Master Privato

MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

tech università tecnologica

tech università tecnologica

Master Privato
MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Università Tecnologica**
- Orario: **a scelta**
- Esami: **online**

Accesso al sito web: www.techtitute.com/it/informatica/master/master-mba-cybersecurity-management-ciso-chief-information-security-officer

Indice

01

Presentazione

Con il progredire della tecnologia, infatti, aumentano anche le minacce perfezionando le tecniche di attacco. In altre parole, le possibilità e i modi in cui i cybercriminali possono raggiungere i loro obiettivi sono in aumento. È in questo contesto che TECH presenta un diploma con cui i professionisti potranno aggiornarsi, imparando in modo esaustivo a proteggere e garantire diversi ambienti digitali. Tutto questo, attraverso una metodologia rivoluzionaria, il Relearning; e in un comodo formato completamente online, che permetterà al laureato di acquisire competenze e abilità senza un tempo prestabilito. Così, al termine di questo corso, il professionista acquisirà le capacità e le competenze necessarie per esercitare con grande efficienza Chief Information Security Officer, una posizione di alto livello e con grande prestigio, e con alte prospettive di crescita ed espansione.

Con l'avanzare della tecnologia e della connettività, aumentano anche il numero e la tipologia delle potenziali minacce. Per questo è fondamentale che i futuri Chief Information Security Officer aggiornino le loro conoscenze per offrire soluzioni più adatte alle idiosincrasie dell'azienda"

Oggi abbiamo a che fare con l'era dell'informazione e della comunicazione, in quanto tutti sono connessi, sia in casa che in azienda. In questo modo, è possibile accedere a una moltitudine di informazioni con un solo clic, con una sola ricerca su uno qualsiasi dei motori a nostra disposizione, sia da uno smartphone che da un computer personale o di lavoro.

Con il progredire della tecnologia per il cittadino e il dipendente medio, aumentano anche le minacce e le tecniche di attacco. Più nuove funzionalità ci sono e più comunichiamo, più la nostra zona di attacco aumenta. Alla luce di questo preoccupante contesto, TECH propone questo MBA in Cybersecurity Management (CISO, Chief Information Security Officer), che è stato elaborato da un team con diversi profili professionali specializzati in vari settori, coniugando l'esperienza professionale internazionale nel settore privato in R&S+I e un'ampia esperienza di insegnamento.

Inoltre, questo Master Privato fornisce allo studente eccellenti e complete lezioni extra, impartite da uno specialista di intelligence, sicurezza informatica e tecnologie dirompenti di fama internazionale. Questo contenuto innovativo sarà accessibile con il formato di 10 *Master class* esclusive, che permetteranno allo studente di aggiornarsi in Sicurezza informatica e dirigere i dipartimenti responsabili di questi compiti nelle più importanti aziende del settore tecnologico.

Il programma comprende le diverse materie fondamentali dell'area della Sicurezza Informatica, accuratamente selezionate per abbracciare in modo rigoroso un ampio spettro di tecnologie applicabili a diverse aree di lavoro. Tratterà anche un altro ramo di materie che sono spesso scarse nel catalogo accademico altre istituzioni e che nutriranno in modo profondo il curriculum del professionista. In questo modo, e grazie alle conoscenze trasversali offerte da TECH con questo programma, lo studente acquisirà le competenze per esercitare come manager nell'area della sicurezza informatica (Chief Information Security Officer) aumentando così le loro prospettive di crescita personale e professionale.

Questo **MBA in Cybersecurity Management (CISO, Chief Information Security Officer)** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del programma sono:

- Sviluppo di casi pratici presentati da esperti in cybersecurity
- Contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni scientifiche e pratiche sulle discipline essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- Speciale enfasi sulle metodologie innovative
- Lezioni teoriche, domande all'esperto e/o al tutor, forum di discussione su questioni controverse e compiti di riflessione individuale
- Disponibilità di accesso ai contenuti da qualsiasi dispositivo fisso o portatile con una connessione internet

Preparati con i migliori professionisti! Approfitta delle 10 Master class tenute da un docente di fama internazionale"

Eccelli in un settore in crescita e diventa un esperto di sicurezza informatica con questo MBA di TECH. È il più completo del mercato"

Le modalità di scambio di informazioni sono in rapida evoluzione. Ciò richiede nuove forme di protezione informatica per i professionisti.

Un programma 100% online con un approccio estremamente pratico che getterà le basi per la tua crescita professionale.

Il personale docente del programma comprende rinomati specialisti del settore e altre aree correlate, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

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

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

02

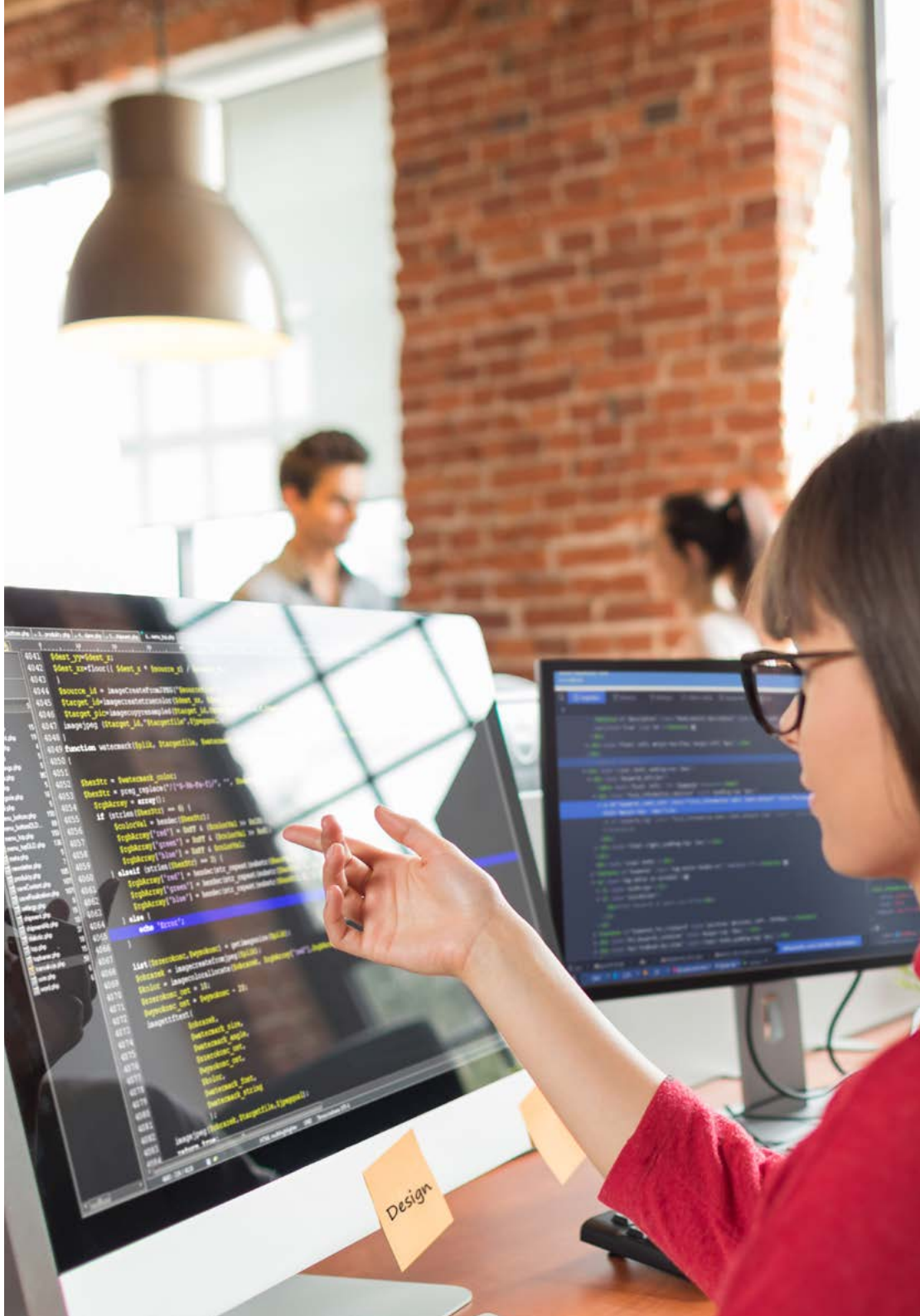
Obiettivi

Essendo pienamente consapevole dell'importanza della sicurezza informatica per le aziende e le persone, TECH ha sviluppato questo MBA che mira a nutrire e aggiornare le conoscenze dei professionisti in materia di rilevamento, protezione e prevenzione della criminalità informatica. In questo modo, lo studente diventerà un pezzo chiave nella cura dei dati e delle informazioni, minimizzando la possibilità che i criminali traggano vantaggio da potenziali lacune di sicurezza esistenti. Una competenza che il professionista che studia in TECH potrà acquisire in soli 12 mesi.

Si tratta di un'opportunità unica per realizzare i propri sogni e obiettivi e diventare un esperto di Sicurezza Informatica"

Obiettivi generali

- Analizzare il ruolo dell'Analista di Cybersecurity
- Approfondire la comprensione dell'ingegneria sociale e dei suoi metodi
- Esaminare le metodologie OSINT, HUMINT, OWASP, PTEC, OSSTM, OWISAM
- Condurre l'analisi dei rischi e comprendere le metriche di rischio
- Determinare l'uso appropriato dell'anonimato e l'uso di reti come TOR, I2P e Freenet
- Raccogliere le normative esistenti in materia di cybersecurity
- Generare conoscenze specialistiche per condurre un audit di sicurezza
- Sviluppare politiche di utilizzo appropriate
- Esaminare i sistemi di rilevamento e prevenzione delle minacce più importanti
- Valutare i nuovi sistemi di rilevamento delle minacce e la loro evoluzione rispetto alle soluzioni più tradizionali
- Analizzare le principali piattaforme mobili attuali, le loro caratteristiche e il loro utilizzo
- Identificare, analizzare e valutare i rischi per la sicurezza delle parti di un progetto IoT
- Valutare le informazioni ottenute e sviluppare meccanismi di prevenzione e Hacking
- Applicare il Reverse Engineering all'ambiente della cybersecurity
- Specificare i test da eseguire sul software sviluppato
- Raccogliere tutte le prove e i dati esistenti per realizzare un rapporto forense
- Presentare regolarmente il rapporto forense
- Analizzare lo stato attuale e futuro della sicurezza informatica
- Esaminare i rischi delle tecnologie nuove ed emergenti
- Raccogliere le diverse tecnologie in relazione alla sicurezza informatica



Obiettivi specifici

Modulo 1. Cyberintelligence e Cybersicurezza

- Sviluppare le metodologie utilizzate in materia di sicurezza informatica
- Esaminare il ciclo dell'intelligence e stabilirne l'applicazione nella cyberintelligence
- Determinare il ruolo dell'analista di intelligence e gli ostacoli all'attività di evacuazione
- Analizzare le metodologie OSINT, OWISAM, OSSTM, PTES, OWASP
- Stabilire gli strumenti più comuni per la produzione di intelligence
- Condurre un'analisi dei rischi e comprendere le metriche utilizzate
- Concretizzare le opzioni per l'anonimato e l'uso di reti come TOR, I2P, FreeNet
- Dettagliare le normative vigenti in materia di cyber-sicurezza

Modulo 2. Sicurezza in host

- Specificare le politiche di *Backup* dei dati personali e professionali
- Valutare i diversi strumenti per fornire soluzioni a problemi di sicurezza specifici
- Stabilire i meccanismi per avere un sistema aggiornato
- Eseguire la scansione dell'apparecchiatura per individuare eventuali intrusi
- Determinare le regole di accesso al sistema
- Esaminare e classificare la posta per prevenire le frodi
- Generare elenchi di software consentiti

Modulo 3. Sicurezza di rete (perimetro)

- Analizzare le attuali architetture di rete per identificare il perimetro da proteggere
- Sviluppare configurazioni specifiche di firewall e Linux per mitigare gli attacchi più comuni
- Raccogliere le soluzioni più comunemente utilizzate, come Snort e Suricata, e la loro configurazione
- Esaminare i diversi livelli aggiuntivi forniti dai *firewall* di nuova generazione e dalle funzionalità di rete negli ambienti Cloud
- Identificare gli strumenti per la protezione della rete e dimostrare perché sono fondamentali per una difesa a più livelli

Modulo 4. Sicurezza degli smartphone

- Esaminare i diversi vettori di attacco per evitare di diventare un bersaglio facile
- Determinare i principali attacchi e tipi di Malware a cui sono esposti gli utenti di dispositivi mobili
- Analizzare i dispositivi più recenti per stabilire una configurazione più sicura
- Specificare i passaggi principali per eseguire un test di intrusione su entrambe le piattaforme iOS e Android
- Sviluppare una conoscenza specialistica dei diversi strumenti di protezione e sicurezza
- Stabilire le migliori pratiche di programmazione orientata al mobile

Modulo 5. Sicurezza in IoT
- Analizzare le principali architetture IoT
- Esame delle tecnologie di connettività
- Sviluppare i principali protocolli di attuazione
- Specificare i diversi tipi di dispositivi esistenti
- Valutare i livelli di rischio e le vulnerabilità note
- Sviluppare politiche di utilizzo sicuro
- Stabilire condizioni d'uso appropriate per questi dispositivi

Modulo 6. Hacking etico
- Esaminare i metodi IOSINT
- Raccogliere le informazioni disponibili sui media pubblici
- Eseguire la scansione delle reti per ottenere informazioni in maniera attiva
- Sviluppare laboratori di prova
- Analizzare gli strumenti per le prestazioni del *Pentesting*
- Catalogare e valutare le diverse vulnerabilità dei sistemi
- Concretizzare le diverse metodologie di *Hacking*

Modulo 7. Ingegneria inversa
- Analizzare le fasi di un compilatore
- Esaminare l'architettura del processore x86 e l'architettura del processore ARM
- Determinare i diversi tipi di analisi
- Applicare il *Sandboxing* in diversi ambienti
- Sviluppare diverse tecniche di analisi del *Malware*
- Stabilire strumenti orientati all'analisi del *Malware*

Modulo 8. Sviluppo sicuro
- Stabilire i requisiti necessari per il corretto funzionamento di un'applicazione in modo sicuro
- Esaminare i file di *Log* per comprendere i messaggi di errore
- Analizzare i diversi eventi e decidere cosa mostrare all'utente e cosa salvare nei *Log*
- Generare un codice sanificato, facilmente verificabile e di qualità
- Valutare la documentazione appropriata per ogni fase di sviluppo
- Concretizzare il comportamento del server per ottimizzare il sistema
- Elaborare un codice modulare, riutilizzabile e mantenibile

Modulo 9. Analisi forense
- Identificare i diversi elementi che rivelano un reato
- Generare conoscenze specializzate per ottenere dati da diversi supporti prima che vadano persi
- Recuperare i dati cancellati intenzionalmente
- Analizzare i log e le registrazioni del sistema
- Determinare il modo in cui i dati vengono duplicati per non alterare gli originali
- Dimostrare che le prove sono coerenti
- Generare un rapporto solido e senza interruzioni
- Presentare le conclusioni in modo coerente
- Stabilire come difendere la relazione davanti all'autorità competente
- Concretizzare le strategie per un telelavoro sicuro

Modulo 10. Le sfide attuali e future della sicurezza informatica

- Esaminare l'uso delle criptovalute, l'impatto sull'economia e sulla sicurezza
- Analizzare la situazione degli utenti e del grado di analfabetismo digitale
- Determinare l'ambito di utilizzo del *Blockchain*
- Presentare alternative all'IPv4 nell'indirizzamento di rete
- Sviluppare strategie per educare la popolazione all'uso corretto delle tecnologie
- Generare conoscenze specialistiche per affrontare le nuove sfide della sicurezza e prevenire il furto di identità
- Concretizzare le strategie per un telelavoro sicuro

Modulo 11. Leadership, Etica e Responsabilità Sociale d'Impresa

- Analizzare l'impatto della globalizzazione sulla governance e la governance aziendale
- Valutare l'importanza di una leadership efficace nella gestione e nel successo delle imprese
- Definire le strategie di gestione interculturale e la loro rilevanza in diversi ambienti aziendali
- Sviluppare capacità di leadership e comprendere le sfide attuali che i leader affrontano
- Determinare i principi e le pratiche dell'etica aziendale e la loro applicazione nel processo decisionale aziendale
- Strutturare strategie per l'implementazione e il miglioramento della sostenibilità e della responsabilità sociale nelle aziende

Modulo 12. Direzione del personale e gestione del talento

- Determinare il rapporto tra la direzione strategica e la gestione delle risorse umane
- Approfondire le competenze necessarie per una gestione efficace delle risorse umane in base alle competenze
- Approfondire le metodologie per la valutazione delle prestazioni e la gestione delle prestazioni
- Integrare le innovazioni nella gestione dei talenti e il loro impatto sulla fidelizzazione del personale
- Sviluppare strategie per la motivazione e lo sviluppo di team ad alte prestazioni
- Proporre soluzioni efficaci per la gestione del cambiamento e la risoluzione dei conflitti nelle organizzazioni

Modulo 13. Gestione Economico-Finanziaria

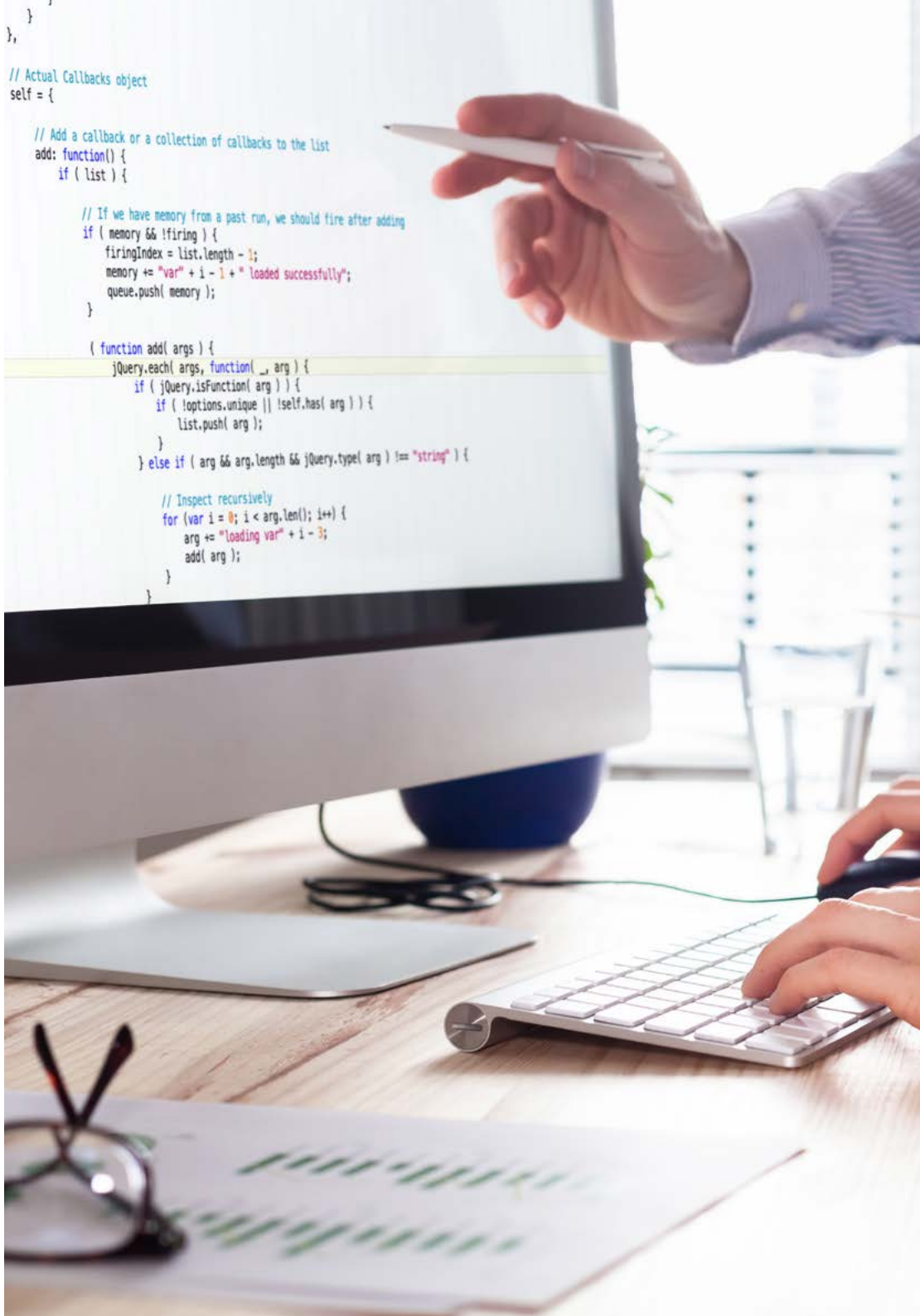
- Analizzare il contesto macroeconomico e la sua influenza sul sistema finanziario internazionale
- Definire i sistemi di informazione e Business Intelligence per il processo decisionale finanziario
- Differenziare le decisioni finanziarie chiave e la gestione del rischio nella direzione finanziaria
- Valutare le strategie per la pianificazione finanziaria e ottenere finanziamenti aziendali

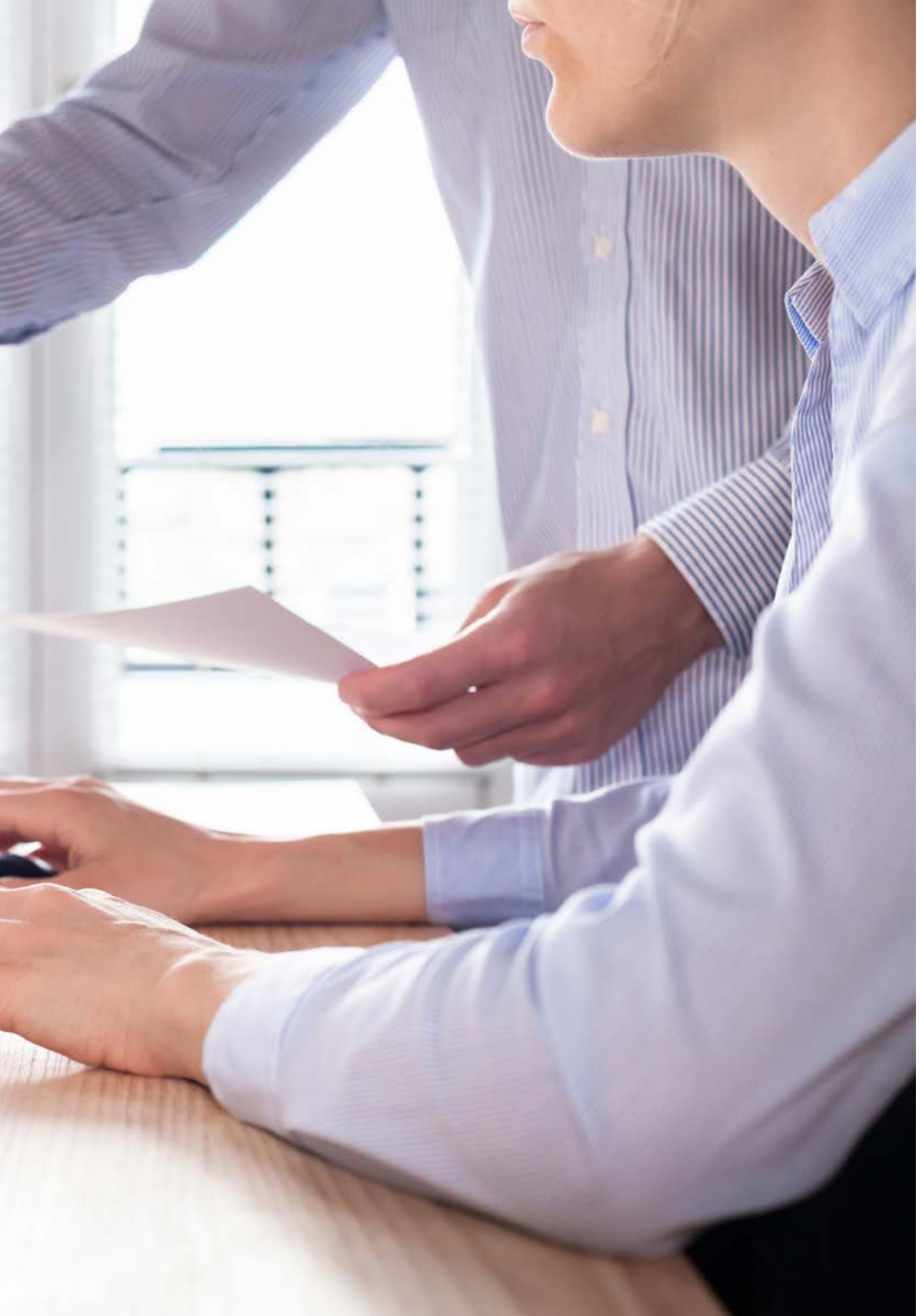
Modulo 14. Direzione Commerciale e Marketing Strategico

- Strutturare il quadro concettuale e l'importanza della direzione commerciale nelle imprese
- Approfondire gli elementi e le attività fondamentali del marketing e il loro impatto sull'organizzazione
- Determinare le fasi del processo di pianificazione strategica di marketing
- Valutare strategie per migliorare la comunicazione aziendale e la reputazione digitale dell'azienda

Modulo 15. *Management* Direttivo

- Definire il concetto di General Management e la sua rilevanza nella gestione aziendale
- Valutare i ruoli e le responsabilità del manager nella cultura organizzativa
- Analizzare l'importanza della gestione operativa e della qualità nella catena del valore
- Sviluppare capacità di comunicazione interpersonale e oratoria per la formazione dei portavoce





Un programma unico e ideale se stai cercando di aumentare le tue conoscenze sulla sicurezza informatica"

03

Competenze

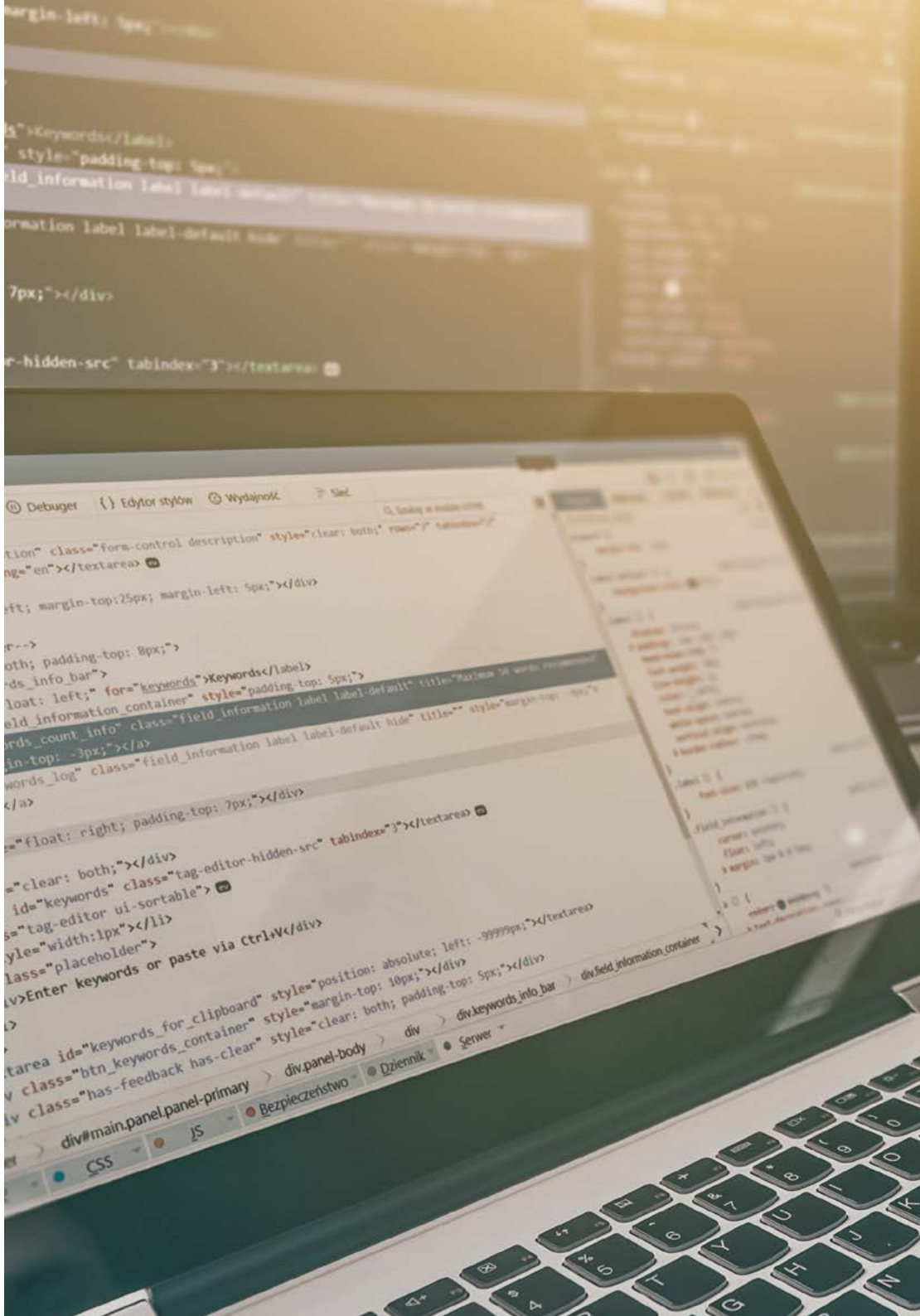
Al termine del processo di valutazione di questo Master Privato, il professionista avrà acquisito una serie di conoscenze, strumenti e competenze che gli permetteranno di lavorare in questo settore con maggiori garanzie di successo. Lo studente non solo diventerà così un esperto di Cybersecurity, ma contribuirà anche in modo positivo alla riduzione della criminalità informatica grazie alla creazione di una rete più sicura e più forte per tutti. Raggiungendo posti di alta dirigenza come Chief Information Security Officer.

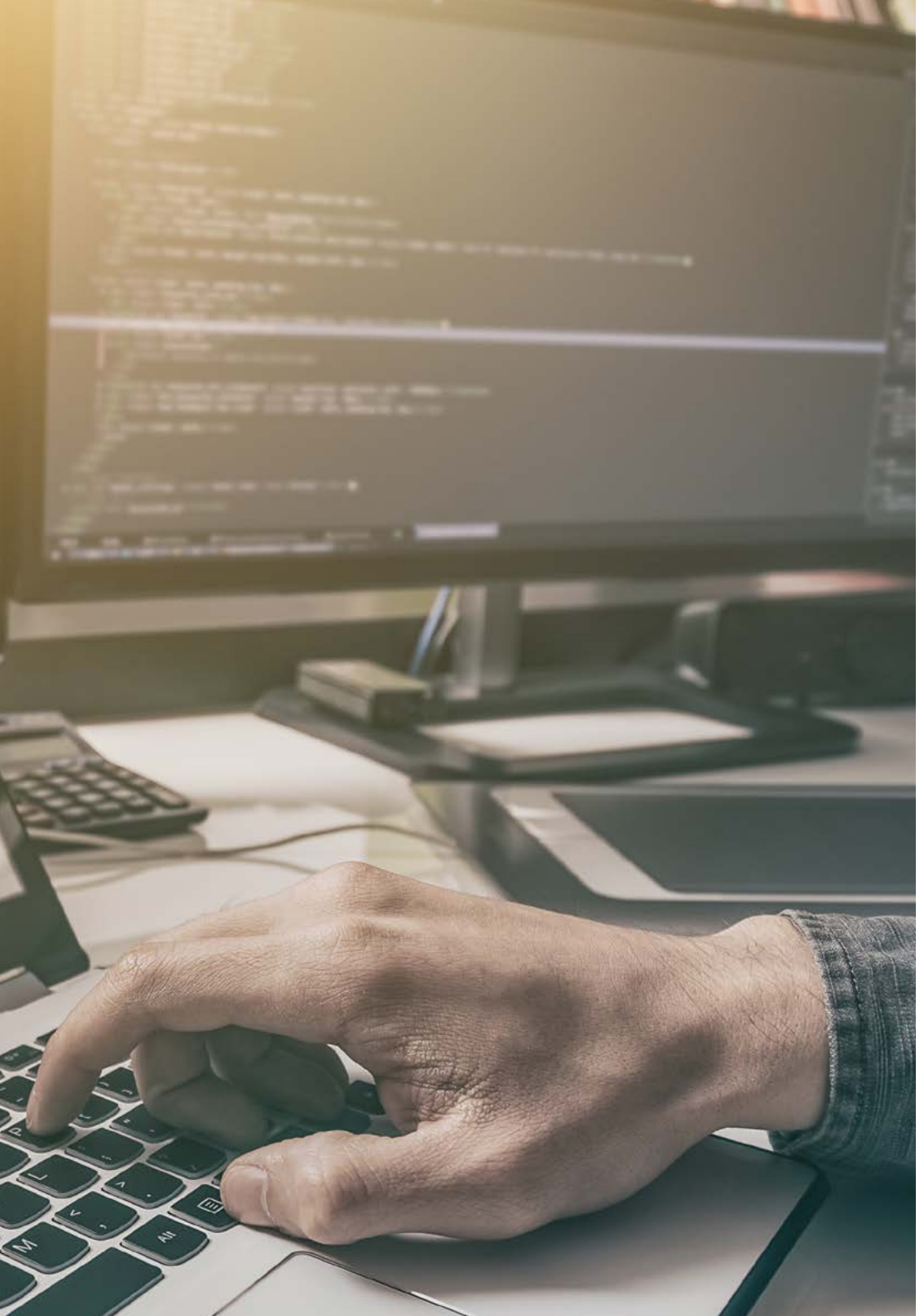
Il settore della cybersecurity richiede un costante aggiornamento delle conoscenze. Grazie a programmi come quello qui proposto, il professionista riesce a raggiungere questo obiettivo in modo rapido ed efficace"

Competenze generali

- Conoscere le metodologie utilizzate in materia di sicurezza informatica
- Saper valutare ogni tipo di minaccia per offrire una soluzione ottimale in ogni caso
- Essere in grado di generare soluzioni intelligenti complete per automatizzare il comportamento in caso di imprevisti
- Saper valutare i rischi associati alle vulnerabilità interne ed esterne all'azienda
- Comprendere l'evoluzione e l'impatto dell'IoT nel tempo
- Essere in grado di dimostrare che un sistema è vulnerabile, attaccarlo in modo proattivo e risolvere tali problemi
- Saper applicare il *sandboxing* in diversi ambienti
- Conoscere le linee guida che un buon sviluppatore deve seguire per conformarsi ai requisiti di sicurezza necessari

Migliorare le tue competenze in un ambito utile a tutti ti permetterà di migliorare la tua carriera professionale





Competenze specifiche

- Saper condurre operazioni di sicurezza difensiva
- Possedere una percezione approfondita e specializzata della sicurezza informatica
- Avere conoscenze specialistiche nel campo della cybersecurity e della cyberintelligence
- Approfondire aspetti fondamentali quali il ciclo dell'intelligence, le relative fonti, l'ingegneria sociale, la metodologia OSINT, HUMINT, *l'Anonimizzazione*, l'analisi del rischio, le metodologie esistenti (OWASP, OWISAM, OSSTM, PTES) e le normative vigenti in materia di cybersecurity
- Comprendere l'importanza di concepire una difesa a più livelli, nota anche come "*Defense in Depth*", comprendendo tutti gli aspetti di una rete aziendale, dove alcuni dei concetti e dei sistemi che In questo modo possono essere utilizzati e applicati anche in un ambiente domestico
- Saper applicare i processi di sicurezza per smartphone e dispositivi portatili
- Sapere come effettuare il cosiddetto Hacking etico e proteggere un'azienda da un attacco informatico
- Essere in grado di indagare su un incidente di cybersecurity
- Conoscere le diverse tecniche di attacco e di difesa disponibili
- Analizzare il ruolo dell'Analista di Cybersecurity
- Capire come funziona l'ingegneria sociale e i suoi metodi

04

Direzione del corso

L'MBA in Cybersecurity Management (CISO, Chief Information Security Officer) è stato sviluppato da un personale docente eterogeneo e specializzato in diversi settori, che ha unito l'esperienza professionale maturata a livello internazionale nel settore privato in R&D+i a un'ampia esperienza di insegnamento. Non solo sono aggiornati su ogni singola tecnologia, ma hanno anche una visione delle esigenze future del settore e le presentano in modo didattico. In questo modo, il professionista ha la certezza di imparare dai migliori del settore, con la garanzia di avere le conoscenze più aggiornate.

Durante l'MBA sarai affiancato da esperti professionisti che renderanno unica la tua esperienza educativa"

Direttore Ospite Internazionale

Il Dottor Frederic Lemieux è riconosciuto a livello internazionale come esperto innovatore e leader ispiratore nei campi **dell'Intelligence**, della **Sicurezza Nazionale**, della **Sicurezza Interna**, **della Cibersicurezza** e delle **Tecnologie Dirompenti**. Il suo impegno costante e i suoi contributi rilevanti alla Ricerca e all'Educazione lo pongono come una figura chiave nella **promozione della sicurezza** e **della comprensione delle tecnologie emergenti** di oggi. Nel corso della sua carriera professionale, ha ideato e diretto programmi accademici all'avanguardia presso diverse istituzioni rinomate, tra cui **l'Università di Montreal**, la **la George Washington University** e la **Georgetown University.**

Durante il corso della sua vasta esperienza, ha pubblicato numerosi libri di grande rilevanza, tutti legati all'intelligence criminale, all'attività di polizia, alle minacce cibernetiche e alla sicurezza internazionale. Ha inoltre contribuito in modo significativo al campo della sicurezza **informatica** pubblicando numerosi articoli in riviste accademiche, che esaminano il controllo del crimine durante i grandi disastri, l'antiterrorismo, le agenzie di intelligence e la cooperazione di polizia. Inoltre, è stato relatore e relatore principale in varie conferenze nazionali e internazionali, affermandosi come punto di riferimento nell'ambiente accademico e professionale.

Il Dottor Lemieux ha ricoperto ruoli editoriali e di valutazione in diverse organizzazioni accademiche, private e governative, a testimonianza della sua influenza e del suo impegno per l'eccellenza nel suo campo di competenza. In questo modo, la sua prestigiosa carriera accademica lo ha portato a svolgere come Professore di Tirocinio e Direttore della Facoltà dei programmi MPS in **Intelligence Applicata**, **Gestione del Rischio in Sicurezza Informatica**, **Gestione Tecnologica** e **Gestione delle Tecnologie dell'Informazione** alla **Georgetown University.**

Dott. Lemieux, Frederic

- Direttore del Master in Cybersecurity Risk Management di Washington, Stati Uniti
- Direttore del MasterTechnology Management presso la Georgetown University
- Direttore del Master in Applied Intelligence presso la Georgetown University
- Docente di Pratica all'Università di Leioa
- Dottorato di Ricerca in Criminologia presso la Scuola di Criminologia dell'Università di Montreal
- Laurea in Sociologia e laurea minore in Psicologia presso l'Università di Laval
- Membro di: New Program Roundtable Committee presso la Georgetown University

Grazie a TECH potrai apprendere al fianco dei migliori professionisti del mondo"

Direttrice Ospite Internazionale

Con oltre 20 anni di esperienza nella progettazione e gestione di team globali per **l'acquisizione di talenti**, Jennifer Dove è un'esperta in **assunzioni** e **strategia tecnologica**. Nel corso della sua esperienza professionale ha ricoperto posizioni di leadership in diverse organizzazioni tecnologiche all'interno delle aziende ***Fortune 50***, tra cui **NBCUniversal** e **Comcast**. La sua esperienza gli ha permesso di distinguersi in ambienti competitivi e ad alta crescita.

In qualità di **Vice Presidentessa per l'Acquisizione dei Talenti** presso **Mastercard**, è responsabile della supervisione della strategia e dell'esecuzione del processo di assunzione dei talenti, collaborare con i leader aziendali e i responsabili delle **Risorse Umane** per raggiungere gli obiettivi operativi e strategici di assunzione. In particolare, il suo obiettivo è **creare team diversificati**, **inclusivi** e **ad alte prestazioni** che promuovano l'innovazione e la crescita dei prodotti e dei servizi dell'azienda. Inoltre, è esperta nell'uso di strumenti per attrarre e trattenere i migliori professionisti da tutto il mondo. Inoltre, si occupa di **amplificare** il **marchio del datore** di lavoro e la proposta di valore di **Mastercard** attraverso pubblicazioni, eventi e social media.

Jennifer Dove ha dimostrato il suo impegno per lo sviluppo professionale continuo, partecipare attivamente alle reti di professionisti delle **Risorse Umane** e contribuire all'inserimento di numerosi lavoratori in diverse aziende**.** Dopo aver conseguito la laurea in **Comunicazione Organizzativa** presso l'Università di **Miami**, ha ricoperto incarichi dirigenziali nella selezione del personale in aziende di diversi settori.

D'altra parte, è stata riconosciuta per la sua capacità di guidare le trasformazioni organizzative, **integrare le tecnologie** nei **processi di reclutamento** e sviluppare programmi di leadership che preparano le istituzioni per le sfide future. Ha anche implementato con successo programmi di **benessere sul lavoro** che hanno aumentato in modo significativo la soddisfazione e la fidelizzazione dei dipendenti.

Dott.ssa Dove, Jennifer

- Vice presidentessa per l'Acquisizione di Talenti alla Mastercard, New York, Stati Uniti
- Direttrice Acquisizione di Talenti in NBCUniversal, New York, Stati Uniti
- Responsabile della Selezione del Personale Comcast
- Direttrice del Reclutamento presso Rite Hire Advisory
- Vice Presidentessa Esecutiva della Divisione Vendite di Ardor NY Real Estate
- Direttrice del Personale presso Valerie August & Associates
- Responsabile dei Conti presso BNC
- Responsabile dei Conti presso Vault
- Laurea in Comunicazione Organizzativa presso l'Università di Miami

TECH ha un gruppo distinto e specializzato di Direttori Ospiti Internazionali, con importanti ruoli di leadership nelle aziende più all'avanguardia del mercato globale"

Direttore Ospite Internazionale

Leader tecnologico con decenni di esperienza nelle **principali multinazionali tecnologiche**, Rick Gauthier si è sviluppato in modo prominente nel campo dei **servizi cloud** e del miglioramento dei processi end-to-end. È stato riconosciuto come un leader e responsabile di team con grande efficienza, mostrando un talento naturale per garantire un alto livello di impegno tra i suoi dipendenti.

Possiede doti innate nella strategia e nell'innovazione esecutiva, sviluppando nuove idee e supportando il suo successo con dati di qualità. Il suo percorso in **Amazon** gli ha permesso di gestire e integrare i servizi IT della società negli Stati Uniti. In **Microsoft** ha guidato un team di 104 persone, incaricati di fornire l'infrastruttura informatica a livello aziendale e supportare i dipartimenti di ingegneria dei prodotti in tutta l'azienda.

Questa esperienza gli ha permesso di distinguersi come un manager ad alto impatto, con notevoli capacità per aumentare l'efficienza, la produttività e la soddisfazione generale del cliente.

Dott. Gauthier, Rick

- Direttore Regionale di IT in Amazon, Seattle, Stati Uniti
- Responsabile dei programmi senior in Amazon
- Vicepresidente di Wimmer Solutions
- Direttore senior dei servizi di ingegneria produttiva in Microsoft
- Laureato in Sicurezza Informatica presso la Western Governors University
- Certificato Tecnico in *Commercial Diving* per Divers Institute of Technology
- Studi Ambientali presso l'Evergreen State College

Cogli l'occasione per conoscere gli ultimi sviluppi in questo campo e applicarlo alla tua pratica quotidiana"

Direttore Ospite Internazionale

Romi Arman è un esperto internazionale di fama con oltre due decenni di esperienza in **Digital Transformation**, **Marketing, Strategia** e **Consulenza**. In questo lungo percorso ha assunto diversi rischi ed è un sostenitore **costante dell'innovazione** e del **cambiamento** nella congiuntura aziendale. Con questa esperienza, ha collaborato con amministratori delegati e organizzazioni aziendali di tutto il mondo, spingendoli a mettere da parte i modelli di business tradizionali. Ha contribuito a rendere aziende come la Shell Energy **leader nel mercato,** focalizzate sui **clienti** e sul **mondo digitale.**

Le strategie ideate da Arman hanno un impatto latente, poiché hanno permesso a diverse aziende di **migliorare le esperienze dei consumatori, del personale** e **degli** azionisti. Il successo di questo esperto è misurabile attraverso metriche tangibili come **CSAT**, **l'impegno dei dipendenti** presso le istituzioni in cui ha esercitato e la crescita **dell'indicatore finanziario EBITDA** in ciascuna di esse.

Inoltre, nel suo percorso professionale ha nutrito e **guidato team ad alte prestazioni che hanno anche ricevuto riconoscimenti** per il loro **potenziale di trasformazione**. Con Shell, in particolare, il dirigente si è sempre proposto di superare tre sfide: soddisfare le complesse **richieste** di **decarbonizzazione** dei clienti, **sostenere** una "**decarbonizzazione redditizia**" e **rivedere** un panorama frammentato di **dati, digitali e tecnologici**. Così, i loro sforzi hanno evidenziato che per raggiungere un successo sostenibile è fondamentale partire dalle esigenze dei consumatori e gettare le basi della trasformazione dei processi, Dati, tecnologia e cultura.

Inoltre, il dirigente si distingue per la sua padronanza delle **applicazioni aziendali dell'Intelligenza Artificiale,** argomento in cui ha conseguito un master presso la Business School di Londra. Allo stesso tempo, ha accumulato esperienze in **IoT** e **Salesforce.**

Dott. Arman, Romi

- Direttore della Trasformazione Digitale (CDO) presso la Corporation Shell Energy, Londra, Regno Unito
- Direttore Globale di E-commerce e Assistenza Clienti alla Shell Energy Corporation
- Responsabile Nazionale dei Conti Chiave (produttori di apparecchiature originali e rivenditori di automobili) per Shell a Kuala Lumpur, Malesia
- Consulente Senior di Gestione (settore dei servizi finanziari) per Accenture da Singapore
- Laurea presso l'Università di Leeds
- Post-Laurea in Applicazioni Aziendali IA per Dirigenti della Business School di Londra
- Certificazione Professionale in Esperienza del cliente CCXP
- Corso di Trasformazione Digitale per Dirigenti IMD

Vuoi aggiornare le tue conoscenze con la massima qualità educativa? TECH ti offre i contenuti più aggiornati del mercato accademico, progettati da autentici esperti di fama internazionale"

Direttore Ospite Internazionale

Manuel Arens è un **esperto nella gestione** dei dati e leader di un team altamente qualificato. Infatti, Arens è il **responsabile globale degli acquisti** nella divisione di Google per le infrastrutture tecniche e i data center, la sua carriera professionale si è svolta in un'azienda dove ha svolto la maggior parte della sua attività. Con sede a Mountain View, in California, ha fornito soluzioni per le sfide operazioni del gigante tecnologico, come **l'integrità dei dati di riferimento,** gli **aggiornamenti dati dei fornitori** e la **loro priorizzazione**. Ha guidato la pianificazione della supply chain del data center e la valutazione dei rischi del fornitore, generando miglioramenti nel processo e la gestione dei flussi di lavoro che hanno portato a risparmi significativi sui costi.

Con oltre un decennio di lavoro fornendo soluzioni digitali e leadership per le aziende in vari settori, ha una vasta esperienza in tutti gli aspetti della fornitura di soluzioni strategiche, tra cui **Marketing, analisi dei media, misurazione** e **attribuzione**. Ha ricevuto diversi riconoscimenti per il suo lavoro, tra cui il **Premio per la leadership BIM**, il **Leadership Search Award**, il **Premio per il programma di generazione di lead all'esportazione** e **Best Sales Model EMEA.**

Inoltre, Arens ha lavorato come **Sales Manager** a Dublino, in Irlanda. In questa posizione, ha costruito un team di 4-14 membri in tre anni e ha guidato il team di vendita per ottenere risultati e collaborare bene tra loro e con team interfunzionali. Ha anche lavorato come **Analista Senior** di settore ad Amburgo, in Germania, creando storylines per oltre 150 clienti utilizzando strumenti interni e di terze parti a supporto dell'analisi. Ha sviluppato e redatto rapporti approfonditi per dimostrare la sua padronanza dell'argomento, compresa la comprensione dei **fattori macroeconomici e politici/normativi** che influenzano l'adozione e la diffusione della tecnologia.

Ha anche guidato team in aziende come **Eaton, Airbus e Siemens**, dove ha acquisito una preziosa esperienza nella gestione dei clienti e della supply chain. Sottolinea in particolare il suo impegno a superare continuamente le aspettative **costruendo relazioni preziose con i clienti e** lavorando senza problemi con persone a tutti i livelli di un'organizzazione, **compresi gli stakeholder, la gestione**, i membri del team e i clienti. Il suo approccio basato sui dati e la sua capacità di sviluppare soluzioni innovative e scalabili per le sfide del settore lo hanno reso un leader nel suo campo.

Dott. Arens, Manuel

- Responsabile degli Acquisti Globali in Google, Mountain View, USA
- Senior Analyst e Technology B2B presso Google, Stati Uniti
- Direttore delle Vendite presso Google, Irlanda
- Analista Industriale Senior presso Google, Germania
- Account Manager presso Google, Irlanda
- Accounts Payable in Eaton, Reino Unido
- Responsabile della Catena di Somministro in Airbus, Germania

Scegli TECH! Potrai accedere ai migliori materiali didattici, all'avanguardia tecnologica ed educativa, implementati da rinomati specialisti di fama internazionale nel settore"

Direttore Ospite Internazionale

Andrea La Sala è un esperto dirigente del Marketing i cui progetti hanno avuto un impatto significativo sull'ambiente della Moda. Nel corso della sua carriera di successo ha svolto diversi compiti relativi a **Prodott**, **Merchandising** e **Comunicazione**. Tutto questo, legato a marchi di prestigio come **Giorgio Armani**, **Dolce&Gabbana**, **Calvin Klein**, tra gli altri.

I risultati di questo leader internazionale di **alto profilo internazionale** sono stati legati alla sua comprovata capacità di **sintetizzare le informazioni** in quadri chiari e di attuare **azioni concrete** allineate a specifici **obiettivi aziendali**. Inoltre, è riconosciuto per la sua **proattività** y **adattamento ad un ritmo accelerato** di lavoro. A tutto questo, un esperto aggiunge una **forte consapevolezza commerciale**, **visione del mercato** e una vera **passione** per i **prodotti**.

In qualità di **Global Brand and Merchandising Director** presso **Giorgio Armani**, ha supervisionato diverse **strategie di marketing** per **abbigliamento** e **accessori**. Inoltre, le loro tattiche sono state focalizzate nel settore della **vendita al dettaglio** e delle **esigenze** e del **comportamento dei consumatori**. Da questo in qualità di responsabile della commercializzazione dei prodotti nei diversi mercati, ha lavorato come **team leader** nei **reparti Design**, **Comunicazione** e **Vendite**.

In aziende come **Calvin Klein** o il **Gruppo Coin**, ha inoltre avviato progetti per promuovere la **struttura**, lo **sviluppo** e la **commercializzazione** di **diverse collezioni**. A sua volta, è stato incaricato di **creare calendari efficaci** per le **campagne** di acquisto e vendita. Ha inoltre avuto sotto la sua direzione i **termini**, **costi**, **processi** e **tempi di consegna** di diverse operazioni.

Queste esperienze hanno reso Andrea La Sala uno dei **leader aziendali** più importanti e qualificati nel settore della **Moda** e del **Lusso**. Un'elevata capacità manageriale con la quale è riuscito a implementare in modo efficace il **posizionamento positivo** di **diversi marchi** e ridefinire i suoi indicatori chiave di prestazione (KPI).

Dott. La Sala, Andrea

- Direttore Globale del Marchio e Merchandising Armani Exchange presso Giorgio Armani, Milano
- Direttore del Merchandising di Calvin Klein
- Responsabile del marchio presso il Gruppo Coin
- Brand Manager in Dolce&Gabbana
- Direttore del marchio presso Sergio Tacchini S.p.A.
- Analista di Mercato presso Fastweb
- Laurea in Economia e Commercio presso l'Università del Piemonte Orientale

I professionisti più qualificati ed esperti a livello internazionale ti aspettano al TECH per offrirti un insegnamento di primo livello, aggiornato e basato sulle ultime prove scientifiche. Cosa aspetti ad iscriverti?"

Direttore Ospite Internazionale

Mick Gram è sinonimo di innovazione ed eccellenza nel campo della **Business Intelligence** a livello internazionale. La sua carriera di successo è legata a posizioni di leadership in multinazionali come **Walmart** e **Red Bull.** Inoltre, questo esperto è noto per la sua visione **nell'identificare le tecnologie emergenti** che, a lungo termine, hanno un impatto duraturo sull'ambiente aziendale.

D'altra parte, l'esecutivo è considerato un **pioniere** nell'uso di **tecniche di visualizzazione dei dati** che semplificano set complessi, rendendoli accessibili e facilitanti nel processo decisionale. Questa abilità divenne il pilastro del suo profilo professionale, rendendolo un bene desiderabile per molte organizzazioni che puntavano a **raccogliere informazioni** e **generare azioni** concrete da loro.

Uno dei suoi progetti più importanti degli ultimi anni è stato la **piattaforma Walmart Data Cafe**, la più grande del suo genere al mondo che è ancorata al cloud per **l'analisi** di ***Big Data***. Ha inoltre ricoperto la carica di **Direttore** della **Business Intelligence** in **Red Bull,** occupandosi di aree **quali vendite, distribuzione, marketing e supply chain operations**. Il suo team è stato recentemente riconosciuto per la sua costante innovazione nell'utilizzo della nuova API di Walmart Luminate per gli insight di Buyer e Channel.

Per quanto riguarda la sua formazione, il manager ha diversi master e studi post-laurea presso prestigiosi centri come **l'Università di Berkeley**, negli Stati Uniti, e **l'Università di Copenaghen**, in Danimarca. Attraverso questo aggiornamento continuo, l'esperto ha raggiunto competenze all'avanguardia. In questo modo, è diventato un **leader nato** della **nuova economia mondiale**, incentrata sull'impulso dei dati e sulle loro infinite possibilità.

Dott. Gram, Mick

- Direttore di *Business Intelligence* e analisi in Red Bull, Los Angeles, Stati Uniti
- Architetto di soluzioni di *Business Intelligence* per Walmart Data Cafe
- Consulente indipendente di *Business Intelligence* e *Data Science*
- Direttore di *Business Intelligence* presso Capgemini
- Analista Capo in Nordea
- Consulente Capo di *Bussiness Intelligence* per SAS
- Executive Education in IA e Machine Learning in UC Berkeley College of Engineering
- MBA Executive en e-commerce presso l'Università di Copenaghen
- Laurea e Master in Matematica e Statistica presso l'Università di Copenaghen

Studia nella migliore università Online del mondo secondo Forbes! In questo MBA avrai accesso a una vasta libreria di risorse multimediali, elaborate da docenti riconosciuti di rilevanza internazionale"

Direttore Ospite Internazionale

Scott Stevenson è un illustre esperto del settore del **Marketing Digitale** che, per oltre 19 anni, è stato associato a una delle più potenti aziende del settore dell'intrattenimento, **Warner Bros. Discovery** In questo ruolo, è stato determinante nella **supervisione della logistica** e dei flussi di lavoro creativi su diverse piattaforme digitali, tra cui social media, ricerca, display e media lineari.

La sua leadership è stata cruciale nel guidare le **strategie di produzione** dei **media a pagamento**, che hanno portato a un netto **miglioramento** dei tassi di conversione **dell'azienda** Allo stesso tempo, ha assunto altri ruoli, come quello di Direttore dei Servizi di Marketing e di Responsabile del Traffico presso la stessa multinazionale durante il suo precedente mandato dirigenziale.

Stevenson si è occupato anche della distribuzione globale di videogiochi e **di campagne immobiliari digitali. È stato anche responsabile dell'introduzione di strategie operative relative alla creazione, alla finalizzazione e alla consegna di contenuti audio e immagini per** spot televisivi e ***trailer.***

D'altra parte, l'esperto ha una laurea in Telecomunicazioni dall'Università della Florida e un Master in Scrittura Creativa dalla University of California, che dimostra le sue abilità nella **comunicazione** e nella **narrazione**. **Inoltre, ha partecipato alla School of Professional Development dell'Università di Harvard a programmi all'avanguardia sull'uso dell'** Intelligenza Artificiale nel **business**. Così, il suo profilo professionale si erge come uno dei più importanti nel campo del **Marketing** e dei **Media Digitali.**

Dott. Stevenson, Scott

- Direttore del Marketing Digitale di Warner Bros Discovery, Burbank, Stati Uniti
- Responsabile del Traffico della Warner Bros Entertainment
- Master in Scrittura Creativa presso l'Università della California
- Laurea in Telecomunicazioni presso l'Università della Florida

Raggiungi i tuoi obiettivi accademici e professionali con gli esperti più qualificati del mondo! I docenti di questo MBA ti guideranno attraverso l'intero processo di apprendistato"

Direttore Ospite Internazionale

Il Dottor Eric Nyquist è un importante professionista nel **campo dello sport internazionale**, che ha costruito una carriera impressionante, distinguendosi per la sua **leadership strategica** e la sua capacità di promuovere il cambiamento e **l'innovazione** nelle **organizzazioni sportive** di primo livello.

Infatti, ha ricoperto ruoli di alto livello, come quello di **Direttore delle Comunicazioni e dell'Impatto** alla **NASCAR**, con sede in **Florida, Stati Uniti**. Con molti anni di esperienza alle spalle in questa entità, il Dottor Nyquist ha anche ricoperto diverse posizioni di leadership, tra cui **Vicepresidente Senior dello Sviluppo Strategico** e **Direttore Generale degli Affari Commerciali,** gestendo più di una dozzina di discipline che vanno dallo **sviluppo strategico** al **Marketing dell'intrattenimento.**

Inoltre, Nyquist ha lasciato un segno significativo nei **principali franchising** sportivi di Chicago. In qualità di **Vicepresidente Esecutivo** del franchising dei **Chicago Bulls** e dei **Chicago White Sox**, ha dimostrato la sua capacità di promuovere il **successo aziendale** e **strategico** nel mondo dello **sport professionale.**

Infine, va notato che ha iniziato la sua **carriera sportiva** mentre lavorava a **New York** come **analista strategico principale** per **Roger Goodell** nella **National Football League (NFL)** e, in precedenza, come **stagista legale** nella **Federcalcio degli Stati Uniti.**

Dott. Nyquist, Eric

- Direttore delle Comunicazioni e dell'Impatto alla NASCAR, Florida, Stati Uniti
- Vicepresidente Senior dello Sviluppo Strategico alla NASCAR
- Vice Presidente della Pianificazione Strategica alla NASCAR
- Direttore Generale degli Affari Commerciali alla NASCAR
- Vicepresidente Esecutivo del Franchising Chicago White Sox
- Vicepresidente Esecutivo del Franchising Chicago Bulls
- Responsabile della Pianificazione Aziendale presso la National Football League (NFL)
- Affari Commerciali/Stagista Legale presso la Federcalcio degli Stati Uniti
- Dottorato in Giurisprudenza all'Università di Chicago
- Master in Business Administration-MBA presso la Booth School of Business presso l'Università di Chicago
- Laurea in Economia Internazionale presso Carleton College

Grazie a questo titolo universitario, 100% online, potrai conciliare lo studio con i tuoi impegni quotidiani, insieme ai maggiori esperti internazionali nel campo che ti interessa. Iscriviti subito!"

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 E-Council
- Formatrice nelle seguenti certificazioni: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation, Madrid
- Esperta Formatrice accreditata dal CAM per i seguenti certificati di professionalità: Sicurezza informatica (IFCT0190), Gestione di reti voce e dati (IFCM0310), Amministrazione di reti dipartimentali (IFCT0410), Gestione degli allarmi nelle reti di telecomunicazione (IFCM0410), Operatore di reti 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
- Máster en DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Personale docente

Dott.ssa Marcos Sbarbaro, Victoria Alicia

- Sviluppatrice di Applicazioni Mobili Native Android presso B60 Regno Unito
- Analista programmatore per la gestione, il coordinamento e la documentazione dell'ambiente di allarme di sicurezza virtualizzato
- Analista Programmatrice di applicazioni Java per ATM
- Sviluppo di Software Applicativo per la Convalida della Firma e la Gestione dei Documenti Professionale
- Tecnico di Sistemi per la Migrazione delle Apparecchiature e per la Gestione, Manutenzione e Formazione dei Dispositivi Mobili PDA
- Ingegnere Tecnico di Sistemi Informatici presso l'Università di Oberta de Catalogna
- Master in Sicurezza Informatica e Hacking Etico Ufficiale EC- Council e CompTIA dalla Scuola Professionale di Nuove Tecnologie CICE

Dott. Redondo, Jesús Serrano

- Sviluppatore Web e Tecnico di Cibersicurezza
- Sviluppatore Web presso Roams, Palencia, Spagna
- Sviluppatore *FrontEnd* presso Telefónica, Madrid
- Sviluppatore *FrontEnd* presso Best Pro Consulting SL, Madrid
- Installatore di Apparecchiature e Servizi di Telecomunicazione presso il Grupo Zener, Castiglia e León
- Installatore di Apparecchiature e Servizi di Telecomunicazione in Lican Comunicaciones SL, Castiglia e León
- Certificato in Sicurezza Informatica, CFTIC Getafe, Madrid
- Tecnico Superiore in Telecomunicazioni e Sistemi Informatici presso IES Trinidad Arroyo, Palencia
- Tecnico superiore in Installazioni Elettrotecniche MT e BT dell'IES Trinidad Arroyo, Palencia
- Preparazione al Reverse Engineering, alla Stenografia e alla Crittografia con Incibe Hacker Academy

Dott. Catalá Barba, José Francisco

- Tecnico Elettronico Esperto di Cybersecurity
- Sviluppatore di Applicazioni Mobile
- Tecnico Elettronico presso il Comando Intermedio del Ministero della Difesa Spagnolo
- Tecnico Elettronico presso la Fabbrica Ford Sita di Valencia

Dott. Peralta Alonso, Jon

- Consulente senior per la protezione dei dati e la cybersecurity presso Altia
- Avvocato/Consulente legale presso Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Consulente legale/tirocinante presso uno studio legale professionale: Óscar Padura
- Laurea in Giurisprudenza presso l'Università Pubblica dei Paesi Baschi
- Master in Protezione dei dati personali conseguito presso la Scuola Innovativa EIS
- Laurea in Giurisprudenza presso l'Università pubblica dei Paesi Baschi
- Master specialistico in pratica del contenzioso civile presso l'Università Internazionale Isabel I di Castiglia
- Docente del Master in Protezione dei dati personali, Cibersicurezza e Diritto delle TIC Dott. Jiménez Ramos, Álvaro

Dott. Jiménez Ramos, Álvaro

- Analista di Cibersicurezza
- Analista Senior di Sicurezza presso The Workshop
- Analista di sicurezza informatica L1 presso Axians
- Analista di Cibersicurezza L2 presso Axians
- Analista di Cibersicurezza presso SACYR S.A.
- Laurea in Ingegneria Telematica presso l'Università Politecnica di Madrid
- Master in Cybersecurity e Hacking Etico realizzato presso il CICE
- Corso Avanzato sulla Cybersecurity organizzato da Deusto Formación

Cogli l'occasione per conoscere gli ultimi sviluppi in questo campo e applicarlo alla tua pratica quotidiana"

05

Struttura e contenuti

Per garantire che lo studente acquisisca le conoscenze più rigorose e all'avanguardia nella Sicurezza Informatica, TECH ha realizzato una serie di materiali che raccolgono gli ultimi aggiornamenti della professione. Questi contenuti sono stati elaborati da un gruppo di esperti del settore, in modo da adattarsi alle esigenze attuali delle posizioni offerte nel settore. Un'opportunità unica ed estremamente professionale che consentirà agli studenti di raggiungere il successo nel proprio percorso lavorativo.

Un piano di studi di alto livello, ideato da esperti del settore e per professionisti di alto livello: intendi perdere questa opportunità?"

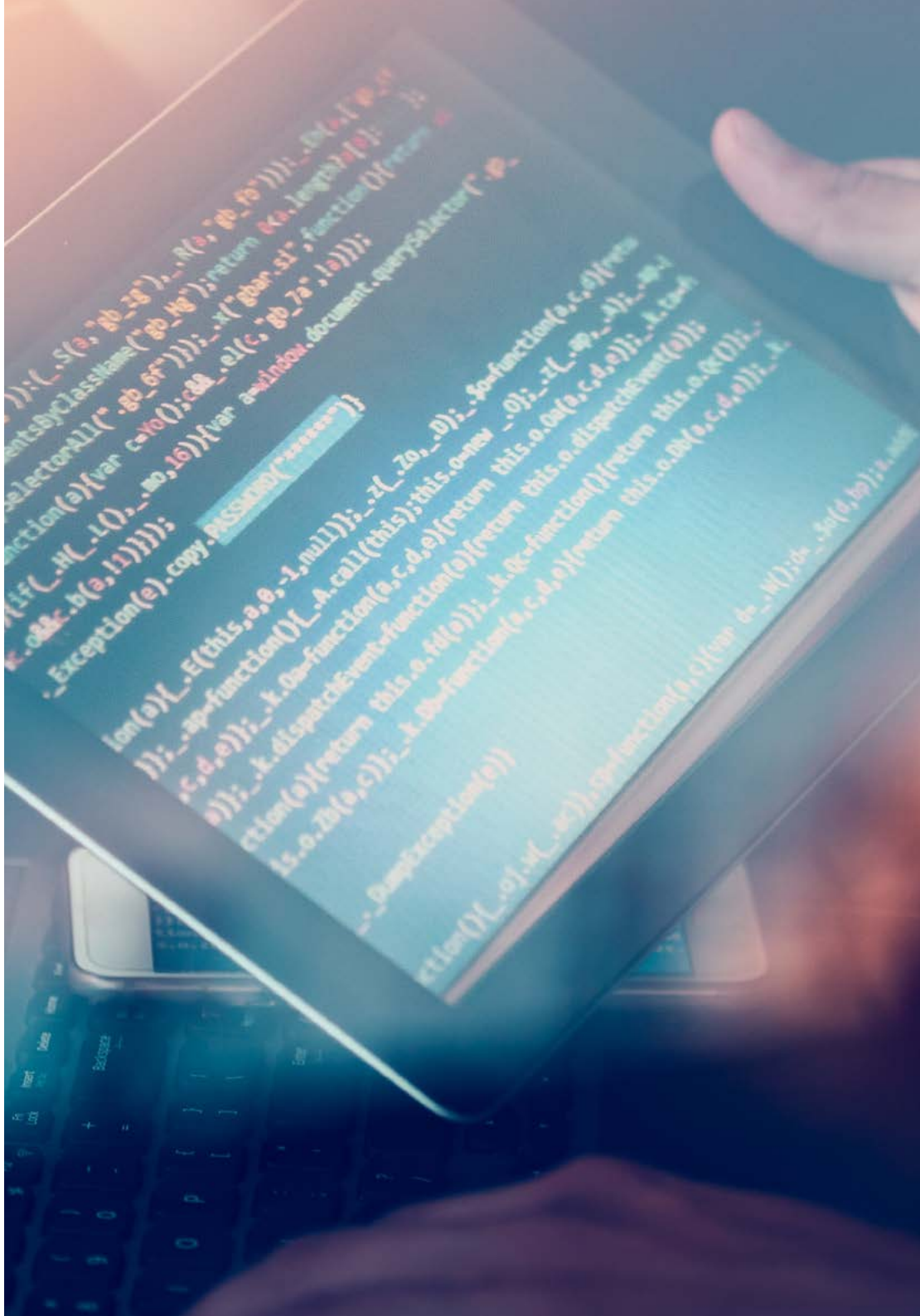
Modulo 1. Cyberintelligence e Cybersicurezza

1.1. Cyberintelligence
- 1.1.1. Cyberintelligence
  - 1.1.1.1. L'intelligence
    - 1.1.1.1.1. Ciclo dell'intelligence
  - 1.1.1.2. Cyberintelligence
  - 1.1.1.3. Cyberintelligence e Cybersicurezza
- 1.1.2. L'analista di intelligence
  - 1.1.2.1. Il ruolo dell'analista di intelligence
  - 1.1.2.2. I pregiudizi dell'analista di intelligence nell'attività valutativa

1.2. Cybersicurezza
- 1.2.1. Livelli di sicurezza
- 1.2.2. Identificazione delle minacce informatiche
  - 1.2.2.1. Minacce esterne
  - 1.2.2.2. Minacce interne
- 1.2.3. Azioni avverse
  - 1.2.3.1. Ingegneria sociale
  - 1.2.3.2. Metodi comunemente utilizzati

1.3. Tecniche e Strumenti delle intelligence
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Distribuzioni e strumenti Linux
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

1.4. Metodologie di valutazione
- 1.4.1. L'analisi di intelligence
- 1.4.2. Tecniche di organizzazione delle informazioni acquisite
- 1.4.3. Affidabilità e credibilità delle fonti di informazione
- 1.4.4. Metodologie di analisi
- 1.4.5. Presentazione dei risultati dell'intelligence



1.5. Audit e documentazione
- 1.5.1. L' Audit della sicurezza informatica
- 1.5.2. Documentazione e autorizzazioni per l'Audit
- 1.5.3. Tipi di audit
- 1.5.4. Consegnabili
  - 1.5.4.1. Rapporto tecnico
  - 1.5.4.2. Relazione esecutiva

1.6. Anonimato in rete
- 1.6.1. Uso dell'anonimato
- 1.6.2. Tecniche di anonimato (Proxy, VPN)
- 1.6.3. Reti TOR, Freenet e IP2

1.7. Minacce e tipi di sicurezza
- 1.7.1. Tipologie di minacce
- 1.7.2. Sicurezza fisica
- 1.7.3. Sicurezza di rete
- 1.7.4. Sicurezza logica
- 1.7.5. Sicurezza delle applicazioni web
- 1.7.6. Sicurezza sui dispositivi mobili

1.8. Regolamenti e conformità
- 1.8.1. GDPR
- 1.8.2. La strategia nazionale di cybersecurity per il 2019
- 1.8.3. Famiglia ISO 27000
- 1.8.4. Quadro di sicurezza informatica NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Normativa sul *Cloud*
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Analisi dei rischi e metriche
- 1.9.1. Portata dei rischi
- 1.9.2. I cespiti
- 1.9.3. Le minacce
- 1.9.4. Valutazione del rischio
- 1.9.5. Trattamento del rischio

1.10. Importanti organismi di cybersecurity
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR-PROSUR

Modulo 2. Sicurezza in Host

2.1. Copie di riserva
- 2.1.1. Strategie per i backup
- 2.1.2. Strumenti per Windows
- 2.1.3. Strumenti per Linux
- 2.1.4. Strumenti per MacOS

2.2. Antivirus utente
- 2.2.1. Tipi di antivirus
- 2.2.2. Antivirus per Windows
- 2.2.3. Antivirus per Linux
- 2.2.4. Antivirus per MacOS
- 2.2.5. Antivirus per smartphone

2.3. Rilevatori di intrusione-HIDS
- 2.3.1. Metodi di rilevamento delle intrusioni
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. Firewall local
- 2.4.1. Firewalls per Windows
- 2.4.2. Firewall per Linux
- 2.4.3. Firewall per MacOS

2.5. Gestori di password
- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. StickyPassword
- 2.5.5. RoboForm

2.6. Rilevatori di *phishing*
  2.6.1. Rilevamento manuale del *phishing*
  2.6.2. Strumenti *antiphishing*
2.7. *Spyware*
  2.7.1. Meccanismi di prevenzione
  2.7.2. Strumenti *antispyware*
2.8. Tracciatori
  2.8.1. Misure di protezione del sistema
  2.8.2. Strumenti anti-tracciamento
2.9. EDR-*End point Detection and Response*
  2.9.1. Comportamento del sistema EDR
  2.9.2. Differenze tra EDR e antivirus
  2.9.3. Il futuro dei sistemi EDR
2.10. Controllo dell'installazione del software
  2.10.1. Repository e negozi di software
  2.10.2. Elenchi di software consentiti o vietati
  2.10.3. Criteri di aggiornamento
  2.10.4. Privilegi per l'installazione di software

Modulo 3. Sicurezza di rete (perimetro)

3.1. Sistemi di rilevamento e prevenzione delle minacce
  3.1.1. Quadro generale per gli incidenti di sicurezza
  3.1.2. Sistemi di difesa attuali: *Defense in Depth* e SOC
  3.1.3. Le attuali architetture di rete
  3.1.4. Tipi di strumenti di rilevamento e prevenzione degli incidenti
    3.1.4.1. Sistemi basati sulla rete
    3.1.4.2. Sistemi basati su *host*
    3.1.4.3. Sistemi centralizzati
  3.1.5. Comunicazione e rilevamento di istanze/host, container e serverless
3.2. Firewall
  3.2.1. Tipi di Firewall
  3.2.2. Attacchi e contenimento
  3.2.3. Firewalls comuni nel *Kernel* Linux
    3.2.3.1. UFW
    3.2.3.2. *Nftables* e *iptables*
    3.2.3.3. Firewalld
  3.2.4. Sistemi di rilevamento basati sui log di sistema
    3.2.4.1. Wrapper TCP
    3.2.4.2. BlockHosts e DenyHosts
    3.2.4.3. Fai2ban
3.3. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
  3.3.1. Attacchi agli IDS/IPS
  3.3.2. Sistemi IDS/IPS
    3.3.2.1. Snort
    3.3.2.2. Suricata
3.4. Firewall di nuova generazione (NGFW)
  3.4.1. Differenze tra NGFW e Firewall tradizionali
  3.4.2. Funzionalità chiave
  3.4.3. Soluzioni commerciali
  3.4.4. Firewall per servizi *Cloud*
    3.4.4.1. Architettura VPC del cloud
    3.4.4.2. ACL del cloud
    3.4.4.3. Security Group
3.5. *Proxy*
  3.5.1. Tipi di *Proxy*
  3.5.2. Uso di *Proxy*. Vantaggi e svantaggi
3.6. Motori antivirus
  3.6.1. Contesto generale del *Malware* degli IoC
  3.6.2. Problemi del motore antivirus
3.7. Sistemi di protezione della posta
  3.7.1. Antispam
    3.7.1.1. Whitelisting e blacklisting
    3.7.1.2. Filtri bayesiani
  3.7.2. Mail Gateway (MGW)

3.8. SIEM
- 3.8.1. Componenti e architettura
- 3.8.2. Regole di correlazione e casi d'uso
- 3.8.3. Sfide attuali per i sistemi SIEM

3.9. SOAR
- 3.9.1. SOAR e SIEM: nemici o alleati
- 3.9.2. Il futuro dei sistemi SOAR

3.10. Altri sistemi basati sulla rete
- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. HoneyPots e HoneyNets
- 3.10.4. CASB

Modulo 4. Sicurezza degli smartphone

4.1. Il mondo dei dispositivi mobili
- 4.1.1. Tipi di piattaforme mobili
- 4.1.2. Dispositivi IOS
- 4.1.3. Dispositivi Android

4.2. Gestione della sicurezza mobile
- 4.2.1. Progetto OWASP sulla Sicurezza mobile
  - 4.2.1.1. I 10 punti deboli più importanti
- 4.2.2. Comunicazioni, reti e modalità di connessione

4.3. Il dispositivo mobile in ambito aziendale
- 4.3.1. Rischi
- 4.3.2. Politiche di sicurezza
- 4.3.3. Monitoraggio del dispositivo
- 4.3.4. Gestione dei dispositivi mobili (MDM)

4.4. Privacy degli utenti e sicurezza dei dati
- 4.4.1. Stati di informazione
- 4.4.2. Protezione dei dati e riservatezza
  - 4.4.2.1. Permessi
  - 4.4.2.2. Crittografia
- 4.4.3. Archiviazione sicura dei dati
  - 4.4.3.1. Archiviazione sicura su iOS
  - 4.4.3.2. Archiviazione sicura su Android
- 4.4.4. Buone pratiche nello sviluppo di applicazioni

4.5. Punti deboli e vettori di attacco
- 4.5.1. Vulnerabilità
- 4.5.2. Vettori di attacco
  - 4.5.2.1. Malware
  - 4.5.2.2. Infiltrazione di dati
  - 4.5.2.3. Manipolazione dei dati

4.6. Principali minacce
- 4.6.1. Utente non obbligato
- 4.6.2. *Malware*
  - 4.6.2.1. Tipi di *malware*
- 4.6.3. Ingegneria sociale
- 4.6.4. Perdite di dati
- 4.6.5. Furto di informazioni
- 4.6.6. Reti Wifi non sicure
- 4.6.7. Software obsoleto
- 4.6.8. Applicazioni dannose
- 4.6.9. Password insicure
- 4.6.10. Impostazioni di sicurezza deboli o inesistenti
- 4.6.11. Accesso fisico
- 4.6.12. Perdita o furto del dispositivo
- 4.6.13. Furto d'identità (Integrità)
- 4.6.14. Criptografia debole o non funzionante
- 4.6.15. Negazione del servizio (DoS)

4.7. Principali attacchi
- 4.7.1. Attacchi di *phishing*
- 4.7.2. Attacchi legati alle modalità di comunicazione
- 4.7.3. Attacchi di *smishing*
- 4.7.4. Attacchi di *Criptojacking*
- 4.7.5. *Man in the Middle*

4.8. Hacking
- 4.8.1. *Rooting e jailbreaking*
- 4.8.2. Anatomia di un attacco mobile
- 4.8.2.1. Propagazione della minaccia
- 4.8.2.2. Installazione di *Malware* sul dispositivo
- 4.8.2.3. Persistenza
- 4.8.2.4. Esecuzione del *Payload* ed estrazione delle informazioni
- 4.8.3. Hacking sui *dispositivi* iOS: meccanismi e strumenti
- 4.8.4. Hacking sui *dispositivi* Android: meccanismi e strumenti

4.9. Test di intrusione
- 4.9.1.iOS *pentesting*
- 4.9.2. Android *PenTesting*
- 4.9.3. Strumenti

4.10. Sicurezza e protezione
- 4.10.1. Impostazioni di sicurezza
- 4.10.1.1. Su dispositivi iOS
- 4.10.1.2. Dispositivi Android
- 4.10.2. Misure di sicurezza
- 4.10.3. Strumenti di protezione

Modulo 5. Sicurezza in IoT

5.1. Dispositivi
- 5.1.1. Tipi di dispositivi
- 5.1.2. Architetture standardizzate
- 5.1.2.1. ONEM2M
- 5.1.2.2. IoTWF
- 5.1.3. Protocolli di applicazione
- 5.1.4. Tecnologie di connettività

5.2. Dispositivi IoT. Aree di applicazione
- 5.2.1. *SmartHome*
- 5.2.2. *SmartCity*
- 5.2.3. Trasporto
- 5.2.4. *Wearables*
- 5.2.5. Settore sanitario
- 5.2.6. IioT

5.3. Protocolli di comunicazione
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. *SmartHome*
- 5.4.1. Automazione domestica
- 5.4.2. Reti
- 5.4.3. Elettrodomestici
- 5.4.4. Sorveglianza e sicurezza

5.5. *SmartCity*
- 5.5.1. Illuminazione
- 5.5.2. Meteorologia
- 5.5.3. Sicurezza

5.6. Trasporto
- 5.6.1. Localizzazione
- 5.6.2. Effettuare pagamenti e ottenere servizi
- 5.6.3. Connettività

5.7. *Wearables*
- 5.7.1. Abiti intelligenti
- 5.7.2. Gioielli intelligenti
- 5.7.3. Smartwatch

5.8. Settore sanitario
- 5.8.1. Monitoraggio dell'esercizio e della frequenza cardiaca
- 5.8.2. Monitoraggio di pazienti e anziani
- 5.8.3. Impiantabili
- 5.8.4. Robot chirurgici

5.9. Connettività
- 5.9.1. Wi-Fi/Gateway
- 5.9.2. Bluetooth
- 5.9.3. Connettività integrata

5.10. Cartolarizzazione
- 5.10.1. Reti dedicate
- 5.10.2. Gestione password
- 5.10.3. Utilizzo di protocolli criptati
- 5.10.4. Suggerimenti per l'uso

Modulo 6. Hacking etico

6.1. Ambiente di lavoro
- 6.1.1. Distribuzioni Linux
  - 6.1.1.1. Kali Linux - Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Sistemi di virtualizzazione
- 6.1.3. *Sandbox*
- 6.1.4. Distribuzione dei laboratori

6.2. Metodologie
- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. *Footprinting*
- 6.3.1. Intelligence open source (OSINT)
- 6.3.2. Ricerca di violazioni dei dati e punti deboli
- 6.3.3. Utilizzo di strumenti passivi

6.4. Scansione di rete
- 6.4.1. Strumenti di scansione
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Altri strumenti di scansione
- 6.4.2. Tecniche di Scansione
- 6.4.3. Tecniche di elusione di firewall e IDS
- 6.4.4. Banner *grabbing*
- 6.4.5. Diagrammi di rete

6.5. Enumerazione
- 6.5.1. Enumerazione SMTP
- 6.5.2. Enumerazione DNS
- 6.5.3. Enumerazione NetBIOS e Samba
- 6.5.4. Enumerazione LDAP
- 6.5.5. Enumerazione SNMP
- 6.5.6. Altre tecniche di Enumerazione

6.6. Analisi delle vulnerabilità
- 6.6.1. Soluzioni per l'Analisi dei punti deboli
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2 Sistemi di punteggio dei punti deboli
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Attacchi alle reti wireless
- 6.7.1. Metodologia di hacking nelle reti wireless
  - 6.7.1.1. Wi-fi *Discovery*
  - 6.7.1.2. Analisi del traffico
  - 6.7.1.3. Attacchi *aircrack*
    - 6.7.1.3.1. Attacchi WEP
    - 6.7.1.3.2. Attacchi WPA/WPA2
  - 6.7.1.4. Attacchi *Evil Twin*
  - 6.7.1.5. Attacchi WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Strumenti per la sicurezza wireless

6.8. Hacking di server web
- 6.8.1. *Cross Site Scripting*
- 6.8.2. CSRF
- 6.8.3. *Session Hijacking*
- 6.8.4. *SQLinjection*

6.9. Sfruttamento dei punti deboli
- 6.9.1. Utilizzo di *Exploit* noti
- 6.9.2. Utilizzo di *metasploit*
- 6.9.3. Utilizzo di malware
  - 6.9.3.1. Definizione e campo di applicazione
  - 6.9.3.2. Generazione di *Malware*
  - 6.9.3.3. Bypassare le soluzioni antivirus

6.10. Persistenza
- 6.10.1. Installazione di *rootkits*
- 6.10.2. Utilizzo di Ncat
- 6.10.3. Utilizzo di attività pianificate per le *Backdoor*
- 6.10.4. Creazione di utenti
- 6.10.5. Rilevamento HIDS

Modulo 7. Ingegneria inversa

7.1. I compilatori
- 7.1.1. Tipi di codici
- 7.1.2. Fasi di un compilatore
- 7.1.3. Tabella dei simboli
- 7.1.4. Gestione degli errori
- 7.1.5. Compilatore GCC

7.2. Tipi di analisi nei compilatori
- 7.2.1. Analisi lessicale
  - 7.2.1.1. Terminologia
  - 7.2.1.2. Componenti lessicali
  - 7.2.1.3. Analizzatore lessicale LEX
- 7.2.2. Analisi sintattica
  - 7.2.2.1. Grammatiche libere dal contesto
  - 7.2.2.2. Tipi di analisi sintattica
    - 7.2.2.2.1. Analisi top-down
    - 7.2.2.2.2. Analisi bottom-up
  - 7.2.2.3. Alberi sintattici e derivazioni
  - 7.2.2.4. Tipi di analizzatori sintattici
    - 7.2.2.4.1. Analizzatori LR (*Left To Right*)
    - 7.2.2.4.2. Analizzatori LALR
- 7.2.3. Analisi semantica
  - 7.2.3.1. Grammatiche di attributi
  - 7.2.3.2. S-Attributi
  - 7.2.3.3. Attributi a L

7.3. Strutture dati dell'assemblatore

7.3.1. Variabili
7.3.2. Array
7.3.3. Puntatori
7.3.4. Struttura
7.3.5. Obiettivi
7.4. Strutture del codice assembly
7.4.1. Strutture di selezione
7.4.1.1. *If, else if, Else*
7.4.1.2. *Switch*
7.4.2. Strutture di iterazione
7.4.2.1. *For*
7.4.2.2. *While*
7.4.2.3. Uso del *break*
7.4.3. Funzioni
7.5. Architettura Hardware x86
7.5.1. Architettura dei processori x86
7.5.2. Strutture dati x86
7.5.3. Strutture di codice x86
7.5.3. Strutture di codice x86
7.6. Architettura hardware ARM
7.6.1. Architettura dei processori ARM
7.6.2. Strutture dati ARM
7.6.3. Strutture di codice ARM
7.7. Strutture di codice ARM
7.7.1. Disassemblatori
7.7.2. IDA
7.7.3. Ricostruttori di codici
7.8. Analisi dinamica del codice
7.8.1. Analisi del comportamento
7.8.1.1. Comunicazioni
7.8.1.2. Monitoraggio
7.8.2. Debugger di codice Linux
7.8.3. Debugger di codice Windows
7.9. Sandbox
7.9.1. Architettura *sandbox*
7.9.2. Evasione della *sandbox*
7.9.3. Tecniche di rilevamento
7.9.4. Tecniche di evasione
7.9.5. Contromisure
7.9.6. Sandbox su Linux
7.9.7. Sandbox su Windows
7.9.8. Sandbox en MacOS
7.9.9. Sandbox en Android
7.10. Analisi dei *malware*
7.10.1. Metodi di analisi dei *malware*
7.10.2. Tecniche di offuscamento del *malware*
7.10.2.1. Offuscamento degli eseguibili
7.10.2.2. Limitazione degli ambienti di esecuzione
7.10.3. Strumenti di analisi dei *malware*

Modulo 8. Sviluppo sicuro

8.1. Sviluppo sicuro
8.1.1. Qualità, funzionalità e sicurezza
8.1.2. Riservatezza, integrità e disponibilità
8.1.3. Ciclo di vita dello sviluppo del *software*
8.2. Fase dei requisiti
8.2.1. Controllo dell'autenticazione
8.2.2. Controllo dei ruoli e dei privilegi
8.2.3. Requisiti orientati al rischio
8.2.4. Approvazione dei privilegi
8.3. Fasi di analisi e progettazione
8.3.1. Accesso ai componenti e amministrazione del sistema
8.3.2. Tracce di audit
8.3.3. Gestione delle sessioni
8.3.4. Dati storici

8.3.5. Gestione appropriata degli errori
8.3.6. Separazione delle funzioni
8.4. Fase di implementazione e codifica
8.4.1. Protezione dell'ambiente di sviluppo
8.4.2. Preparazione della documentazione tecnica
8.4.3. Codifica sicura
8.4.4. Sicurezza nelle comunicazioni
8.5. Buone pratiche di codifica sicura
8.5.1. Convalida dei dati di ingresso
8.5.2. Codifica dei dati di uscita
8.5.3. Stile di programmazione
8.5.4. Gestione dei log delle modifiche
8.5.5. Pratiche crittografiche
8.5.6. Gestione degli errori e dei log
8.5.7. Gestione degli archivi
8.5.8. Gestione di. Memoria
8.5.9. Standardizzazione e riutilizzo delle funzioni di sicurezza
8.6. Preparazione del server e *hardening*
8.6.1. Gestione di utenti, gruppi e ruoli sul server
8.6.2. Installazione software
8.6.3. *Hardening* del server
8.6.4. Configurazione robusta del contesto di applicazione
8.7. Preparazione della Base di Dati e dell'*hardening*
8.7.1. Ottimizzazione del motore della Base di Dati
8.7.2. Creare un proprio utente per l'applicazione
8.7.3. Assegnazione dei privilegi necessari all'utente
8.7.4. *hardening* della BBDD
8.8. Fase di test
8.8.1. Controllo qualità negli audit di sicurezza
8.8.2. Ispezione del codice per fasi
8.8.3. Verifica della gestione delle configurazioni
8.8.4. Modello black box
8.9. Preparare il Passaggio alla produzione
8.9.1. Eseguire il controllo delle modifiche
8.9.2. Eseguire la procedura di cambio produzione
8.9.3. Eseguire la procedura di *rollback*
8.9.4. Test di pre-produzione
8.10. Fase di manutenzione
8.10.1. Garanzia basata sul rischio
8.10.2. Test di manutenzione della sicurezza white box
8.10.3. Test di manutenzione della sicurezza black box

Modulo 9. Analisi forense

9.1. Acquisizione e riproduzione dei dati
9.1.1. Acquisizione della memoria volatile
9.1.1.1. Informazioni sul sistema
9.1.1.2. Informazioni di rete
9.1.1.3. Ordine di volatilità
9.1.2. Acquisizione dei dati statici
9.1.2.1. Creazione di un'immagine duplicata
9.1.2.2. Preparazione di un documento per la catena di custodia
9.1.3. Metodi di validazione dei dati acquisiti
9.1.3.1. Metodi per Linux
9.1.3.2. Metodi per Windows

9.2. Valutazione e fallimento delle tecniche anti-forensi
- 9.2.1. Obiettivi delle tecniche anti-forensi
- 9.2.2. Cancellazione dei dati
  - 9.2.2.1. Cancellazione di dati e file
  - 9.2.2.2. Recupero dei file
  - 9.2.2.3. Recupero di partizioni eliminate
- 9.2.3. Protezione con password
- 9.2.4. Steganografia
- 9.2.5. Cancellazione sicura del dispositivo
- 9.2.6. Crittografia

9.3. Sistema operativo forense
- 9.3.1. Analisi forense di Windows
- 9.3.2. Analisi forense di Linux
- 9.3.3. Analisi forense di Mac

9.4. Analisi Forense della Rete
- 9.4.1. Analisi dei Log
- 9.4.2. Correlazione dei dati
- 9.4.3. Ricerca di rete
- 9.4.4. Passi da seguire nell'analisi forense della rete

9.5. Analisi forense web
- 9.5.1. Indagine sugli attacchi web
- 9.5.2. Rilevamento degli attacchi
- 9.5.3. Localizzazione degli indirizzi IP

9.6. Analisi forense dei Database
- 9.6.1. Analisi forense in MSSQL
- 9.6.2. Analisi forense in MySQL
- 9.6.3. Analisi forense in PostgreSQL
- 9.6.4. Analisi forense in MongoDB

9.7. Analisi forense nel *Cloud*
- 9.7.1. Tipi di crimini nel Cloud
  - 9.7.1.1. Cloud come soggetto
  - 9.7.1.2. Cloud come oggetto
  - 9.7.1.3. Cloud come strumento
- 9.7.2. Sfide dell'analisi forense nel Cloud
- 9.7.3. Investigazione dei servizi di archiviazione nel Cloud
- 9.7.4. Strumenti di analisi forense per il Cloud

9.8. Investigazione dei crimini informatici via email
- 9.8.1. Sistemi di posta elettronica
  - 9.8.1.1. Client di posta
  - 9.8.1.2. Server di posta
  - 9.8.1.3. Server SMTP
  - 9.8.1.4. Server POP3
  - 9.8.1.5. Server IMAP4
- 9.8.2. Reati di posta elettronica
- 9.8.3. Messaggio di posta elettronica
  - 9.8.3.1. Intestazioni standard
  - 9.8.3.2. Intestazioni estese
- 9.8.4. Fasi dell'indagine su questi reati
- 9.8.5. Strumenti forensi per la posta elettronica

9.9. Analisi forense dei cellulari
- 9.9.1. Reti cellulari
  - 9.9.1.1. Tipi di reti
  - 9.9.1.2. Contenuti del CDR
- 9.9.2. *Subscriber Identity Module* (SIM)
- 9.9.3. Acquisizione logica
- 9.9.4. Acquisizione fisica
- 9.9.5. Acquisizione del file system

9.10. Stesura e presentazione del rapporto forense
- 9.10.1. Aspetti importanti di un rapporto forense
- 9.10.2. Classificazione e tipi di rapporti
- 9.10.3. Guida alla stesura di un rapporto
- 9.10.4. Presentazione del rapporto
  - 9.10.4.1. Preparazione preventiva alla testimonianza
  - 9.10.4.2. Deposizione
  - 9.10.4.3. Rapporti con i media

Modulo 10. Le sfide attuali e future della sicurezza informatica

10.1. Tecnologia blockchain
- 10.1.1. Ambiti di applicazione
- 10.1.2. Garanzia di riservatezza
- 10.1.3. Garanzia di non ripudio

10.2. Moneta digitale
- 10.2.1. I Bitcoin
- 10.2.2. Criptovalute
- 10.2.3. Mining di criptovalute
- 10.2.4. Schemi piramidali
- 10.2.5. Altri potenziali reati e problemi

10.3. *Deepfake*
- 10.3.1. Impatto mediatico
- 10.3.2. Pericoli per la società
- 10.3.3. Meccanismi di rilevamento

10.4. Il futuro dell'intelligenza artificiale
- 10.4.1. Intelligenza artificiale e cognitive computing
- 10.4.2. Utilizzi per semplificare il servizio clienti

10.5. Privacy digitale
- 10.5.1. Valore dei dati in rete
- 10.5.2. Utilizzo dei dati in rete
- 10.5.3. Privacy e gestione dell'identità digitale

10.6. Cyber conflitti, criminalità informatica e attacchi informatici
- 10.6.1. L'impatto della sicurezza informatica sui conflitti internazionali
- 10.6.2. Conseguenze degli attacchi informatici sulla popolazione generale
- 10.6.3. Tipi di criminali informatici. Misure di protezione

10.7. Lavoro da remoto
- 10.7.1. La rivoluzione dello smartworking durante e dopo il Covid19
- 10.7.2. Collo di bottiglia durante l'accesso
- 10.7.3. Variazione della superficie di attacco
- 10.7.4. Necessità dei lavoratori

10.8. Tecnologie *Wireless* emergenti
- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. Onde millimetriche
- 10.8.4. Tendenza di Get Smart anziché *Get more*

10.9. Futuro dell'indirizzamento nelle reti
- 10.9.1. Problemi attuali con l'indirizzamento IP
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Vantaggi di IPv4+ rispetto a IPv4
- 10.9.5. Vantaggi dell'IPv6 rispetto all'IPv4

10.10. La sfida alla prevenzione e alla sensibilizzazione delle persone
- 10.10.1. Le attuali strategie governative
- 10.10.2. Resistenza da parte delle persone all'apprendimento
- 10.10.3. Programmi di aggiornamento che devono essere adottati dalle aziende

Modulo 11. Leadership, Etica e Responsabilità Sociale d'Impresa

11.1. Globalizzazione e Governance
- 11.1.1. Governance e Corporate Governance
- 11.1.2. Fondamenti della Corporate Governance nelle imprese
- 11.1.3. Il Ruolo del Consiglio di Amministrazione nel quadro della Corporate Governance

11.2. Leadership
- 11.2.1. Leadership: Un approccio concettuale
- 11.2.2. Leadership nelle imprese
- 11.2.3. L'importanza del leader nella direzione di imprese

11.3. *Cross Cultural Management*
- 11.3.1. Concetto di *Cross Cultural Management*
- 11.3.2. Contributi alla conoscenza delle culture nazionali
- 11.3.3. Gestione della Diversità

11.4. Sviluppo manageriale e leadership
- 11.4.1. Concetto di Sviluppo Direttivo
- 11.4.2. Concetto di leadership
- 11.4.3. Teorie di leadership
- 11.4.4. Stili di leadership
- 11.4.5. Le sfide del leader nell'attualità

11.5. Etica d'impresa
- 11.5.1. Etica e Morale
- 11.5.2. Etica Aziendale
- 11.5.3. Leadership ed etica nelle imprese

11.6. Sostenibilità
- 11.6.1. Sostenibilità e sviluppo sostenibile
- 11.6.2. Agenda 2030
- 11.6.3. Le imprese sostenibili

11.7. Responsabilità sociale d'impresa
- 11.7.1. Dimensione internazionale della Responsabilità Sociale d'Impresa
- 11.7.2. Implementazione della Responsabilità Sociale d'Impresa
- 11.7.3. Impatto e misurazione della Responsabilità Sociale d'Impresa

11.8. Sistemi e strumenti di Gestione responsabile
- 11.8.1. RSC: Responsabilità sociale corporativa
- 11.8.2. Aspetti essenziali per implementare una strategia di gestione responsabile
- 11.8.3. Le fasi di implementazione di un sistema di gestione della responsabilità sociale d'impresa
- 11.8.4. Strumenti e standard della RSC

11.9. Multinazionali e diritti umani
- 11.9.1. Globalizzazione, imprese multinazionali e diritti umani
- 11.9.2. Imprese multinazionali di fronte al diritto internazionale
- 11.9.3. Strumenti giuridici per le multinazionali in materia di diritti umani

11.10. Ambiente legale e *Corporate Governance*
- 11.10.1. Regolamenti internazionali di importazione ed esportazione
- 11.10.2. Proprietà intellettuale e industriale
- 11.10.3. Diritto internazionale del lavoro

Modulo 12. Direzione del personale e gestione del talento

12.1. Direzione Strategica di persone
- 12.1.1. Direzione strategica e risorse umane
- 12.1.2. Management strategico del personale

12.2. Gestione delle risorse umane basata sulle competenze
- 12.2.1. Analisi del potenziale
- 12.2.2. Politiche di retribuzione
- 12.2.3. Piani di avanzamento di carriera/successione

12.3. Valutazione e gestione delle prestazioni
- 12.3.1. Gestione del rendimento
- 12.3.2. La gestione delle prestazioni: obiettivi e processi

12.4. Innovazione in gestione del talento e del personale
- 12.4.1. Modelli di gestione del talento strategico
- 12.4.2. Identificazione, aggiornamento professionale e sviluppo dei talenti
- 12.4.3. Fedeltà e fidelizzazione
- 12.4.4. Proattività e innovazione

12.5. Motivazione
- 12.5.1. La natura della motivazione
- 12.5.2. Teoria delle aspettative
- 12.5.3. Teoria dei bisogni
- 12.5.4. Motivazione e compensazione economica

12.6. Sviluppo di team ad alte prestazioni
- 12.4.1. Team ad alte prestazioni: team autogestiti
- 12.6.2. Metodologie per la gestione di team autogestiti ad alte prestazioni

12.7. Gestione del cambiamento
- 12.5.1. Gestione del cambiamento
- 12.7.2. Tipo di processi di gestione del cambiamento
- 12.7.3. Tappe o fasi nella gestione del cambiamento

12.8. Negoziazione e gestione dei conflitti
- 12.6.1. Negoziazione
- 12.8.2. Gestione dei Conflitti
- 12.8.3. Gestione delle Crisi

12.9. Comunicazione direttiva
- 12.7.1. Comunicazione interna ed esterna nel settore delle imprese
- 12.9.2. Dipartimento di comunicazione
- 12.9.3. Il responsabile di comunicazione di azienda. Il profilo del Dircom

12.10. Produttività, attrazione, mantenimento e attivazione del talento
- 12.10.1. La produttività
- 12.10.2. Leve di attrazione e ritenzione del talento

Modulo 13. Gestione Economico-Finanziaria

13.1. Contesto Economico
- 13.1.1. Contesto macroeconomico e sistema finanziario nazionale
- 13.1.2. Istituti finanziari
- 13.1.3. Mercati finanziari
- 13.1.4. Attivi finanziari
- 13.1.5. Altri enti del settore finanziario

13.2. Contabilità direttiva
- 13.2.1. Concetti di base
- 13.2.2. L'Attivo aziendale
- 13.2.3. Il Passivo aziendale
- 13.2.4. Il Patrimonio Netto dell'azienda
- 13.2.5. Il Conto Economico

13.3. Sistemi informativi e *business intelligence*
- 13.3.1. Concetto e classificazione
- 13.3.2. Fasi e metodi della ripartizione dei costi
- 13.3.3. Scelta del centro di costi ed effetti

13.4. Bilancio di previsione e controllo di gestione
- 13.4.1. Il modello di bilancio
- 13.4.2. Bilancio di Capitale
- 13.4.3. Bilancio di Gestione
- 13.4.5. Bilancio del Tesoro
- 13.4.6. Controllo del bilancio

13.5. Direzione finanziaria
- 13.5.1. Decisioni finanziarie dell'azienda
- 13.5.2. Dipartimento finanziario
- 13.5.3. Eccedenza di tesoreria
- 13.5.4. Rischi associati alla direzione finanziaria
- 13.5.5. Gestione dei rischi della direzione finanziaria

13.6. Pianificazione finanziaria
- 13.6.1. Definizione della pianificazione finanziaria
- 13.6.2. Azioni da effettuare nella pianificazione finanziaria
- 13.6.3. Creazione e istituzione della strategia aziendale
- 13.6.4. La tabella *Cash Flow*
- 13.6.5. La tabella di flusso

13.7. Strategia Finanziaria d'Impresa
- 13.7.1. Strategia aziendale e fonti di finanziamento
- 13.7.2. Prodotti finanziari di finanziamento aziendale

13.8. Finanziamento strategico
- 13.8.1. Autofinanziamento
- 13.8.2. Aumento dei fondi propri
- 13.8.3. Risorse ibride
- 13.8.4. Finanziamenti tramite intermediari finanziari

13.9. Analisi e pianificazione finanziaria
- 13.9.1. Analisi dello Stato Patrimoniale
- 13.9.2. Analisi del Conto Economico
- 13.9.3. Analisi del Rendimento

13.10. Analisi e risoluzione di casi/problemi
- 13.10.1. Informazioni finanziarie di Industria di Disegno e Tessile, S.A. (INDITEX)

Modulo 14. Direzione Commerciale e Marketing Strategico

14.1. Direzione commerciale
- 14.1.1. Quadro concettuale della Direzione Commerciale
- 14.1.2. Strategia e pianificazione aziendale
- 14.1.3. Il ruolo dei direttori commerciali

14.2. Marketing
- 14.2.1. Concetto di Marketing
- 14.2.2. Elementi base del marketing
- 14.2.3. Attività di marketing aziendale

14.3. Gestione strategica del Marketing
- 14.3.1. Concetto di Marketing strategico
- 14.3.2. Concetto di pianificazione strategica di marketing
- 14.3.3. Fasi del processo di pianificazione strategica di marketing

14.4. Marketing online ed e-commerce
- 14.4.1. Obiettivi di Marketing digitale e e-commerce
- 14.4.2. Marketing digitale e media che utilizzi
- 14.4.3. E-commerce: Contesto generale
- 14.4.4. Categorie dell'e-commerce
- 14.4.5. Vantaggi e svantaggi *dell'E-commerce* rispetto al commercio tradizionale

14.5. Digital Marketing per rafforzare il marchio
- 14.5.1. Strategie online per migliorare la reputazione del tuo marchio
- 14.5.2. *Branded Content* & *Storytelling*

14.6. Digital Marketing per captare e fidelizzare clienti
- 14.6.1. Strategie di fidelizzazione e creazione di un vincolo mediante internet
- 14.6.2. *Visitor Relationship Management*
- 14.6.3. Ipersegmentazione

14.7. Gestione delle campagne digitali
- 14.7.1. Che cos'è una campagna pubblicitaria digitale?
- 14.7.2. Passi per lanciare una campagna di marketing online
- 14.7.3. Errori nelle campagne pubblicitarie digitali

14.8. Strategie di vendita
- 14.8.1. Strategie di vendita
- 14.8.2. Metodi di vendite

14.9. Comunicazione aziendale
- 14.9.1. Concetto
- 14.9.2. Importanza della comunicazione nell'organizzazione
- 14.9.3. Tipo della comunicazione nell'organizzazione
- 14.9.4. Funzioni della comunicazione nell'organizzazione
- 14.9.5. Elementi della comunicazione
- 14.9.6. Problemi di comunicazione
- 14.9.7. Scenari di comunicazione

14.10. Comunicazione e reputazione online
- 14.10.1. La reputazione online
- 14.10.2. Come misurare la reputazione digitale?
- 14.10.3. Strumenti di reputazione online
- 14.10.4. Rapporto sulla reputazione online
- 14.10.5. *Branding* online

Modulo 15. *Management* Direttivo

15.1. General Management
- 15.1.1. Concetto di General Management
- 15.1.2. L'azione del General Management
- 15.1.3. Il direttore generale e le sue funzioni
- 15.1.4. Trasformazione del lavoro della direzione

15.2. Il direttivo e le sue funzioni: La cultura organizzativa e i suoi approcci
- 15.2.1. Il direttivo e le sue funzioni: La cultura organizzativa e i suoi approcci

15.3. Direzione di operazioni
- 15.3.1. Importanza della direzione
- 15.3.2. La catena di valore
- 15.3.3. Gestione della qualità

15.4. Oratoria e preparazione dei portavoce
- 15.4.1. Comunicazione interpersonale
- 15.4.2. Capacità di comunicazione e influenza
- 15.4.3. Barriere nella comunicazione

15.5. Strumenti di comunicazioni personali e organizzative
- 15.5.1. Comunicazione interpersonale
- 15.5.2. Strumenti della comunicazione interpersonale
- 15.5.3. La comunicazione nelle imprese
- 15.5.4. Strumenti nelle imprese

15.6. Comunicazione in situazioni di crisi
- 15.6.1. Crisi
- 15.6.2. Fasi della crisi
- 15.6.3. Messaggi: contenuti e momenti

15.7. Preparazione di un piano di crisi
- 15.7.1. Analisi dei potenziali problemi
- 15.7.2. Pianificazione
- 15.7.3. Adeguatezza del personale

15.8. Intelligenza emotiva
- 15.8.1. Intelligenza emotiva e comunicazione
- 15.8.2. Assertività, empatia e ascolto attivo
- 15.8.3. Autostima e comunicazione emotiva

15.9. *Branding* personale
- 15.9.1. Strategie per sviluppare il brand personale
- 15.9.2. Leggi del branding personale
- 15.9.3. Strumenti per la costruzione di brand personali

15.10. Leadership e gestione di team
- 15.10.1. Leadership e stile di leadership
- 15.10.2. Capacità e sfide del Leader
- 15.10.3. Gestione dei Processi di Cambiamento
- 15.10.4. Gestione di Team Multiculturali

Il tuo futuro inizia qui. Iscriviti oggi e diventa il Chief Information Officer di grandi aziende"

06

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

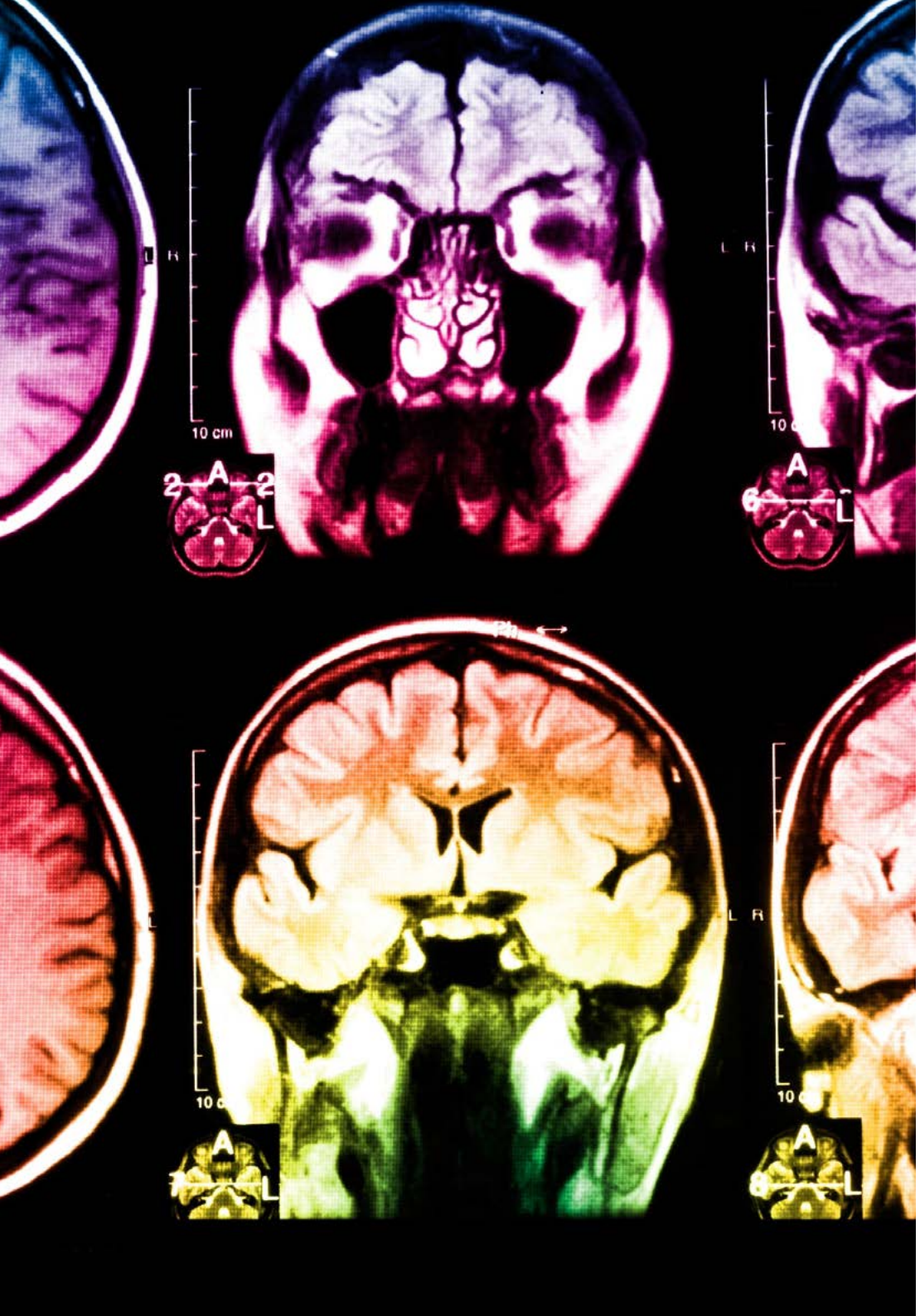
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

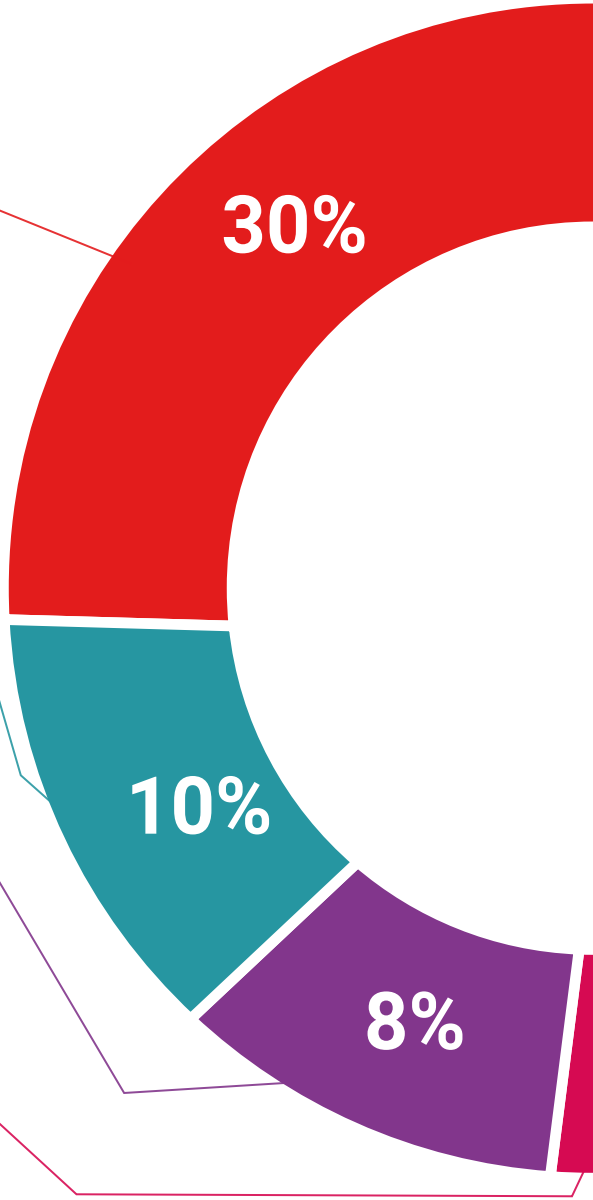
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

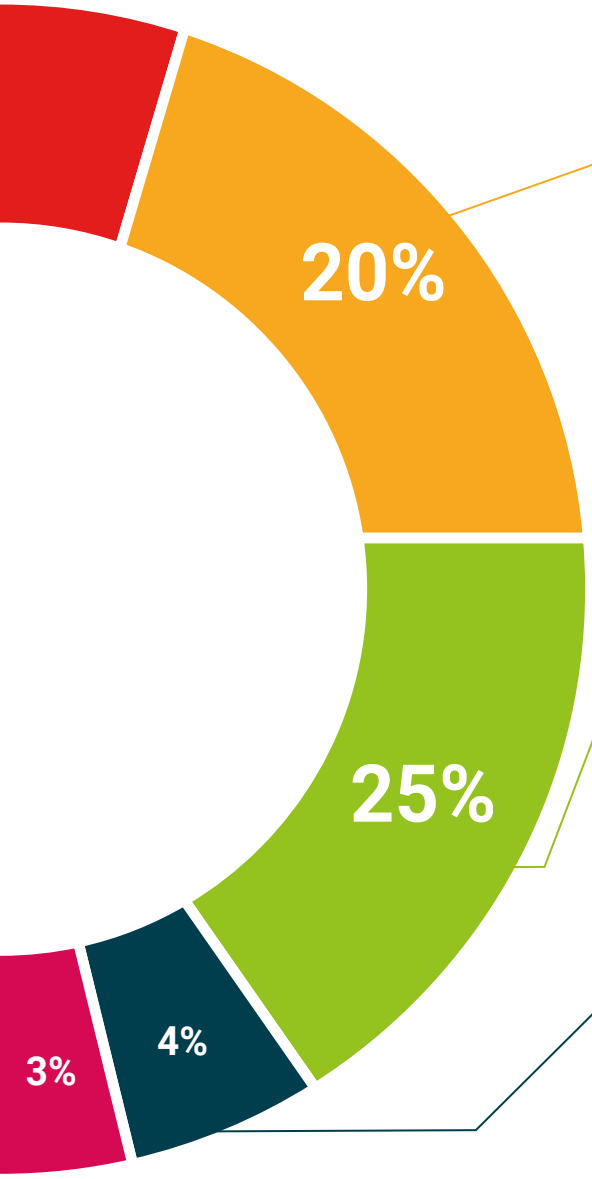
Pratiche di competenze e competenze

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.

07

Titolo

L' MBA in Cybersecurity Management (CISO, Chief Information Security Officer) 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 **MBA in Cybersecurity Management (CISO, Chief Information Security Officer)** 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 **Master Privato** rilasciata da **TECH Università Tecnologica**.

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

Titolo: **Master Privato MBA in Cybersecurity Management (CISO, Chief Information Security Officer)**

Modalità: **online**

Durata: **12 mesi**


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

MASTER PRIVATO

in

MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

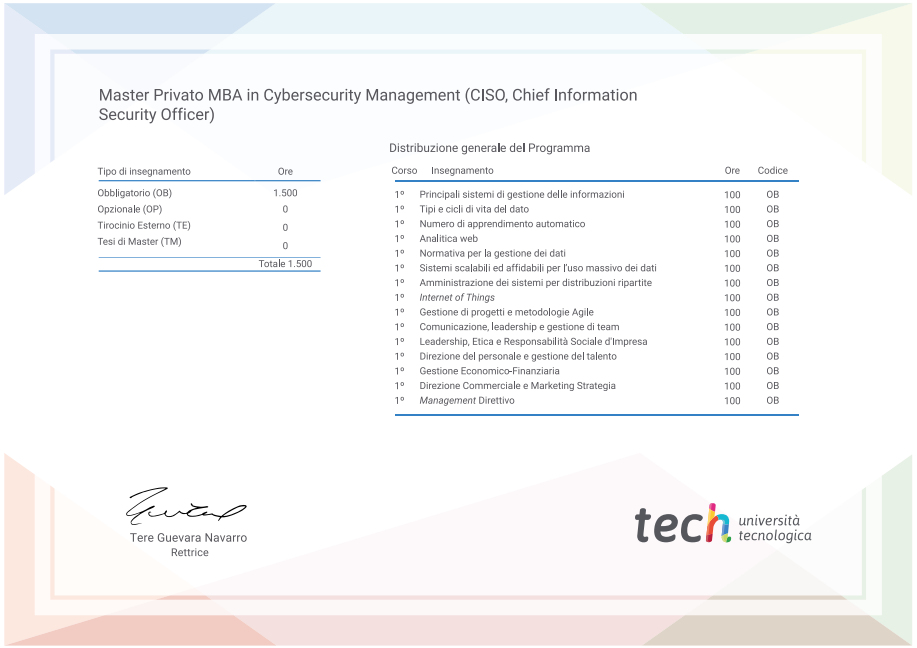
Si tratta di un titolo rilasciato da questa Università ed equivalente a 1.500 ore, con data di inizio gg/mm/aaaa e con data di fine gg/mm/aaaa.

TECH è un Istituto Privato di Istruzione Superiore riconosciuto dal Ministero della Pubblica Istruzione a partire dal 28 giugno 2018.

In data 17 Giugno 2020

Tere Guevara Navarro
Rettrice

codice unico TECH: AFWORD23S techtitute.com/titulos


Master Privato MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

Tipo di insegnamento	Ore
Obbligatorio (OB)	1.500
Opzionale (OP)	0
Tirocinio Esterno (TE)	0
Tesi di Master (TM)	0
	Totale 1.500

Distribuzione generale del Programma

Corso	Insegnamento	Ore	Codice
1º	Principali sistemi di gestione delle informazioni	100	OB
1º	Tipi e cicli di vita del dato	100	OB
1º	Numero di apprendimento automatico	100	OB
1º	Analitica web	100	OB
1º	Normativa per la gestione dei dati	100	OB
1º	Sistemi scalabili ed affidabili per l'uso massivo dei dati	100	OB
1º	Amministrazione dei sistemi per distribuzioni ripartite	100	OB
1º	*Internet of Things*	100	OB
1º	Gestione di progetti e metodologie Agile	100	OB
1º	Comunicazione, leadership e gestione di team	100	OB
1º	Leadership, Etica e Responsabilità Sociale d'Impresa	100	OB
1º	Direzione del personale e gestione del talento	100	OB
1º	Gestione Economico-Finanziaria	100	OB
1º	Direzione Commerciale e Marketing Strategia	100	OB
1º	*Management* Direttivo	100	OB

Tere Guevara Navarro
Rettrice

tech università tecnologica

*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

Master Privato

MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

- Modalità: **online**
- Durata: **12 mesi**
- Titolo: **TECH Università Tecnologica**
- Orario: **a scelta**
- Esami: **online**

Master Privato

MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

tech università tecnologica