Esperto Universitario
Gestione degli Incidenti di Sicurezza Informatica

tech università tecnologica

tech università tecnologica

Esperto Universitario
Gestione degli Incidenti di 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-gestione-incidenti-sicurezza-informatica

Indice

01

Presentazione

Le aziende sanno di essere esposte a un gran numero di attacchi informatici, motivo per cui l'implementazione di politiche di sicurezza è oggi essenziale per garantire la protezione dei dati sensibili. I professionisti informatici devono rispondere agli incidenti prevedibili subiti dall'entità e adottare misure preventive per evitare nuovi attacchi. Questo programma 100% online fornisce agli studenti tutti gli strumenti necessari per affrontare la sicurezza informatica. Il personale docente esperto in questo campo e l'ampia biblioteca con risorse multimediali, favoriranno l'apprendimento e la specializzazione dei professionisti in un settore che richiede elevate qualifiche.

Sarai preparato ad affrontare qualsiasi incidente di Sicurezza Informatica che un'azienda può trovarsi ad affrontare. Iscriviti a questo Esperto Universitario"

La sicurezza informatica sta diventando sempre più necessaria, visto il grande volume di dati sensibili in possesso di aziende e istituzioni. In molti casi, le cattive pratiche del personale o la mancanza di conoscenze in questo campo tecnologico portano a violazioni e incidenti. Questi possono talvolta generare perdite o compromettere seriamente l'immagine di un'entità.

Questo Esperto Universitario offre un insegnamento specializzato che consente l'analisi e la gestione degli incidenti, dal loro rilevamento attraverso i sistemi IDS/IPS e il loro successivo trattamento nel SIEM, fino al processo di notifica e di escalation al dipartimento corrispondente. Un intero processo che richiede professionisti informatici esperti con conoscenza degli strumenti utili per il monitoraggio dei sistemi informativi.

Questo programma, con un approccio eminentemente pratico, metterà gli studenti nella situazione di dover affrontare un attacco *Ransomware*, in modo che possano perfezionare le loro conoscenze nell'adozione di misure d'azione e protocolli di recupero.

La modalità 100% online di questo programma consente ai professionisti dell'informatica di accedere a contenuti multimediali di qualità fin dal primo giorno, senza orari fissi e da qualsiasi dispositivo con accesso a Internet. TECH facilita l'apprendimento degli studenti che desiderano combinare la loro vita lavorativa e personale con un'istruzione accessibile a tutti

Questo **Esperto Universitario in Gestione degli Incidenti 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

Padroneggia alla perfezione software di monitoraggio della rete come Nagios, Zabbix o Pandora con questo Esperto Universitario e tieni sotto controllo la tua strumentazione"

Fai un salto di qualità nella tua carriera professionale. Specializzati e fornisci risposte ai problemi di sicurezza informatica di aziende e istituzioni. Iscriviti ora"

Approfondisci lo standard ISO 27035 ed evita le violazioni della sicurezza che potrebbero minacciare le aziende. Iscriviti a questa qualifica.

Gestisci alla perfezione i protocolli e gli strumenti SNM con questo Esperto Universitario.

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

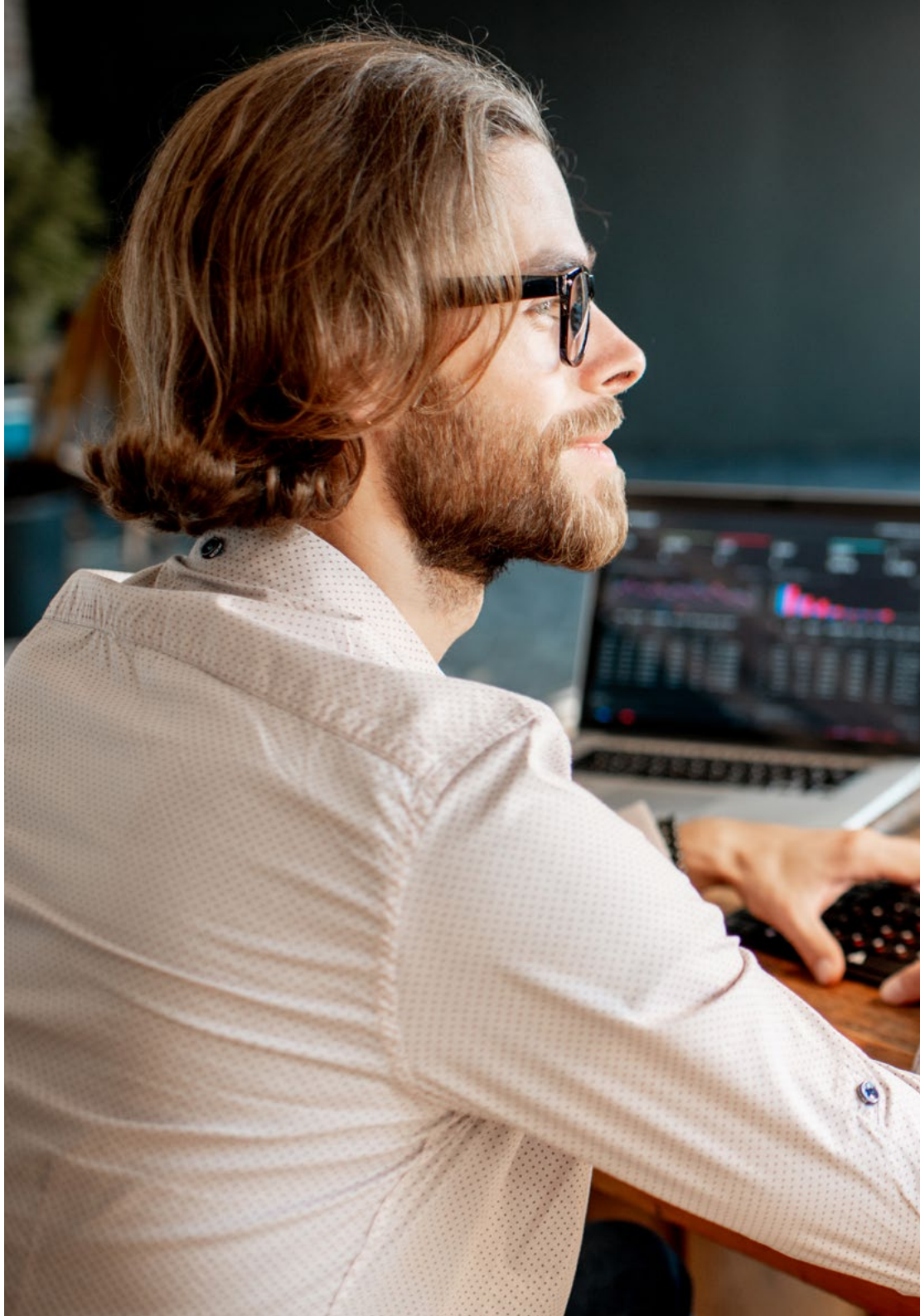
Durante i sei mesi di questo Esperto Universitario, gli studenti approfondiranno le loro conoscenze in materia di sicurezza informatica, che li porteranno, durante il corso, a sviluppare misure efficaci per garantire buone pratiche di sicurezza nelle aziende. Saranno in grado di verificare correttamente i sistemi e monitorare le reti con gli strumenti tecnologici più recenti. Alla fine del programma, saranno in grado di implementare un perfetto piano di sicurezza per le catastrofi. Le sintesi video di ogni argomento e le letture supplementari faciliteranno il raggiungimento di questi obiettivi.

Sviluppa il miglior piano di sicurezza informatica e diventa l'esperto di cui le aziende hanno bisogno per proteggersi”

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

La metodologia pedagogica di TECH ti permetterà di raggiungere i tuoi obiettivi più ambiziosi anche prima di quanto ti aspetti"



Obiettivi specifici

Modulo 1. 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 2. Strumenti di monitoraggio nelle Politiche di Sicurezza dei Sistemi Informativi

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

Modulo 3. Politica di Ripristino pratico in caso di Disastri di Sicurezza

- Generare conoscenze specialistiche sul concetto di continuità della sicurezza delle informazioni.
- Sviluppare un piano di continuità aziendale
- Analizzare un piano di continuità ICT
- Progettare un piano di disaster recovery

03

Direzione del corso

TECH fornisce agli studenti un apprendimento di qualità e adeguato agli ultimi sviluppi del settore, in questo caso della Sicurezza Informatica. In questo Esperto Universitario, il professionista informatico avrà accesso a un'ampia conoscenza, grazie alle conoscenze di un personale docente con una vasta esperienza nel campo della cybersecurity. Gli studenti avranno a disposizione un insegnamento vicino alla realtà che i professionisti vivono quotidianamente di fronte agli attacchi informatici.

Esperti di sicurezza in aziende pubbliche e private ti daranno le indicazioni per incrementare la tua carriera professionale in questo campo"

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. 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

Dott. Ortega López, Florencio

- Consulente per la sicurezza (Identity Management) presso il Gruppo SIA
- Consulente ICT e Sicurezza come libero professionista
- Docente istruttore nel settore dell'informatica
- Laureato in Ingegneria Tecnica Industriale presso l'Università di Alcalá de Henares
- Master per insegnanti dell'UNIR
- MBA in Economia Aziendale e Management di IDE-CESEM
- Master in Direzione e Gestione delle Tecnologie dell'Informazione dell'IDE-CESEM
- Certified Information Security Management (CISM) per la ISACA

04

Struttura e contenuti

Il programma di questo Esperto Universitario è stato pianificato per affrontare nei suoi tre moduli i punti chiave per la gestione degli incidenti di sicurezza informatica. Gli studenti impareranno a conoscere le politiche di gestione, i sistemi di rilevamento e prevenzione delle istruzioni. Inoltre, nel corso del programma, approfondiranno gli strumenti, i protocolli e gli audit nel campo della sicurezza. Un ruolo importante in questa qualifica sarà svolto anche dal recupero pratico dei disastri di sicurezza. I casi di studio e il sistema *Relearning*, basato sulla ripetizione dei contenuti, renderanno più facile e veloce per gli studenti consolidare tutte le conoscenze di questa qualifica.

L'ampia gamma di risorse multimediali arricchisce questo piano di studi messo a punto da esperti nel campo della sicurezza informatica"

Modulo 1. Politiche di Gestione degli Incidenti di Sicurezza

1.1. Politiche e miglioramenti per la gestione degli incidenti di sicurezza delle informazioni
- 1.1.1. Gestione degli imprevisti
- 1.1.2. Responsabilità e procedure
- 1.1.3. Notifica dell'evento

1.2. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 1.2.1. Dati di funzionamento del sistema
- 1.2.2. Tipi di sistemi di rilevamento delle intrusioni
- 1.2.3. Criteri di posizionamento degli IDS/IPS

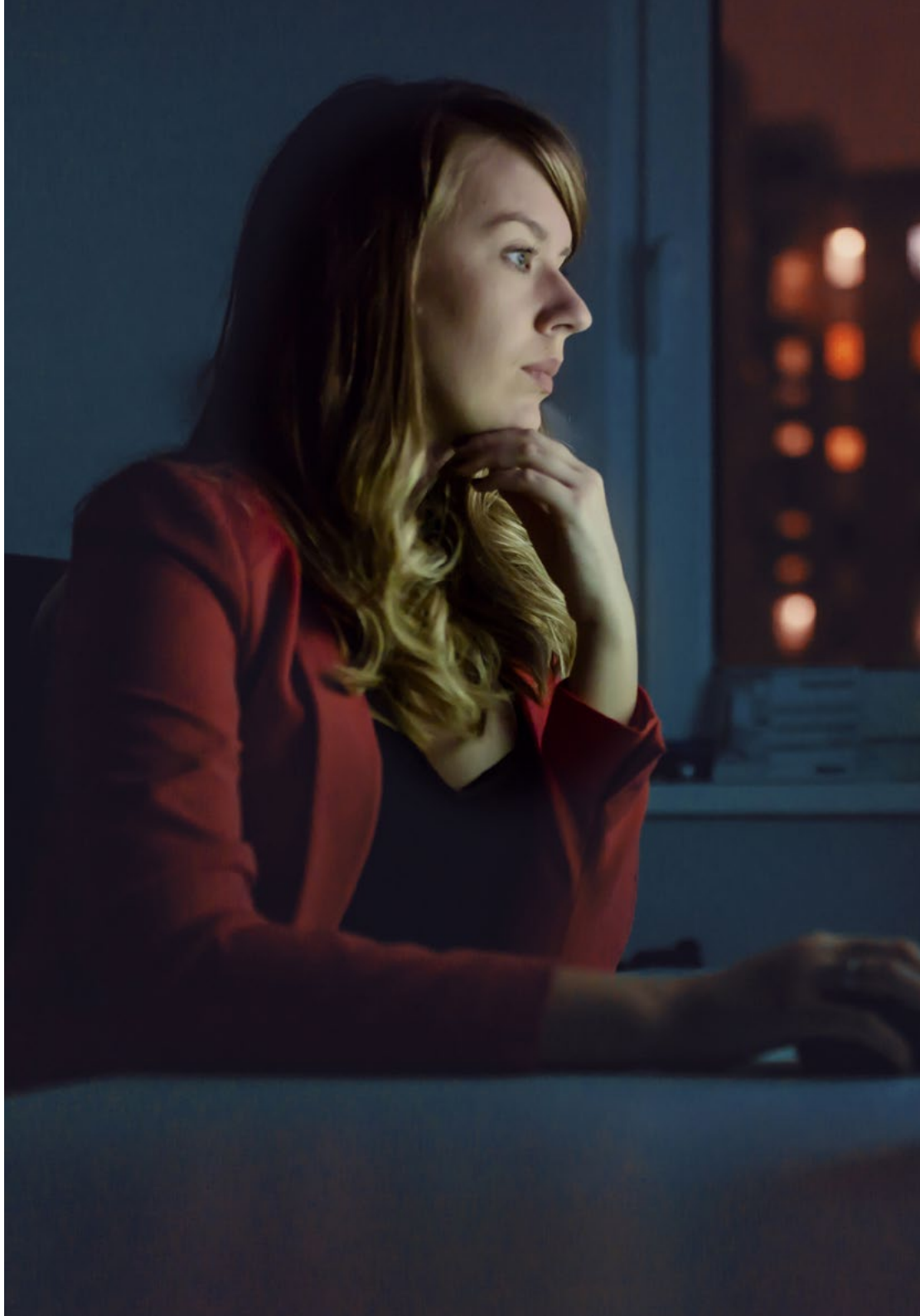
1.3. Risposta agli incidenti di sicurezza
- 1.3.1. Procedura di raccolta delle informazioni
- 1.3.2. Processo di verifica dell'intrusione
- 1.3.3. Organi del CERT

1.4. Processo di notifica e gestione dei tentativi di intrusione
- 1.4.1. Responsabilità nel processo di notifica
- 1.4.2. Classificazione degli incidenti
- 1.4.3. Processo di risoluzione e recupero

1.5. L'analisi forense come politica di sicurezza
- 1.5.1. Prove volatili e non volatili
- 1.5.2. Analisi e raccolta di prove elettroniche
  - 1.5.2.1. Analisi delle prove elettroniche
  - 1.5.2.2. Raccolta di prove elettroniche

1.6. Strumenti di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 1.6.1. Snort
- 1.6.2. Suricata
- 1.6.3. SolarWinds

1.7. Strumenti di centralizzazione degli eventi
- 1.7.1. SIM
- 1.7.2. SEM
- 1.7.3. SIEM



1.8. Guida alla sicurezza CCN-STIC
  1.8.1. Gestione degli incidenti informatici
  1.8.2. Metriche e indicatori
1.9. NIST SP800-61
  1.9.1. Capacità di risposta agli incidenti di sicurezza informatica
  1.9.2. Gestione degli incidenti
  1.9.3. Coordinamento e condivisione delle informazioni
1.10. Norma ISO 27035
  1.10.1. Norma ISO 27035. Principi di gestione degli incidenti
  1.10.2. Linee guida per lo sviluppo di un piano di gestione degli incidenti
  1.10.3. Linee guida per le operazioni di risposta agli incidenti

Modulo 2. Strumenti di monitoraggio nelle Politiche di Sicurezza dei Sistemi Informativi

2.1. Politiche di monitoraggio dei sistemi informativi
  2.1.1. Monitoraggio del sistema
  2.1.2. Metriche
  2.1.3. Tipi di metriche
2.2. Audit e registrazione nei sistemi
  2.2.1. Audit e registrazione nei sistemi
  2.2.2. Audit e registrazione di Windows
  2.2.3. Audit e registrazione su Linux
2.3. Protocollo SNMP. *Simple Network Management Protocol*
  2.3.1. Protocollo SNMP
  2.3.2. Funzionamento SNMP
  2.3.3. Strumenti SNMP
2.4. Monitoraggio della rete
  2.4.1. Monitoraggio della rete nei sistemi di controllo
  2.4.2. Strumenti di monitoraggio per i sistemi di controllo
2.5. Nagios. Sistema di monitoraggio della rete
  2.5.1. Nagios
  2.5.2. Funzionamento di Nagios
  2.5.3. Installazione di Nagios
2.6. Zabbix. Sistema di monitoraggio della rete
  2.6.1. Zabbix.
  2.6.2. Funzionamento di Zabbix
  2.6.3. Installazione di Zabbix
2.7. Cacti. Sistema di monitoraggio della rete
  2.7.1. Cacti.
  2.7.2. Funzionamento di Cacti
  2.7.3. Installazione di Cacti
2.8. Pandora. Sistema di monitoraggio della rete
  2.8.1. Pandora
  2.8.2. Funzionamento di Pandora
  2.8.3. Installazione di Pandora
2.9. SolarWinds. Sistema di monitoraggio della rete
  2.9.1. SolarWinds
  2.9.2. Funzionamento di SolarWinds
  2.9.3. Installazione di SolarWinds
2.10. Monitoraggio dei regolamenti
  2.10.1. Controlli CIS su auditing e logging
  2.10.2. NIST 800-123 (USA)

Modulo 3. Politica di Ripristino pratico in caso di Disastri di Sicurezza

3.1. DRP. Piano di Disaster Recovery
  3.1.1. Obiettivo di un DRP
  3.1.2. Benefici di un DRP
  3.1.3. Conseguenze della mancanza di un DRP e del suo mancato aggiornamento
3.2. Linee guida per la definizione di un DRP (Disaster Recovery Plan)
  3.2.1. Ambito e obiettivi
  3.2.2. Progettazione della strategia di ripristino
  3.2.3. Assegnazione di ruoli e responsabilità
  3.2.4. Inventario di hardware, software e servizi
  3.2.5. Tolleranza ai tempi di inattività e alla perdita di dati
  3.2.6. Stabilire i tipi specifici di DRP richiesti
  3.2.7. Implementazione di un piano di training, sensibilizzazione e comunicazione

3.3. Ambito e obiettivi di un DRP (Disaster Recovery Plan)
- 3.3.1. Garantire la risposta
- 3.3.2. Componenti tecnologiche
- 3.3.3. Ambito di applicazione della politica di continuità

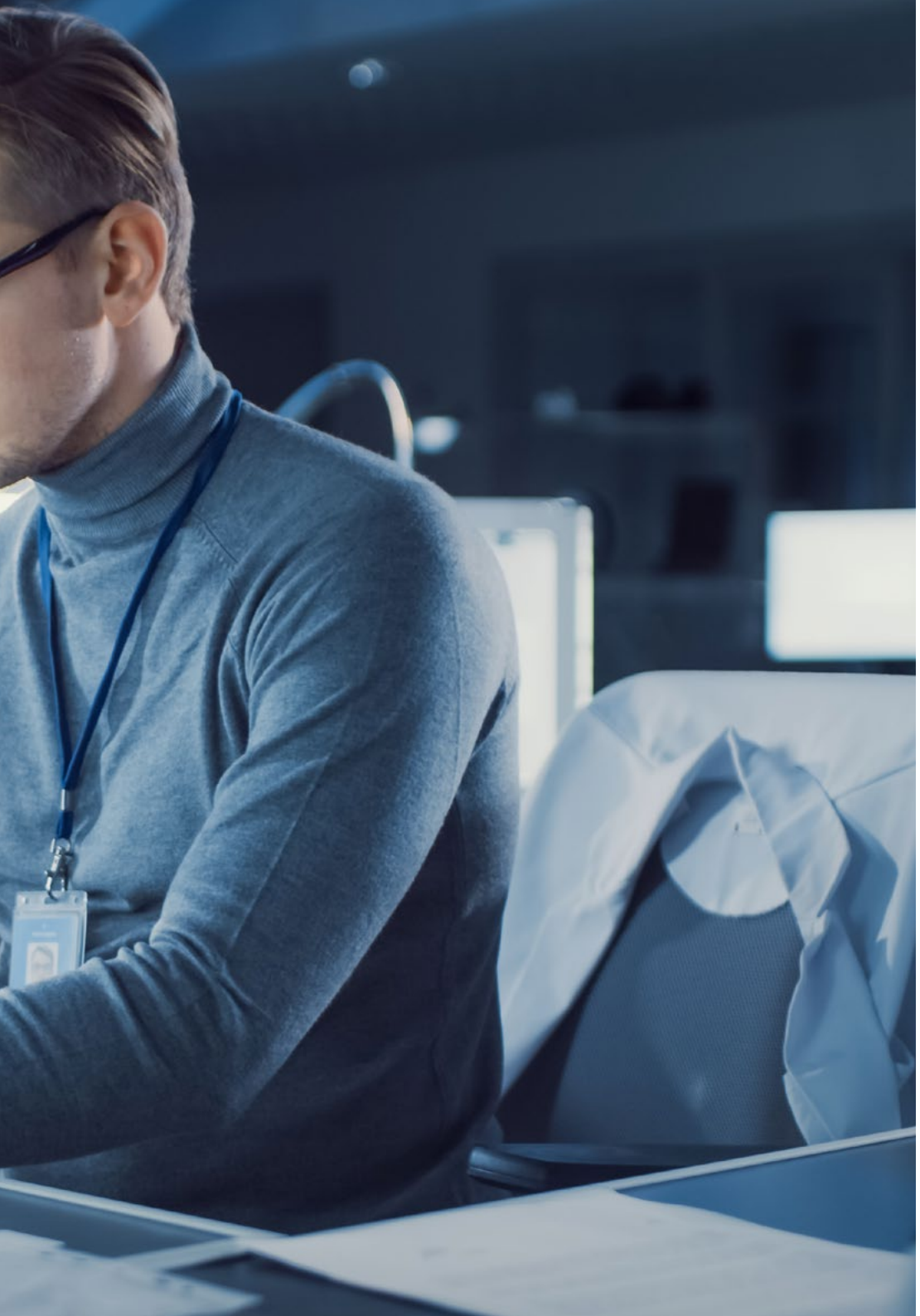
3.4. Progettazione di una strategia DRP (Disaster Recovery Plan)
- 3.4.1. Strategia di Disaster Recovery
- 3.4.2. Budget
- 3.4.3. Risorse umane e Fisiche
- 3.4.4. Posizioni dirigenziali a rischio
- 3.4.5. Tecnologia
- 3.4.6. Dati

3.5. Continuità dei processi informativi
- 3.5.1. Pianificazione della continuità
- 3.5.2. Attuazione della continuità
- 3.5.3. Verifica e valutazione della continuità

3.6. Ambito di applicazione di un BCP (Business Continuity Plan)
- 3.6.1. Determinazione dei processi più critici
- 3.6.2. Approccio basato sugli asset
- 3.6.3. Approccio per processi

3.7. Implementazione di processi aziendali protetti
- 3.7.1. Attività prioritarie (PA)
- 3.7.2. Tempi di recupero ideali (IRT)
- 3.7.3. Strategie di sopravvivenza

3.8. Analisi dell'organizzazione
- 3.8.1. Raccolta di informazioni
- 3.8.2. Analisi dell'impatto aziendale (BIA)
- 3.8.3. Analisi del rischio organizzativo



3.9. Risposta alla contingenza
- 3.9.1. Piano di crisi
- 3.9.2. Piani di recupero dell'ambiente operativo
- 3.9.3. Piani di recupero dell'ambiente operativo

3.10. Standard internazionale ISO 27031 BCP
- 3.10.1. Obiettivi
- 3.10.2. Termini e definizioni
- 3.10.3. Operazione

Il sistema Relearning e la modalità 100% online saranno i tuoi alleati per raggiungere un apprendimento molto utile nel tuo campo 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

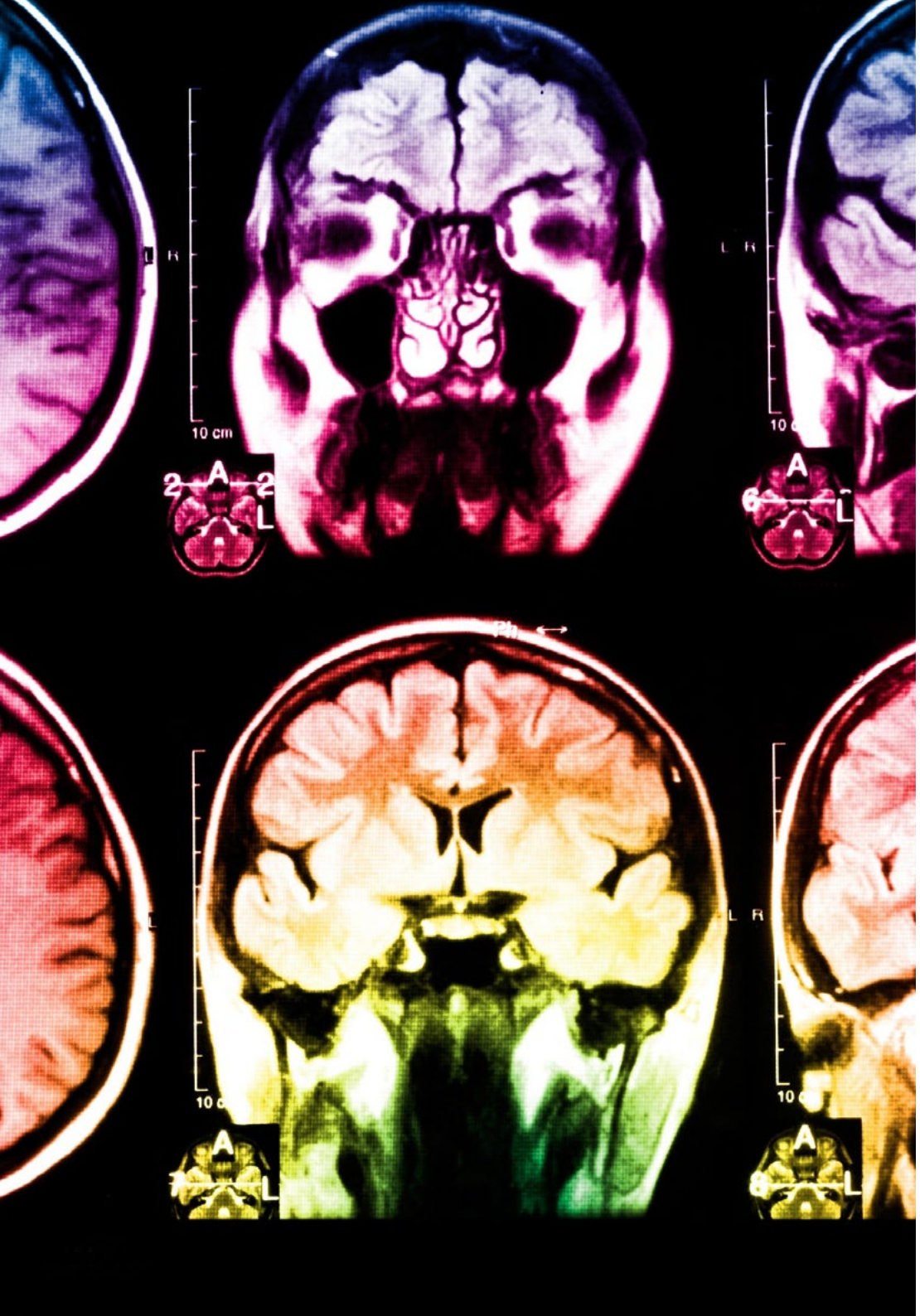
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

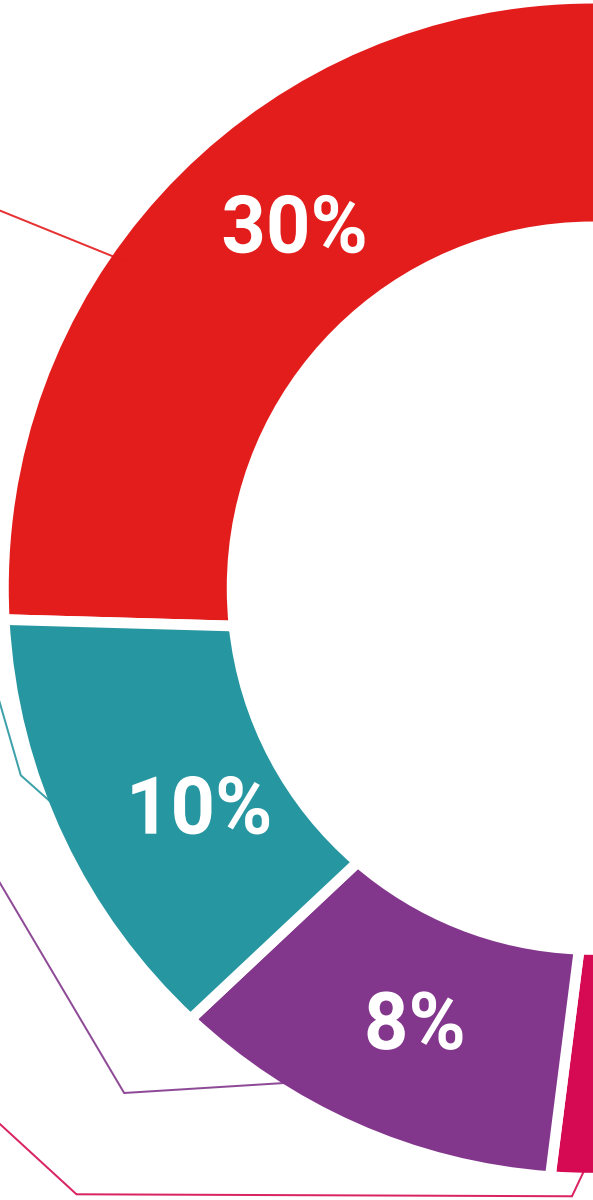
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

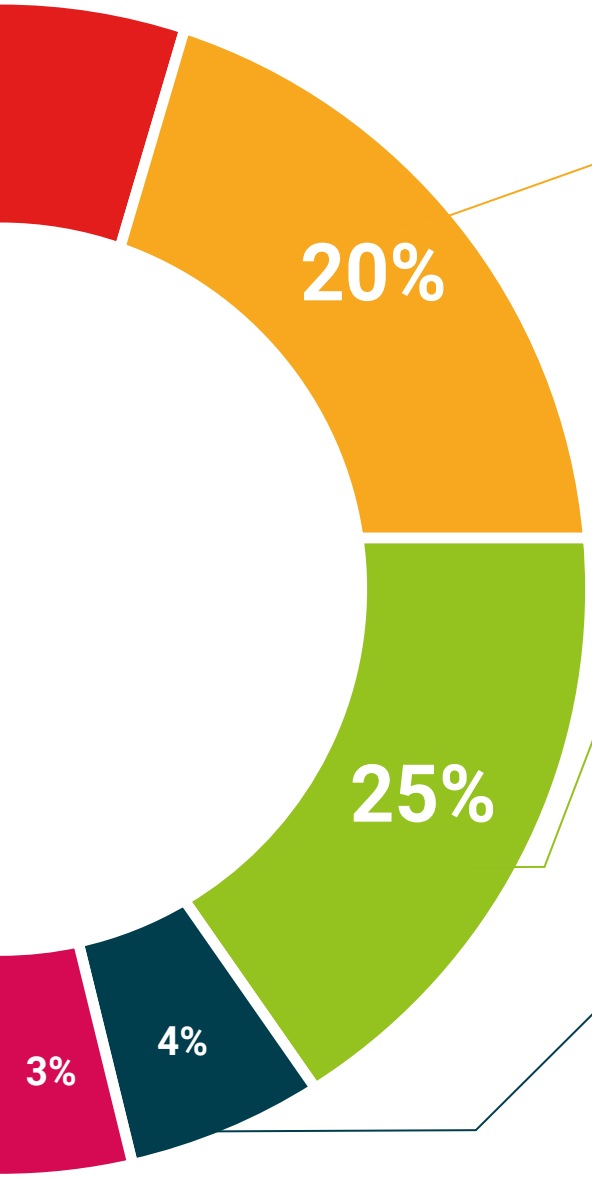
Pratiche di competenze e competenze

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 Gestione degli Incidenti di 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 Gestione degli Incidenti di 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 Gestione degli Incidenti di 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

Gestione degli Incidenti di 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

Gestione degli Incidenti di Sicurezza Informatica

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

Esperto Universitario

Gestione degli Incidenti di Sicurezza Informatica

tech università tecnologica