Master Privato

MBA in Cybersecurity Management Avanzato (CISO)

tech università tecnologica

tech università tecnologica

Master Privato
MBA in Cybersecurity Management Avanzato (CISO)

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

Accesso al sito web: www.techtitute.com/it/informatica/master/master-mba-cybersecurity-management-avanzato

Indice

01

Presentazione

Il mondo odierno sta avanzando verso la completa digitalizzazione. Sono sempre di più i processi basilari, le operazioni e i compiti di qualsiasi tipo che vengono portati a termine mediante un dispositivo elettronico. Ma questo progresso comporta anche alcuni rischi, poiché computer, *smartphone*, *tablet* e ogni tipo di applicazione digitale possono essere soggetti ad attacchi informatici. È per questo motivo che molte aziende sono alla ricerca di esperti in grado di guidare e gestire efficacemente la cybersecurity dei loro servizi. Questo nuovo profilo professionale è molto richiesto, ecco perché è stato ideato questo programma volto a fornire le conoscenze e le tecniche più innovative al professionista informatico. Lo studente potrà così ricoprire il ruolo di direttore della cybersecurity in qualsiasi azienda.

Questo programma ti preparerà in modo intensivo a specializzarti nella gestione della cybersecurity, la professione più richiesta oggi nel campo dell'IT"

Il processo di digitalizzazione ha subito un'accelerazione negli ultimi anni, impulsato dai continui progressi delle tecnologie dell'informazione. Non è solo la tecnologia ad aver registrato grandi miglioramenti, ma anche gli stessi strumenti digitali con cui vengono svolte numerose attività. Questi sviluppi hanno permesso, ad esempio, di effettuare molte transazioni bancarie da un'applicazione mobile. Ci sono stati sviluppi anche nel settore sanitario, nei sistemi per le prenotazioni delle visite e nell'accesso alle cartelle cliniche. Grazie a queste tecnologie, inoltre, è possibile consultare le fatture o richiedere servizi alle aziende in settori come la telefonia.

Tali progressi hanno però portato anche a un aumento delle vulnerabilità dei computer. Di conseguenza, se da un lato si sono ampliate le possibilità di svolgere varie attività e mansioni, dall'altro sono aumentati di pari passo gli attacchi alla sicurezza dei dispositivi, delle applicazioni e dei siti web. Sempre più aziende sono quindi alla ricerca di professionisti di cybersecurity in grado di fornire loro un'adeguata protezione contro tutti i tipi di attacchi informatici.

Il profilo del Direttore della Cybersecurity è pertanto uno dei più ricercati dalle aziende che operano su Internet o che offrono servizi nell'ambiente digitale. Per rispondere a questa richiesta, TECH ha concepito un MBA in Cybersecurity Management Avanzato (CISO), il quale fornirà all'informatico tutti gli strumenti necessari per svolgere la propria mansione in modo efficace e in considerazione degli ultimi sviluppi in materia di protezione e vulnerabilità tecnologica.

Iscrivendoti a questo programma potrai approfondire aspetti quali la sicurezza nello sviluppo e nella progettazione di sistemi, le migliori tecniche di crittografia e la sicurezza negli ambienti di Cloud Computing. La metodologia 100% online ti consentirà di conciliare il tuo lavoro professionale con gli studi, senza dover sottostare a orari rigidi o doverti spostare per raggiungere un centro accademico. Potrai inoltre usufruire di numerose risorse didattiche multimediali, gestite dal personale docente più prestigioso e specializzato nel settore della cybersecurity.

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

- Sviluppo di casi pratici presentati da esperti in Informatica e Cybersecurity
- I contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni scientifiche e pratiche riguardo alle discipline mediche essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- La sua particolare enfasi sulle metodologie innovative
- Lezioni teoriche, domande all'esperto e/o al tutore, 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

Vieni a scoprire in prima persona le migliori tecniche di sicurezza applicate agli ambienti di Cloud Computing o alla tecnologia Blockchain"

Potrai usufruire di numerosi contenuti multimediali per accelerare il tuo processo di apprendimento, beneficiando al contempo del supporto di un personale docente di grande prestigio nel campo della cybersecurity"

La metodologia online di TECH ti consente di scegliere dove e quando studiare, senza ostacolare le tue esigenze professionali.

Potrai diventare il Direttore della Cybersecurity delle migliori aziende della tua zona.

Il personale docente del programma comprende professionisti del settore, che forniscono agli studenti le proprie esperienze professionali, e rinomati esperti provenienti da società di rilievo e università di prestigio.

I suoi contenuti multimediali, sviluppati con le più recenti tecnologie didattiche, consentiranno al professionista un apprendimento situato e contestuale, cioè un ambiente simulato che fornirà un tirocinio immersivo programmato per allenarsi in situazioni reali.

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

02

Obiettivi

Il rapido sviluppo delle tecnologie informatiche ha apportato grandi progressi, garantendo alla popolazione innumerevoli servizi. Tuttavia, anche il numero di vulnerabilità e di attacchi informatici è aumentato, per cui l'obiettivo principale di questo programma è trasformare l'informatico in un vero specialista nella gestione della sicurezza informatica, garantendogli un enorme e immediato progresso professionale. Grazie alle nuove competenze acquisite, avrai l'opportunità di accedere a grandi aziende che operano nel settore digitale in vari campi.

L'obiettivo di questo programma è quello di fornirti le competenze per diventare un professionista qualificato per dirigere il dipartimento di cybersecurity per una grande azienda"

Obiettivi generali

- Generare conoscenze specialistiche relative a un sistema informatico, ai tipi e agli aspetti della sicurezza da tenere in considerazione
- Identificare le debolezze di un sistema informatico
- Definire la regolamentazione giuridica e la perseguibilità del delitto di attacco informatico
- Valutare diversi modelli di organizzazione della sicurezza per stabilire il modello più appropriato per l'azienda
- Identificare i quadri normativi applicabili e le relative basi normative
- Analizzare la struttura organizzativa e funzionale di un'area di sicurezza informatica (l'ufficio del CISO)
- Analizzare e sviluppare il concetto di rischio e incertezza nel contesto in cui viviamo
- Esaminare il modello di gestione del rischio basato sullo standard ISO 31.000
- Esaminare la scienza della crittologia e il rapporto con le sue aree: crittografia, crittoanalisi, steganografia e stegoanalisi
- Analizzare i tipi di crittografia in base al tipo di algoritmo e al suo utilizzo
- Esaminare i certificati digitali
- Analizzare l'infrastruttura a chiave pubblica (PKI)
- Sviluppare il concetto di gestione dell'identità
- Identificare i metodi di autenticazione
- Generare conoscenze specialistiche sull'ecosistema della sicurezza informatica
- Valutare le conoscenze di cybersecurity
- Identificare le aree di sicurezza nel *Cloud*
- Analizzare i servizi e gli strumenti in ogni ambito di sicurezza
- Sviluppare le specifiche di sicurezza per ogni tecnologia LPWAN
- Paragonare la sicurezza delle tecnologie LPWAN

Questo Master Privato ti consentirà di raggiungere i tuoi obiettivi professionali giacché ti fornisce le conoscenze più avanzate nel campo della cybersecurity"

Obiettivi specifici

Modulo 1. Sicurezza nella progettazione e nello sviluppo dei sistemi

- Valutare la sicurezza di un sistema informatico in tutti i suoi componenti e livelli
- Identificare i tipi di minacce alla sicurezza attualmente esistenti e le loro tendenze
- Stabilire le linee guida per la sicurezza definendo politiche, strategie e piani di sicurezza e contingenza
- Analizzare le strategie e gli strumenti per garantire l'integrità e la sicurezza dei sistemi informatici
- Applicare le tecniche e gli strumenti specifici per ogni tipo di attacco o violazione della sicurezza
- Proteggere le informazioni sensibili memorizzate nel sistema informatico
- Disporre del quadro giuridico e della caratterizzazione del reato, integrando la visione con la tipologia del reo e della sua vittima

Modulo 2. Strutture e modelli per la sicurezza delle informazioni

- Allineare il Master Plan per la sicurezza agli obiettivi strategici dell'organizzazione
- Stabilire un quadro di gestione costante dei rischi come parte integrante del Master Plan sulla sicurezza
- Stabilire gli indicatori appropriati per il monitoraggio della messa in atto del SGSI
- Stabilire una strategia di sicurezza basata sulle policy
- Analizzare gli obiettivi e le procedure associate al piano di sensibilizzazione dei dipendenti, dei fornitori e dei partner
- Identificare, all'interno del quadro normativo, i regolamenti, le certificazioni e le leggi applicabili a ciascuna organizzazione
- Definire gli elementi fondamentali richiesti dallo standard ISO 27001:2013
- Implementare un modello di gestione della privacy in linea con il regolamento europeo GDPR/RGPD

Modulo 3. Gestione della sicurezza IT

- Identificare le diverse componenti che un'area di sicurezza informatica può presentare
- Sviluppare un modello di sicurezza basato su tre linee di difesa
- Presentare i diversi comitati periodici e straordinari in cui è coinvolta l'area della cybersecurity
- Definire gli strumenti tecnologici che integrano le funzioni principali del team operativo di sicurezza (SOC)
- Valutare le misure di controllo dei punti di vulnerabilità appropriate per ogni scenario
- Sviluppare un quadro operativo per la sicurezza basato sul NIST CSF
- Specificare l'ambito dei diversi tipi di verifiche (*Red Team*, *Pentesting*, *Bug Bounty*, ecc.)
- Proporre le attività da svolgere dopo un incidente che coinvolge la sicurezza
- Creare un centro di comando per la sicurezza delle informazioni che comprenda tutti i soggetti interessati (autorità, clienti, fornitori, ecc.)

Modulo 4. Analisi dei rischi e ambiente di sicurezza IT

- Esaminare, secondo una visione globale, l'ambiente in cui si opera
- Identificare i principali rischi e opportunità che possono influire sul raggiungimento degli obiettivi
- Analizzare i rischi sulla base delle migliori procedure a disposizione
- Valutare l'impatto potenziale di tali rischi e opportunità
- Sviluppare tecniche per gestire i rischi e le opportunità in modo da massimizzare la resa economica
- Approfondire le diverse tecniche di trasferimento del rischio e del valore
- Generare valore dalla progettazione di modelli specifici per la gestione agile del rischio
- Esaminare i risultati per proporre miglioramenti nella gestione dei progetti e dei processi fondati su modelli di gestione del rischio o *Risk-Driven*
- Innovare e trasformare i dati generali in informazioni rilevanti per il processo decisionale basato sul rischio

Modulo 5. La crittografia nell'IT

- Completare le operazioni fondamentali (XOR, grandi numeri, sostituzione e trasposizione) e i vari componenti (funzioni One-Way, Hash, generatori di numeri casuali)
- Analizzare le tecniche crittografiche
- Sviluppare i diversi algoritmi crittografici
- Dimostrare l'uso delle firme digitali e la loro applicazione nei certificati digitali
- Valutare i sistemi di gestione delle crittografie e l'importanza della lunghezza delle chiavi crittografiche
- Esaminare gli algoritmi di derivazione delle chiavi crittografiche
- Analizzare il ciclo di vita delle chiavi crittografiche
- Valutare le modalità di cifratura a blocchi e di cifratura a flusso
- Determinare i generatori di numeri pseudorandom
- Sviluppare casi reali di applicazioni crittografiche, come Kerberos, PGP o smart card
- Esaminare associazioni e organismi correlati, come ISO, NIST o NCSC
- Individuare gli ostacoli nella crittografia dell'informatica quantistica

Modulo 6. Gestione dell'identità e degli accessi nella sicurezza informatica

- Sviluppare il concetto di identità digitale
- Valutare il controllo dell'accesso fisico alle informazioni
- Giustificare l'autenticazione biometrica e l'autenticazione MFA
- Valutare gli attacchi legati alla confidenzialità delle informazioni
- Analizzare la federazione di identità
- Stabilire il controllo dell'accesso alla rete

Modulo 7. Sicurezza nelle comunicazioni e nel funzionamento del software
- Sviluppare competenze in materia di sicurezza fisica e logica
- Dimostrare la conoscenza delle comunicazioni e delle reti
- Identificare i principali attacchi dannosi
- Stabilire un quadro di sviluppo sicuro
- Dimostrare di conoscere le principali normative sui sistemi di gestione della sicurezza informatica
- Stabilire il funzionamento di un centro operativo per la cybersecurity
- Dimostrare l'importanza delle pratiche di sicurezza informatica per i disastri organizzativi

Modulo 8. Sicurezza negli ambienti Cloud
- Identificare i rischi di installazione di un'infrastruttura di *Cloud* pubblico
- Definire i requisiti di sicurezza
- Sviluppo di un piano di sicurezza per l'implementazione del *Cloud*
- Identificare i servizi *Cloud* da implementare per la realizzazione di un piano di sicurezza
- Determinare le misure operative necessarie per i meccanismi di prevenzione
- Stabilire le Linee Guida per un sistema di *Logging* e monitoraggio
- Proporre azioni di risposta agli incidenti

Modulo 9. Sicurezza delle comunicazioni nei dispositivi IoT
- Introdurre l'architettura IoT semplificata
- Spiegare le differenze tra le tecnologie di connettività generaliste e le tecnologie di connettività per l'IoT
- Stabilire il concetto di triangolo di ferro della connettività IoT
- Analizzare le specifiche di sicurezza della tecnologia LoRaWAN, NB-IoT e WiSUN
- Motivare la scelta della giusta tecnologia IoT per ogni progetto

Modulo 10. Piano di continuità operativa associato alla sicurezza
- Presentare gli elementi chiave di ciascuna fase e analizzare le caratteristiche del piano di continuità operativa (BCP)
- Giustificare la necessità di un piano di continuità operativa
- Stabilire le mappe di successo e di rischio per ogni fase del piano di continuità operativa
- Specificare come viene stabilito un piano d'azione per la realizzazione del BCP
- Valutare la completezza di un piano di continuità operativa (BCP)
- Sviluppare l'implementazione di un Piano di continuità operativa

Modulo 11. Leadership, Etica e Responsabilità Sociale d'Impresa
- Analizzare l'impatto della globalizzazione sul governo societario e sulla corporate governance
- 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 ambienti aziendali diversi
- Sviluppare le capacità di leadership e comprendere le attuali sfide che i leader devono affrontare
- Identificare 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 imprese

Modulo 12. Management del personale e gestione del talento
- Determinare la relazione tra direzione strategica e gestione delle risorse umane
- Approfondire le competenze necessarie per una gestione efficace delle risorse umane in base alle competenze
- Approfondire le metodologie di valutazione e gestione della performance
- Integrare le innovazioni nella gestione dei talenti e il loro impatto sulla fidelizzazione del personale
- Sviluppare strategie per la motivazione e lo sviluppo del team ad alte prestazioni
- Proporre soluzioni efficaci per la gestione del cambiamento e della risoluzione di conflitti nelle organizzazioni

Modulo 13. Direzione Economico-Finanziaria

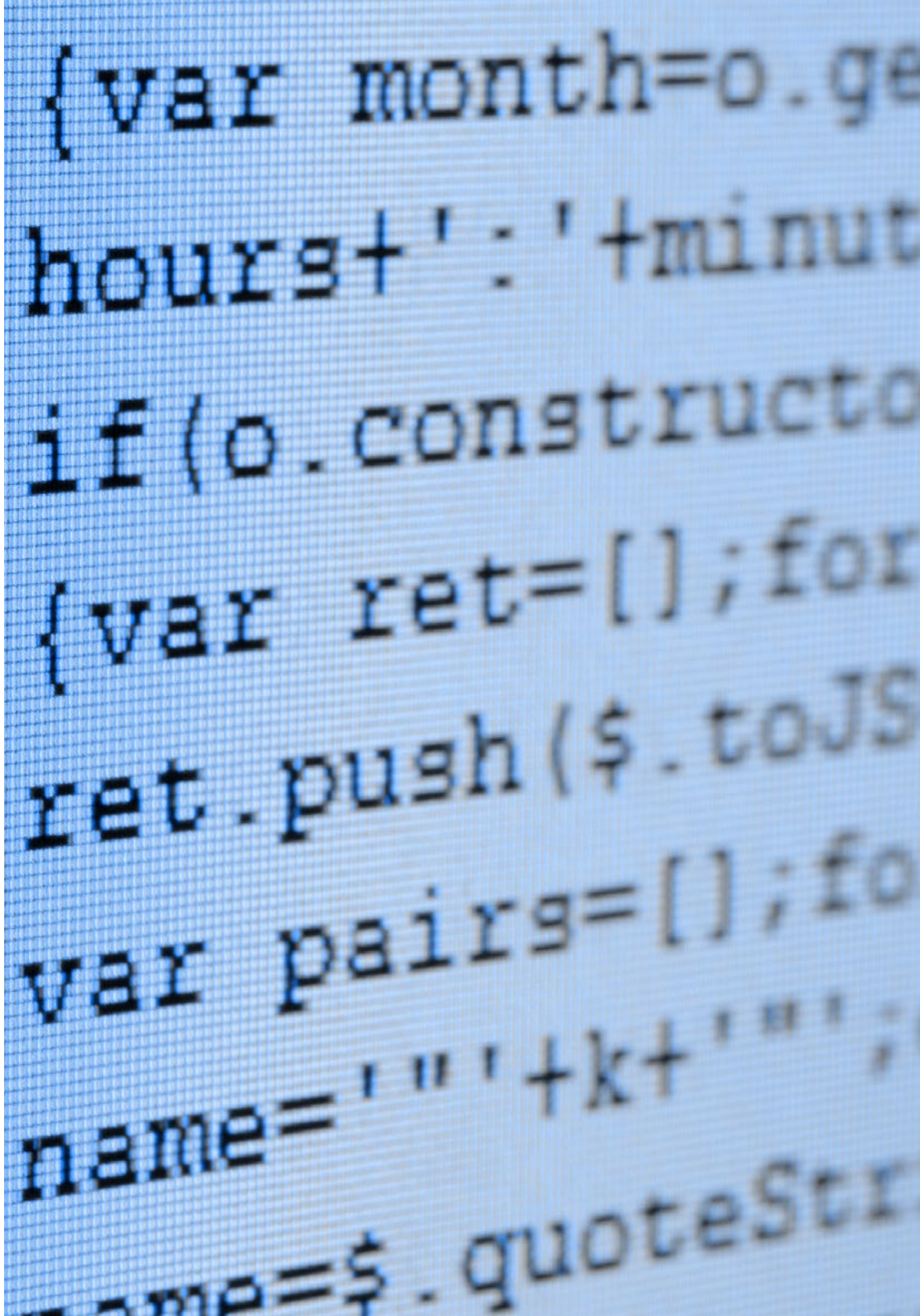
- Analizzare il contesto macroeconomico e la sua influenza sul sistema finanziario internazionale
- Definire i sistemi informativi e la Business Intelligence per le decisioni finanziarie
- Differenziare le decisioni finanziarie chiave e la gestione del rischio nella direzione finanziaria
- Valutare le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

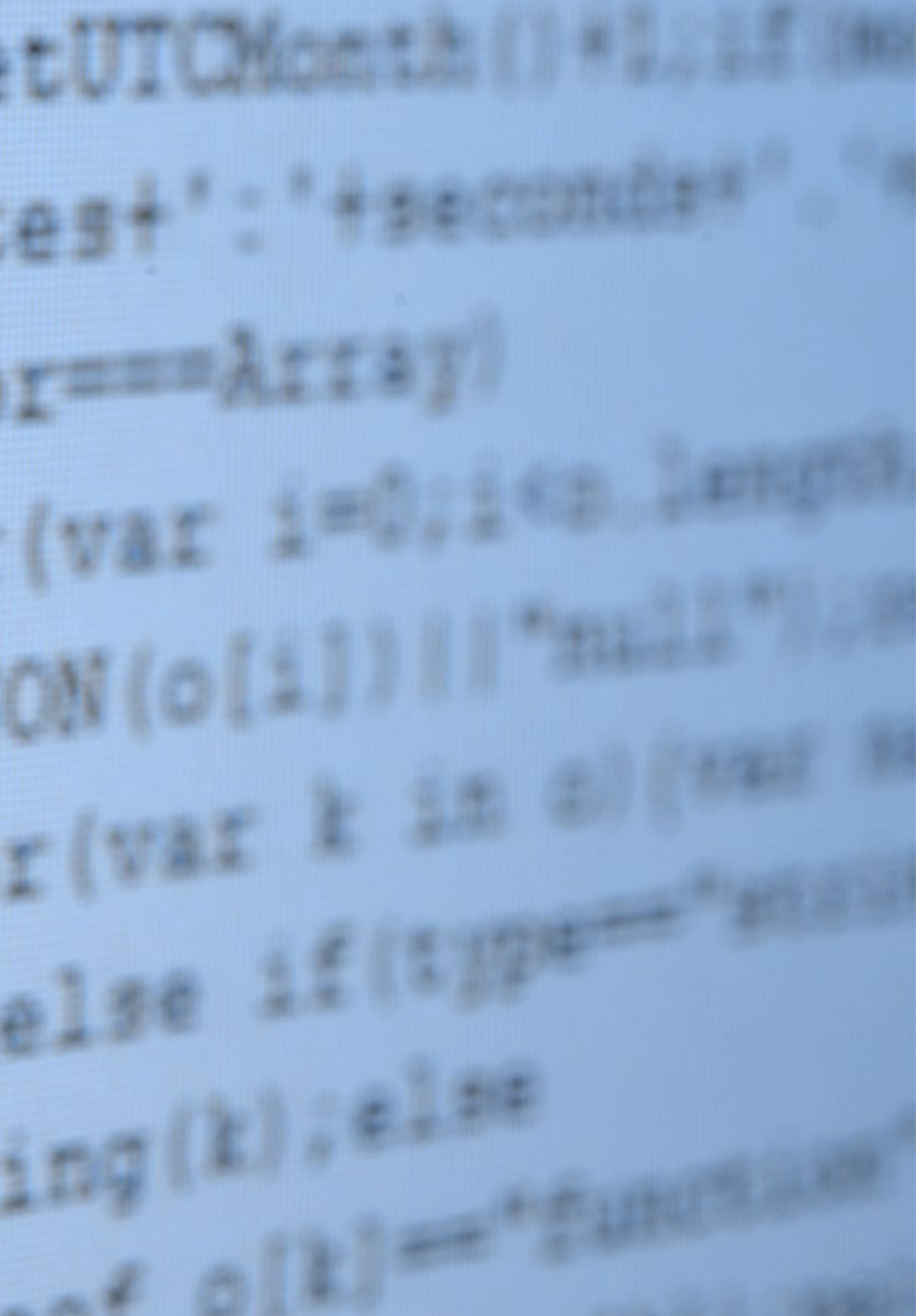
Modulo 14. Direzione Commerciale e Marketing Strategico

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

Modulo 15. Executive *Management*

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





Questo Master Privato ti consentirà di raggiungere i tuoi obiettivi professionali giacché ti fornisce le conoscenze più avanzate nel campo della cybersecurity"

03

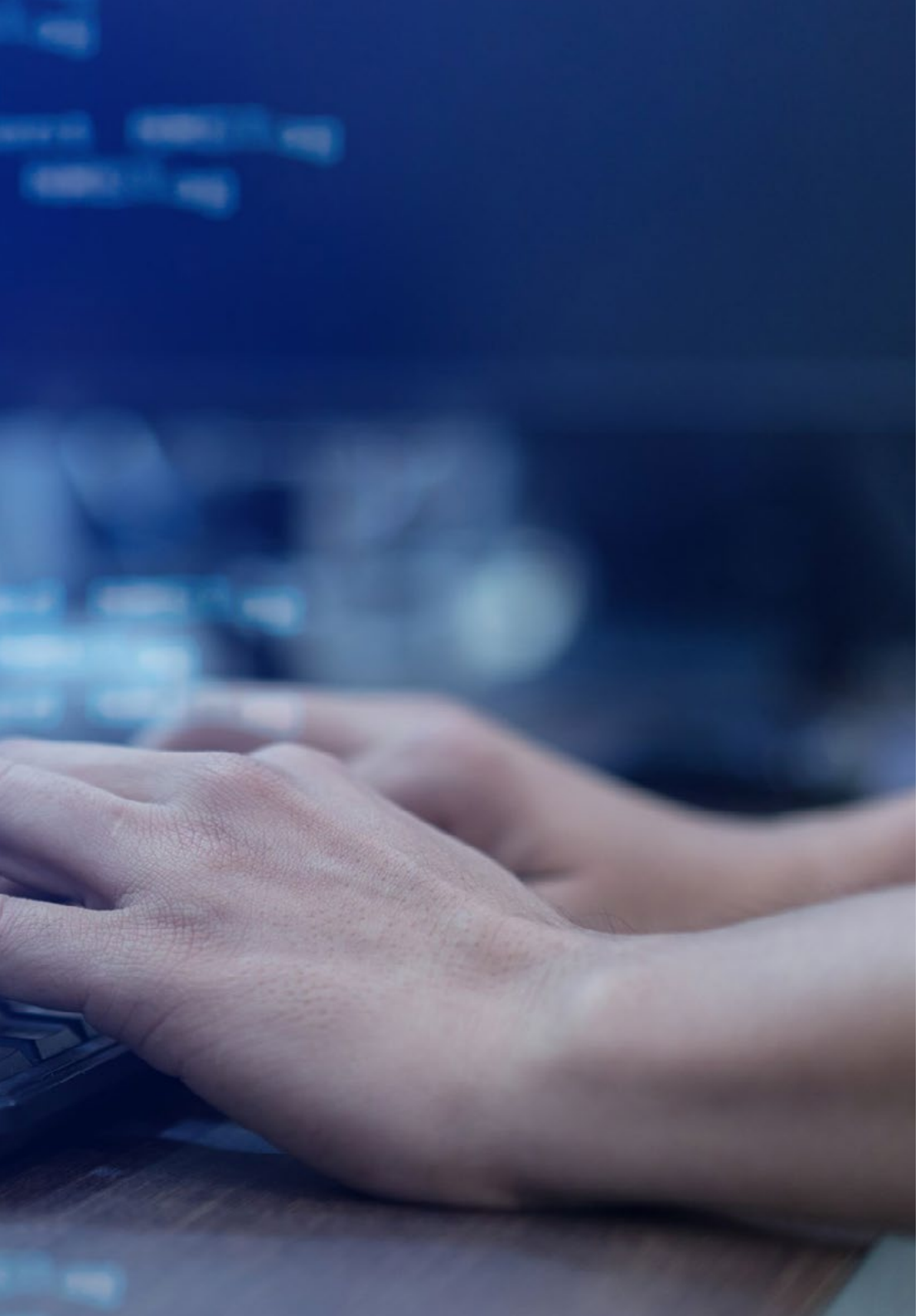
Competenze

Grazie a questo Master Privato, il professionista acquisirà molteplici nuove competenze nel campo della cybersecurity. L'emergere negli ultimi anni di tecnologie come il *Blockchain*, il *Cloud Computing* o l'intelligenza artificiale ha portato allo sviluppo di nuove aree di cybersecurity. Il presente programma è stato concepito appositamente per offrire ai professionisti tutte le competenze necessarie affinché possano adattarsi alle tecnologie in espansione.

Le competenze che questo programma ti fornirà permetterà di aggiornarti e adattarti al nuovo ambiente informatico, dove tecnologie come la Blockchain e l'intelligenza artificiale hanno fatto irruzione"

Competenze generali

- Applicare le misure di sicurezza più appropriate in base alle minacce
- Determinare la politica e il piano di sicurezza del sistema informatico di un'azienda, ultimando la progettazione e l'implementazione del piano di contingenza
- Stabilire un programma di verifica che soddisfi le esigenze di autovalutazione della sicurezza informatica all'interno dell'organizzazione
- Sviluppare un programma di analisi e monitoraggio dei punti di vulnerabilità e un piano di risposta agli incidenti di cybersecurity
- Massimizzare le opportunità che si presentano ed eliminare l'esposizione a tutti i rischi potenziali derivanti dalla progettazione stessa
- Redigere sistemi di gestione delle chiavi
- Valutare la sicurezza informatica di un'azienda
- Analizzare i sistemi di accesso alle informazioni
- Definire le migliori pratiche per uno sviluppo sicuro
- Presentare i rischi che le aziende corrono se non dispongono di un ambiente di sicurezza informatica



Competenze specifiche

- Sviluppare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
- Identificare gli elementi chiave che compongono un SGSI
- Applicare la metodologia MAGERIT per perfezionare il modello e progredire ulteriormente
- Progettare nuove metodologie di gestione del rischio basate sul concetto di *agile Risk Management*
- Identificare, analizzare, valutare e gestire i rischi che il professionista deve affrontare da una nuova prospettiva aziendale basata su un modello *Risk-Driven* che permette non solo di sopravvivere nel proprio ambiente professionale, ma anche di apportare valore
- Esaminare il processo di progettazione di una strategia di sicurezza per l'implementazione in azienda di servizi *Cloud*
- Valutare le differenze nelle implementazioni concrete dei diversi fornitori di *Cloud* pubblico
- Valutare le opzioni di connettività IoT per realizzare un progetto, con particolare attenzione alle tecnologie LPWAN
- Presentare le specifiche di base delle principali tecnologie LPWAN per l'IoT

04

Direzione del corso

La complessità della cybersecurity contemporanea richiede un processo di apprendimento approfondito e dettagliato. È per questo motivo che TECH ha deciso di riunire i migliori docenti specializzati in questo campo. Il professionista potrà così avvalersi del supporto e della supervisione di un personale docente preparato sugli ultimi progressi del settore. Questo gli permetterà di integrare le migliori tecniche di cybersecurity nel suo lavoro quotidiano, acquisendo allo stesso tempo le competenze manageriali necessarie in questo ambito.

Avrai a disposizione veri e propri specialisti di cybersecurity. È questa l'opportunità che stavi cercando"

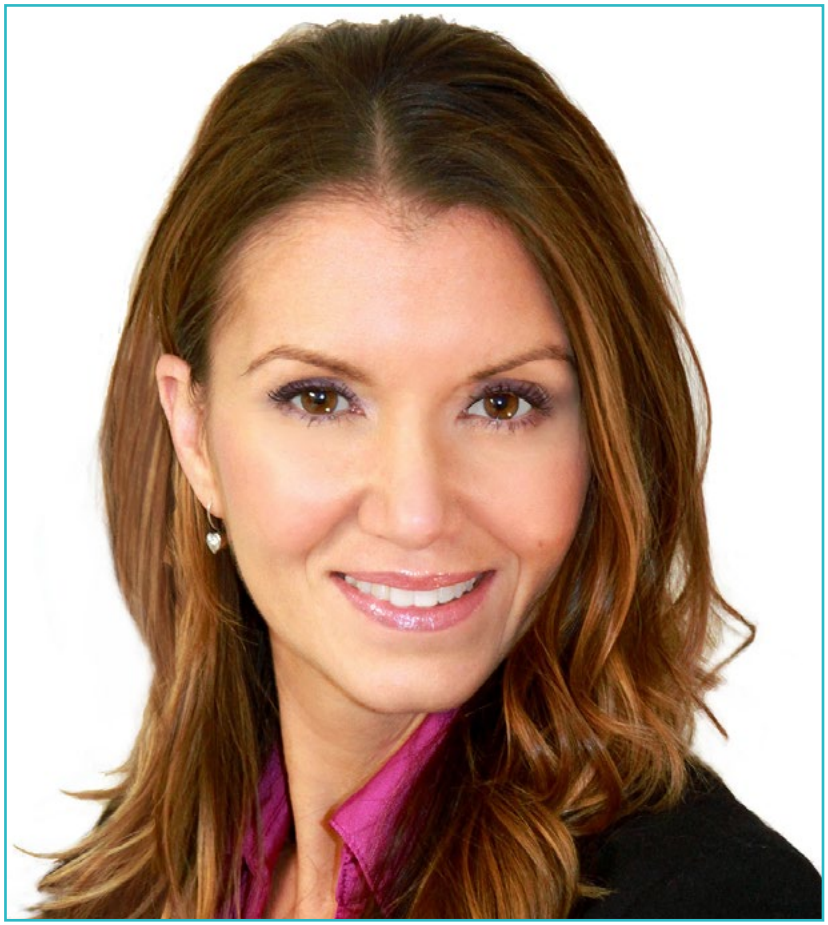
Direttrice Ospite Internazionale

Con oltre 20 anni di esperienza nella progettazione e gestione di team globali di acquisizione di talenti, Jennifer Dove è esperta in reclutamento e strategia tecnologica. Nel corso della sua carriera ha ricoperto posizioni dirigenziali in varie organizzazioni etecnologia all'interno delle aziende Fortune 50, come NBCUniversal e Comcast. Il suo percorso gli ha permesso di eccellere in ambienti competitivi e ad alta crescita.

In qualità di Vicepresidentessa di Acquisizione del Talento, supervisiona la strategia e l'esecuzione dell'onboarding dei talenti, collaborando con i leader aziendali e i responsabili delle risorse umane per raggiungere gli obiettivi operativi e strategici di assunzione. In particolare, mira a 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 in tutto il mondo. Si occupa anche di amplificare il marchio del datore di lavoro e la proposta di valore di Mastercard attraverso post, eventi e social network.

Jennifer Dove ha dimostrato il suo impegno per lo sviluppo professionale continuo, partecipando attivamente alle reti di professionisti delle Risorse Umane e contribuendo all'inserimento di numerosi dipendenti in diverse aziende. Dopo aver conseguito la laurea in Comunicazione organizzativa presso l'Università di Miami, ha ricoperto posizioni manageriali di selezione del personale in aziende di varie aree.

Inoltre, 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 alle sfide future. Ha anche implementato con successo programmi di benessere sul lavoro che hanno aumentato significativamente la soddisfazione e la fidelizzazione dei dipendenti.



Dott.ssa Dove, Jennifer

- Vice Presidentessa per l'acquisizione di talenti alla Mastercard di New York, Stati Uniti
- Direttrice per l'Acquisizione di Talenti presso NBCUniversal Media, Stati Uniti
- Responsabile della Selezione del Personale Comcast
- Responsabile della Selezione del Personale presso Rite Hire Advisory
- Vicepresidentessa esecutiva della Divisione Vendite presso Ardor NY Real Estate
- Responsabile della Selezione del Personale presso Valerie August & Associates
- Account Executive presso BNC
- Account Executive presso Vault
- Laurea in Comunicazione Organizzativa presso l'Università di Miami

Grazie a TECH potrai apprendere con i migliori professionisti del mondo"

Direttore Ospite Internazionale

Leader tecnologico con decenni di esperienza in importanti aziende tecnologiche multinazionali, Rick Gauthier si è sviluppato in modo significativo nel campo dei servizi cloud e del miglioramento dei processi end-to-end. È stato riconosciuto come un team leader e un manager molto efficiente, che dimostra un talento naturale nel garantire un alto livello di impegno tra i suoi dipendenti.

Ha un dono innato per la strategia e l'innovazione esecutiva, sviluppando nuove idee e supportandone il successo con dati di qualità. La sua carriera in Amazon gli ha permesso di gestire e integrare i servizi IT dell'azienda negli Stati Uniti. In Microsoft ha guidato un team di 104 persone, responsabile della fornitura dell'infrastruttura IT a livello aziendale e del supporto ai reparti di ingegneria dei prodotti in tutta l'azienda.

Questa esperienza gli ha permesso di distinguersi come manager di grande impatto, con notevoli capacità di aumentare l'efficienza, la produttività e la soddisfazione generale dei clienti.

Dott. Gauthier, Rick

- Direttore regionale di IT presso Amazon, Seattle, USA
- Responsabile di programma senior presso Amazon
- Vicepresidente di Wimmer Solutions
- Direttore senior dei servizi di ingegneria della produttività di Microsoft
- Laurea in Cybersecurity presso la Western Governors University
- Certificato tecnico in immersione commerciale rilasciato dal Divers Institute of Technology
- Titolo in Studi Ambientali presso l'Evergreen State College

Cogli l'occasione per conoscere gli ultimi sviluppi in materia e applicali alla tua pratica quotidiana"

Direttore Ospite Internazionale

Romi Arman è un esperto di fama internazionale con più di due decenni di esperienza nella trasformazione digitale, nel marketing, nella strategia e nella consulenza. Nel corso della sua lunga carriera, ha corso molti rischi ed è un costante sostenitore dell'innovazione e del cambiamento nell'ambiente aziendale. Grazie a questa esperienza, ha lavorato con amministratori delegati e organizzazioni aziendali di tutto il mondo, spingendoli ad abbandonare i modelli di business tradizionali. Ha aiutato aziende come Shell Energy a diventare veri leader di mercato, concentrandosi sui clienti e sul mondo digitale.

Le strategie ideate da Arman hanno un impatto latente, in quanto hanno permesso a diverse aziende di migliorare l'esperienza di consumatori, personale e azionisti. Il successo di questo esperto è quantificabile attraverso metriche tangibili come il CSAT, il coinvolgimento dei dipendenti nelle istituzioni in cui ha lavorato e la crescita dell'indicatore finanziario EBITDA in ciascuna di esse.

Ha inoltre coltivato e guidato team ad alte prestazioni che sono stati persino premiati per il loro potenziale di trasformazione. Con Shell in particolare, l'esecutivo si è sempre prefissato di superare tre sfide: soddisfare le complesse richieste di decarbonizzazione dei clienti, sostenere una "decarbonizzazione efficace dal punto di vista dei costi" e rivedere un panorama di dati, digitale e tecnologico frammentato. I loro sforzi hanno quindi dimostrato che, per ottenere un successo sostenibile, è essenziale partire dalle esigenze dei consumatori e porre le basi per la trasformazione di processi, dati, tecnologia e cultura.

D'altra parte, il dirigente si distingue per la sua padronanza delle applicazioni aziendali dell'intelligenza artificiale, materia in cui ha conseguito un diploma post-laurea presso la London Business School. Allo stesso tempo, ha accumulato esperienza nell'IoT e in Salesforce.

Dott. Arman, Romi

- Direttore della Trasformazione Digitale (CDO) presso Shell Energy Corp. Shell Energy Corporation, Londra, Regno Unito
- Responsabile globale del commercio elettronico e dell'assistenza clienti presso Shell Energy Corporation
- National Key Account Manager (OEM e rivenditori di autoveicoli) per Shell a Kuala Lumpur, Malesia
- Consulente di gestione senior (settore servizi finanziari) per Accenture da Singapore
- Laurea presso l'Università di Leeds
- Corso post-laurea in Applicazioni Aziendali dell'IA per Dirigenti di Alto Livello Scuola aziendale di Londra
- Certificazione Professionale in Esperienza del cliente CCXP
- Corso in Trasformazione Digitale presso IMD

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

Direttore Ospite Internazionale

Manuel Arens è un professionista esperto nella gestione dei dati e leader di un team altamente qualificato. Infatti, Arens ricopre la posizione di responsabile degli acquisti globali nella divisione Technical Infrastructure and Data Centre di Google, dove ha trascorso la maggior parte della sua carriera. Con sede a Mountain View, in California, ha fornito soluzioni alle sfide operative del gigante tecnologico, come l'integrità dei dati anagrafici, gli aggiornamenti dei dati dei fornitori e la prioritizzazione dei dati dei fornitori. Ha guidato la pianificazione della catena di approvvigionamento dei centri dati e la valutazione del rischio dei fornitori, portando a miglioramenti dei processi e alla gestione dei flussi di lavoro con significativi risparmi sui costi.

Con oltre un decennio di lavoro nella fornitura di soluzioni digitali e di leadership per aziende di diversi settori, ha una vasta esperienza in tutti gli aspetti della fornitura di soluzioni strategiche, tra cui marketing, media analytics, misurazione e attribuzione. Per il suo lavoro ha ricevuto diversi riconoscimenti, tra cui il BIM Leadership Award, il Search Leadership Award, l'Export Lead Generation Programme Award e l'EMEA Best Sales Model Award.

Arens è stato anche responsabile delle vendite a Dublino, in Irlanda. In questo ruolo, ha costruito un team da 4 a 14 membri in tre anni e ha portato il team di vendita a raggiungere risultati e a collaborare bene tra loro e con team interfunzionali. Ha inoltre ricoperto il ruolo di Senior Industry Analyst ad Amburgo, Germania, creando storyline per oltre 150 clienti e utilizzando strumenti interni e di terzi a supporto dell'analisi. Ha sviluppato e scritto relazioni approfondite per dimostrare la padronanza della materia, compresa la comprensione dei fattori macroeconomici e politico-normativi che influenzano l'adozione e la diffusione della tecnologia.

Ha inoltre guidato team di aziende come Eaton, Airbus e Siemens, dove ha acquisito una preziosa esperienza nella gestione dei clienti e della supply chain. È particolarmente noto per il suo lavoro volto a superare continuamente le aspettative costruendo relazioni preziose con i clienti e lavorando senza problemi con le persone a tutti i livelli di un'organizzazione, compresi gli stakeholder, il management, 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 di spicco nel suo campo.

Dott. Arens, Manuel

- Responsabile Acquisti Globali presso Google, Mountain View, USA
- Senior Manager, B2B Analytics and Technology, Google, USA
- Direttore Vendite di Google, Irlanda
- Analista di settore senior presso Google, Germania
- Responsabile account Google, Irlanda
- Accounts Payable presso Eaton, Regno Unito
- Responsabile della Catena di Approvvigionamento presso Airbus, Germania

Scegli TECH! Potrai accedere ai migliori materiali didattici, all'avanguardia della tecnologia e della formazione, realizzati da specialisti del settore di fama internazionale"

Direttore Ospite Internazionale

Andrea La Sala è un esperto dirigente di marketing i cui progetti hanno avuto un impatto significativo sull'ambiente della moda. Nel corso della sua carriera di successo ha sviluppato una varietà di compiti legati al prodotto, al merchandising e alla comunicazione. Tutto questo, legato a marchi prestigiosi come Giorgio Armani, Dolce&Gabbana, Calvin Klein, tra gli altri.

I risultati di questo manager internazionale di alto profilo sono legati alla sua comprovata capacità di sintetizzare le informazioni in quadri chiari e di eseguire azioni concrete allineate a specifici obiettivi aziendali. Inoltre, è riconosciuto per la sua proattività e la sua capacità di adattamento a ritmi veloci. A tutto ciò, questo esperto aggiunge una forte consapevolezza commerciale, visione del mercato e una vera passione per i prodotti.

Come Global Brand and Merchandising Director di Giorgio Armani, ha supervisionato diverse strategie di marketing per l'abbigliamento e gli accessori Inoltre, le sue tattiche si sono concentrate sulla vendita al dettaglio e sulle esigenze e i comportamenti dei consumatori. La Sala è stata anche responsabile della commercializzazione dei prodotti in diversi mercati, agendo come team leader nei reparti Design, Comunicazione e Vendite.

D'altra parte, in aziende come Calvin Klein o Gruppo Coin, ha intrapreso progetti per potenziare la struttura, lo sviluppo e il marketing di diverse collezioni. Allo stesso tempo, si è occupato della creazione di calendari efficaci per le campagne di acquisto e vendita.
È stato inoltre responsabile delle condizioni, dei costi, dei processi e dei tempi di consegna di diverse operazioni.

Queste esperienze hanno fatto di Andrea La Sala uno dei più importanti e qualificati leader aziendali nel settore della moda e del lusso. Un'elevata capacità manageriale con la quale è stato in grado di implementare efficacemente il posizionamento positivo di diversi marchi e di ridefinire i loro KPI.

Dott. La Sala, Andrea

- Responsabile globale del marchio e del merchandising Armani Exchange presso Giorgio Armani, Milano, Italia
- Direttore del Merchandising e Calvin Klein
- Responsabile del marchio presso il Gruppo Coin
- Brand Manager in Dolce&Gabbana
- Brand Manager in Sergio Tacchini S.p.A.
- Analista di mercato in Fastweb
- Laurea in Economia e Business presso l'Università degli Studi del Piemonte Orientale

I professionisti più qualificati ed esperti a livello internazionale ti aspettano in TECH per offrirti un insegnamento di alto livello, aggiornato e basato sulle ultime prove scientifiche. Cosa aspetti a 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. È noto anche per la sua lungimiranza nell'individuare le tecnologie emergenti che, a lungo termine, avranno un impatto duraturo sull'ambiente aziendale.

D'altra parte, l'esecutivo è considerato un pioniere nell'uso di tecniche di visualizzazione dei dati che hanno semplificato insiemi complessi, rendendoli accessibili e facilitando il processo decisionale. Questa competenza è diventata il pilastro del suo profilo professionale, trasformandolo in una risorsa desiderata da molte organizzazioni impegnate a raccogliere informazioni e a generare azioni concrete sulla base di esse.

Uno dei suoi progetti più importanti degli ultimi anni è stata la piattaforma Walmart Data Cafe, la più grande al mondo nel suo genere, basata sul cloud per l'analisi dei Big Data. Ha anche ricoperto il ruolo di Direttore della Business Intelligence presso Red Bull, occupandosi di aree quali vendite, distribuzione, marketing e operazioni di supply chain. Il suo team è stato recentemente premiato per la costante innovazione nell'uso della nuova API Walmart Luminate per gli insight su shopper e canali.

Per quanto riguarda la sua formazione, il dirigente vanta diversi master e studi post-laurea presso centri prestigiosi come l'Università di Berkeley, negli Stati Uniti, e l'Università di Copenhagen, in Danimarca. Grazie a questo continuo aggiornamento, l'esperto ha raggiunto competenze all'avanguardia. Per questo motivo, è stato considerato un leader nato della nuova economia globale, incentrata sulla spinta dei dati e sulle loro infinite possibilità.

Dott. Gram, Mick

- Direttore di Business Intelligence e Analytics presso Red Bull, Los Angeles, Stati Uniti
- Architetto di soluzioni di business intelligence per Walmart Data Cafè
- Consulente indipendente di Business Intelligence e Data Science
- Direttore della Business Intelligence presso Capgemini
- Analista senior presso Nordea
- Consulente senior di business intelligence per SAS
- Executive Education in IA e Machine Learning presso UC Berkeley College of Engineering
- Executive MBA in e-commerce presso l'Università di Copenhagen
- 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 esperto distinto nel settore del Marketing Digitale che, per oltre 19 anni, è stato collegato con una delle più potenti aziende del settore dello spettacolo, 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 network, 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.*

Inoltre, ha conseguito una Laurea in Telecomunicazioni presso l'Università della Florida e un Master in Scrittura Creativa presso l'Università della California, a dimostrazione delle sue capacità comunicative e narrative. **Inoltre, ha partecipato alla School of Professional Development dell'Università di Harvard a programmi all'avanguardia sull'uso dell'**Intelligenza Artificiale nel **business. Il suo profilo professionale è quindi uno dei più rilevanti nell'attuale settore del** Marketing e dei **Media Digitali.**

Dott. Stevenson, Scott

- Direttore del Marketing Digitale di Warner Bros. Discovery 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 al mondo! Gli insegnanti di questo MBA ti guideranno durante l'intero processo di apprendimento"

Direttore Ospite Internazionale

Il Dott. Eric Nyquist è un professionista di spicco nel campo dello sport internazionale, che ha costruito una carriera impressionante, distinguendosi per la sua leadership strategica e la sua capacità di guidare il cambiamento e l'innovazione nelle organizzazioni sportive di alto 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 dott. 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 presso NASCAR, Florida, Stati Uniti
- Vicepresidente senior dello sviluppo strategico presso NASCAR
- Vicepresidente della Pianificazione Strategica presso NASCAR
- Direttore Generale degli Affari Commerciali presso NASCAR
- Vicepresidente Esecutivo del Franchising Chicago White Sox
- Vicepresidente Esecutivo del Franchising Chicago Bulls
- Responsabile della Pianificazione Aziendale nella National Football League (NFL)
- Affari commerciali/Stagista legale presso la Federcalcio degli Stati Uniti
- Dottorato in Giurisprudenza presso l'Università di Chicago
- Master in Business Administration-MBA presso la Booth School of Business presso l'Università di Chicago
- Laurea in Economia Internazionale presso il Carleton College

Grazie a questo titolo universitario in modalità 100% online, potrai conciliare gli studi con i tuoi impegni quotidiani, con l'aiuto dei maggiori esperti internazionali nel settore di tuo interesse. Iscriviti ora!"

Direzione

Dott. Olalla Bonal, Martín

- Responsabile Senior della Pratica Blockchain presso EY
- Specialista Tecnico Blockchain Client presso IBM
- Direttore dell'Architettura di Blocknitive
- Coordinatore del Team per i Database Distribuiti Non-Relazionali per wedoIT, filiale presso IBM
- Architetto di Infrastrutture presso Bankia
- Responsabile del Dipartimento di Layout di T-Systems
- Coordinatore del Dipartimento per Bing Data España SL

Personale docente

Dott. Nogales Ávila, Javier

- Enterprise Cloud and sourcing senior consultant. Quint
- Cloud and Technology Consultant. Indra
- Associate Technology Consultant. Accenture
- Laureato presso l'Università di Jaen e University of Technology and Economics of Budapest (BME)
- Laurea in Ingegneria dell'Organizzazione Industriale

Dott. Rodrigo Estébanez, Juan Manuel

- Co-fondatore di Ismet Tech
- Responsabile della Sicurezza delle Informazioni presso Ecix Group
- *Operational Security Officer* presso Atos IT Solutions and Services A/S
- Docente di Gestione della sicurezza informatica negli studi universitari
- Laureato in Ingegneria presso l'Università di Valladolid
- Master in Sistemi di Gestione Integrata presso l'Università CEU San Pablo

Personale docente

Dott. Gómez Rodríguez, Antonio

- Ingegnere Principale di Soluzioni Cloud per Oracle
- Co-organizzatore del Malaga Developer Meetup
- Consulente Specializzato presso Sopra Group e Everis
- Leader dei team presso System Dynamics
- Sviluppatore software presso SGO Software
- Master in E-Business presso la Business School di La Salle
- Studi post-laurea sulle Tecnologie e i Sistemi Informatici svolti presso l'Istituto Catalano di Tecnologia
- Laurea in Ingegneria delle Telecomunicazioni presso l'Università Politecnica della Catalogna

Dott. Del Valle Arias, Jorge

- Smart City Solutions & Software Business Development Manager España. Itron, Inc Consultor IoT
- Direttore Business. TCOMET
- Responsabile della Business Unit IoT, Industria 4.0. Diode España
- Area Sales Manager per IoT e Telecomunicazioni. Aicox Soluciones
- Chief Technical Officer (CTO) e Business Development Manager. Consulente TELYC
- Fondatore e CEO di Sensor Intelligence
- Responsabile delle Operazioni e dei Progetti. Codio
- Direttore Operativo di Codium Networks
- Ingegnere capo di progettazione hardware e firmware. AITEMIN
- Responsabile regionale della pianificazione e ottimizzazione RF - Rete LMDS 3,5 GHz. Clearwire
- Ingegnere delle Telecomunicazioni presso l'Università Politecnica di Madrid
- Executive MBA presso la Scuola Internazionale di La Salle di Madrid
- Master in Energie Rinnovabili. CEPYME

Dott. Gonzalo Alonso, Félix

- Direttore Generale e Fondatore di Smart REM Solutions
- Socio Fondatore e Responsabile dell'Ingegneria dei Rischi e dell'Innovazione. Dynargy
- Direttore Generale e Socio Fondatore. Risknova (Ufficio specializzato in Tecnologia)
- Laurea in Ingegneria dell'Organizzazione Industriale presso l'Universidad Pontificia de Comillas ICAI
- Laurea in Ingegneria tecnica industriale con specializzazione in Elettronica industriale presso l'Universidad Pontificia de Comillas ICAI
- Master in Gestione delle Assicurazioni presso ICEA (Istituto per la Collaborazione tra le Imprese di Assicurazione)

Dott. Entrenas, Alejandro

- Responsabile di Progetto in Cibersicurezza. Entelgy Innotec Security
- Consulente di Cibersicurezza. Entelgy
- Analista di Sicurezza dell'Informazione. Innovery España
- Analista in Sicurezza dell'Informazione. Atos
- Laurea in Ingegneria Tecnica dei Sistemi Informatici presso l'Università di Cordoba
- Master in Gestione e Amministrazione della Sicurezza Informatica presso l'Università Politecnica di Madrid
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

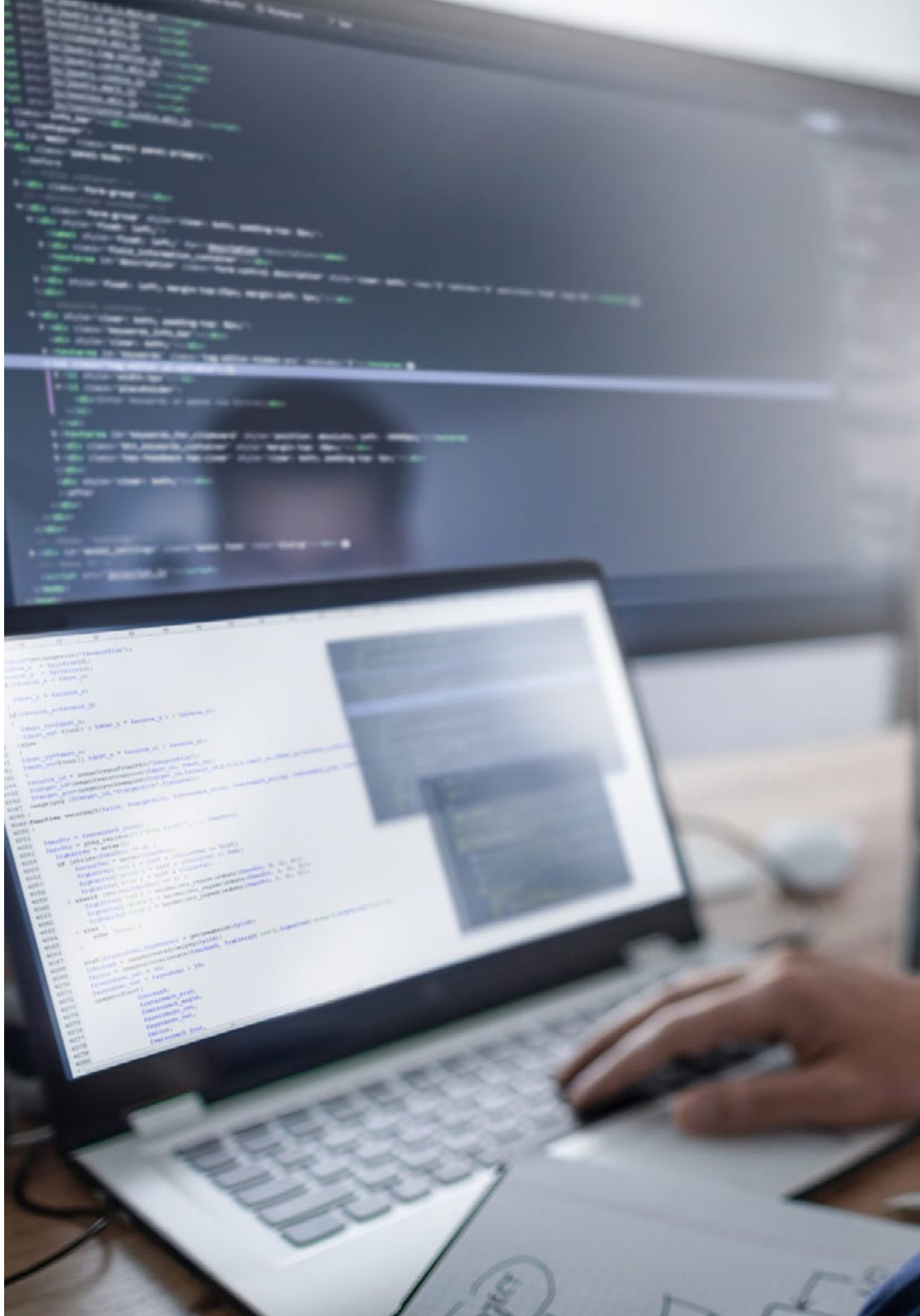
- Sviluppatore delle Applicazioni presso l'Università Politecnica di Madrid
- Laurea in Ingegneria Informatica presso l'Università Alfonso X El Sabio
- Ingegnere tecnico in gestione informatica presso l'Università Politecnica di Madrid Certified Data Privacy Solutions Engineer (CDPSE) presso ISACA

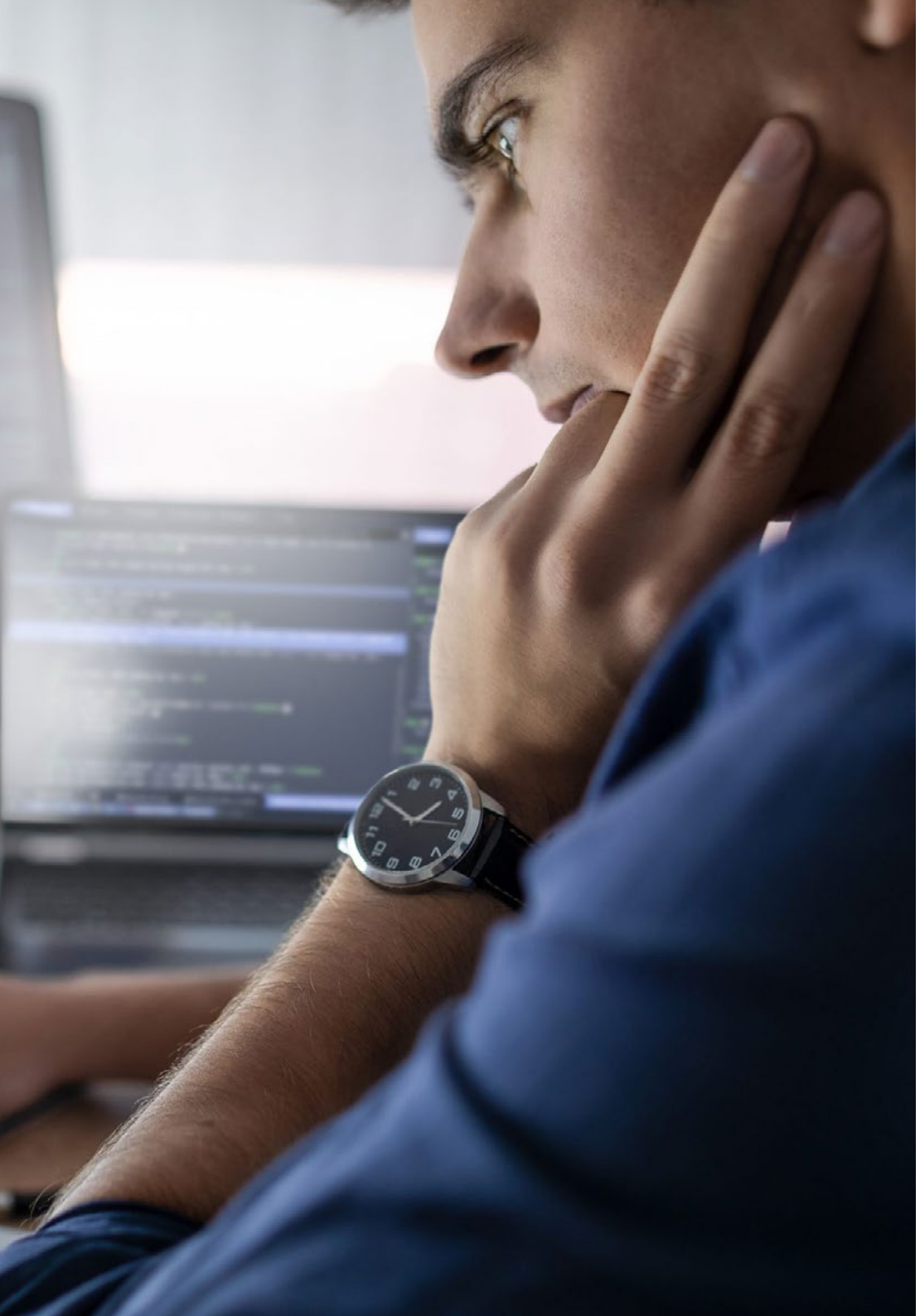
Dott. Ortega, Octavio

- Specialista in Marketing e Sviluppo Web
- Programmatore di Applicazioni Informatiche e Sviluppatore Web *Freelance*
- *Chief Operating* Officer presso Smallsquid SL
- Amministratore e-commerce di Ortega y Serrano
- Docente nei corsi del Certificato Professionale di Informatica e Comunicazioni
- Docente di corsi per la Sicurezza Informatica
- Laurea in Psicologia presso l'Università Aperta di Catalogna
- Tecnico Superiore Universitario in Analisi, Progettazione e Soluzioni di *Software*
- Tecnico Superiore Universitario in Programmazione Avanzata

Dott. Embid Ruiz, Mario

- Avvocato Esperto in ICT e Protezione dei Dati presso Martínez-Echevarría Abogados
- Responsabile legale presso Branddocs SL
- Analista del Rischio del Segmento Pymes di BBVA
- Docente in studi universitari post-laurea relativi al Diritto
- Laurea in Giurisprudenza presso l'Università Rey Juan Carlos
- Laurea in Amministrazione e Direzione Aziendale conseguita presso l'Università Rey Juan Carlos
- Master in Nuove Tecnologie, Internet e Diritto dell'Audiovisivo presso il Centro di Studi Universitari Villanueva





Dott. Gozalo Fernández, Juan Luis

- Responsabile dei Prodotti Blockchain per Open Canarias
- Direttore Blockchain DevOps presso Alastria
- Direttore della Tecnologia a Livello di Servizio presso Santander Spagna
- Responsabile per lo Sviluppo dell'Applicazione Mobile di Tinkerlink presso Cronos Telecom
- Direttore della Tecnologia di Gestione dei Servizi IT presso Barclays Bank Spagna
- Laurea in Ingegneria Informatica presso l'UNED
- Specializzazione in *Deep Learning* presso DeepLearning.ai

Dott.ssa Jurado Jabonero, Lorena

- Responsabile della Sicurezza Informatica (CISO) presso Grupo Pascual
- Cybersecurity Manager presso KPMG. Spagna
- Consulente per il controllo e la gestione di progetti di processi e infrastrutture IT presso Bankia
- Ingegnere degli Strumenti operativi presso Dalkia
- Sviluppatore presso il Grupo Banco Popular

05

Struttura e contenuti

Questo MBA in Cybersecurity Management Avanzato (CISO) è strutturato in 10 moduli specialistici che permetteranno al professionista di approfondire aspetti come l'identificazione digitale, i sistemi per il controllo degli accessi, l'architettura della sicurezza informatica, la struttura dell'area della sicurezza, i sistemi di gestione della sicurezza informatica in ambito di comunicazioni e software, lo sviluppo del piano di continuità operativa associato alla sicurezza. Ciò consentirà all'informatico di acquisire una comprensione completa di tutte le questioni rilevanti riguardanti lo stato attuale della cybersecurity.

Nessun programma di specializzazione in Cybersecurity Management avanzato include contenuti più completi e innovativi di quelli offerti da TECH"

Modulo 1. Sicurezza nella progettazione e nello sviluppo dei sistemi

1.1. Sistemi di informazione
- 1.1.1. Settori di un sistema di informazione
- 1.1.2. Componenti di un sistema di informazione
- 1.1.3. Attività di un sistema di informazione
- 1.1.4. Ciclo di vita di un sistema di informazione
- 1.1.5. Risorse di un sistema di informazione

1.2. Sistemi di informazione. Tipologia
- 1.2.1. Tipi di sistemi di informazione
  - 1.2.1.1. Aziendali
  - 1.2.1.2. Strategici
  - 1.2.1.3. In base all'ambito di applicazione
  - 1.2.1.4. Specifici
- 1.2.2. Sistemi di Informazione. Esempi reali
- 1.2.3. Evoluzione dei sistemi di informazione: le fasi
- 1.2.4. Metodologie dei sistemi di informazione

1.3. Sicurezza dei sistemi di informazione. Implicazioni giuridiche
- 1.3.1. Accesso ai dati
- 1.3.2. Minacce alla sicurezza: vulnerabilità
- 1.3.3. Implicazioni giuridiche: reati penali
- 1.3.4. Procedure per la manutenzione di un sistema di informazione

1.4. Sicurezza di un sistema di informazione. Protocolli di sicurezza
- 1.4.1. Sicurezza di un sistema di informazione
  - 1.4.1.1. Integrità
  - 1.4.1.2. Riservatezza
  - 1.4.1.3. Disponibilità
  - 1.4.1.4. Autenticazione
- 1.4.2. Servizi di sicurezza
- 1.4.3. Protocolli di sicurezza delle informazioni Tipologia
- 1.4.4. Sensibilità di un sistema informativo

1.5. Sicurezza in un sistema informativo. Misure e sistemi di controllo degli accessi
- 1.5.1. Misure di sicurezza
- 1.5.2. Tipo di misure di sicurezza
  - 1.5.2.1. Prevenzione
  - 1.5.2.2. Screening
  - 1.5.2.3. Correzione
- 1.5.3. Sistema di controllo degli accessi. Tipologia
- 1.5.4. Crittografia

1.6. Sicurezza di rete e Internet
- 1.6.1. Firewall
- 1.6.2. Identificazione digitale
- 1.6.3. Virus e worm
- 1.6.4. *Hacking*
- 1.6.5. Esempi e casi reali

1.7. Crimini informatici
- 1.7.1. Reato informatico
- 1.7.2. Reati informatici. Tipologia
- 1.7.3. Reato Informatico. Attacco. Tipologie
- 1.7.4. Il caso della realtà virtuale
- 1.7.5. Profili degli colpevoli e delle vittime. Penalizzazione del reato
- 1.7.6. Reati informatici. Esempi e casi reali

1.8. Piano di sicurezza in un sistema informatico
- 1.8.1. Piano di sicurezza. Obiettivi
- 1.8.2. Piano di sicurezza. Pianificazione
- 1.8.3. Piano di rischio. Analisi
- 1.8.4. Politica di sicurezza. Implementazione nell'organizzazione
- 1.8.5. Piano di sicurezza. Implementazione nell'organizzazione
- 1.8.6. Procedure di sicurezza. Tipologie
- 1.8.7. Piani di sicurezza. Esempi

1.9. Piano di contingenza
- 1.9.1. Piano di contingenza. Funzioni
- 1.9.2. Piano di emergenza: Elementi e obiettivi
- 1.9.3. Piani di contingenza all'interno dell'organizzazione. Implementazione
- 1.9.4. Piano di contingenza. Esempi

1.10. Governance della sicurezza dei sistemi informatici
- 1.10.1. Normativa legale
- 1.10.2. Standard
- 1.10.3. Certificazioni
- 1.10.4. Tecnologie

Modulo 2. Strutture e modelli per la sicurezza delle informazioni

2.1. Struttura di sicurezza delle informazioni
- 2.1.1. ISMS/PDS
- 2.1.2. Allineamento strategico
- 2.1.3. Gestione del rischio
- 2.1.4. Misurazione della performance

2.2. Modelli di sicurezza delle informazioni
- 2.2.1. In base alle politiche di sicurezza
- 2.2.2. In base agli strumenti di protezione
- 2.2.3. In base alle apparecchiature di lavoro

2.3. Modello di sicurezza. Componenti chiave
- 2.3.1. Identificazione dei rischi
- 2.3.2. Definizione dei controlli
- 2.3.3. Valutazione continua dei livelli di rischio
- 2.3.4. Piano di sensibilizzazione per dipendenti, fornitori, partner, ecc.

2.4. Processo di gestione dei rischi
- 2.4.1. Identificazione delle risorse
- 2.4.2. Identificazione delle minacce
- 2.4.3. Valutazione dei rischi
- 2.4.4. Priorità dei controlli
- 2.4.5. Rivalutazione e rischio residuo

2.5. Processi operativi e sicurezza delle informazioni
- 2.5.1. Processi aziendali
- 2.5.2. Valutazione del rischio in base ai parametri aziendali
- 2.5.3. Analisi dell'impatto aziendale
- 2.5.4. Operazioni aziendali e sicurezza delle informazioni

2.6. Processo di miglioramento continuo
- 2.6.1. Il ciclo di Deming
  - 2.6.1.1. Pianificare
  - 2.6.1.2. Fare
  - 2.6.1.3. Verificare
  - 2.6.1.4. Agire

2.7. Architetture di sicurezza
- 2.7.1. Selezione e omogeneizzazione delle tecnologie
- 2.7.2. Gestione dell'identità. Autenticazione
- 2.7.3. Gestione degli accessi. Autorizzazione
- 2.7.4. Sicurezza dell'infrastruttura di rete
- 2.7.5. Tecnologie e soluzioni di crittografia
- 2.7.6. Sicurezza delle apparecchiature terminali (EDR)

2.8. Quadro normativo
- 2.8.1. Regolamenti settoriali
- 2.8.2. Certificazioni
- 2.8.3. Legislazione

2.9. Standard ISO 27001
- 2.9.1. Implementazione
- 2.9.2. Certificazione
- 2.9.3. Verifiche e penetration test
- 2.9.4. Gestione continua del rischio
- 2.9.5. Classificazione delle informazioni

2.10. Legislazione sulla privacy. RGPD (GDPR)
- 2.10.1. Ambito di applicazione del Regolamento generale sulla protezione dei dati (RGPD)
- 2.10.2. Dati personali
- 2.10.3. Ruoli nel trattamento dei dati personali
- 2.10.4. Diritti ARCO
- 2.10.5. Il DPO. Funzioni

Modulo 3. Gestione della sicurezza IT

3.1. Gestione della sicurezza
- 3.1.1. Operazioni di sicurezza
- 3.1.2. Aspetti giuridici e normativi
- 3.1.3. Abilitazione all'esercizio dell'attività
- 3.1.4. Gestione dei rischi
- 3.1.5. Gestione dell'identità e degli accessi

3.2. Struttura dell'area di sicurezza. L'ufficio del CISO
- 3.2.1. Struttura organizzativa. Posizione del CISO nella struttura
- 3.2.2. Linee di difesa
- 3.2.3. Organigramma dell'ufficio del CISO
- 3.2.4. Gestione del bilancio

3.3. Governance della sicurezza
- 3.3.1. Comitato per la sicurezza
- 3.3.2. Comitato per il monitoraggio dei rischi
- 3.3.3. Comitato per il controllo
- 3.3.4. Comitato per le crisi

3.4. Governance della sicurezza. Funzioni
- 3.4.1. Politiche e standard
- 3.4.2. Piano generale di sicurezza
- 3.4.3. Quadro di controllo
- 3.4.4. Sensibilizzazione e corsi di aggiornamento
- 3.4.5. Sicurezza della catena di approvvigionamento

3.5. Operazioni di sicurezza
- 3.5.1. Gestione dell'identità e degli accessi
- 3.5.2. Configurazione delle regole di sicurezza della rete. *Firewall*
- 3.5.3. Gestione di piattaforme IDS/IPS
- 3.5.4. Analisi dei punti deboli

3.6. Quadro di riferimento per la cybersecurity. NIST CSF
- 3.6.1. Metodologia NIST
  - 3.6.1.1. Identificare
  - 3.6.1.2. Proteggere
  - 3.6.1.3. Rilevare
  - 3.6.1.4. Rispondere
  - 3.6.1.5. Recuperare

3.7. Centro Operativo di Sicurezza (SOC). Funzioni
- 3.7.1. Protezione. *Red Team, pentesting, threat intelligence*
- 3.7.2. Rilevamento. SIEM, *user behavior analytics, fraud prevention*
- 3.7.3. Risposta

3.8. Audit di sicurezza
- 3.8.1. Penetration test
- 3.8.2. Esercizi di *red team*
- 3.8.3. Verifiche del codice sorgente. Sviluppo sicuro
- 3.8.4. Sicurezza dei componenti (*software supply chain*)
- 3.8.5. Analisi forense

3.9. Risposta agli incidenti
- 3.9.1. Preparazione
- 3.9.2. Rilevamento, analisi e reporting
- 3.9.3. Contenimento, eliminazione e recupero
- 3.9.4. Attività in seguito all'incidente
  - 3.9.4.1. Conservazione delle prove
  - 3.9.4.2. Analisi forense
  - 3.9.4.3. Gestire una violazione dei dati
- 3.9.5. Guide ufficiali per la gestione degli incidenti informatici

3.10. Gestione delle vulnerabilità
- 3.10.1. Analisi dei punti deboli
- 3.10.2. Valutazione della vulnerabilità
- 3.10.3. Base di sistema
- 3.10.4. Vulnerabilità 0-day. *Zero-day*

Modulo 4. Analisi dei rischi e ambiente di sicurezza IT

4.1. Analisi del contesto
- 4.1.1. Analisi della situazione economica
  - 4.1.1.1. Ambienti VUCA
    - 4.1.1.1.1. Volatilità
    - 4.1.1.1.2. Incertezza
    - 4.1.1.1.3. Complessità
    - 4.1.1.1.4. Ambiguità
  - 4.1.1.2. Ambienti BANI
    - 4.1.1.2.1. Fragilità
    - 4.1.1.2.2. Ansia
    - 4.1.1.2.3. Non linearità
    - 4.1.1.2.4. Incomprensibilità
- 4.1.2. Analisi del contesto generale PESTEL
  - 4.1.2.1. Politica
  - 4.1.2.2. Economica
  - 4.1.2.3. Sociale
  - 4.1.2.4. Tecnologica
  - 4.1.2.5. Ecologica/Ambientale
  - 4.1.2.6. Giuridica
- 4.1.3. Analisi della situazione interna. SWOT
  - 4.1.3.1. Obiettivi
  - 4.1.3.2. Minacce
  - 4.1.3.3. Opportunità
  - 4.1.3.4. Punti di forza

4.2. Rischio e incertezza
- 4.2.1. Rischio
- 4.2.2. Gestione del rischio
- 4.2.3. Standard di gestione del rischio

4.3. Linee guida per la gestione del rischio ISO 31.000:2018
- 4.3.1. Oggetto
- 4.3.2. Principi
- 4.3.3. Quadro di riferimento
- 4.3.4. Processo

4.4. Metodologia per l'analisi e la gestione dei rischi dei sistemi informatici (MAGERIT)
- 4.4.1. Metodologia MAGERIT
  - 4.4.1.1. Obiettivi
  - 4.4.1.2. Metodologia
  - 4.4.1.3. Elementi
  - 4.4.1.4. Tecniche
  - 4.4.1.5. Strumenti disponibili (PILAR)

4.5. Trasferimento del rischio informatico
- 4.5.1. Trasferimento del rischio
- 4.5.2. Rischi informatici. Tipologia
- 4.5.3. Assicurazione contro i rischi informatici

4.6. Metodologie agili per la gestione del rischio
- 4.6.1. Metodologie agili
- 4.6.2. Scrum per la gestione del rischio
- 4.6.3. *Agile risk management*

4.7. Tecnologie per la gestione del rischio
- 4.7.1. Intelligenza artificiale applicata alla gestione del rischio
- 4.7.2. *Blockchain* e crittografia. Metodi di conservazione del valore
- 4.7.3. Computazione quantistica Opportunità o minaccia

4.8. Mappatura dei rischi informatici basata su metodologie agili
- 4.8.1. Rappresentare la probabilità e l'impatto in ambienti agili
- 4.8.2. Il rischio come minaccia al valore
- 4.8.3. Ri-evoluzione nella gestione dei progetti agili e nei processi basati sui KRI

4.9. *Risk-Driven* nella gestione del rischio
- 4.9.1. *Risk driven*
- 4.9.2. *Risk-Driven* nella gestione del rischio
- 4.9.3. Sviluppo di un modello di gestione aziendale orientato al rischio

4.10. Innovazione e trasformazione digitale nella gestione del rischio IT
- 4.10.1. La gestione del rischio agile come fonte di innovazione aziendale
- 4.10.2. Trasformare i dati in informazioni utili per le decisioni
- 4.10.3. Visione olistica dell'impresa tramite il rischio

Modulo 5. La crittografia nell'IT

5.1. Crittografia
- 5.1.1. Crittografia
- 5.1.2. Fondamenti matematici

5.2. Criptologia
- 5.2.1. Criptologia
- 5.2.2. Crittoanalisi
- 5.2.3. Steganografia e stegoanalisi

5.3. Protocolli crittografici
- 5.3.1. Blocchi di base
- 5.3.2. Protocolli di base
- 5.3.3. Protocolli intermedi
- 5.3.4. Protocolli avanzati
- 5.3.5. Protocolli esoterici

5.4. Tecniche crittografiche
- 5.4.1. Lunghezza della chiave di crittografia
- 5.4.2. Gestione delle chiavi
- 5.4.3. Tipi di algoritmi
- 5.4.4. Funzioni di riepilogo. *Hash*
- 5.4.5. Generatori di numeri pseudocasuali
- 5.4.6. Uso degli algoritmi

5.5. Crittografia simmetrica
- 5.5.1. Cifrari a blocchi
- 5.5.2. DES (*Data Encryption Standard*)
- 5.5.3. Algoritmo RC4
- 5.5.4. AES (*Advanced Encryption Standard*)
- 5.5.5. Combinazione di cifrari a blocchi
- 5.5.6. Derivazione delle chiavi

5.6. Crittografia asimmetrica
- 5.6.1. Diffie-Hellman
- 5.6.2. DSA (*Digital Signature Algorithm*)
- 5.6.3. RSA (Rivest, Shamir y Adleman)
- 5.6.4. Curva ellittica
- 5.6.5. Crittografia asimmetrica. Tipologia

5.7. Certificati digitali
- 5.7.1. Firma digitale
- 5.7.2. Certificati X509
- 5.7.3. Infrastruttura a chiave pubblica (PKI)

5.8. Implementazione
- 5.8.1. Kerberos
- 5.8.2. IBM CCA
- 5.8.3. *Pretty Good Privacy* (PGP)
- 5.8.4. ISO *Authentication Framework*
- 5.8.5. SSL e TLS
- 5.8.6. Smart card nei mezzi di pagamento (EMV)
- 5.8.7. Protocolli di telefonia mobile
- 5.8.8. *Blockchain*

5.9. Steganografia
- 5.9.1. Steganografia
- 5.9.2. Stegoanalisi
- 5.9.3. Applicazioni e usi

5.10. Crittografia quantistica
- 5.10.1. Algoritmi quantistici
- 5.10.2. Protezione degli algoritmi dalla computazione quantistica
- 5.10.3. Distribuzione quantistica delle chiavi

Modulo 6. Gestione dell'identità e degli accessi nella sicurezza informatica

6.1. Gestione dell'identità e degli accessi (IAM)
- 6.1.1. Identità digitale
- 6.1.2. Gestione dell'identità
- 6.1.3. Federazione di identità

6.2. Controllo degli accessi fisici
- 6.2.1. Sistemi di protezione
- 6.2.2. Sicurezza delle aree
- 6.2.3. Strutture di recupero

6.3. Controllo logico degli accessi
- 6.3.1. Autenticazione: tipologia
- 6.3.2. Protocolli di autenticazione
- 6.3.3. Attacchi di autenticazione

6.4. Controllo logico degli accessi. Autenticazione MFA
- 6.4.1. Controllo logico degli accessi. Autenticazione MFA
- 6.4.2. Password. Importanza
- 6.4.3. Attacchi di autenticazione

6.5. Controllo logico degli accessi. Autenticazione biometrica
- 6.5.1. Controllo logico degli accessi. Autenticazione biometrica
  - 6.5.1.1. Autenticazione biometrica. Requisiti
- 6.5.2. Funzionamento
- 6.5.3. Modelli e tecniche

6.6. Sistemi di gestione dell'autenticazione
- 6.6.1. *Single sign on*
- 6.6.2. Kerberos
- 6.6.3. Sistemi AAA

6.7. Sistemi di gestione dell'autenticazione: Sistemi AAA
- 6.7.1. TACACS
- 6.7.2. RADIUS
- 6.7.3. DIAMETER

6.8. Servizi per il controllo degli accessi
- 6.8.1. FW - Firewall
- 6.8.2. VPN - Reti Private Virtuali
- 6.8.3. IDS - Sistema di Rilevamento delle Intrusioni

6.9. Sistemi di controllo degli accessi alla rete
- 6.9.1. NAC
- 6.9.2. Architettura ed elementi
- 6.9.3. Funzionamento e standardizzazione

6.10. Accesso alle reti wireless
- 6.10.1. Tipi di reti wireless
- 6.10.2. Sicurezza nelle reti wireless
- 6.10.3. Attacchi alla rete wireless

Modulo 7. Sicurezza nelle comunicazioni e nel funzionamento del software

7.1. Sicurezza informatica nelle comunicazioni e nel funzionamento del software
- 7.1.1. Sicurezza informatica
- 7.1.2. Cibersicurezza
- 7.1.3. Sicurezza del cloud

7.2. Sicurezza informatica nelle comunicazioni e nel funzionamento del software. Tipologia
- 7.2.1. Sicurezza fisica
- 7.2.2. Sicurezza logica

7.3. Sicurezza nelle comunicazioni
- 7.3.1. Elementi principali
- 7.3.2. Sicurezza di rete
- 7.3.3. Le migliori prassi

7.4. Cyberintelligence
- 7.4.1. Ingegneria sociale
- 7.4.2. *Deep web*
- 7.4.3. *Phishing*
- 7.4.4. *Malware*

7.5. Sviluppo sicuro nelle comunicazioni e nel funzionamento del software
- 7.5.1. Sviluppo sicuro. Protocollo HTTP
- 7.5.2. Sviluppo sicuro. Ciclo di vita
- 7.5.3. Sviluppo sicuro. Sicurezza PHP
- 7.5.4. Sviluppo sicuro. Sicurezza NET
- 7.5.5. Sviluppo sicuro. Le migliori prassi

7.6. Sistemi di gestione della sicurezza delle informazioni nelle comunicazioni e nel controllo del software
- 7.6.1. GDPR
- 7.6.2. ISO 27021
- 7.6.3. ISO 27017/18

7.7. Tecnologie SIEM
- 7.7.1. Tecnologie SIEM
- 7.7.2. Operazioni SOC
- 7.7.3. SIEM *Vendors*

7.8. Il ruolo della sicurezza nelle organizzazioni
- 7.8.1. Ruoli nelle organizzazioni
- 7.8.2. Il ruolo degli specialisti IoT nelle aziende
- 7.8.3. Certificazioni riconosciute dal mercato

7.9. Analisi forense
- 7.9.1. Analisi forense
- 7.9.2. Analisi forense. Metodologia
- 7.9.3. Analisi forense. Strumenti e implementazione

7.10. Cybersecurity oggi
- 7.10.1. Principali attacchi informatici
- 7.10.2. Previsioni di impiego
- 7.10.3. Sfide

Modulo 8. Sicurezza negli ambienti Cloud

8.1. Sicurezza negli ambienti *Cloud Computing*
- 8.1.1. Sicurezza negli ambienti *Cloud Computing*
- 8.1.2. Sicurezza negli ambienti *Cloud Computing* Minacce e rischi per la sicurezza
- 8.1.3. Sicurezza negli ambienti *Cloud Computing* Aspetti chiave della sicurezza

8.2. Tipi di infrastruttura *Cloud*
- 8.2.1. Pubblico
- 8.2.2. Privato
- 8.2.3. Ibrido

8.3. Modello di gestione condivisa
- 8.3.1. Caratteristiche di sicurezza gestite dal fornitore
- 8.3.2. Elementi gestiti dal cliente
- 8.3.3. Definizione della strategia di sicurezza

8.4. Meccanismi di prevenzione
- 8.4.1. Sistemi di gestione dell'autenticazione
- 8.4.2. Sistema di gestione delle autorizzazioni: politiche di accesso
- 8.4.3. Sistemi di gestione delle chiavi

8.5. Protezione dei sistemi
- 8.5.1. Protezione dei sistemi di archiviazione
- 8.5.2. Protezione dei sistemi di database
- 8.5.3. Protezione dei dati in transito

8.6. Protezione dell'infrastruttura
- 8.6.1. Progettazione e implementazione di reti sicure
- 8.6.2. Sicurezza delle risorse informatiche
- 8.6.3. Strumenti e risorse per la protezione delle infrastrutture

8.7. Rilevamento di minacce e attacchi
- 8.7.1. Sistemi di verifica, *Logging* e monitoraggio
- 8.7.2. Sistemi di eventi e allarmi
- 8.7.3. Sistemi SIEM

8.8. Risposta agli incidenti
- 8.8.1. Piano di risposta agli incidenti
- 8.8.2. Continuità operativa
- 8.8.3. Analisi forense e correzione di incidenti della stessa natura

8.9. Sicurezza nei *Cloud* pubblici
- 8.9.1. AWS (Amazon Web Services)
- 8.9.2. Microsoft Azure
- 8.9.3. Google GCP
- 8.9.4. Oracle Cloud

8.10. Regolamenti e conformità
- 8.10.1. Conformità alle norme di sicurezza
- 8.10.2. Gestione dei rischi
- 8.10.3. Personale e procedure nelle organizzazioni

Modulo 9. Sicurezza delle comunicazioni nei dispositivi IoT

9.1. Dalla telemetria all'IoT
- 9.1.1. Telemetria
- 9.1.2. Connettività M2M
- 9.1.3. Democratizzazione della telemetria

9.2. Modelli di riferimento IoT
- 9.2.1. Modello di riferimento IoT
- 9.2.2. Architettura IoT semplificata

9.3. Vulnerabilità della sicurezza IoT
- 9.3.1. Dispositivi IoT
- 9.3.2. Dispositivi IoT. Casi di utilizzo
- 9.3.3. Dispositivi IoT. Punti deboli

9.4. Connettività IoT
- 9.4.1. Reti PAN, LAN, WAN
- 9.4.2. Tecnologie wireless non IoT
- 9.4.3. Tecnologie wireless LPWAN

9.5. Tecnologie LPWAN
- 9.5.1. Il triangolo di ferro delle reti LPWAN
- 9.5.2. Bande di frequenza libere vs. Bande con licenza
- 9.5.3. Opzioni tecnologiche LPWAN

9.6. Tecnologia LoRaWAN
- 9.6.1. Tecnologia LoRaWAN
- 9.6.2. Casi d'uso di LoRaWAN. Ecosistema
- 9.6.3. Sicurezza in LoRaWAN

9.7. Tecnologia Sigfox
- 9.7.1. Tecnologia Sigfox
- 9.7.2. Casi d'uso di Sigfox. Ecosistema
- 9.7.3. Sicurezza in Sigfox

9.8. Tecnologia cellulare IoT
- 9.8.1. Tecnologia cellulare IoT (NB-IoT e LTE-M)
- 9.8.2. Casi d'uso cellulare IoT. Ecosistema
- 9.8.3. Sicurezza cellulare IoT

9.9. Tecnologia WiSUN
- 9.9.1. Tecnologia WiSUN
- 9.9.2. Casi d'uso di WiSUN. Ecosistema
- 9.9.3. Sicurezza di WiSUN

9.10. Altre tecnologie IoT
- 9.10.1. Altre tecnologie IoT
- 9.10.2. Casi d'uso ed ecosistema di altre tecnologie IoT
- 9.10.3. Sicurezza in altre tecnologie IoT

Modulo 10. Piano di continuità operativa associato alla sicurezza

10.1. Piano di Continuità Operativa
- 10.1.1. I piani di Continuità Operativa (BCP)
- 10.1.2. Piano di Continuità Operativa (BCP). Aspetti chiave
- 10.1.3. Piano di Continuità Operativa (BCP) per la valutazione dell'azienda

10.2. Parametri in un Piano di Continuità Operativa (BCP)
- 10.2.1. *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO)
- 10.2.2. Tempo massimo tollerabile (MTD)
- 10.2.3. Livelli minimi di recupero (ROL)
- 10.2.4. Obiettivo del punto di recupero (RPO)

10.3. Progetti di continuità. Tipologia
- 10.3.1. Piano di Continuità Operativa (BCP)
- 10.3.2. Piano di continuità ICT
- 10.3.3. Piano di ripristino in caso di disastro (DRP)

10.4. Gestione dei rischi connessi al BCP
- 10.4.1. Analisi dell'impatto aziendale
- 10.4.2. Vantaggi dell'implementazione di un BCP
- 10.4.3. Mentalità basata sul rischio

10.5. Ciclo di vita di un piano di continuità operativa
- 10.5.1. Fase 1: Analisi dell'organizzazione
- 10.5.2. Fase 2: Determinazione della strategia di continuità
- 10.5.3. Fase 3: Risposta alla contingenza
- 10.5.4. Fase 4: Test, manutenzione e revisione

10.6. Fase di analisi organizzativa di un BCP
- 10.6.1. Identificazione dei processi che rientrano nell'ambito di applicazione del BCP
- 10.6.2. Identificazione delle aree aziendali critiche
- 10.6.3. Identificazione delle dipendenze tra aree e processi
- 10.6.4. Determinazione del MTD appropriato
- 10.6.5. Prodotti. Creazione di un piano

10.7. Fase di determinazione della strategia di continuità in un BCP
- 10.7.1. Ruoli nella fase di determinazione della strategia
- 10.7.2. Compiti nella fase di determinazione della strategia
- 10.7.3. Risultati

10.8. Fase di risposta alla contingenza di un BCP
- 10.8.1. Ruoli nella fase di risposta
- 10.8.2. Compiti di questa fase
- 10.8.3. Risultati

10.9. Fase di test, manutenzione e revisione di un BCP
- 10.9.1. Ruoli nella fase di test, manutenzione e revisione
- 10.9.2. Lavori nella fase di test, manutenzione e revisione
- 10.9.3. Risultati

10.10. Standard ISO associati ai piani di Continuità Operativa (BCP)
- 10.10.1. ISO 22301:2019
- 10.10.2. ISO 22313:2020
- 10.10.3. Altri standard ISO e internazionali correlati

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 di Corporate Governance nelle aziende
- 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 in azienda
- 11.2.3. L'importanza del leader nella direzione aziendale

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. L'intelligenza nella Leadership
- 11.4.6. 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 RSI

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 legali per le multinazionali nel campo dei 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. Management del personale e gestione del talento

12.1. Direzione Strategica del personale
- 12.1.1. Direzione Strategica e risorse umane
- 12.1.2. Direzione strategica 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. 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
- 12.6.1. Team ad alte prestazioni: team autogestiti
- 12.6.2. Metodologie per la gestione di team autogestiti ad alte prestazioni

12.7. Gestione del cambiamento
- 12.7.1. Gestione del cambiamento
- 12.7.2. Tipo di processi di gestione del cambiamento
- 12.7.3. Stadi o fasi nella gestione del cambiamento

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

12.9. Comunicazione direttiva
- 12.9.1. Comunicazione interna ed esterna nel contesto aziendale
- 12.9.2. Dipartimenti di Comunicazione
- 12.9.3. Il responsabile della comunicazione aziendale. 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. Direzione Economico-Finanziaria

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

13.2. Contabilità Direttiva
- 13.2.1. Concetti di base
- 13.2.2. L'Attivo dell'azienda
- 13.2.3. Il Passivo dell'azienda
- 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. Budget e Controllo di Gestione
- 13.4.1. Il modello di budget
- 13.4.2. Bilancio di Capitale
- 13.4.3. Il bilancio operativo
- 13.4.5. Bilancio del Tesoro
- 13.4.6. Monitoraggio del budget

13.5. Direzione Finanziaria
- 13.5.1. Le decisioni finanziarie dell'azienda
- 13.5.2. Dipartimento finanziario
- 13.5.3. Eccedenze di cassa
- 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 intraprendere nella pianificazione finanziaria
- 13.6.3. Creazione e definizione della strategia aziendale
- 13.6.4. La tabella *Cash Flow*
- 13.6.5. La tabella dell'attivo circolante

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. Incremento dei fondi propri
- 13.8.3. Risorse Ibride
- 13.8.4. Finanziamento tramite intermediari

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 su Industria de Diseño y Textil, 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 di 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 del Digital Marketing ed e-commerce
- 14.4.2. Digital Marketing e mezzi impiegati
- 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 il lancio di una campagna di marketing online
- 14.7.3. Errori delle 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 aziendale
- 14.9.3. Tipo di comunicazione nell'azienda
- 14.9.4. Funzioni della comunicazione nell'azienda
- 14.9.5. Elementi della comunicazione
- 14.9.6. Problemi di comunicazione
- 14.9.7. Scenari della 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 Manager Generale
- 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 personale 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 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 comunicazione personale e organizzativa
- 15.5.1. La comunicazione interpersonale
- 15.5.2. Strumenti di comunicazione interpersonale
- 15.5.3. La comunicazione nell'azienda
- 15.5.4. Strumenti nell'azienda

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 miglior personale docente e un sistema di insegnamento innovativo, uniti al programma di studio più completo e aggiornato: ecco una grande opportunità per migliorare la propria carriera di informatico"

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

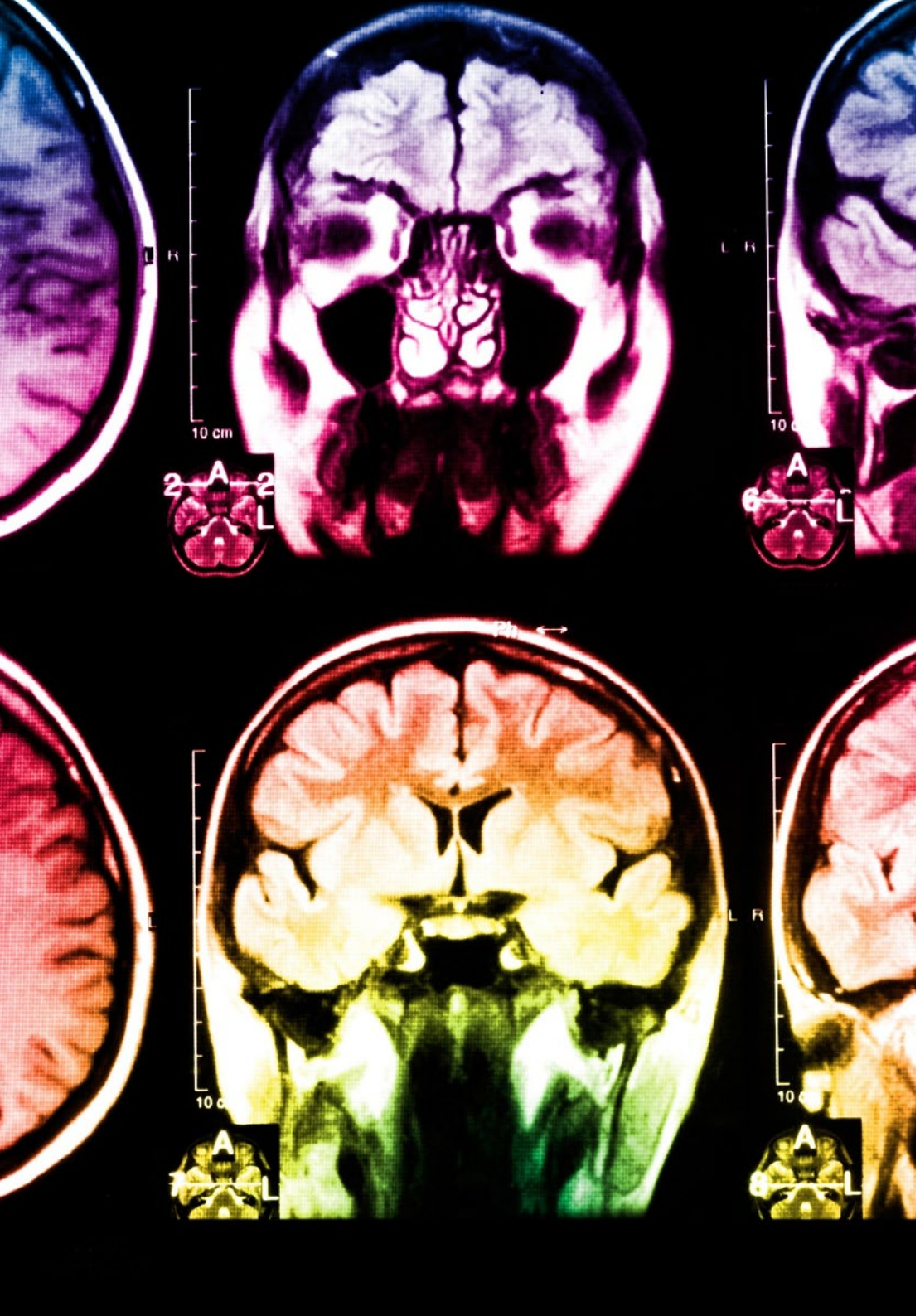
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

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.

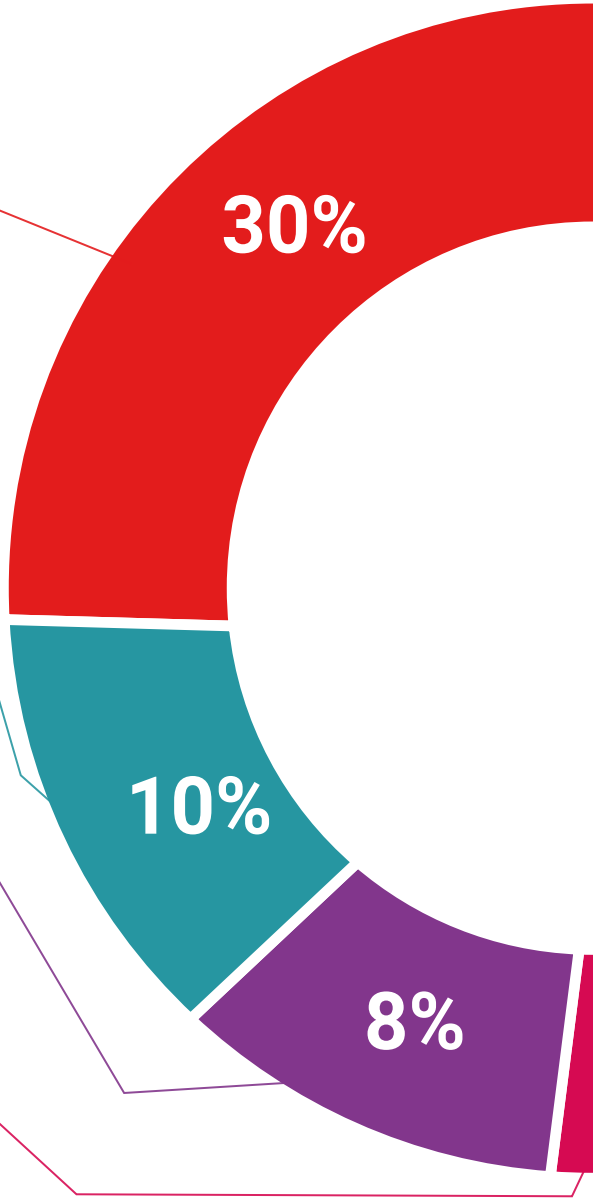
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

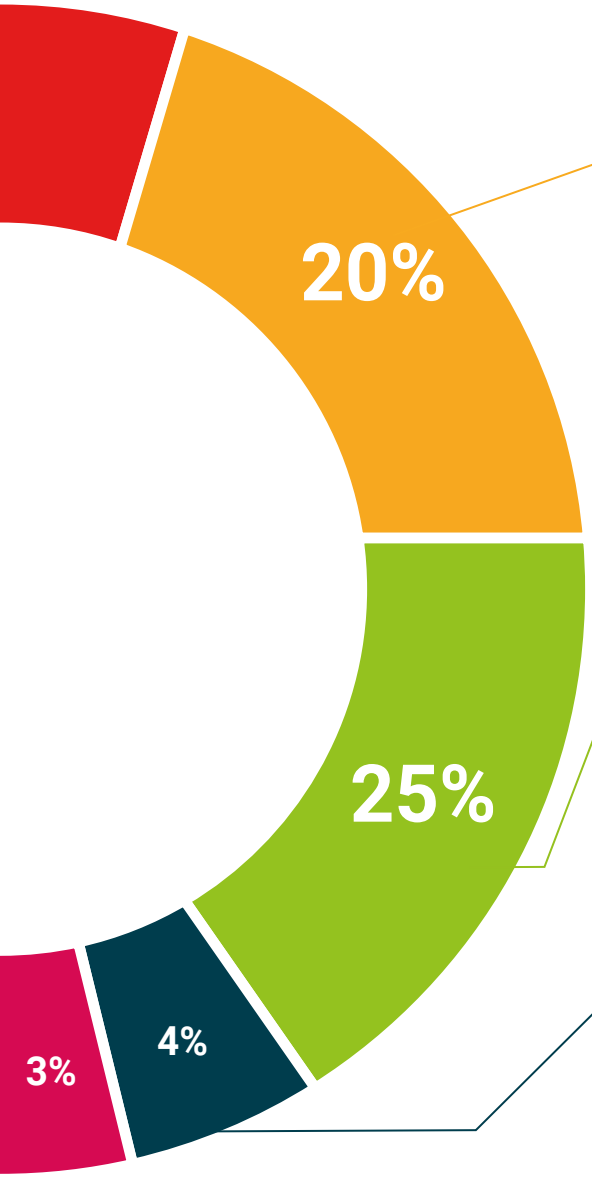
Pratiche di competenze e competenze

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 Avanzato (CISO) 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 il tuo titolo universitario senza spostamenti o fastidiose formalità"

Questo **MBA in Cybersecurity Management Avanzato (CISO)** 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 Avanzato (CISO)**

Modalità: **online**

Durata: **12 mesi**


tech università tecnologica

Conferisce il presente

DIPLOMA

a

Dott./Dott.ssa _____, con documento d'identità n°_____

Per aver completato con esito positivo e accreditato il programma di

MASTER PRIVATO

in

MBA in Cybersecurity Management Avanzato (CISO)

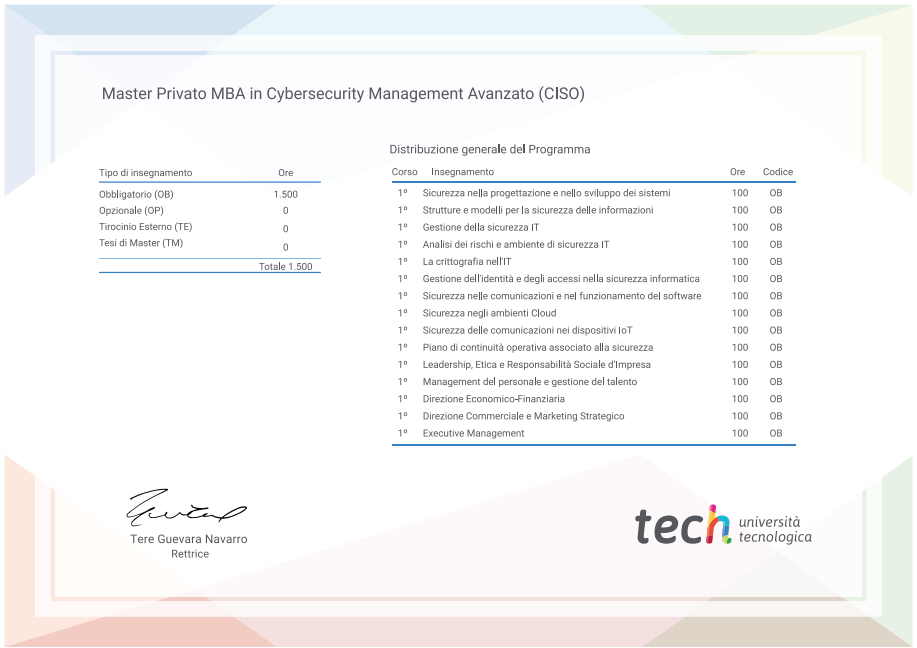
Si tratta di un titolo rilasciato da questa Università ed equivalente a 1.500 ore, con data di inizio gg/mm/aaaa e con data di fine gg/mm/aaaa.

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

In data 7 Giugno 2020

Tere Guevara Navarro
Rettrice

codice unico TECH: AFWORD23S techtitute.com/titulos


Master Privato MBA in Cybersecurity Management Avanzato (CISO)

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
1°	Sicurezza nella progettazione e nello sviluppo dei sistemi	100	OB
1°	Strutture e modelli per la sicurezza delle informazioni	100	OB
1°	Gestione della sicurezza IT	100	OB
1°	Analisi dei rischi e ambiente di sicurezza IT	100	OB
1°	La crittografia nell'IT	100	OB
1°	Gestione dell'identità e degli accessi nella sicurezza informatica	100	OB
1°	Sicurezza nelle comunicazioni e nel funzionamento del software	100	OB
1°	Sicurezza negli ambienti Cloud	100	OB
1°	Sicurezza delle comunicazioni nei dispositivi IoT	100	OB
1°	Piano di continuità operativa associato alla sicurezza	100	OB
1°	Leadership, Etica e Responsabilità Sociale d'Impresa	100	OB
1°	Management del personale e gestione del talento	100	OB
1°	Direzione Economico-Finanziaria	100	OB
1°	Direzione Commerciale e Marketing Strategico	100	OB
1°	Executive Management	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 Global University effettuerà le gestioni opportune per ottenerla pagando un costo aggiuntivo.

tech università tecnologica

Master Privato
MBA in Cybersecurity Management Avanzato (CISO)

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

Master Privato

MBA in Cybersecurity Management Avanzato (CISO)

tech università tecnologica