approfondito i sistemi biometrici e la protezione da fattori ambientali come incendi o terremoti. Questo piano di studi presta, inoltre, particolare attenzione agli strumenti di monitoraggio dei sistemi e agli algoritmi crittografici. Il sistema *Relearning*, basato sulla reiterazione dei contenuti, e i casi eminentemente pratici permetteranno agli studenti di acquisire un solido apprendimento in modo semplice.

Adatta il carico didattico di questo corso alle tue esigenze. Accedi ai contenuti in qualsiasi momento e in qualsiasi luogo. Iscriviti"

Modulo 1. Implementazione pratica delle Politiche di sicurezza Software e Hardware

1.1. Implementazione pratica delle politiche di sicurezza del software e dell'hardware
- 1.1.1. Implementazione dell'identificazione e dell'autorizzazione
- 1.1.2. Implementazione delle tecniche di identificazione
- 1.1.3. Misure tecniche per l'autorizzazione

1.2. Tecnologie di identificazione e autorizzazione
- 1.2.1. Identificatore e OTP
- 1.2.2. *Token* USB o smart card PKI
- 1.2.3. Il tasto "Difesa riservata".
- 1.2.4. Il RFID Attivo

1.3. Politiche di sicurezza per l'accesso al software e ai sistemi
- 1.3.1. Implementazione delle politiche di controllo degli accessi
- 1.3.2. Implementazione delle politiche di accesso alle comunicazioni
- 1.3.3. Tipi di strumenti di sicurezza per il controllo degli accessi

1.4. Gestione degli accessi degli utenti
- 1.4.1. Gestione dei diritti di accesso
- 1.4.2. Segregazione dei ruoli e delle funzioni di accesso
- 1.4.3. Implementazione dei diritti di accesso nei sistemi

1.5. Controllo dell'accesso ai sistemi e alle applicazioni
- 1.5.1. Regola minima di accesso
- 1.5.2. Tecnologie di accesso sicuro
- 1.5.3. Politiche di sicurezza delle password

1.6. Tecnologie per i sistemi di identificazione
- 1.6.1. Directory attiva
- 1.6.2. OTP
- 1.6.3. PAP, CHAP
- 1.6.4. KERBEROS, DIAMETER, NTLM

1.7. CIS Controlli per il basamento del sistema
- 1.7.1. Controlli CIS di base
- 1.7.2. Controlli CIS fondamentali
- 1.7.3. Controlli CIS organizzativi

1.8. Sicurezza operativa
- 1.8.1. Protezione contro il codice maligno
- 1.8.2. Copie di backup
- 1.8.3. Registro di attività e monitoraggio

1.9. Gestione delle vulnerabilità tecniche
- 1.9.1. Vulnerabilità tecniche
- 1.9.2. Gestione delle vulnerabilità tecniche
- 1.9.3. Restrizioni all'installazione del software

1.10. Implementazione delle pratiche di politica di sicurezza
- 1.10.1. Vulnerabilità logiche
- 1.10.2. Implementazione delle politiche di difesa

Modulo 2. Implementare le Politiche di Sicurezza Fisica e Ambientale in Azienda

2.1. Aree sicure
- 2.1.1. Perimetro di sicurezza fisica
- 2.1.2. Lavorare in aree sicure
- 2.1.3. Sicurezza di uffici, sedi e risorse

2.2. Controlli fisici all'ingresso
- 2.2.1. Politiche di controllo degli accessi fisici
- 2.2.2. Sistemi di controllo dell'ingresso fisico

2.3. Vulnerabilità dell'accesso fisico
- 2.3.1. Principali vulnerabilità fisiche
- 2.3.2. Implementazione delle misure di salvaguardia

2.4. Sistemi biometrici fisiologici
- 2.4.1. Impronte digitali
- 2.4.2. Riconoscimento facciale
- 2.4.3. Riconoscimento dell'iride e della retina
- 2.4.4. Altri sistemi biometrici fisiologici

2.5. Sistemi biometrici comportamentali
- 2.5.1. Riconoscimento della firma
- 2.5.2. Riconoscimento della scrittura
- 2.5.3. Riconoscimento vocale
- 2.5.4. Altri sistemi biometrici comportamentali

2.6. Gestione del rischio nella biometria
- 2.6.1. Implementazione dei sistemi biometrici
- 2.6.2. Vulnerabilità dei sistemi biometrici

2.7. Implementazione dei criteri negli *Hosts*
- 2.7.1. Installazione del cablaggio e della sicurezza
- 2.7.2. Posizionamento delle apparecchiature
- 2.7.3. Uscita delle apparecchiature all'esterno dei locali
- 2.7.4. Apparecchiature informatiche incustodite e politica delle postazioni libere

2.8. Protezione dell'ambiente
- 2.8.1. Sistemi di protezione antincendio
- 2.8.2. Sistemi di protezione antisismica
- 2.8.3. Sistemi antisismici

2.9. Sicurezza dei centri di elaborazione dati
- 2.9.1. Porte di sicurezza
- 2.9.2. Sistemi di videosorveglianza (CCTV)
- 2.9.3. Controllo di sicurezza

2.10. Regolamenti internazionali sulla sicurezza fisica
- 2.10.1. IEC 62443- 62443-1 (europea)
- 2.10.2. NERC CIP-005-5 (USA)
- 2.10.3. NERC CIP-014-2 (USA)

Modulo 3. Politiche di Comunicazione Sicura in Azienda

3.1. Gestione della sicurezza nelle reti
- 3.1.1. Controllo e monitoraggio della rete
- 3.1.2. Segregazione della rete
- 3.1.3. Sistemi di sicurezza della rete

3.2. Protocolli di comunicazione sicuri
- 3.2.1. Modello TCP/IP
- 3.2.2. Protocollo IPSEC
- 3.2.3. Protocollo TLS

3.3. Protocollo TLS 1.3
- 3.3.1. Fasi di un processo TLS 1.3
- 3.3.2. Protocollo di Handshake
- 3.3.3. Protocollo di registrazione
- 3.3.4. Differenze con TLS 1.2

3.4. Algoritmi crittografici
- 3.4.1. Algoritmi crittografici utilizzati nelle comunicazioni
- 3.4.2. *Cipher-suites*
- 3.4.3. Algoritmi crittografici ammessi per TLS 1.3

3.5. Funzioni *Digest*
- 3.5.1. MD6
- 3.5.2. SHA

3.6. PKI. Infrastruttura a chiave pubblica
- 3.6.1. La PKI e le sue entità
- 3.6.2. Certificato digitale
- 3.6.3. Tipi di certificati digitali

3.7. Comunicazioni tunnel e trasporto
- 3.7.1. Comunicazioni a tunnel
- 3.7.2. Comunicazioni di trasporto
- 3.7.3. Implementazione del tunnel crittografato

3.8. SSH. *Secure Shell*
- 3.8.1. SSH. Capsula sicura
- 3.8.2. Funzionamento SSH
- 3.8.3. Strumenti SSH

3.9. Verifica dei sistemi crittografici
- 3.9.1. Test di integrità
- 3.9.2. Test del sistema crittografico

3.10. Sistemi crittografici
- 3.10.1. Vulnerabilità dei sistemi crittografici
- 3.10.2. Salvaguardie crittografiche

Modulo 4. Strumenti di monitoraggio nelle Politiche di Sicurezza dei Sistemi Informativi

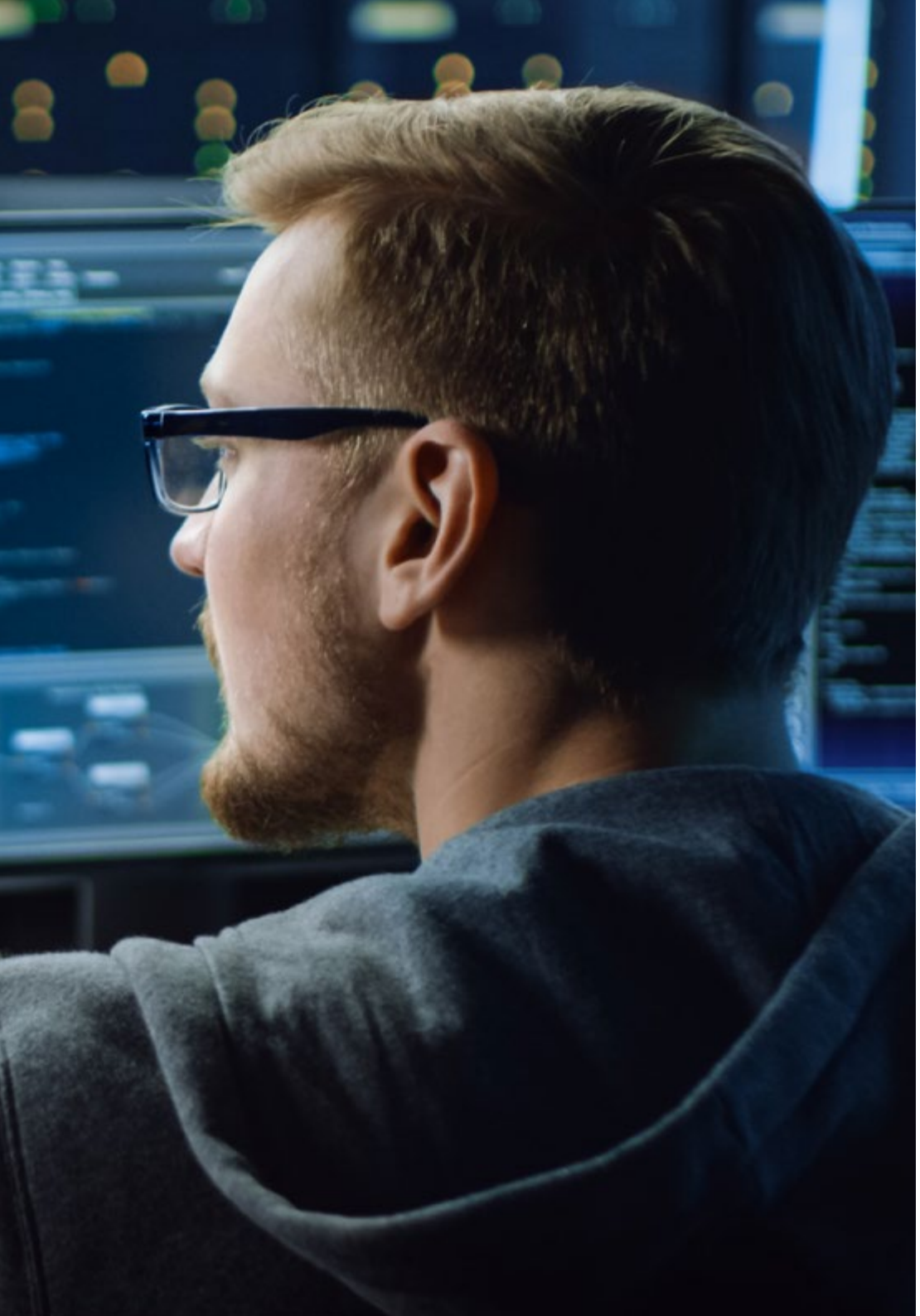
4.1. Politiche di monitoraggio dei sistemi informativi
- 4.1.1. Monitoraggio del sistema
- 4.1.2. Metriche
- 4.1.3. Tipi di metriche

4.2. Audit e registrazione nei sistemi
- 4.2.1. Audit e registrazione di Windows
- 4.2.2. Audit e registrazione su Linux

4.3. Protocollo SNMP. *Simple Network Management Protocol*
- 4.3.1. Protocollo SNMP
- 4.3.2. Funzionamento SNMP
- 4.3.3. Strumenti SNMP

4.4. Monitoraggio della rete
- 4.4.1. Monitoraggio della rete nei sistemi di controllo
- 4.4.2. Strumenti di monitoraggio per i sistemi di controllo

4.5. Nagios. Sistema di monitoraggio della rete
- 4.5.1. Nagios
- 4.5.2. Funzionamento di Nagios
- 4.5.3. Installazione di Nagios



4.6. Zabbix. Sistema di monitoraggio della rete
- 4.6.1. Zabbix.
- 4.6.2. Funzionamento di Zabbix
- 4.6.3. Installazione di Zabbix

4.7. Cacti. Sistema di monitoraggio della rete
- 4.7.1. Cacti.
- 4.7.2. Funzionamento di Cacti
- 4.7.3. Installazione di Cacti

4.8. Pandora. Sistema di monitoraggio della rete
- 4.8.1. Pandora
- 4.8.2. Funzionamento di Pandora
- 4.8.3. Installazione di Pandora

4.9. SolarWinds. Sistema di monitoraggio della rete
- 4.9.1. SolarWinds
- 4.9.2. Funzionamento di SolarWinds
- 4.9.3. Installazione di SolarWinds

4.10. Monitoraggio dei regolamenti
- 4.10.1. Controlli CIS su auditing e logging
- 4.10.2. NIST 800-123 (USA)

I riassunti interattivi e i casi di studio sviluppati dal personale docente ti forniranno i contenuti di cui hai bisogno per progredire nella tua carriera"

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

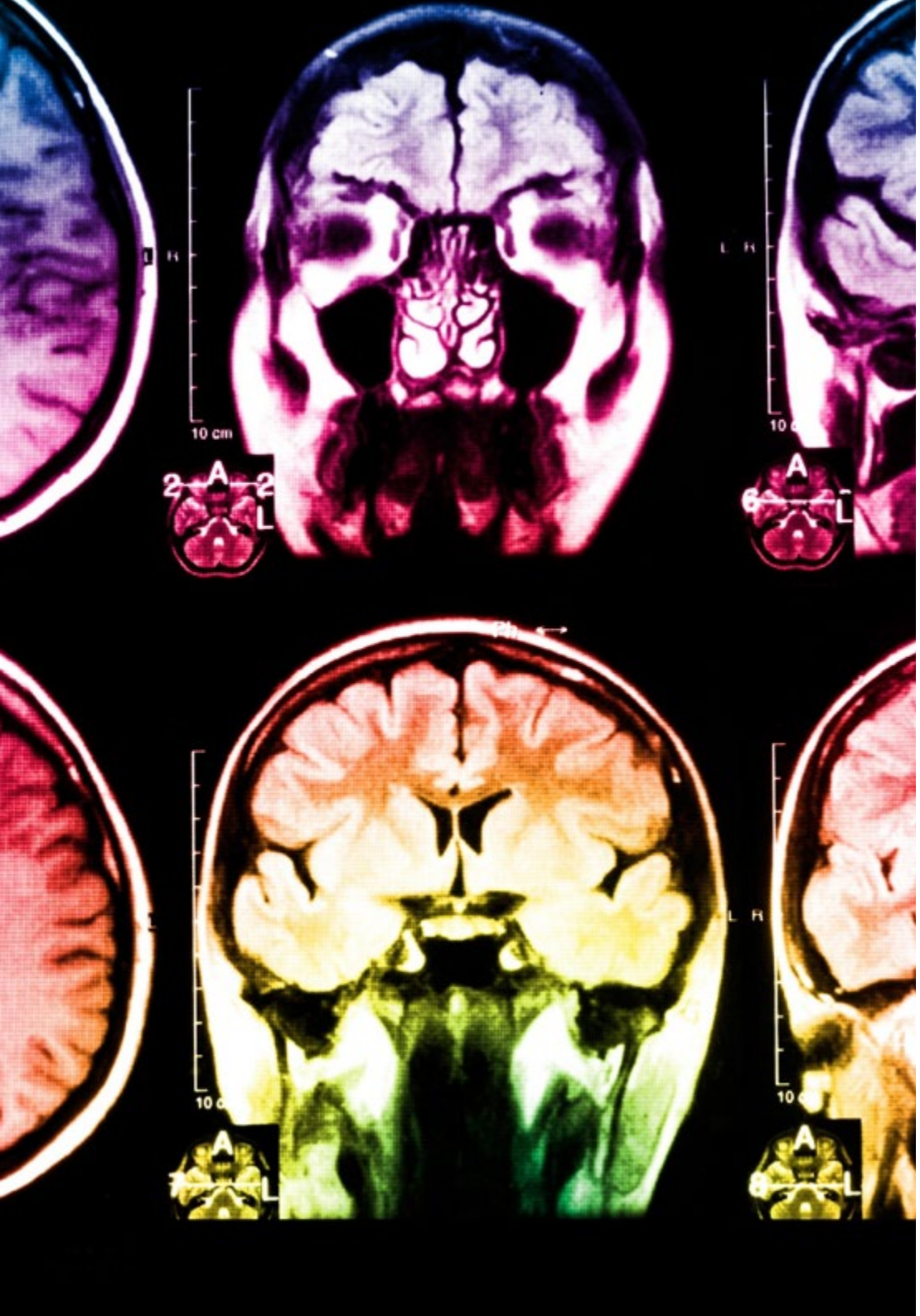
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

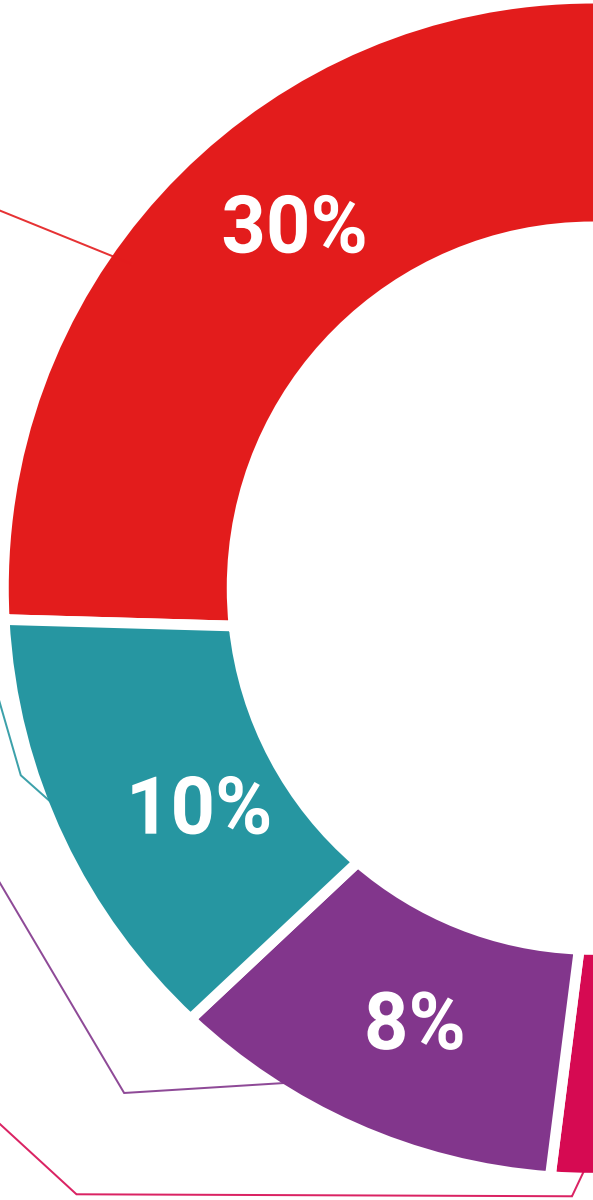
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

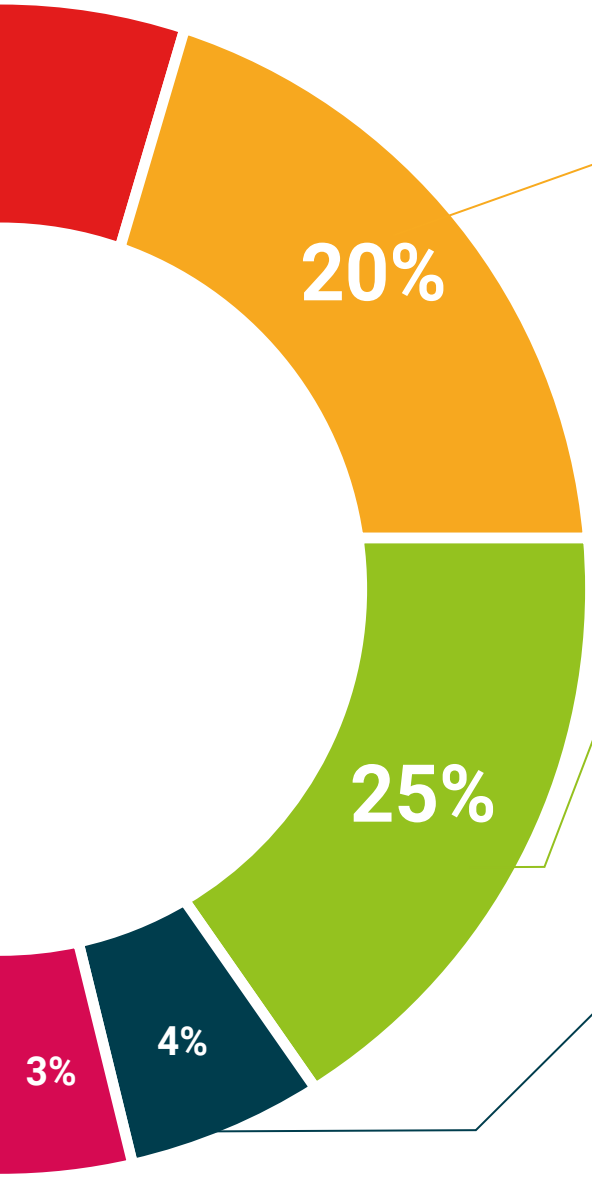
Pratiche di competenze e competenze

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 Implementazione delle Politiche di Sicurezza Informatica garantisce, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di 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 Implementazione delle Politiche di Sicurezza Informatica** 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 Implementazione delle Politiche di Sicurezza Informatica**

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 Implementazione delle Politiche di Sicurezza Informatica

Si tratta di un titolo di studio privato corrispondente a 450 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: AFWOR23S 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

Implementazione delle Politiche di Sicurezza Informatica

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

Esperto Universitario

Implementazione delle Politiche di Sicurezza Informatica

tech global university