Master Privato in

Gestione delle Politiche Aziendali di Cybersicurezza

MGPCE

tech universidad tecnológica

tech universidad tecnológica

Master Privato in
Gestione delle Politiche Aziendali di Cybersicurezza

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Università Tecnologica**
- Dedizione: **16 ore/settimana**
- Orario: **a scelta**
- Esami: **online**
- Rivolto a: **Laureati che abbiano precedentemente conseguito una qualsiasi delle qualifiche del campo delle Scienze Sociali e Giuridiche, Amministrative e Aziendali.**

Accesso al sito web: **www.techtitute.com/it/business-school/master/gestione-politiche-aziendali-cybersicurezza**

Indice

01

Benvenuto

Al giorno d'oggi, le perdite dovute agli attacchi cibernetici sono stimate in milioni e milioni di euro. L'esposizione agli attacchi cibernetici è tale che anche gli Stati possono essere bersaglio di questo tipo di incidenti. Ciò ha evidenziato l'importanza di avere a disposizione responsabili specializzati nella gestione delle politiche di cybersicurezza, in possesso dei giusti strumenti organizzativi, di implementazione e di monitoraggio per coordinare tutti gli sforzi di sicurezza informatica. Questo programma prepara i manager ad affrontare scenari incerti con sicurezza e conoscenze avanzate, fornendo soluzioni di qualità nel campo della sicurezza informatica. Mediante un contenuto teorico esaustivo, basato su casi di studio reali, si potrà acquisire una prospettiva moderna e completa rispetto a tutte le funzioni che deve svolgere un manager della cybersicurezza. Il tutto, inoltre, in un formato 100% online, senza lezioni frontali e orari prestabiliti, con una flessibilità totale.

Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza.
TECH Università Tecnologica

Apporta un valore aggiunto incalcolabile alle tue politiche di Cybersicurezza, grazie alla conoscenza di tutte le sfumature, degli stessi sistemi di sicurezza e delle pratiche di analisi delle minacce, che ti daranno gli elementi chiave per ottenere una posizione di vantaggio nella tua organizzazione"

02

Perché studiare in TECH?

TECH è la più grande business school del mondo che opera al 100% in modalità online. Si tratta di una Business School d'élite, con un modello dotato dei più alti standard accademici. Un centro internazionale ad alto rendimento per la preparazione intensiva di competenze manageriali.

TECH è l'università all'avanguardia della tecnologia, che mette tutte le sue risorse a disposizione dello studente con l'obiettivo di aiutarlo a raggiungere il successo aziendale"

In TECH Università Tecnologica

Innovazione

L'università offre un modello di apprendimento online che combina le ultime tecnologie educative con il massimo rigore pedagogico. Un metodo unico con il più alto riconoscimento internazionale che fornirà allo studente le chiavi per inserirsi in un mondo in costante cambiamento, in cui l'innovazione è concepita come la scommessa essenziale di ogni imprenditore.

"Caso di Successo Microsoft Europa" per aver incorporato l'innovativo sistema multivideo interattivo nei nostri programmi.

Massima esigenza

Il criterio di ammissione di TECH non si basa su criteri economici. Non è necessario effettuare un grande investimento per studiare in questa Università. Tuttavia, per ottenere una qualifica rilasciata da TECH, i limiti dell'intelligenza e della capacità dello studente saranno sottoposti a prova. I nostri standard accademici sono molto alti...

95% | **degli studenti di TECH termina i suoi studi con successo.**

Networking

In TECH partecipano professionisti provenienti da tutti i Paesi del mondo al fine di consentire allo studente di creare una vasta rete di contatti utile per il suo futuro.

+100.000
manager specializzati ogni anno

+200
nazionalità differenti

Empowerment

Lo studente cresce di pari passo con le migliori aziende e con professionisti di grande prestigio e influenza. TECH ha sviluppato alleanze strategiche e una preziosa rete di contatti con i principali esponenti economici dei 7 continenti.

+500 | **Accordi di collaborazione con le migliori aziende**

Talento

Il nostro programma è una proposta unica per far emergere il talento dello studente nel mondo imprenditoriale. Un'opportunità unica di affrontare i timori e la propria visione relativi al business.

TECH si propone di aiutare gli studenti a mostrare al mondo il proprio talento grazie a questo programma.

Contesto Multiculturale

Gli studenti che intraprendono un percorso con TECH possono godere di un'esperienza unica. Studierai in un contesto multiculturale. Lo studente, inserito in un contesto globale, potrà addentrarsi nella conoscenza dell'ambito lavorativo multiculturale mediante una raccolta di informazioni innovativa e che si adatta al proprio concetto di business.

Gli studenti di TECH provengono da oltre 200 nazioni differenti.

Impara con i migliori

Il personale docente di TECH contribuisce a mostrare agli studenti il proprio bagaglio di esperienze attraverso un contesto reale, vivo e dinamico. Si tratta di docenti impegnati a offrire una specializzazione di qualità che permette allo studente di avanzare nella sua carriera e distinguersi in ambito imprenditoriale.

Professori provenienti da 20 nazionalità differenti.

In TECH avrai accesso ai casi di studio più rigorosi e aggiornati del mondo accademico"

TECH punta all'eccellenza e dispone di una serie di caratteristiche che la rendono unica:

Analisi

In TECH esploriamo il lato critico dello studente, la sua capacità di mettere in dubbio le cose, la sua competenza nel risolvere i problemi e le sue capacità interpersonali.

Eccellenza accademica

TECH offre agli studenti la migliore metodologia di apprendimento online. L'università combina il metodo *Relearning* (la metodologia di apprendimento post-laurea meglio valutata a livello internazionale), con i casi di studio. Tradizione e avanguardia in un difficile equilibrio e nel contesto del più esigente itinerario educativo.

Economia di scala

TECH è la più grande Università online del mondo. Dispone di oltre 10.000 corsi di specializzazione universitaria. Nella nuova economia **volume + tecnologia = prezzo dirompente**. In questo modo, garantiamo che lo studio non sia eccessivamente costoso rispetto ad altre università.

03

Perché scegliere il nostro programma?

Studiare con TECH significa moltiplicare le tue possibilità di raggiungere il successo professionale nell'ambito del Senior Management.

È una sfida che comporta sforzo e dedizione, ma che apre le porte a un futuro promettente. Lo studente imparerà dai migliori insegnanti e con la metodologia educativa più flessibile e innovativa.

Disponiamo del personale docente più prestigioso e del programma più completo del mercato, il che ci permette di offrire una qualifica di altissimo livello accademico"

Questo programma fornirà molteplici vantaggi professionali e personali, tra i seguenti:

01 Dare una spinta decisiva alla carriera di studente

Studiando in TECH, lo studente può prendere le redini del suo futuro e sviluppare tutto il suo potenziale. Completando il nostro programma acquisirà le competenze necessarie per ottenere un cambio positivo nella sua carriera in poco tempo.

Il 70% dei partecipanti a questa specializzazione ottiene un cambiamento di carriera positivo in meno di 2 anni.

02 Svilupperai una visione strategica e globale dell'azienda

TECH offre una visione approfondita della gestione generale per comprendere come ogni decisione influenzi le diverse aree funzionali dell'azienda.

La nostra visione globale di azienda migliorerà la tua visione strategica.

03 Consolidare lo studente nella gestione aziendale superiore

Studiare in TECH significa avere accesso ad un panorama professionale di grande rilevanza, che permette agli studenti di ottenere un ruolo di manager di alto livello e di possedere un'ampia visione dell'ambiente internazionale.

Lavorerai con più di 100 casi reali di alta direzione.

04 Assumerai nuove responsabilità

Durante il programma vengono mostrate le ultime tendenze, gli sviluppi e le strategie per svolgere il lavoro professionale in un contesto in continuo cambiamento.

Il 45% degli studenti ottiene una promozione interna nel proprio lavoro.

05

Accesso a un'importante rete di contatti

TECH crea reti di contatti tra i suoi studenti per massimizzare le opportunità. Studenti con le stesse preoccupazioni e il desiderio di crescere. Così, sarà possibile condividere soci, clienti o fornitori.

Troverai una rete di contatti essenziali per la tua crescita professionale.

06

Sviluppare il progetto di business in modo rigoroso

Lo studente acquisirà una profonda visione strategica che lo aiuterà a sviluppare il proprio progetto, considerando le diverse aree dell'azienda.

Il 20% dei nostri studenti sviluppa la propria idea di business.

07

Migliorare le *soft skills* e le competenze direttive

TECH aiuta lo studente ad applicare e sviluppare le conoscenze acquisite e migliorare le capacità interpersonali per diventare un leader che faccia la differenza.

Migliora le tue capacità di comunicazione e di leadership e dai una spinta alla tua professione.

08

Farai parte di una comunità esclusiva

Lo studente farà parte di una comunità di manager d'élite, grandi aziende, istituzioni rinomate e professori qualificati delle università più prestigiose del mondo: la comunità di TECH Università Tecnologica.

Ti diamo l'opportunità di specializzarti con un personale docente di reputazione internazionale.

04

Obiettivi

Essendo la cybersicurezza un aspetto cruciale nello sviluppo di qualsiasi azienda moderna, l'obiettivo di questo programma non poteva che essere quello di offrire la migliore specializzazione possibile nella gestione delle politiche relative a questa tematica. A tal fine, il personale docente, composto da esperti informatici, ha compilato un materiale didattico completo, interamente centrato sul miglioramento delle capacità, delle competenze e delle abilità del manager.

Diventa un leader nella gestione della sicurezza informatica della tua organizzazione, imparando tutti i dettagli delle politiche di sicurezza informatica più efficaci"

TECH fa suoi gli obiettivi dei suoi studenti. Lavoriamo insieme per raggiungerli.

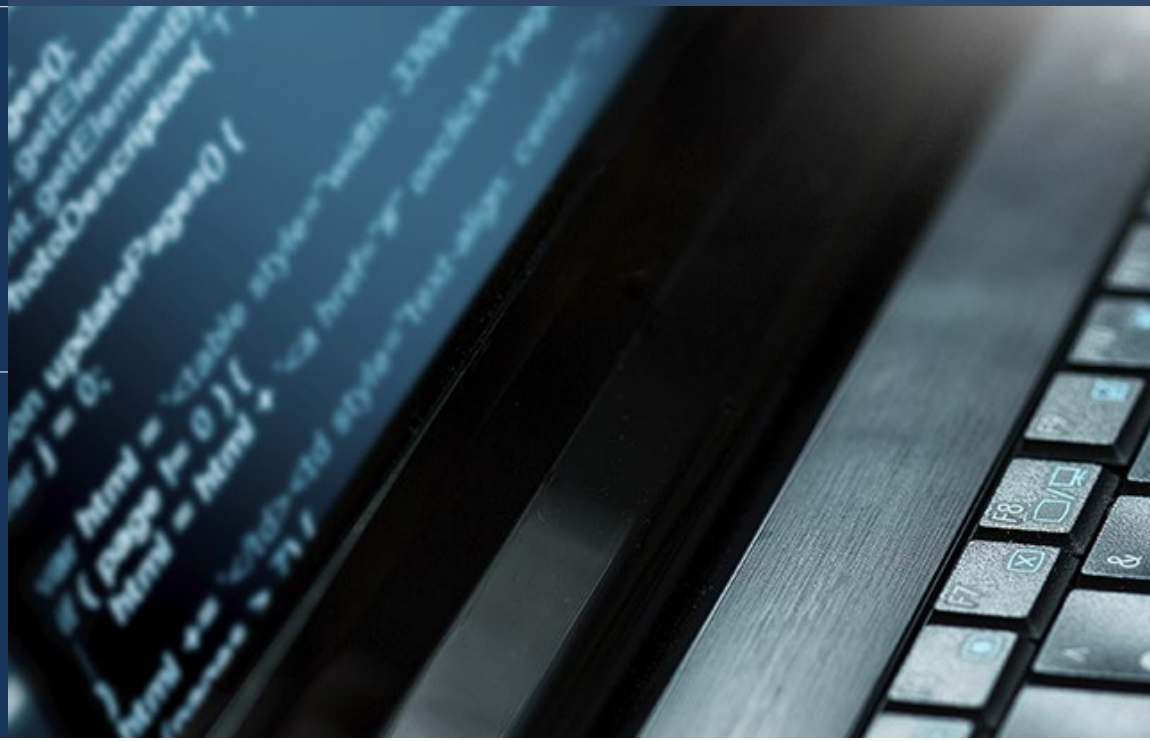
Il **Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza** preparerà lo studente per:

01 Approfondire la comprensione dei concetti chiave della sicurezza informatica

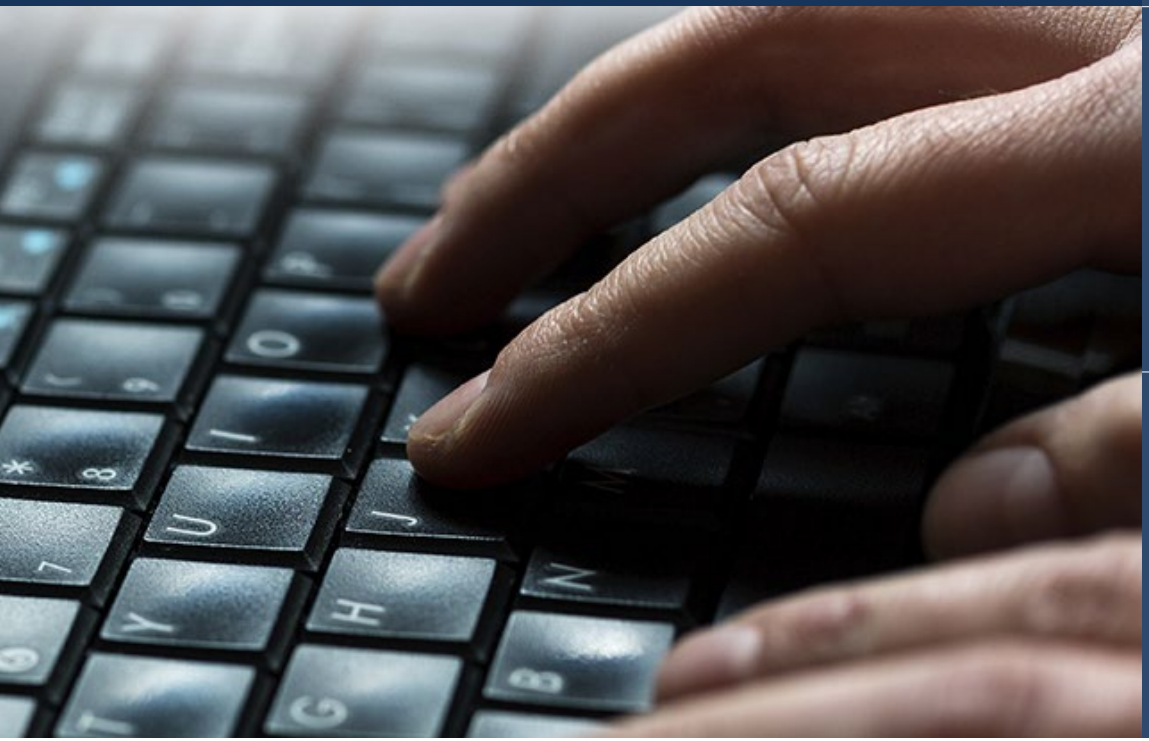
02 Analizzare le normative e gli standard attualmente applicabili ai SGSI

03 Implementare un SGSI aziendale

04 Determinare quali dipartimenti devono essere coperti dal sistema di gestione della sicurezza



05 Sviluppare le misure necessarie per garantire buone pratiche di sicurezza informatica



06 Determinare cosa si intende per autenticazione e identificazione

07 Analizzare i diversi metodi di autenticazione esistenti e la loro implementazione pratica

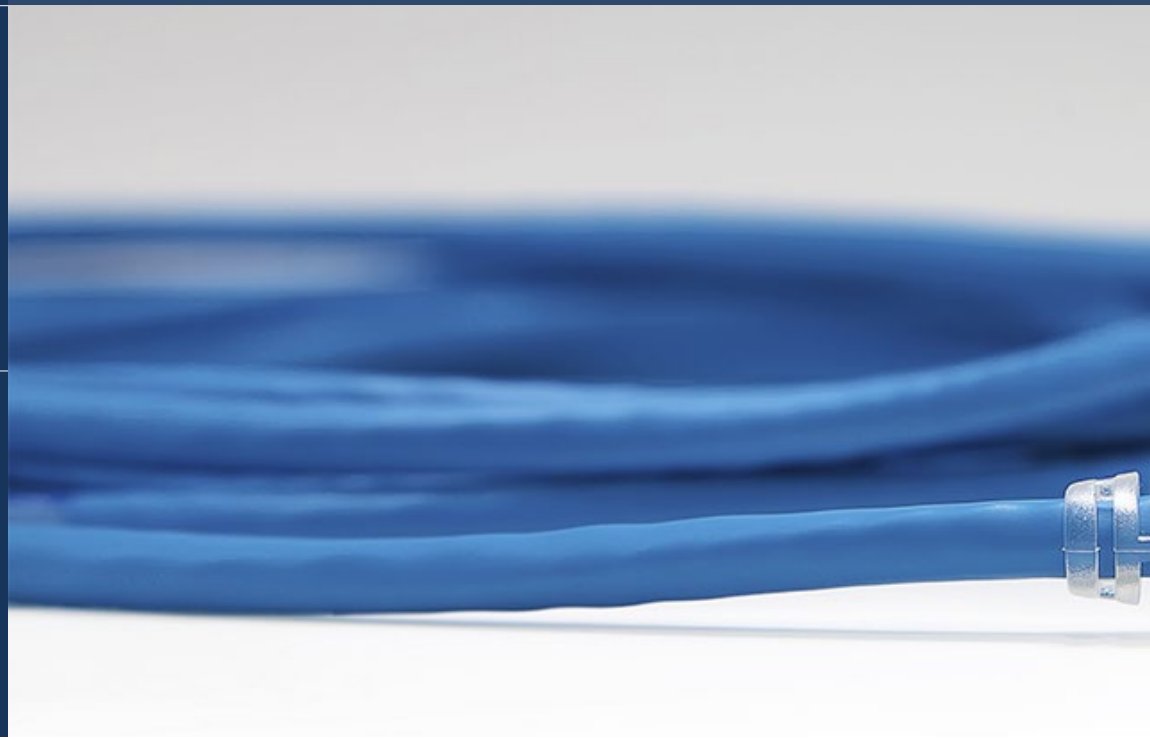
08 Implementare la corretta politica di controllo degli accessi per il software e i sistemi

09 Sviluppare competenze su come gestire gli incidenti causati da eventi di sicurezza informatica

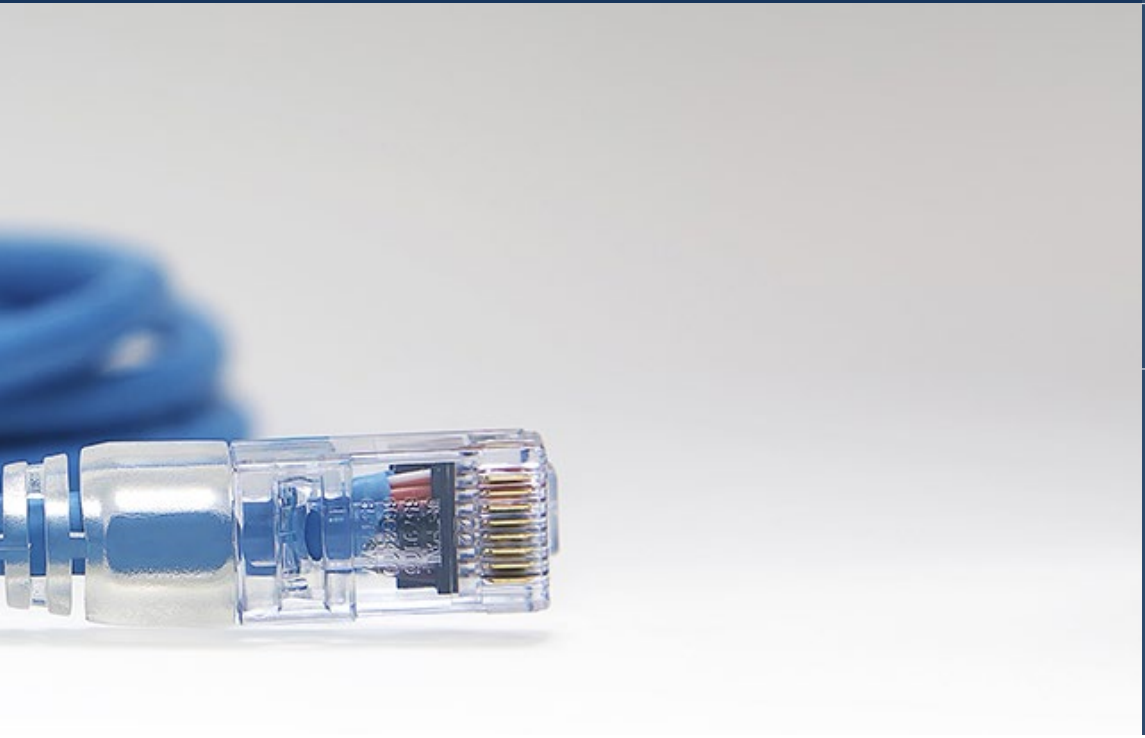
10 Analizzare i termini area sicura e perimetro sicuro

11 Analizzare i diversi algoritmi di crittografia utilizzati nelle reti di comunicazione

12 Determinare i diversi attacchi effettivi al nostro sistema informatico



13 Valutare le diverse politiche di sicurezza per mitigare gli attacchi



14 Sviluppare il concetto di monitoraggio e di implementazione delle metriche

15 Generare competenze sul concetto di continuità della sicurezza delle informazioni

16 Determinare cos'è la crittografia e i tipi di crittografia

05

Competenze

Un'adeguata gestione delle politiche di cybersicurezza richiede una grande capacità organizzativa, oltre a conoscenze e competenze informatiche e tecnologiche di alto livello. Per questo motivo, nel corso di questo programma, il manager non solo troverà un'utile guida di riferimento per la gestione della sicurezza informatica, ma rafforzerà anche le proprie capacità di leadership e di gestione amministrativa.

Affinerai le competenze necessarie a eccellere come manager esperto in politiche di cybersicurezza e ti troverai in una posizione di vantaggio per occupare le più prestigiose posizioni dirigenziali"

01 Determinare il coinvolgimento di un SGSI nell'organizzazione interna dell'ente, nonché lo stato del SGSI

02 Stabilire le politiche di sicurezza aziendale

03 Determinare le misure da attuare con i fornitori e la manutenzione dei sistemi informativi

04 Generare conoscenze specialistiche sul controllo delle minacce

05 Determinare le fasi della gestione preventiva delle minacce

06 Sviluppare metodologie per l'analisi delle minacce informatiche

07 Classificare le minacce in base all'impatto e alla gravità

08 Progettare una metodologia propria per l'analisi e il controllo preventivo delle minacce

09 Implementare la politica corretta di controllo degli accessi alla rete e ai servizi

10 Analizzare l'importanza di una corretta gestione degli incidenti di sicurezza

11 Compilare i diversi sistemi biometrici esistenti

12 Esaminare la biometria e i sistemi biometrici

13 Implementare le corrette politiche di sicurezza fisica e i sistemi di controllo degli accessi fisici nei data center

14 Implementare una rete sicura

16 Stabilire i tipi di ingegneria sociale e imparare a mitigarli

17 Analizzare il concetto di monitoraggio e di implementazione delle metriche

15 Esaminare le vulnerabilità nelle piattaforme mobili e negli IoT e come evitarle

18 Determinare la necessità di continuità della sicurezza delle informazioni

06

Struttura e contenuti

TECH ha strutturato questo programma sulla base della metodologia *Relearning*, il che significa che il manager non dovrà dedicare lunghe ore di studio ad acquisire tutte le conoscenze proposte. I termini e i concetti chiave della politica di cybersicurezza sono forniti in modo naturale e reiterato nel corso del programma e ciò si traduce in un processo di apprendimento molto più progressivo.

Sarai libero di accedere all'aula virtuale 24 ore su 24, potendo scegliere e adattare il ritmo di studio ai tuoi interessi"

Piano di studi

Il Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza di TECH Università Tecnologica è un programma intensivo che prepara gli studenti nelle aree più impegnative della cybersicurezza aziendale.

Il contenuto del Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza è progettato per promuovere lo sviluppo di competenze manageriali che permettano un processo decisionale più rigoroso in ambienti incerti.

Questo Master Privato affronta argomenti relativi al mondo digitale, alla sicurezza in questo campo e all'introduzione dell'e-commerce nelle aziende, ed è stato ideato per preparare dirigenti che concepiscano la Gestione delle Politiche Aziendali di Cybersicurezza da una prospettiva strategica, internazionale e innovativa.

Questo Master Privato ha la durata di 12 mesi e si suddivide in 10 moduli:

Modulo 1	Sistema di gestione della sicurezza delle informazioni (SGSI)
Modulo 2	Aspetti organizzativi della politica di sicurezza delle informazioni
Modulo 3	Politiche di sicurezza per l'analisi delle minacce nei sistemi informatici
Modulo 4	Implementazione pratica delle politiche di sicurezza del software e dell'hardware
Modulo 5	Politiche di gestione degli incidenti di sicurezza
Modulo 6	Implementazione delle politiche di sicurezza fisica e ambientale in azienda
Modulo 7	Politiche di comunicazione sicura in azienda
Modulo 8	Implementazione pratica delle politiche di sicurezza in caso di attacchi
Modulo 9	Strumenti di monitoraggio delle politiche di sicurezza dei sistemi informativi
Modulo 10	Politica di sicurezza pratica per il ripristino di emergenza

Dove, quando e come si svolge?

TECH ti offre la possibilità di frequentare questo Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza completamente in modalità online. Durante i 12 mesi di durata della specializzazione, lo studente potrà avere accesso a tutti i contenuti del programma in qualsiasi momento, il che gli consentirà di autogestire il suo tempo di studio.

Un'esperienza educativa unica, chiave e decisiva per potenziare la crescita professionale e dare una svolta definitiva.

Modulo 1. Sistema di gestione della sicurezza delle informazioni

1.1. Sicurezza delle informazioni. Aspetti chiave
1.1.1. Sicurezza delle informazioni
1.1.1.1. Riservatezza
1.1.1.2. Integrità
1.1.1.3. Disponibilità
1.1.1.4. Misure di sicurezza delle informazioni

1.2. Sistema di gestione della sicurezza delle informazioni
1.2.1. Modelli di gestione della sicurezza delle informazioni
1.2.2. Documenti per l'implementazione di un SGSI
1.2.3. Livelli e controlli di un SGSI

1.3. Norme e standard internazionali
1.3.1. Standard internazionali di sicurezza informatica
1.3.2. Origine ed evoluzione dello standard
1.3.3. Standard internazionali nella gestione della sicurezza delle informazioni
1.3.4. Altre norme di riferimento

1.4. Norma ISO/IEC 27000
1.4.1. Obiettivi e ambito di applicazione
1.4.2. Struttura della normativa
1.4.3. Certificazione
1.4.4. Fasi di accreditamento
1.4.5. Benefici della norma ISO/IEC 27000

1.5. Progettazione e implementazione di un sistema generale di sicurezza delle informazioni
1.5.1. Fasi di implementazione di un sistema generale di sicurezza delle informazioni
1.5.2. Piano di continuità operativa

1.6. Fase I: diagnostico
1.6.1. Diagnostico preliminare
1.6.2. Identificazione del livello di stratificazione
1.6.3. Livello di conformità agli standard/norme

1.7. Fase II: preparazione
1.7.1. Contesto dell'Organizzazione
1.7.2. Analisi delle norme di sicurezza applicabili
1.7.3. Portata del sistema complessivo di sicurezza delle informazioni
1.7.4. Politica del sistema complessivo di sicurezza delle informazioni
1.7.5. Obiettivi del sistema complessivo di sicurezza delle informazioni

1.8. Fase III: pianificazione
1.8.1. Classificazione degli attivi
1.8.2. Valutazione dei rischi
1.8.3. Identificazione di minacce e rischi

1.9. Fase IV: implementazione e monitoraggio
1.9.1. Analisi dei risultati
1.9.2. Assegnazione di responsabilità
1.9.3. Tempistica del piano d'azione
1.9.4. Monitoraggio e audit

1.10. Politiche di sicurezza nella gestione degli incidenti
1.10.1. Fasi
1.10.2. Categorizzazione degli incidenti
1.10.3. Gestione degli incidenti e procedure

Modulo 2. Aspetti organizzativi della politica di sicurezza delle informazioni

2.1. Organizzazione interna
2.1.1. Assegnazione di responsabilità
2.1.2. Segregazione dei compiti
2.1.3. Contatti con le autorità
2.1.4. La sicurezza delle informazioni nella gestione dei progetti

2.2. Risparmio gestito
2.2.1. Responsabilità sugli attivi
2.2.2. Classificazione delle informazioni
2.2.3. Gestione dei supporti di archiviazione

2.3. Politiche di sicurezza nella gestione del business
2.3.1. Analisi dei processi aziendali vulnerabili
2.3.2. Analisi dell'impatto del business
2.3.3. Classificazione dei processi in base all'impatto sul business

2.4. Politiche di sicurezza legate alle Risorse Umane
2.4.1. Prima dell'assunzione
2.4.2. Durante l'assunzione
2.4.3. Licenziamento o cambio di incarico

2.5. Politiche di sicurezza all'indirizzo
2.5.1. Direttive della gestione nella sicurezza delle informazioni
2.5.2. BIA-Analisi dell'impatto
2.5.3. Piano di recupero come politica di sicurezza

2.6. Acquisizione e mantenimento di sistemi informativi
2.6.1. Requisiti di sicurezza dei sistemi informativi
2.6.2. Sicurezza dei dati di sviluppo e di supporto
2.6.3. Dati di prova

2.7. Sicurezza con i fornitori
2.7.1. Sicurezza informatica con i fornitori
2.7.2. Gestione dell'erogazione del servizio con garanzia
2.7.3. Sicurezza nella supply chain

2.8. Sicurezza sul lavoro
2.8.1. Responsabilità sul lavoro
2.8.2. Protezione contro il codice maligno
2.8.3. Copie di backup
2.8.4. Registri di attività e monitoraggio

2.9. Gestione della sicurezza e normativa
2.9.1. Conformità ai requisiti legali
2.9.2. Revisioni della sicurezza informatica

2.10. La sicurezza nella gestione della continuità operativa
2.10.1. Continuità della sicurezza informatica
2.10.2. Ridondanze

Modulo 3. Politiche di sicurezza per l'analisi delle minacce nei sistemi informatici

3.1. Gestione delle minacce nelle politiche di sicurezza
3.1.1. Gestione del rischio
3.1.2. Il rischio nella sicurezza
3.1.3. Metodologie nella gestione delle minacce
3.1.4. Messa in atto delle metodologie

3.2. Fasi di gestione delle minacce
3.2.1. Identificazione
3.2.2. Analisi
3.2.3. Localizzazione
3.2.4. Misure di salvaguardia

3.3. Sistemi di audit per la localizzazione delle minacce
3.3.1. Classificazione e flusso di informazioni
3.3.2. Analisi dei processi vulnerabili

3.4. Classificazione del rischio
3.4.1. Tipi di rischi
3.4.2. Calcolo della probabilità di minaccia
3.4.3. Rischio residuo

3.5. Trattamento del rischio
3.5.1. Attuazione delle misure di salvaguardia
3.5.2. Trasferimento o rilevamento

3.6. Controllo del rischio
3.6.1. Processo continuo di gestione del rischio
3.6.2. Implementazione delle metriche di sicurezza
3.6.3. Modello strategico di metriche sulla sicurezza delle informazioni

3.7. Metodologie pratiche per l'analisi e il controllo delle minacce
3.7.1. Catalogo delle minacce
3.7.2. Catalogo delle misure di controllo
3.7.3. Catalogo delle misure di sicurezza

3.8. Norma ISO 27005
3.8.1. Identificazione dei rischi
3.8.2. Analisi dei rischi
3.8.3. Valutazione dei rischi

3.9. Fonti di rischio, impatto e minaccia
3.9.1. Dati, sistemi e personale
3.9.2. Probabilità di minaccia
3.9.3. Entità del danno

3.10. Progettazione di fasi e processi nell'analisi delle minacce
3.10.1. Identificazione degli elementi critici dell'organizzazione
3.10.2. Determinazione delle minacce e degli impatti
3.10.3. Analisi dell'impatto e dei rischi
3.10.4. Metodologie

Modulo 4. Implementazione pratica delle politiche di sicurezza del software e dell'hardware

4.1. Implementazione pratica delle politiche di sicurezza del software e dell'hardware
4.1.1. Implementazione dell'identificazione e dell'autorizzazione
4.1.2. Implementazione di tecniche di identificazione
4.1.3. Misure tecniche di autorizzazione

4.2. Tecnologie di identificazione e di autorizzazione
4.2.1. Identificativo e OTP
4.2.2. Token USB o smart card PKI
4.2.3. Il comando "Difesa confidenziale"
4.2.4. RFID attivo

4.3. Politiche di sicurezza per l'accesso a software e sistemi
4.3.1. Implementazione delle politiche di controllo degli accessi
4.3.2. Implementazione delle politiche di accesso alle comunicazioni
4.3.3. Tipi di strumenti di sicurezza per il controllo degli accessi

4.4. Gestione dell'accesso degli utenti
4.4.1. Gestione dei diritti di accesso
4.4.2. Segregazione dei ruoli e delle funzioni di accesso
4.4.3. Attivazione dei diritti di accesso nei sistemi

4.5. Controllo degli accessi ai sistemi e alle applicazioni
4.5.1. Regola di accesso minimo
4.5.2. Tecnologie di login sicure
4.5.3. Politiche di sicurezza nelle password

4.6. Tecnologie dei sistemi di identificazione
4.6.1. Active Directory
4.6.2. OTP
4.6.3. PAP, CHAP
4.6.4. KERBEROS, DIAMETER, NTLM

4.7. Controlli CIS per la difesa del sistema
4.7.1. Controlli CIS basilari
4.7.2. Controlli CIS fondamentali
4.7.3. Controlli CIS organizzativi

4.8. Sicurezza sul lavoro
4.8.1. Protezione contro il codice maligno
4.8.2. Copie di backup
4.8.3. Registri di attività e monitoraggio

4.9. Gestione delle vulnerabilità tecniche
4.9.1. Vulnerabilità tecniche
4.9.2. Gestione delle vulnerabilità tecniche
4.9.3. Restrizioni all'installazione del software

4.10. Implementazione di pratiche di politica di sicurezza
4.10.1. Vulnerabilità logiche
4.10.2. Attuazione delle politiche di difesa

Modulo 5. Politiche di gestione degli incidenti di sicurezza

5.1. Politica di gestione degli incidenti di sicurezza delle informazioni e miglioramenti
5.1.1. Gestione degli incidenti
5.1.2. Responsabilità e procedure
5.1.3. Notifica degli eventi

5.2. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
5.2.1. Dati operativi del sistema
5.2.2. Tipi di sistemi di rilevamento delle intrusioni
5.2.3. Criteri per la collocazione di IDS/IPS

5.3. Risposta agli incidenti di sicurezza
5.3.1. Procedura di raccolta dei dati
5.3.2. Processo di verifica delle intrusioni
5.3.3. Organismi CERT

5.4. Processo di notifica e gestione dei tentativi di intrusione
5.4.1. Responsabilità nel processo di notifica
5.4.2. Classificazione di incidenti
5.4.3. Processo di risoluzione e recupero

5.5. L'analisi forense come politica di sicurezza
5.5.1. Prove volatili e non volatili
5.5.2. Analisi e raccolta di prove elettroniche
5.5.2.1. Analisi di prove elettroniche
5.5.2.2. Raccolta di prove elettroniche

5.6. Strumenti di Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
5.6.1. Snort
5.6.2. Suricata
5.6.3. Solar-Winds

5.7. Strumenti di centralizzazione degli eventi
5.7.1. SIM
5.7.2. SEM
5.7.3. SIEM

5.8. Guida di sicurezza CCN-STIC 817
5.8.1. Guida di sicurezza CCN-STIC 817
5.8.2. Gestione degli incidenti informatici
5.8.3. Metriche e indicatori

5.9. NIST SP800-61
5.9.1. Capacità di risposta agli incidenti di sicurezza informatica
5.9.2. Gestione di un incidente
5.9.3. Coordinamento e condivisione delle informazioni

5.10. Norma ISO 27035
5.10.1. Norma ISO 27035. Principi di gestione degli incidenti
5.10.2. Linee guida per lo sviluppo di un piano di gestione degli incidenti
5.10.3. Linee guida per le operazioni di risposta agli incidenti

Modulo 6. Implementazione delle politiche di sicurezza fisica e ambientale in azienda

6.1. Aree di sicurezza
6.1.1. Perimetro di sicurezza fisica
6.1.2. Lavorare in aree sicure
6.1.3. Sicurezza di uffici, sedi e risorse

6.2. Controlli di ingresso fisici
6.2.1. Politiche di controllo degli accessi fisici
6.2.2. Sistemi di controllo dell'ingresso fisico

6.3. Vulnerabilità dell'accesso fisico
6.3.1. Principali vulnerabilità fisiche
6.3.2. Attuazione delle misure di salvaguardia

6.4. Sistemi biometrici fisiologici
6.4.1. Impronta digitale
6.4.2. Riconoscimento facciale
6.4.3. Riconoscimento dell'iride e della retina
6.4.4. Altri sistemi biometrici fisiologici

6.5. Sistemi biometrici di comportamento
6.5.1. Riconoscimento della firma
6.5.2. Riconoscimento della grafia
6.5.3. Riconoscimento vocale
6.5.4. Altri sistemi biometrici di comportamento

6.6. Gestione dei rischi in Biometria
6.6.1. Attuazione di sistemi Biometrici
6.6.2. Vulnerabilità dei sistemi Biometrici

6.7. Implementazione della politica negli host
6.7.1. Installazione del cablaggio di alimentazione e di sicurezza
6.7.2. Posizione delle apparecchiature
6.7.3. Uscita delle apparecchiature all'esterno dei locali
6.7.4. Apparecchiature informatiche non presidiate e politica di stallo chiara

6.8. Protezione ambientale
6.8.1. Sistemi di protezione antincendio
6.8.2. Sistemi di protezione in caso di terremoto
6.8.3. Sistemi di protezione antisismica

6.9. Sicurezza nel centro di elaborazione dati
6.9.1. Porte di sicurezza
6.9.2. Sistemi di videosorveglianza (CCTV)
6.9.3. Controllo di sicurezza

6.10. Regolamenti internazionali sulla sicurezza fisica
6.10.1. IEC 62443-2-1 (europea)
6.10.2. NERC CIP-005-5 (USA)
6.10.3. NERC CIP-014-2 (USA)

Modulo 7. Politiche di comunicazione sicura in azienda

7.1. Gestione della sicurezza nelle reti
7.1.1. Controllo e monitoraggio della rete
7.1.2. Segregazione delle reti
7.1.3. Sistemi di sicurezza di rete

7.2. Protocolli di comunicazione sicuri
7.2.1. Modello TCP/IP
7.2.2. Protocollo IPSEC
7.2.3. Protocollo TLS

7.3. Protocollo TLS 1.3
7.3.1. Fasi di un processo TLS1.3
7.3.2. Protocollo *Handshake*
7.3.3. Protocollo di registrazione
7.3.4. Differenze con TLS 1.2

7.4. Algoritmi crittografici
7.4.1. Algoritmi crittografici utilizzati nelle comunicazioni
7.4.2. *Cipher-suites*
7.4.3. Algoritmi crittografici consentiti per TLS 1.3

7.5. Funzioni Digest
7.5.1. Funzioni Digest
7.5.2. MD6
7.5.3. SHA

7.6. PKI. Infrastruttura a chiave pubblica
7.6.1. PKI e le sue entità
7.6.2. Certificato digitale
7.6.3. Tipi di certificati digitali

7.7. Comunicazioni di tunnel e trasporto
7.7.1. Comunicazioni tunnel
7.7.2. Comunicazioni di trasporto
7.7.3. Implementazione del tunnel crittografato

7.8. SSH. *Secure Shell*
7.8.1. SSH. Capsula sicura
7.8.2. Funzioni dell'SSH
7.8.3. Strumenti SSH

7.9. Revisioni dei sistemi crittografici
7.9.1. Test di integrità
7.9.2. Test dei sistemi crittografici

7.10. Sistemi crittografici
7.10.1. Vulnerabilità dei sistemi crittografici
7.10.2. Salvaguardie nella crittografia

Modulo 8. Implementazione pratica delle politiche di sicurezza in caso di attacchi

8.1. *System Hacking*
8.1.1. Rischi e vulnerabilità
8.1.2. Contromisure

8.2. DoS nei servizi
8.2.1. Rischi e vulnerabilità
8.2.2. Contromisure

8.3. *Session Hijacking*
8.3.1. Il processo di *Hijacking*
8.3.2. Contromisure per l'*Hijacking*

8.4. Evasione di IDS, *Firewall* e Honeypots
8.4.1. Tecniche di elusione
8.4.2. Attuazione delle contromisure

8.5. *Hacking Web Servers*
8.5.1. Attacchi ai server web
8.5.2. Attuazione delle misure di difesa

8.6. *Hacking Web Applications*
8.6.1. Attacchi alle applicazioni web
8.6.2. Attuazione delle misure di difesa

8.7. *Hacking Wireless Networks*
8.7.1. Vulnerabilità nelle reti wifi
8.7.2. Attuazione delle misure di difesa

8.8. *Hacking Mobile Platforms*
8.8.1. Vulnerabilità della piattaforma mobile
8.8.2. Attuazione delle contromisure

8.9. *Ramsonware*
8.9.1. Le vulnerabilità che causano il *Ramsonware*
8.9.2. Attuazione delle contromisure

8.10. Ingegneria sociale
8.10.1. Tipi di Ingegneria sociale
8.10.2. Contromisure per l'ingegneria sociale

Modulo 9. Strumenti di monitoraggio delle politiche di sicurezza dei sistemi informativi

9.1. Politiche di monitoraggio dei sistemi informativi
9.1.1. Monitoraggio dei sistemi
9.1.2. Parametri
9.1.3. Tipi di metriche

9.2. Revisione e registrazione dei sistemi
9.2.1. Revisione e registrazione dei sistemi
9.2.2. Revisione e registrazione su Windows
9.2.3. Revisione e registrazione su Linux

9.3. Protocollo SNMP. *Simple Network Management Protocol*
9.3.1. Protocollo SNMP
9.3.2. Funzioni dell'SNMP
9.3.3. Strumenti SNMP

9.4. Monitoraggio delle reti
9.4.1. Monitoraggio della rete nei sistemi di controllo
9.4.2. Strumenti di monitoraggio per i sistemi di controllo

9.5. Nagios. Sistema di monitoraggio della rete
9.5.1. Nagios.
9.5.2. Come funziona Nagios
9.5.3. Installazione di Nagios

9.6. Zabbix. Sistema di monitoraggio della rete
9.6.1. Zabbix.
9.6.2. Come funziona Zabbix
9.6.3. Installazione di Zabbix

9.7. Cacti. Sistema di monitoraggio della rete
9.7.1. Cacti
9.7.2. Come funziona Cacti
9.7.3. Installazione di Cacti

9.8. Pandora. Sistema di monitoraggio della rete
9.8.1. Pandora
9.8.2. Come funziona Pandora
9.8.3. Installazione di Pandora

9.9. SolarWinds. Sistema di monitoraggio della rete
9.9.1. SolarWinds
9.9.2. Come funziona SolarWinds
9.9.3. Installazione di SolarWinds

9.10. Regolamento sul monitoraggio
9.10.1. Controlli CIS su audit e registrazione
9.10.2. NIST 800-123 (EE.UU)

Modulo 10. Politica di sicurezza pratica per il ripristino di emergenza

10.1. DRP. Piano di disaster recovery
10.1.1. Obiettivo del DRP
10.1.2. Benefici del DRP
10.1.3. Conseguenze della mancanza di un PRA e del suo mancato aggiornamento

10.2. Guida alla definizione di un DRP (Disaster Recovery Plan)
10.2.1. Ambito e obiettivi
10.2.2. Progetto della strategia di recupero
10.2.3. Assegnazione di ruoli e responsabilità
10.2.4. Esecuzione di un inventario di hardware, software e servizi
10.2.5. Tolleranza ai tempi di inattività e alla perdita di dati
10.2.6. Stabilire i tipi specifici di DRP da richiedere
10.2.7. Implementazione di un piano di specializzazione, sensibilizzazione e comunicazione

10.3. Ambito e obiettivi di un DRP (Disaster Recovery Plan)
10.3.1. Garanzia di risposta
10.3.2. Componenti tecnologiche
10.3.3. Risultati della politica di continuità

10.4. Progettazione di una strategia DRP (Disaster Recovery)
10.4.1. Strategia di disaster recovery
10.4.2. Budget
10.4.3. Risorse umane e fisiche
10.4.4. Posizioni dirigenziali a rischio
10.4.5. Tecnologia
10.4.6. Dati

10.5. Continuità dei processi informatici
10.5.1. Pianificazione della continuità
10.5.2. Messa in atto della continuità
10.5.3. Verifica e valutazione della continuità

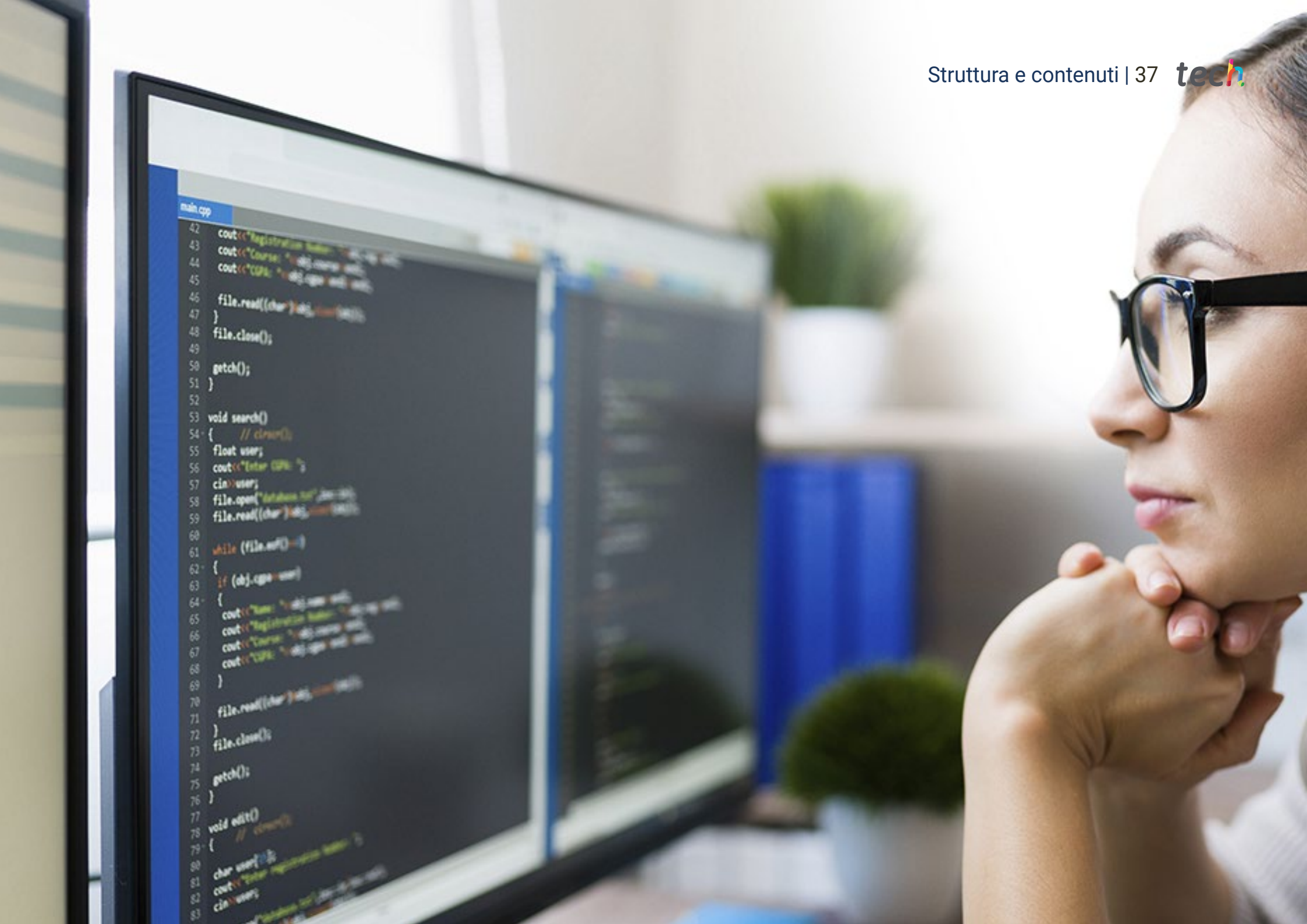
10.6. Ambito di applicazione di un BCP (Business Continuity Plan)
10.6.1. Determinazione dei processi più critici
10.6.2. Approccio basato sugli asset
10.6.3. Approccio basato sul processo

10.7. Implementazione di processi aziendali protetti
10.7.1. Attività prioritarie (PA)
10.7.2. Tempi di recupero ideali (IRT)
10.7.3. Strategie di sopravvivenza

10.8. Analisi delle organizzazioni
10.8.1. Ottenere informazioni
10.8.2. Analisi dell'impatto sul business (BIA)
10.8.3. Analisi dei rischi nell'organizzazione

10.9. Risposta alla contingenza
10.9.1. Piano di crisi
10.9.2. Piani di ripristino dell'ambiente operativo
10.9.3. Procedure tecniche di lavoro o di incidenti

10.10. Norma internazionale ISO 27031 BCP
10.10.1. Obiettivi
10.10.2. Termini e definizioni
10.10.3. Operazione


main.cpp

07

Metodologia

Questo programma di specializzazione propone un modo alternativo di studiare. 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"

TECH Business School utilizza lo studio casistico per contestualizzare tutti i contenuti

Il nostro programma offre un metodo rivoluzionario per sviluppare le abilità e 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"

Il nostro programma ti prepara ad affrontare sfide in ambienti incerti e a raggiungere il successo del tuo business.

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

Un metodo di apprendimento innovativo e differente

Il programma TECH è un corso di studi intensivo, creato ex novo per offrire ai manager sfide e decisioni aziendali ai massimi livelli, sia a livello nazionale che internazionale. Grazie a questa metodologia, la crescita personale e professionale viene potenziata, compiendo un passo decisivo verso il successo. Il metodo casistico, la tecnica che sottende a questi contenuti, garantisce che venga rispettata la realtà economica, sociale e aziendale più attuale.

> *Imparerai, attraverso attività collaborative e casi reali, a risolvere situazioni complesse in ambienti aziendali reali"*

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori business school del mondo da quando esistono. Sviluppato nel 1912 per consentire agli studenti di Diritto di non studiare le leggi solamente dal punto di vista teorico, ma, applicando il metodo casistico, potessero vedersi immersi in situazioni complesse e reali, che li obbligassero a prendere delle decisioni e ad esprimere dei giudizi di valore fondati rispetto alla soluzione delle stesse. 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 ci confrontiamo nel Metodo Casistico, un metodo di apprendimento orientato all'azione. Gli studenti si confronteranno con diversi casi reali nel corso del programma. Dovranno integrare tutte le loro conoscenze, effettuare ricerche, argomentare e difendere le proprie idee e decisioni.

Metodologia Relearning

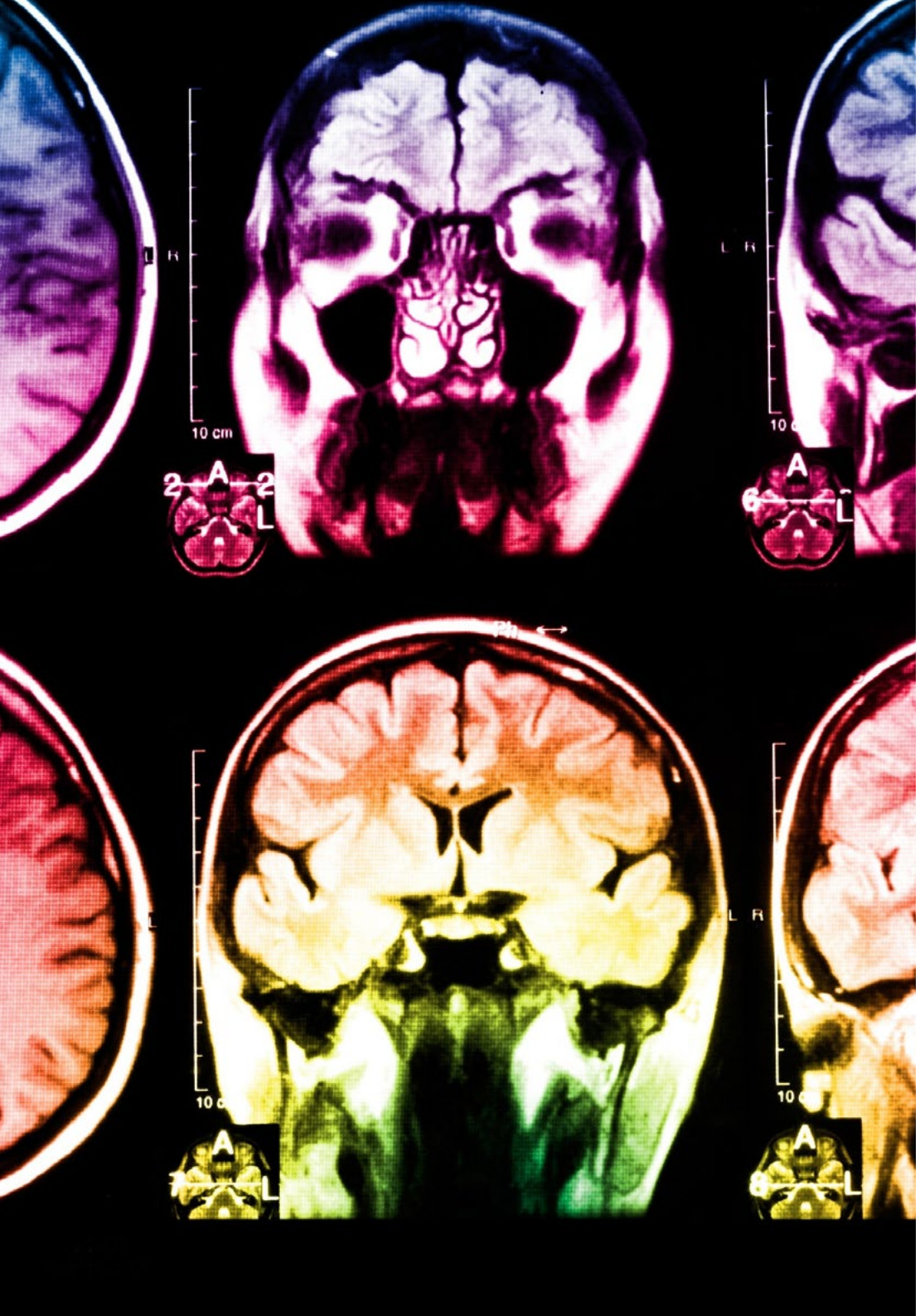
TECH combina efficacemente la metodologia dei Studi di Casi con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

Abbiamo migliorato lo studio dei casi mediante il miglior metodo di insegnamento 100% online: il Relearning.

Il nostro sistema online ti permetterà di organizzare il tuo tempo e il tuo ritmo di apprendimento, adattandolo ai tuoi impegni. Sarai in grado di accedere ai contenuti disponibili da qualsiasi dispositivo fisso o mobile dotato di connessione a internet.

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 Business School 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 in spagnolo.



Nel nostro programma, l'apprendimento non è un processo lineare, ma avviene in spirale (impariamo, disimpariamo, dimentichiamo e re-impariamo). Pertanto, combiniamo ciascuno di questi elementi in modo concentrico. Con questa metodologia abbiamo preparato più di 650.000 studenti con un successo senza precedenti, in ambiti molto 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 contesto molto esigente, con un corpo di studenti universitari di alto profilo socioeconomico e un'età media di 43,5 anni.

Il Relearning ti permetterà di apprendere con meno sforzo e maggior rendimento, impegnandoti maggiormente nella tua specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando le opinioni: un'equazione che punta direttamente 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.

Grazie a questo programma avrai accesso ai migliori materiali didattici, preparati appositamente per te:

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 prove scientifiche sull'utilità dell'osservazione di terzi esperti.

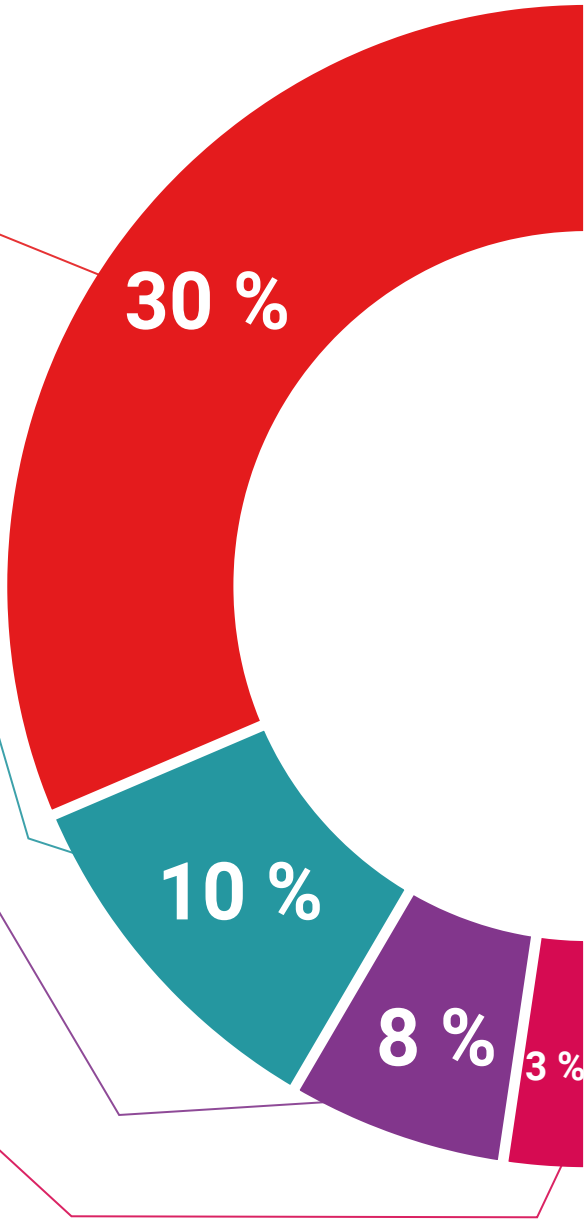
Il cosiddetto Learning from an Expert rafforza le conoscenze e i ricordi e genera sicurezza nel futuro processo decisionale.

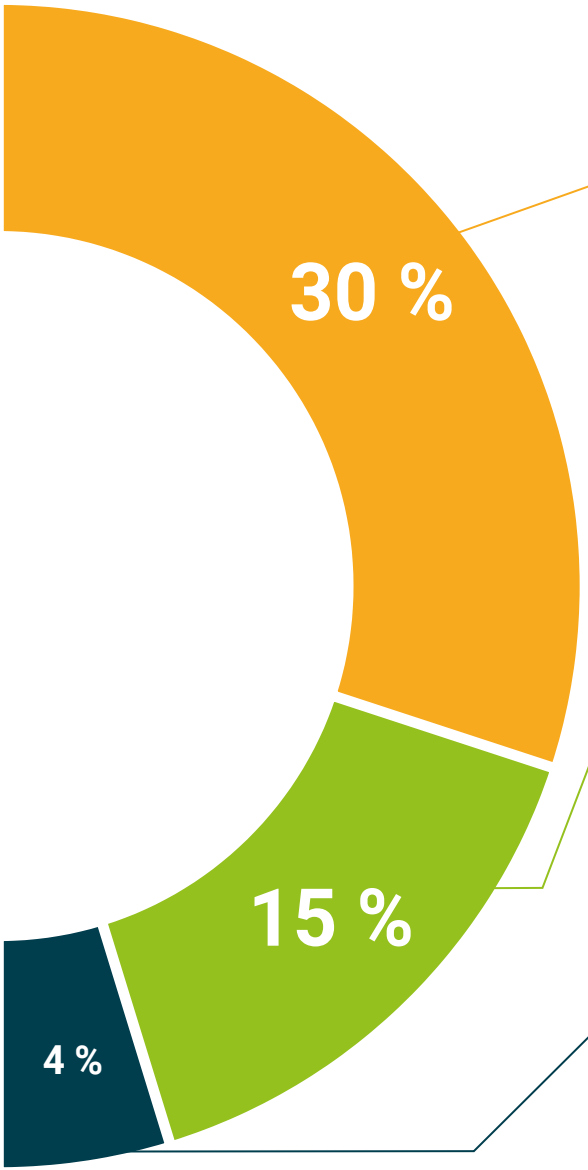
Stage di competenze manageriali

Svolgerai attività per sviluppare competenze manageriali specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che un senior manager deve sviluppare nel quadro della globalizzazione in cui viviamo.

Letture complementari

Articoli recenti, documenti di consenso, linee guida internazionali e molto altro. Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua istruzione.





Case studies

Il programma del corso prevede inoltre una selezione dei migliori casi di studio scelti in modo specifico. Casi di studio presentati, analizzati e spiegati dai migliori specialisti in senior management di tutto il panorama internazionale.

Riepiloghi interattivi

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

Questo esclusivo sistema didattico 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 di autovalutazione, affinché tu possa verificare come raggiungi progressivamente i tuoi obiettivi.

08

Profilo dei nostri studenti

Il Master Privato è rivolto a laureati che abbiano precedentemente conseguito una qualsiasi delle qualifiche nel campo delle Scienze sociali e giuridiche, amministrative ed economiche.

La presenza di studenti provenienti da paesi diversi contribuisce a fornire a questo programma un approccio multidisciplinare.

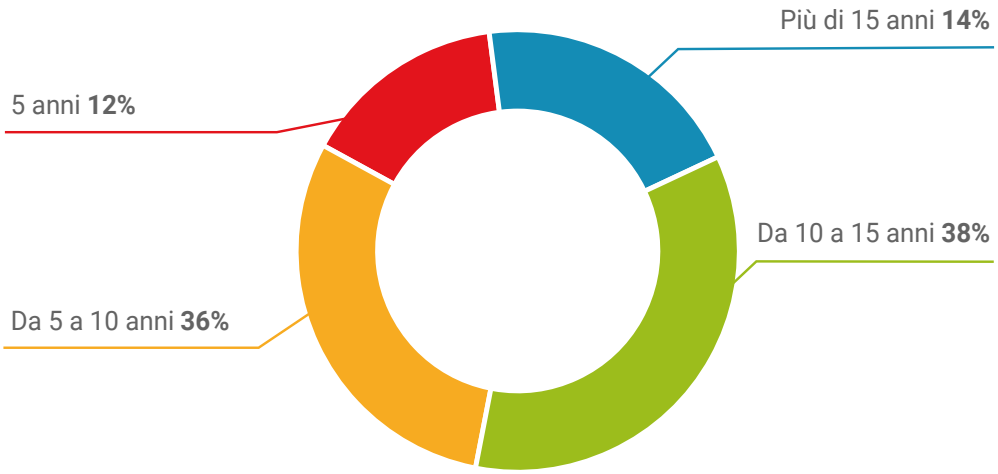
Potranno realizzare questo Master Privato anche professionisti che, avendo titoli universitari in qualsiasi area, abbiano maturato un'esperienza lavorativa di almeno due anni nel settore della Gestione delle Politiche di Cybersicurezza.

Se desideri progredire nella tua carriera professionale acquisendo conoscenze di qualità, basate sulla realtà più attuale della cybersicurezza, iscriviti subito a questo programma"

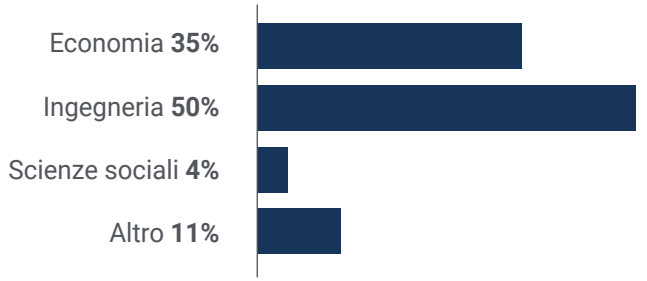
Età media

Da **35** a **45** anni

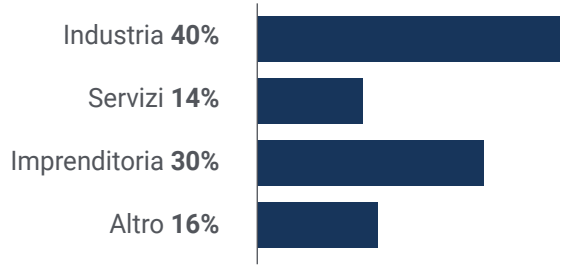
Anni di esperienza



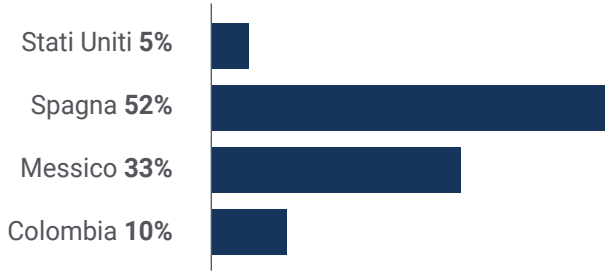
Educazione



Profilo accademico



Distribuzione geografica



Gabriel Gutiérrez Gómez

Responsabile della cybersicurezza

"Dopo aver subito un grave attacco informatico all'interno della nostra organizzazione, abbiamo posto maggiore enfasi sulla protezione dei nostri database e vi abbiamo dedicato un piccolo reparto. Grazie a questo programma, ho potuto guidare questo sforzo, progettando e implementando le politiche di cybersicurezza che utilizziamo ancora oggi"

09

Direzione del corso

Per ottenere la massima qualità possibile di tutti i contenuti didattici, TECH ha selezionato un personale docente di esperti nelle diverse aree coinvolte nella cybersicurezza. In questo modo, il manager avrà accesso a un programma creato da professionisti con una vasta esperienza nella gestione delle politiche di cybersicurezza, che hanno dato un contributo alla teoria con la loro visione pratica e distintiva relativamente a ciascuno degli argomenti trattati.

Sarai affiancato da un personale docente con esperienza nel senior management e nella gestione della sicurezza informatica complessa, che impartisce materie dedicate alla manutenzione dei sistemi informativi, all'analisi forense e all'Hijacking"

Direzione

Dott.ssa Fernández Sapena, Sonia

- Istruttrice in sicurezza informatica e hacking etico presso il Centro di riferimento nazionale per l'informatica e le telecomunicazioni di Getafe, Madrid
- Istruttrice certificata da E-Council
- Formatrice nelle seguenti certificazioni: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation. Madrid
- 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 (2018)
- Master in DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Personale docente

Dott. Solana Villarias, Fabián

- Consulente di Tecnologie dell'Informazione
- Sviluppatore e amministratore di servizi di indagine presso Investigación, Planificación y Desarrollo, S.A.
- Specialista dei mercati finanziari e della manutenzione dei sistemi IT presso Iberia Financial Software
- Sviluppatore web e specialista dell'accessibilità presso Indra
- Laurea in Ingegneria Informatica conseguita presso l'Università del Galles/CESINE
- Corso Universitario in Ingegneria Tecnica dei Sistemi Informatici presso l'Università del Galles/CESINE

Dott.ssa López García, Rosa María

- Specialista in informazioni gestionali
- Docente presso l'Istituto professionale Linux
- Collaboratrice di Incibe Hacker Academy
- Responsabile dei talenti della sicurezza informatica presso Teamciberhack
- Responsabile amministrativa, contabile e finanziaria presso Integra2Transportes
- Assistente amministrativa per le risorse di approvvigionamento presso il Centro educativo Cardinal Marcelo Espínola
- Tecnico superiore in Cybersecurity e Ethical Hacking
- Membro di Ciberpatrulla

Dott. Oropesiano Carrizosa, Francisco

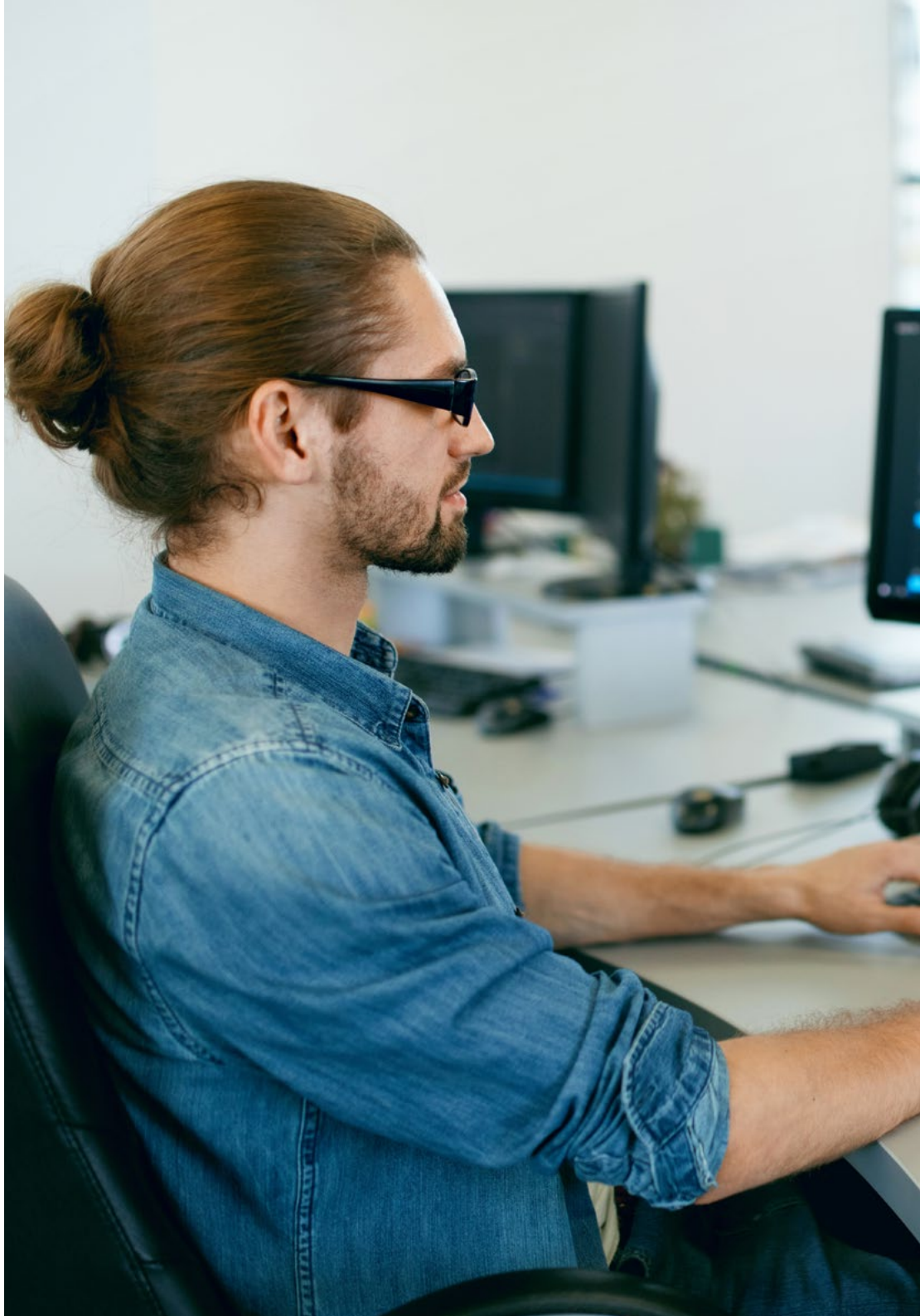
- Ingegnere informatico
- Tecnico di microcomputing, reti e sicurezza presso Cas-Training
- Sviluppatore di servizi web, CMS, e-commerce, UI e UX presso Fersa Riparazioni
- Responsabile servizi web, contenuti, posta e DNS presso Oropesia Web & Network
- Progettista di applicazioni grafiche e web presso Xarxa Sakai Projectes
- Laurea in Sistemi Informatici presso l'Università di Alcalá de Henares
- Master in DevOps: Docker and Kubernetes presso Da Cyber Business Center
- Tecnico di rete e sicurezza informatica presso l'Università delle Isole Baleari
- Esperto in Design 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
- Istruttore di insegnanti nel settore IT
- Laurea in Ingegneria Tecnica Industriale presso l'Università di Alcalá de Henares
- Master in Scienze dell'Educazione presso l'UNIR
- MBA in gestione e amministrazione aziendale di IDE-CESEM
- Master in Gestione delle Tecnologie dell'Informazione di IDE-CESEM
- Certified Information Security Management (CISM) presso ISACA

Dott. Peralta Alonso, Jon

- Consulente senior - Protezione dei dati e sicurezza informatica. Altia
- Avvocato / Consulente legale. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Consulente legale / Apprendista. Studio professionale: Oscar Padura
- Laurea in Giurisprudenza Università Pubblica dei Paesi Baschi
- Master in Protezione dei Dati. EIS Innovative School
- Master Universitario in Giurisprudenza. Università Pubblica dei Paesi Baschi
- Master in Pratica del Contenzioso Civile. Università Internazionale Isabella I di Castiglia
- Docente del Master in Protezione dei Dati Personali, Cybersecurity e Diritto delle TIC



TECH ha selezionato con cura il personale docente per questo programma, in modo che tu possa imparare dai migliori specialisti del momento”

10

Impatto sulla tua carriera

TECH è consapevole dello sforzo che i manager devono compiere per ottenere una qualifica di queste caratteristiche, per questo si impegna in modo particolare affinché tutti i contenuti e i materiali didattici forniti rispondano agli standard di qualità più esigenti. In questo modo, la biblioteca multimediale a cui dà accesso funge da eccezionale riferimento nel campo della cybersicurezza e può essere completamente scaricata per essere utilizzata anche dopo la fine del corso.

Otterrai la proiezione economica e professionale che cerchi grazie al costante supporto di un personale docente e tecnico impegnato a farti arrivare ai più alti livelli del management in Cybersecurity Policy"

Sei pronto a fare questo passo? Un eccellente miglioramento professionale ti aspetta

Il Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza di TECH è un programma intensivo che prepara gli studenti ad affrontare sfide e decisioni imprenditoriali nell'ambito aziendale della cybersicurezza. Il suo obiettivo principale è quello di favorire la tua crescita personale e professionale e aiutarti a raggiungere il successo.

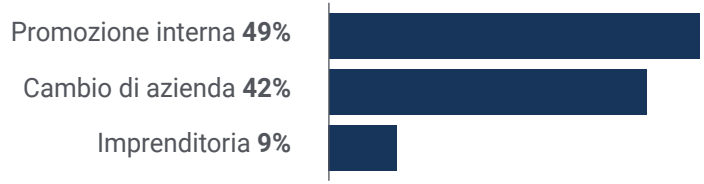
Se vuoi superare te stesso, ottenere un cambiamento positivo a livello professionale e creare una rete con i migliori contatti, questo è il posto che fa per te.

Otterrai una promozione molto più velocemente di quello che immagini grazie alla metodologia didattica che offre TECH.

Non aspettare oltre, iscriviti ora a questo Master per apportare un cambiamento positivo alla tua vita.

Momento del cambiamento

Tipo di cambiamento



Miglioramento salariale

La realizzazione di questo programma prevede per i nostri studenti un incremento salariale superiore al **25,22%**

Salario precedente	Incremento salariale del	Salario posteriore
57.900 €	**25,22%**	**72.500 €**

11

Benefici per la tua azienda

Il Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza aiuta ad elevare il talento dell'organizzazione al suo massimo potenziale mediante la specializzazione di leader di alto livello.

Partecipare a questo Master Privato è un'opportunità unica per avere accesso a una potente rete di contatti in cui trovare futuri soci professionisti, clienti o fornitori.

Le minacce informatiche sono una delle maggiori vulnerabilità a cui sono esposte le aziende di ogni tipo e dimensione. Specializzati nell'area con la maggiore proiezione futura"

Sviluppare e trattenere il talento nelle aziende è il miglior investimento a lungo termine.

01

Crescita del talento e del capitale intellettuale

Il professionista apporterà all'azienda nuovi concetti, strategie e prospettive che possono portare cambiamenti significativi nell'organizzazione.

02

Trattenere i manager ad alto potenziale ed evitare la fuga di cervelli

Questo programma rafforza il legame tra l'azienda e il professionista e gli apre nuove vie di crescita professionale all'interno della stessa.

03

Creare agenti di cambiamento

Sarai in grado di prendere decisioni in tempi di incertezza e di crisi, aiutando l'organizzazione a superare gli ostacoli.

04

Incremento delle possibilità di espansione internazionale

Grazie a questo programma, l'azienda entrerà in contatto con i principali mercati dell'economia mondiale.

05

Sviluppo di progetti propri

Il professionista può lavorare su un progetto esistente o svilupparne di nuovi nell'ambito di R&S o del Business Development della sua azienda.

06

Aumento della competitività

Questo Master Privato fornirà ai rispettivi professionisti le competenze per affrontare nuove sfide e portare avanti l'organizzazione.

12

Titolo

Il Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza garantisce, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di una qualifica di Master Privato rilasciata da TECH Università Tecnologica.

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

Questo **Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza** possiede il programma educativo più completo e aggiornato del mercato.

Dopo aver superato le valutazioni, lo studente riceverà, mediante lettera certificata con ricevuta di ritorno, la corrispondente qualifica di **Master Privato** rilasciata da **TECH Università Tecnologica.**

Il titolo rilasciato da **TECH Università Tecnologica** indica la qualifica ottenuta nel Master Privato e soddisfa i requisiti comunemente richiesti da borse di lavoro, concorsi e commissioni di valutazione di carriere professionali.

Titolo: **Master Privato in Gestione delle Politiche Aziendali di Cybersicurezza**

Ore Ufficiali: **1.500**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MÁSTER TÍTULO PROPIO

en

Gestión de Políticas de Ciberseguridad en la Empresa

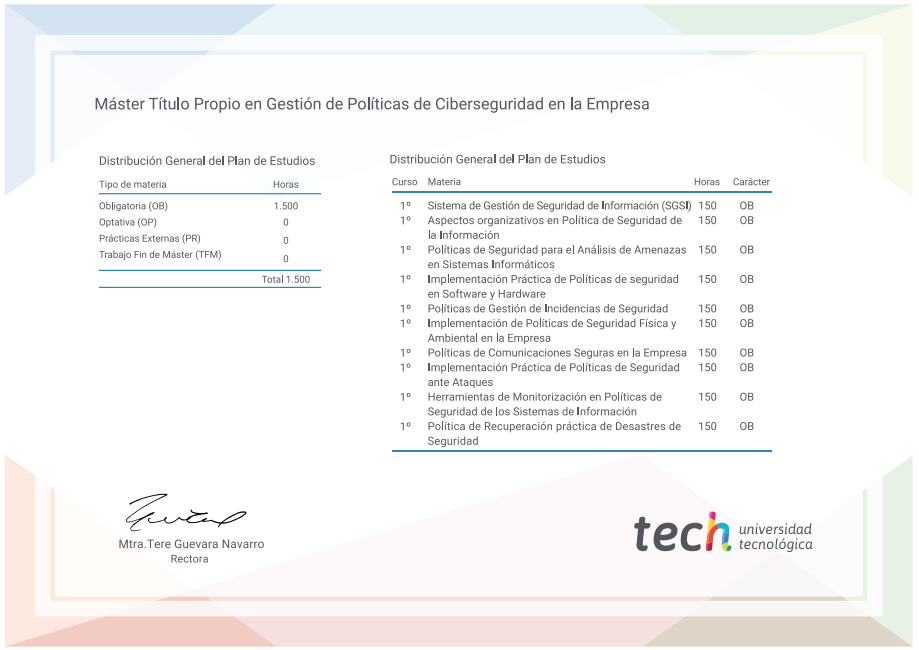
Se trata de un título propio de esta Universidad con una duración de 1.500 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una Institución Particular de Educación Superior reconocida por la Secretaría de Educación Pública a partir del 28 de junio de 2018.

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos


Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa

Distribución General del Plan de Estudios

Tipo de materia	Horas
Obligatoria (OB)	1.500
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
	Total 1.500

Distribución General del Plan de Estudios

Curso	Materia	Horas	Carácter
1º	Sistema de Gestión de Seguridad de Información (SGSI)	150	OB
1º	Aspectos organizativos en Política de Seguridad de la Información	150	OB
1º	Políticas de Seguridad para el Análisis de Amenazas en Sistemas Informáticos	150	OB
1º	Implementación Práctica de Políticas de seguridad en Software y Hardware	150	OB
1º	Políticas de Gestión de Incidencias de Seguridad	150	OB
1º	Implementación de Políticas de Seguridad Física y Ambiental en la Empresa	150	OB
1º	Políticas de Comunicaciones Seguras en la Empresa	150	OB
1º	Implementación Práctica de Políticas de Seguridad ante Ataques	150	OB
1º	Herramientas de Monitorización en Políticas de Seguridad de los Sistemas de Información	150	OB
1º	Política de Recuperación práctica de Desastres de Seguridad	150	OB

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

*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 universidad tecnológica

Master Privato in

Gestione delle Politiche Aziendali di Cybersicurezza

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Università Tecnologica**
- Dedizione: **16 ore/settimana**
- Orario: **a scelta**
- Esami: **online**

Master Privato in

Gestione delle Politiche Aziendali di Cybersicurezza

tech universidad tecnológica