Master Specialistico

Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer)

tech università tecnologica

tech università tecnologica

Master Specialistico in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer)

- Modalità: **online**
- Durata: **2 anni**
- Titolo: **TECH Università Tecnologica**
- Orario: **a tua scelta**
- Esami: **online**

Accesso al sito web: www.techtitute.com/it/informatica/master-specialistico/master-specialistico-alta-direzione-cibersicurezza-ciso-chief-information-security-officer

Índice

01

Presentación

Nel mondo di oggi, la sicurezza informatica è un elemento fondamentale per i privati e le aziende, che sono più esposti degli altri agli attacchi. Ciò è dovuto al continuo sviluppo di nuove tecnologie e al processo di digitalizzazione, che ha prodotto trasformazioni in tutti i tipi di aziende, velocizzando numerose attività ma anche provocando l'emergere di nuove vulnerabilità. Per questo motivo, uno dei profili più ricercati al momento è quello di direttore della sicurezza informatica, una figura in crescita che dispone di numerose opportunità professionali. Questo programma approfondisce questa figura e prepara l'informatico ad affrontare, in modo efficace e completo, tutte le sfide attuali in questo settore, dove sono inoltre necessarie capacità manageriali e una prospettiva imprenditoriale. Inoltre, la qualifica si svolge in un formato 100% online, quindi è perfetta per combinarla con il lavoro, consentendo al professionista di studiare quando lo desidera.

Questo programma ti preparerà ad affrontare tutte le sfide attuali e future nel campo della sicurezza informatica, permettendoti di specializzarti nella gestione in questa importante area dell'informatica"

Processi bancari, acquisti via internet, comunicazioni interne in diverse organizzazioni, procedure amministrative, ecc. Oggi la digitalizzazione ha trasformato il modo in cui individui e aziende operano quotidianamente. Ha reso più rapide numerose attività, ha permesso di evitare certi spostamenti, migliorando la qualità della vita della popolazione e risparmiando costi alle compagnie. Tuttavia, questi vantaggi hanno portato, in via accessoria, in materia di sicurezza informatica.

Molte delle tecnologie e degli strumenti digitali attualmente in uso sono in continuo sviluppo, quindi sono esposti agli attacchi. Con l'uso diffuso di applicazioni e *dispositivi* digitali, un difetto in essi è critico, poiché può influenzare lo sviluppo dell'organizzazione, non solo in termini di marketing e vendite, ma nel suo funzionamento interno, che dipende anche da questi profitti.

Proprio per questo motivo, è importante disporre dei migliori strumenti in ambito sanitario in grado di rispondere ai diversi problemi che possono sorgere a questo proposito. Uno dei profili più ricercati è quello di Direttore della Sicurezza Informatica, una carica che comporta una visione globale di questo settore e per la quale questo Master Specialistico prepara in modo completo. Questo programma rappresenta quindi una grande opportunità per l'informatico, in quanto si approccerà a tutte le novità in questo settore, preparandolo, allo stesso tempo, ad affrontare decisioni di carattere manageriale, che hanno bisogno delle migliori conoscenze e capacità di leadership.

Tutto questo, a partire da una metodologia di apprendimento online che sarà adattato alle circostanze professionali dello studente, mentre è accompagnato da un personale docente di grande prestigio in questo settore dell'informatica. Inoltre, avrà a disposizione la migliore tecnologia didattica e le più recenti risorse didattiche: riassunti interattivi, video, lezioni magistrali, analisi di casi o letture complementari.

Senza dimenticare i materiali complementari al programma, come le 10 *Master class* tenute da un esperto di fama internazionale in Intelligence, Sicurezza Informatica e Tecnologie Dirompenti. Grazie a questo contenuto aggiuntivo, lo studente approfondirà le sue conoscenze sull'Alta Direzione della Cibersicurezza (CISO, Chief Information Security Officer) e i concetti relativi alla ciberintelligence e alla sicurezza delle informazioni.

Questo **Master Specialistico in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer)** possiede il programma educativo più completo e aggiornato del mercato. Le sue caratteristiche principali sono:

- Sviluppo di casi pratici presentati da esperti in informatica e cibersicurezza
- Contenuti grafici, schematici ed eminentemente pratici che forniscono informazioni scientifiche e pratiche riguardo alle discipline essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- Speciale enfasi sulle metodologie innovative nella direzione di imprese creative
- Lezioni teoriche, domande all'esperto, forum di discussione su argomenti controversi e lavoro di riflessione individuale
- Disponibilità di accesso ai contenuti da qualsiasi dispositivo fisso o portatile con una connessione internet

Specializzati in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer), rafforzando le tue conoscenze grazie alle 10 Master class impartite da un professionista di fama internazionale"

Grazie a questo Master Specialistico potrai approfondire la sicurezza nell'IoT, nel cloud computing, nella Blockchain e imparerai a fare audit di alto livello a tutti i tipi di aziende e organizzazioni"

Godrai dell'accompagnamento di un personale docente di grande prestigio, che si assicurerà che tu ottenga tutti gli aspetti chiave del settore della direzione della sicurezza informatica.

Avrai a disposizione le più recenti risorse didattiche per garantire un processo di apprendimento rapido ed efficace.

Il personale docente del programma comprende rinomati specialisti dell'ambito della Informatica, che forniscono agli studenti le competenze necessarie a intraprendere un percorso di studio eccellente.

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

La creazione di questo programma è incentrata sull'Apprendimento Basato 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

Objetivos

L'obiettivo principale di questo Master Specialistico è quello di trasformare l'informatico in un grande specialista in questo settore, permettendogli di accedere alle migliori opportunità professionali. Per questo, non solo fornirà tutte le novità nel campo della sicurezza informatica, ma anche i migliori strumenti per ottenere una visione globale delle esigenze aziendali in questo settore. In questo modo, potrà lavorare come responsabile della sicurezza delle aziende di tutto il mondo, conoscendo i metodi migliori per procedere in ogni caso.

Questo Master Specialistico ti aiuterà a raggiungere il progresso professionale che cerchi, grazie ai suoi contenuti ampi e aggiornati, e al suo prestigioso personale docente composto da esperti di sicurezza informatica in attività"

Obiettivi generali

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

Obiettivi specifici

Modulo 1. Cyberintelligence e Cibersicurezza

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

Modulo 2. Sicurezza in Host

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

Modulo 3. Sicurezza di Rete (Perimetrale)

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

Modulo 4. Sicurezza degli smartphone

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

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

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

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

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

Modulo 9. Implementazione pratica delle politiche di sicurezza *software* e hardware
- Determinare cosa sono l'autenticazione e l'identificazione
- Analizzare i diversi metodi di autenticazione esistenti e la loro implementazione pratica
- Implementare la corretta politica di controllo degli accessi per *software* e sistemi
- Stabilire le principali tecnologie di identificazione attuali
- Generare una conoscenza specialistica delle diverse metodologie esistenti per il bastioning dei sistemi

Modulo 10. Analisi forense

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

Modulo 11. 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 l'informazione sensibile memorizzata nel sistema di informazione
- Disporre del quadro giuridico e della caratterizzazione del reato, integrando la visione con la tipologia del reo e della sua vittima

Modulo 12. Strutture e modelli per la sicurezza delle informazioni

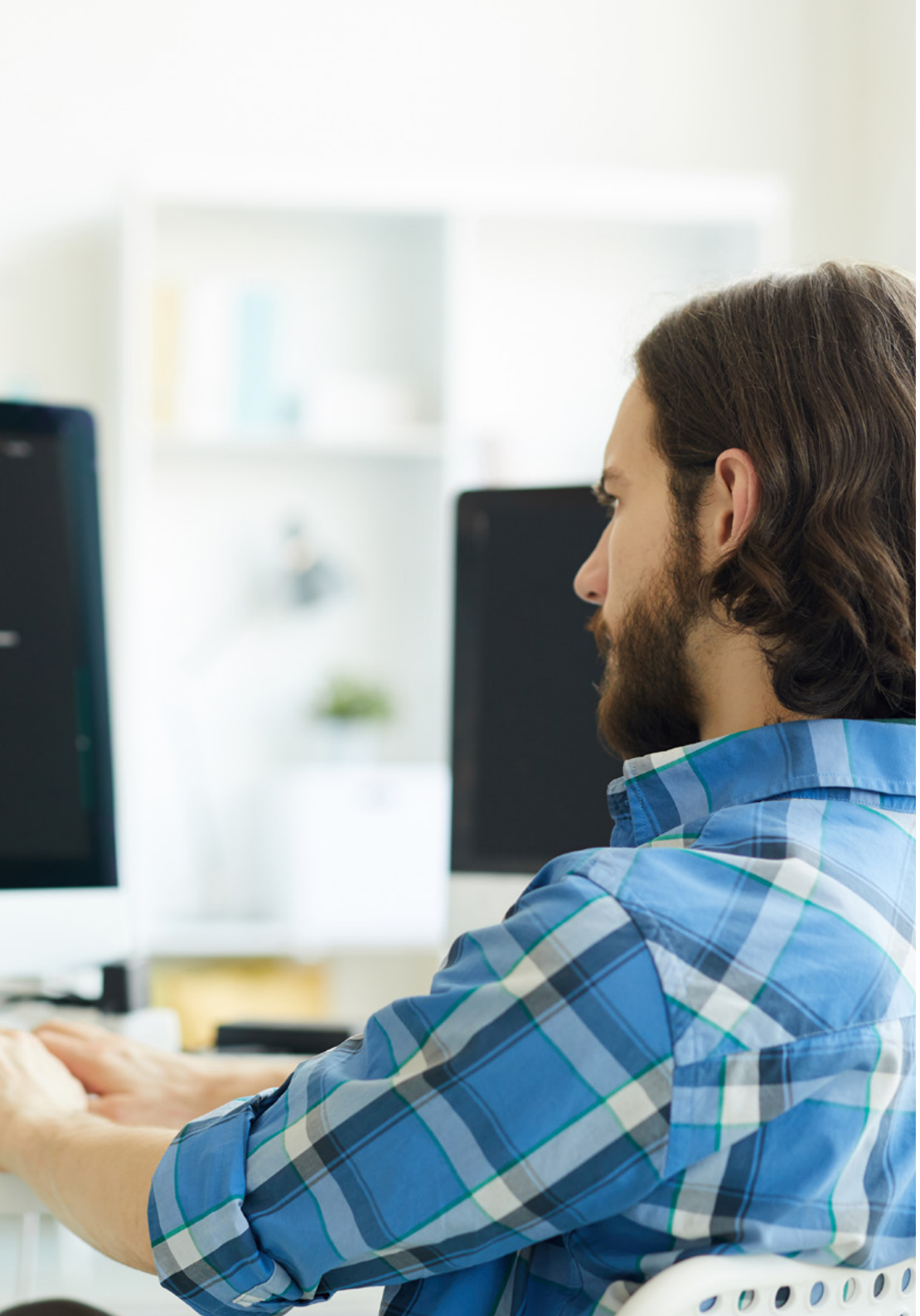
- Allineare il Master Plan per la sicurezza agli obiettivi strategici dell'organizzazione
- Stabilire un quadro di gestione costante dei rischi come parte integrante del Master Plan sulla sicurezza
- Stabilire gli indicatori appropriati per il monitoraggio della messa in atto del SGSI
- Stabilire una 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 13. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

- Analizzare le normative e gli standard attualmente applicabili ai sistemi di gestione ambientale
- Sviluppare le fasi necessarie per implementare un ISMS in un'entità
- Analizzare le procedure di gestione degli incidenti di sicurezza di informazione e implementazione

Modulo 14. Gestione della sicurezza IT

- Identificare le diverse strutture che possono avere un'area di sicurezza dell'informazione
- 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 gli attori interessati (autorità, clienti, fornitori ecc.)

Modulo 15. Politiche di Gestione degli Incidenti di Sicurezza

- Sviluppare competenze su come gestire gli incidenti causati da eventi di sicurezza informatica
- Determinare il funzionamento di un team di gestione degli incidenti di sicurezza
- Analizzare le diverse fasi della gestione degli eventi di sicurezza informatica
- Esaminare i protocolli standardizzati per la gestione degli incidenti di sicurezza

Modulo 16. 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 che ci consentano di affrontare i rischi e le opportunità in modo da massimizzare il contributo di valore
- 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 17. Politiche di Sicurezza per l'Analisi delle Minacce dei Sistemi Informatici

- Analizzare il significato delle minacce
- Determinare le fasi della gestione preventiva delle minacce
- Comparazione di diverse metodologie di gestione delle minacce

Modulo 18. Implementazione Pratica di Politiche di Sicurezza contro gli Attacchi

- Determinare i diversi attacchi effettivi al sistema di informazioni
- Valutare le diverse politiche di sicurezza per mitigare gli attacchi
- Implementare tecnicamente le misure per mitigare le principali minacce

Modulo 19. La crittografia nell'IT

- Conoscere 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 20. 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 21. 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 delle informazioni
- Stabilire il funzionamento di un centro operativo per la cybersecurity
- Dimostrare l'importanza delle pratiche di sicurezza informatica per i disastri organizzativi

Modulo 22. Sicurezza negli ambienti Cloud

- Identificare i rischi di installazione di un'infrastruttura in un cloud pubblico
- Definire i requisiti di sicurezza
- Stabilire un piano di sicurezza per l'implementazione in 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 23. Strumenti di monitoraggio nelle Politiche di Sicurezza dei Sistemi di Informazione

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

Modulo 24. 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 25. 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 26. Politica di Ripristino pratico in caso di Emergenze di Sicurezza

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

Modulo 27. Implementare le politiche di sicurezza fisica e ambientale in azienda

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

Modulo 28. Politiche di Comunicazione Sicura in Azienda

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

Modulo 29. Aspetti organizzativi della Politica di Sicurezza delle Informazioni

- Implementare un ISMS in azienda
- Determinare quali dipartimenti devono essere coperti dall'implementazione del sistema di gestione della sicurezza
- Implementare le necessarie contromisure di sicurezza nell'operazione

03

Competenze

Durante questo Master Specialistico, il professionista acquisirà una serie di strumenti e competenze che lo abiliteranno a lavorare nella direzione della sicurezza informatica di una grande azienda. Per questo motivo, questo programma non si concentra solo sugli aspetti informatici, ma presta attenzione al processo di digitalizzazione, alle tecnologie emergenti e a come questi elementi hanno influenzato le attività comuni e quotidiane delle organizzazioni. In questo modo, lo studente sarà stato in grado di adattarsi al contesto attuale, conoscendo le migliori soluzioni in materia di sicurezza per ogni azienda.

Migliora le tue capacità per diventare il miglior specialista di sicurezza informatica del tuo ambiente"

Competenze generali

- Conoscere le metodologie utilizzate in materia di sicurezza informatica
- Saper valutare ogni tipo di minaccia per offrire una soluzione ottimale in ogni caso
- Essere in grado di generare soluzioni intelligenti complete per automatizzare il comportamento in caso di imprevisti
- Saper valutare i rischi associati alle vulnerabilità interne ed esterne all'azienda
- Comprendere l'evoluzione e l'impatto dell'IoT nel tempo
- Essere in grado di dimostrare che un sistema è vulnerabile, attaccarlo in modo proattivo e risolvere tali problemi
- Saper applicare il *sandboxing* in diversi ambienti
- Conoscere le linee guida che un buon sviluppatore deve seguire per conformarsi ai requisiti di sicurezza necessari
- Applicare le misure di sicurezza più appropriate in base alle minacce
- Determinare la politica e il piano di sicurezza del sistema di informazione di un'azienda, ultimando la progettazione e l'implementazione del piano di contingenza
- Stabilire un programma di audit che soddisfi le esigenze di autovalutazione dell'organizzazione in materia di sicurezza informatica
- Sviluppare un programma di analisi e controllo delle vulnerabilità e un piano di risposta agli incidenti di sicurezza informatica
- 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 dell'informazione 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

Questo programma ti porterà nel futuro della sicurezza informatica"

Competenze specifiche

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

Dirección del curso

Questo Master Specialistico in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer) dispone di un personale docente composto da professionisti attivi che conoscono perfettamente lo stato attuale di questo settore, e che trasferirà, quindi, tutte le chiavi della sicurezza informatica attuale allo studente. In questo modo, lo studente di questo programma è garantito per ottenere le ultime novità in questo campo, essendo in grado di accedervi grazie al prestigioso personale docente che ha selezionato TECH.

Iscriviti e inizia ad accedere alle conoscenze più avanzate in questo settore, trasmesse da professionisti con una grande esperienza nel campo della sicurezza informatica"

Direttore Ospite Internazionale

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

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

Il Dottor Lemieux ha ricoperto ruoli editoriali e di valutazione in diverse organizzazioni accademiche, private e governative, a testimonianza della sua influenza e del suo impegno per l'eccellenza nel suo campo di competenza. In questo modo, sua prestigiosa carriera accademica lo ha portato a ricoprire il ruolo di Professore di Pratica e Direttore di Facoltà dei programmi MPS in **Intelligenza applicata, Gestione del rischio di Cibersicurezza, Gestione della Tecnologia e Gestione della tecnologia dell'Informazione**, presso la **Georgetown University.**

Dott. Lemieux, Frederic

- Ricercatore in Intelligence, Cibersicurezza e Tecnologie dirompenti presso la Georgetown University
- Direttore del Master in Information Technology Management presso la Georgetown University
- Direttore del MasterTechnology Management presso la Georgetown University
- Direttore del Master in Cybersecurity Risk Management presso la Georgetown University
- Direttore del Master in Applied Intelligence presso la Georgetown University
- Docente di Pratica presso la Georgetown University
- Dottorato di Ricerca in Criminologia presso la Scuola di Criminologia dell'Università di Montreal
- Laurea in Sociologia, Minor Degree in Psicologia, Università di Laval
- Membro di: New Program Roundtable Committee presso la Georgetown University

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

Direzione

Dott.ssa Fernández Sapena, Sonia

- Istruttrice in Sicurezza Informatica e Hacking Etico presso il Centro di Riferimento Nazionale per l'Informatica e le Telecomunicazioni di Getafe, Madrid
- Istruttrice certificata E-Council
- Formatrice nelle seguenti certificazioni: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation, Madrid
- Esperta Formatrice accreditata dal CAM per i seguenti certificati di professionalità: Sicurezza informatica (IFCT0190), Gestione di reti voce e dati (IFCM0310), Amministrazione di reti dipartimentali (IFCT0410), Gestione degli allarmi nelle reti di telecomunicazione (IFCM0410), Operatore di reti voce e dati (IFCM0110) e Amministrazione di servizi Internet (IFCT0509)
- Collaboratrice esterna CSO/SSA (*Chief Security Officer/Senior Security Architect*) presso l'Università delle Isole Baleari
- Laurea in Ingegneria Informatica presso l'Università di Alcalá de Henares a Madrid
- Master in DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies, E-Council

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.ssa Marcos Sbarbaro, Victoria Alicia

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

Dott. Catalá Barba, José Francisco

- Tecnico Elettronico Esperto di Cibersicurezza
- Sviluppatore di Applicazioni per *Dispositivi* Mobili
- Tecnico Elettronico presso il Comando Intermedio del Ministero della Difesa Spagnolo
- Tecnico Elettronico presso la Factoría *Ford* Sita di Valencia

Dott. Jiménez Ramos, Álvaro

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

Dott. Peralta Alonso, Jon

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

Dott. Redondo, Jesús Serrano

- Sviluppatore Web e Tecnico di Cibersicurezza
- Sviluppatore Web presso Roams, Palencia
- Sviluppatore *FrontEnd* presso Telefónica, Madrid
- Sviluppatore *FrontEnd* presso Best Pro Consulting SL, Madrid
- Installatore di Apparecchiature e Servizi di Telecomunicazione presso il Grupo Zener, Castilla y León
- Installatore di Apparecchiature e Servizi di Telecomunicazione presso Lican Comunicaciones SL, Castilla y León
- Certificato in Sicurezza Informatica presso CFTIC Getafe, Madrid
- Tecnico Superiore in Telecomunicazioni e Sistemi Informatici presso IES Trinidad Arroyo, Palencia
- Tecnico superiore in Installazioni Elettrotecniche MT e BT dell'IES Trinidad Arroyo, Palencia
- Formazione in Ingegneria Inversa, Stenografia e Crittografia presso l'Accademia Hacker Incibe

Dott. Nogales Ávila, Javier

- Enterprise Cloud e Sourcing Senior Consultant quinto
- Cloud e Technology Consultant presso Indra
- Associate Technology Consultant presso Accenture
- Laurea in ingegneria dell'organizzazione industriale presso l'Università di Jaén
- MBA in Amministrazione e Direzione Aziendale presso ThePower Business School

Dott. Gómez Rodríguez, Antonio

- Ingegnere principale delle 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 La Salle
- Studi post-laurea sulle Tecnologie e i Sistemi di Informazioni presso l'Istituto Catalano di Tecnologia
- Laurea in Ingegneria delle Telecomunicazioni presso l'Università Politecnica della Catalogna

Dott. Gonzalo Alonso, Félix

- Direttore Generale e Fondatore di Smart REM Solutions
- Responsabile di Risk & Innovation Engineering presso Dynargy
- Direttore e socio fondatore dello studio di esperti in tecnologie Risknova
- Master in Gestione delle Assicurazioni presso ICEA (Istituto per la Collaborazione tra le Imprese di Assicurazione)
- Laurea in Ingegneria tecnica industriale con specializzazione in Elettronica industriale presso l'Universidad Pontificia de Comillas

Dott. del Valle Arias, Jorge

- Ingegnere delle telecomunicazioni esperto in sviluppo aziendale
- Smart City Solutions & Software Business Development Manager España, Itron, Inc
- Consulente IoT
- Direttore Commerciale Interinale IoT, TCOMET
- Responsabile dell'unità di business IoT, Industria 4.0, Diode España
- Responsabile delle vendite IoT e telecomunicazioni, Aicox Soluciones
- Direttore tecnico (CTO) e responsabile dello sviluppo aziendale, Consultoría TELYC
- Fondatore e CEO di Sensor Intelligence
- Capo delle operazioni e dei progetti, Codio
- Direttore Operativo di Codium Networks
- Ingegnere capo per la progettazione di hardware e firmware, AITEMIN
- Responsabile regionale di 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. Gozalo Fernández, Juan Luis

- Responsabile dei Prodotti Blockchain presso 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 la UNED
- Specializzazione in Deep Learning presso DeepLearning.ai

Dott.ssa Jurado Jabonero, Lorena

- Responsabile della Sicurezza delle Informazioni (CISO) presso Grupo Pascual
- Cybersecurity Manager presso KPMG, Spagna
- Consulente di processi IT e controllo e gestione dei progetti infrastrutturali in Bankia
- Ingegnere degli strumenti di sfruttamento a Dalkia
- Sviluppatore nel Gruppo Banca Popolare
- Sviluppatori Applicazioni dell'Università Politecnica di Madrid
- Laurea in Ingegneria Informatica presso l'Università Alfonso X el Sabio
- Ingegnere Tecnico in Informatica di Gestione presso l'Università Politecnica di Madrid
- Certified Data Privacy Solutions Engineer (CDPSE) presso ISACA

Dott. Embid Ruiz, Mario

- Esperto di TIC e Protezione dei Dati presso Martínez-Echevarría Abogados
- Responsabile legale di Branddocs SL
- Analista di rischio nel segmento Pymes di BBVA
- Docente in studi universitari post-laurea di Giurisprudenza
- Laureato in Giurisprudenza presso l'Università Rey Juan Carlos
- Laurea in Amministrazione e Direzione Aziendale conseguita presso l'Università Rey Juan Carlos
- Master in Giurisprudenza delle nuove tecnologie, Internet e audiovisivo dal Centro di Studi Universitari Villanueva

Dott. Rodrigo Estébanez, Juan Manuel

- Cofondatore di Ismet Tech
- Responsabile della Sicurezza delle Informazioni (CISO) presso Ecix Group
- *Operational Security Officer* presso Atos IT Solutions and Services A/S

- Docente di gestione della sicurezza informatica in studi universitari
- Laureato in Ingegneria presso l'Università di Valladolid
- Master in sistemi di gestione integrati presso l'Università CEU San Pablo

Dott. Entrenas, Alejandro

- Responsabile di Progetti di Cibersicurezza, Entelgy Innotec Security
- Consulente di Cibersicurezza, Entelgy
- Analista di Sicurezza delle Informazioni, Innovery España
- Analista di Sicurezza delle Informazioni, Atos
- Laurea in Ingegneria Tecnica in Informatica dei Sistemi presso l'Università di Cordoba
- Master in Gestione e Amministrazione della Sicurezza delle Informazioni 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

Dott. Ortega Esteban, Octavio

- Specialista in Marketing e Sviluppo Web
- Sviluppatore di Applicazioni Informatiche e sviluppatore web freelance
- *Chief Operating Officer* presso Smallsquid SL
- Amministratore e-commerce presso Ortega y Serrano
- Docente nei corsi di Certificati di Professionalità in Informatica e Comunicazioni
- Docente di corsi di Sicurezza Informatica
- Laurea in Psicologia presso l'Università Aperta di Catalogna
- Tecnico Superiore Universitario in Analisi, Progettazione e Soluzioni Software
- Tecnico Superiore Universitario in Programmazione Avanzata

05

Struttura e contenuti

Questo Master Specialistico in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer) è composto da 20 moduli, ed è stato progettato con cura per portare al professionista le ultime novità in questo campo. In questo modo, potrà conoscere i più recenti sviluppi su questioni come la sicurezza negli smartphone, la sicurezza nell'internet delle cose, lo sviluppo sicuro, la crittografia o la sicurezza negli ambienti di *Cloud Computing*. Con questo programma, quindi, l'informatico avrà accesso alle conoscenze più aggiornate e complete, preparandosi, in modo rapido, a diventare uno specialista di sicurezza informatica di grande prestigio.

Non troverai contenuti più completi di questi per aggiornarti nell'ambito della sicurezza informatica"

Modulo 1. Cyberintelligence e Cibersicurezza

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

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

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

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

1.5. Audit e documentazione
- 1.5.1. L'audit nella sicurezza informatica
- 1.5.2. Documentazione e autorizzazioni per l'audit
- 1.5.3. Tipi di audit
- 1.5.4. Risultati
  - 1.5.4.1. Rapporto tecnico
  - 1.5.4.2. Rapporto esecutivo

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

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

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

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

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

Modulo 2. Sicurezza in Host

2.1. Backup
- 2.1.1. Strategie per i backup
- 2.1.2. Strumenti per Windows
- 2.1.3. Strumenti per Linux
- 2.1.4. Strumenti per MacOS

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

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

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

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

2.6. Rilevatori di *phishing*
- 2.6.1. Rilevamento del *phishing* manualmente
- 2.6.2. Strumenti *antiphishing*

2.7. *Spyware*
- 2.7.1. Meccanismi di prevenzione
- 2.7.2. Strumenti *antispyware*

2.8. Tracciatori
- 2.8.1. Misure di protezione del sistema
- 2.8.2. Strumenti anti-tracciamento

2.9. EDR-*End Point Detection and Response*
- 2.9.1. Comportamento del sistema EDR
- 2.9.2. Differenze tra EDR e antivirus
- 2.9.3. Il futuro dei sistemi EDR

2.10. Controllo dell'installazione del *software*
- 2.10.1. Archivio e negozi di *software*
- 2.10.2. Elenchi di *software* consentiti o vietati
- 2.10.3. Criteri di aggiornamento
- 2.10.4. Privilegi di installazione del *software*

Modulo 3. Sicurezza di rete (perimetro)

3.1. Sistemi di rilevamento e prevenzione delle minacce
- 3.1.1. Quadro generale per gli incidenti di sicurezza
- 3.1.2. Sistemi di difesa attuali: *Defense in Depth* e SOC
- 3.1.3. Le attuali architetture di rete
- 3.1.4. Tipi di strumenti di rilevamento e prevenzione degli incidenti
  - 3.1.4.1. Sistemi basati sulla rete
  - 3.1.4.2. Sistemi basati su *host*
  - 3.1.4.3. Sistemi centralizzati
- 3.1.5. Comunicazione e scoperta di istanze/*hosts*, container e serverless

3.2. Firewall
- 3.2.1. Tipi di Firewall
- 3.2.2. Attacchi e contenimento
- 3.2.3. Firewall comuni in *kernel* Linux
  - 3.2.3.1. UFW
  - 3.2.3.2. *Nftables e iptables*
  - 3.2.3.3. Firewalld
- 3.2.4. Sistemi di rilevamento basati sui log di sistema
  - 3.2.4.1. TCP Wrappers
  - 3.2.4.2. BlockHosts e DenyHosts
  - 3.2.4.3. Fai2ban

3.3. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 3.3.1. Attacchi agli IDS/IPS
- 3.3.2. Sistemi IDS/IPS
  - 3.3.2.1. Snort
  - 3.3.2.2. Suricata

3.4. Firewall di nuova generazione (NGFW)
- 3.4.1. Differenze tra NGFW e Firewall tradizionali
- 3.4.2. Funzionalità chiave
- 3.4.3. Soluzioni commerciali
- 3.4.4. Firewall per servizi *Cloud*
  - 3.4.4.1. Architettura *Cloud* VPC
  - 3.4.4.2. ACL per il*Cloud*
  - 3.4.4.3. Security Group

3.5. *Proxy*
- 3.5.1. Tipi di *Proxy*
- 3.5.2. Uso di *Proxy*. Vantaggi e svantaggi

3.6. Motori antivirus
- 3.6.1. Contesto generale del *Malware* degli IoC
- 3.6.2. Problemi del motore antivirus

3.7. Sistemi di protezione della posta
- 3.7.1. Antispam
  - 3.7.1.1. Whitelisting e blacklisting
  - 3.7.1.2. Filtri bayesiani
- 3.7.2. Mail Gateway (MGW)

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

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

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

Modulo 4. Sicurezza degli smartphone

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

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

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

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

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

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

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

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

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

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

Modulo 5. Sicurezza in IoT

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

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

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

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

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

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

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

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

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

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

Modulo 6. Hacking etico

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

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

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

6.4. Scansione di rete
- 6.4.1. Strumenti di scansione
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Altri strumenti di scansione

6.4.2. Tecniche di Scansione
6.4.3. Tecniche di elusione di firewall e IDS
6.4.4. *Banner Grabbing*
6.4.5. Diagrammi di rete
6.5. Enumerazione
6.5.1. Enumerazione SMTP
6.5.2. Enumerazione DNS
6.5.3. Enumerazione NetBIOS e Samba
6.5.4. Enumerazione LDAP
6.5.5. Enumerazione SNMP
6.5.6. Altre tecniche di Enumerazione
6.6. Analisi delle vulnerabilità
6.6.1. Soluzioni per l'Analisi dei punti deboli
6.6.1.1. Qualys
6.6.1.2. Nessus
6.6.1.3. CFI LanGuard
6.6.2. Sistemi di punteggio dei punti deboli
6.6.2.1. CVSS
6.6.2.2. CVE
6.6.2.3. NVD
6.7. Attacchi alle reti wireless
6.7.1. Metodologia di hacking nelle reti wireless
6.7.1.1. Wi-Fi *Discovery*
6.7.1.2. Analisi del traffico
6.7.1.3. Attacchi *aircrack*
6.7.1.3.1. Attacchi WEP
6.7.1.3.2. Attacchi WPA/WPA2
6.7.1.4. Attacchi *Evil Twin*
6.7.1.5. Attacchi WPS
6.7.1.6. *Jamming*
6.7.2. Strumenti per la sicurezza wireless
6.8. Hacking di server web
6.8.1. *Cross Site Scripting*
6.8.2. CSRF
6.8.3. *Session Hijacking*
6.8.4. *SQLinjection*
6.9. Sfruttamento dei punti deboli
6.9.1. Utilizzo di *Exploit* noti
6.9.2. Utilizzo di *metasploit*
6.9.3. Utilizzo di *malware*
6.9.3.1. Definizione e campo di applicazione
6.9.3.2. Generazione di *Malware*
6.9.3.3. Bypassare le soluzioni antivirus
6.10. Persistenza
6.10.1. Installazione di *Rootkit*
6.10.2. Utilizzo di Ncat
6.10.3. Utilizzo di attività pianificate per le *Backdoor*
6.10.4. Creazione di utenti
6.10.5. Rilevamento HIDS

Modulo 7. Ingegneria inversa

7.1. I compilatori
7.1.1. Tipi di codici
7.1.2. Fasi di un compilatore
7.1.3. Tabella dei simboli
7.1.4. Gestione degli errori
7.1.5. Compilatore GCC
7.2. Tipi di analisi nei compilatori
7.2.1. Analisi lessicale
7.2.1.1. Terminologia
7.2.1.2. Componenti lessicali
7.2.1.3. Analizzatore lessicale LEX

7.2.2. Analisi sintattica
7.2.2.1. Grammatiche libere dal contesto
7.2.2.2. Tipi di analisi sintattica
7.2.2.2.1. Analisi top-down
7.2.2.2.2. Analisi bottom-up
7.2.2.3. Alberi sintattici e derivazioni
7.2.2.4. Tipi di analizzatori sintattici
7.2.2.4.1. Analizzatori LR (*Left To Right*)
7.2.2.4.2. Analizzatori LALR
7.2.3. Analisi semantica
7.2.3.1. Grammatiche di attributi
7.2.3.2. Attribuiti a S
7.2.3.3. Attribuiti a L
7.3. Strutture dati dell'assemblatore
7.3.1. Variabili
7.3.2. Array
7.3.3. Puntatori
7.3.4. Struttura
7.3.5. Obiettivi
7.4. Strutture del codice assembly
7.4.1. Strutture di selezione
7.4.1.1. *If, else if, Else*
7.4.1.2. *Switch*
7.4.2. Strutture di iterazione
7.4.2.1. *For*
7.4.2.2. *While*
7.4.2.3. Uso del *break*
7.4.3. Funzioni
7.5. Architettura Hardware x86
7.5.1. Architettura dei processori x86
7.5.2. Strutture dati x86
7.5.3. Strutture di codice x86
7.6. Architettura hardware ARM
7.6.1. Architettura dei processori ARM
7.6.2. Strutture dati ARM
7.6.3. Strutture di codice ARM
7.7. Strutture di codice ARM
7.7.1. Disassemblatori
7.7.2. IDA
7.7.3. Ricostruttori di codici
7.8. Analisi dinamica del codice
7.8.1. Analisi del comportamento
7.8.1.1. Comunicazioni
7.8.1.2. Monitoraggio
7.8.2. Debugger di codice Linux
7.8.3. Debugger di codice Windows
7.9. *Sandbox*
7.9.1. Architettura *sandbox*
7.9.2. Evasione del *sandbox*
7.9.3. Tecniche di rilevamento
7.9.4. Tecniche di evasione
7.9.5. Contromisure
7.9.6. *Sandbox* su Linux
7.9.7. *Sandbox* su Windows
7.9.8. *Sandbox* su MacOS
7.9.9. *Sandbox* su Android
7.10. Analisi dei *malware*
7.10.1. Metodi di analisi dei *malware*
7.10.2. Tecniche di offuscamento del *malware*
7.10.2.1. Offuscamento degli eseguibili
7.10.2.2. Limitazione degli ambienti di esecuzione
7.10.3. Strumenti di analisi dei *malware*

Modulo 8. Sviluppo sicuro

8.1. Sviluppo sicuro
- 8.1.1. Qualità, funzionalità e sicurezza
- 8.1.2. Riservatezza, integrità e disponibilità
- 8.1.3. Ciclo di vita dello sviluppo del *software*

8.2. Fase dei requisiti
- 8.2.1. Controllo dell'autenticazione
- 8.2.2. Controllo dei ruoli e dei privilegi
- 8.2.3. Requisiti orientati al rischio
- 8.2.4. Approvazione dei privilegi

8.3. Fasi di analisi e progettazione
- 8.3.1. Accesso ai componenti e amministrazione del sistema
- 8.3.2. Tracce di audit
- 8.3.3. Gestione delle sessioni
- 8.3.4. Dati storici
- 8.3.5. Gestione appropriata degli errori
- 8.3.6. Separazione delle funzioni

8.4. Fase di implementazione e codifica
- 8.4.1. Protezione dell'ambiente di sviluppo
- 8.4.2. Preparazione della documentazione tecnica
- 8.4.3. Codifica sicura
- 8.4.4. Sicurezza nelle comunicazioni

8.5. Buone pratiche di codifica sicura
- 8.5.1. Convalida dei dati di ingresso
- 8.5.2. Codifica dei dati di uscita
- 8.5.3. Stile di programmazione
- 8.5.4. Gestione dei log delle modifiche
- 8.5.5. Pratiche crittografiche
- 8.5.6. Gestione degli errori e dei log
- 8.5.7. Gestione degli archivi
- 8.5.8. Gestione della Memoria
- 8.5.9. Standardizzazione e riutilizzo delle funzioni di sicurezza

8.6. Preparazione del server e *hardening*
- 8.6.1. Gestione di utenti, gruppi e ruoli sul server
- 8.6.2. Installazione *software*
- 8.6.3. *Hardening* del server
- 8.6.4. Configurazione robusta del contesto di applicazione

8.7. Preparazione della Base di Dati e dell'*hardening*
- 8.7.1. Ottimizzazione del motore della Base di Dati
- 8.7.2. Creare un proprio utente per l'applicazione
- 8.7.3. Assegnazione dei privilegi necessari all'utente
- 8.7.4. *Hardening* del database

8.8. Fase di test
- 8.8.1. Controllo qualità negli audit di sicurezza
- 8.8.2. Ispezione del codice per fasi
- 8.8.3. Verifica della gestione delle configurazioni
- 8.8.4. Modello black box

8.9. Preparare il passaggio alla produzione
- 8.9.1. Eseguire il controllo delle modifiche
- 8.9.2. Eseguire la procedura di cambio produzione
- 8.9.3. Eseguire la procedura di *rollback*
- 8.9.4. Test di pre-produzione

8.10. Fase di manutenzione
- 8.10.1. Garanzia basata sul rischio
- 8.10.2. Test di manutenzione della sicurezza white box
- 8.10.3. Test di manutenzione della sicurezza black box

Modulo 9. Implementazione pratica delle politiche di sicurezza del *software* e dell'hardware

9.1. Implementazione pratica delle politiche di sicurezza del *software* e dell'hardware
- 9.1.1. Implementazione dell'identificazione e dell'autorizzazione
- 9.1.2. Implementazione delle tecniche di identificazione
- 9.1.3. Misure tecniche per l'autorizzazione

9.2. Tecnologie di identificazione e autorizzazione
- 9.2.1. Identificatore e OTP
- 9.2.2. Token USB o smart card PKI
- 9.2.3. Il tasto "Difesa riservata"
- 9.2.4. Il RFID Attivo

9.3. Politiche di sicurezza per l'accesso al *software* e ai sistemi
- 9.3.1. Implementazione delle politiche di controllo degli accessi
- 9.3.2. Implementazione delle politiche di accesso alle comunicazioni
- 9.3.3. Tipi di strumenti di sicurezza per il controllo degli accessi

9.4. Gestione degli accessi degli utenti
- 9.4.1. Gestione dei diritti di accesso
- 9.4.2. Segregazione dei ruoli e delle funzioni di accesso
- 9.4.3. Implementazione dei diritti di accesso nei sistemi

9.5. Controllo dell'accesso ai sistemi e alle applicazioni
- 9.5.1. Regola minima di accesso
- 9.5.2. Tecnologie di accesso sicuro
- 9.5.3. Politiche di sicurezza delle password

9.6. Tecnologie per i sistemi di identificazione
- 9.6.1. Directory attiva
- 9.6.2. OTP
- 9.6.3. PAP, CHAP
- 9.6.4. KERBEROS, DIAMETER, NTLM

9.7. CIS Controlli per il basamento del sistema
- 9.7.1. Controlli CIS di base
- 9.7.2. Controlli CIS fondamentali
- 9.7.3. Controlli CIS organizzativi

9.8. Sicurezza operativa
- 9.8.1. Protezione contro il codice maligno
- 9.8.2. Copie di backup
- 9.8.3. Registro di attività e monitoraggio

9.9. Gestione delle vulnerabilità tecniche
- 9.9.1. Vulnerabilità tecniche
- 9.9.2. Gestione delle vulnerabilità tecniche
- 9.9.3. Restrizioni all'installazione del *software*

9.10. Implementazione delle pratiche di politica di sicurezza
- 9.10.1. Vulnerabilità logiche
- 9.10.2. Implementazione delle politiche di difesa

Modulo 10. Analisi forense

10.1. Acquisizione e riproduzione dei dati
- 10.1.1. Acquisizione della memoria volatile
  - 10.1.1.1. Informazione del sistema
  - 10.1.1.2. Informazione della rete
  - 10.1.1.3. Ordine di volatilità
- 10.1.2. Acquisizione dei dati statici
  - 10.1.2.1. Creazione di un'immagine duplicata
  - 10.1.2.2. Preparazione di un documento per la catena di custodia
- 10.1.3. Metodi di validazione dei dati acquisiti
  - 10.1.3.1. Metodi per Linux
  - 10.1.3.2. Metodi per Windows

10.2. Valutazione e sconfitta delle tecniche antiforensi
- 10.2.1. Obiettivi delle tecniche antiforensi
- 10.2.2. Cancellazione dei dati
  - 10.2.2.1. Cancellazione di dati e file
  - 10.2.2.2. Recupero dei file
  - 10.2.2.3. Recupero di partizioni eliminate
- 10.2.3. Protezione con password
- 10.2.4. Steganografia
- 10.2.5. Cancellazione sicura del *dispositivo*
- 10.2.6. Crittografia

10.3. Analisi forense del sistema operativo
- 10.3.1. Analisi forense di Windows
- 10.3.2. Analisi forense di Linux
- 10.3.3. Analisi forense di Mac

10.4. Analisi forense della rete
- 10.4.1. Analisi dei Log
- 10.4.2. Correlazione dei dati
- 10.4.3. Ricerca di rete
- 10.4.4. Passi da seguire nell'analisi forense della rete

10.5. Analisi forense web
- 10.5.1. Indagine sugli attacchi web
- 10.5.2. Rilevamento degli attacchi
- 10.5.3. Localizzazione degli indirizzi IP

10.6. Analisi forense dei Database
- 10.6.1. Analisi forense MSSQL
- 10.6.2. Analisi forense MySQL
- 10.6.3. Analisi forense PostgreSQL
- 10.6.4. Analisi forense MongoDB

10.7. Analisi forense *Cloud*
- 10.7.1. Tipi di reati nel *Cloud*
  - 10.7.1.1. *Cloud* come soggetto
  - 10.7.1.2. *Cloud* come oggetto
  - 10.7.1.3. *Cloud* come strumento
- 10.7.2. Sfide dell'analisi forense *Cloud*
- 10.7.3. Ricerca sui servizi di archiviazione in *Cloud*
- 10.7.4. Strumenti di analisi forense *Cloud*

10.8. Investigazione dei crimini informatici via email
- 10.8.1. Sistemi di posta elettronica
  - 10.8.1.1. Client di posta
  - 10.8.1.2. Server di posta
  - 10.8.1.3. Server SMTP
  - 10.8.1.4. Server POP3
  - 10.8.1.5. Server IMAP4
- 10.8.2. Reati di posta elettronica
- 10.8.3. Messaggio di posta elettronica
  - 10.8.3.1. Intestazioni standard
  - 10.8.3.2. Intestazioni estese
- 10.8.4. Fasi dell'indagine su questi reati
- 10.8.5. Strumenti forensi per la posta elettronica

10.9. Analisi forense mobile
- 10.9.1. Reti cellulari
  - 10.9.1.1. Tipi di reti
  - 10.9.1.2. Contenuti del CDR
- 10.9.2. *Subscriber Identity Module* (SIM)
- 10.9.3. Acquisizione logica
- 10.9.4. Acquisizione fisica
- 10.9.5. Acquisizione del file system

10.10. Redazione e presentazione di rapporti forensi
- 10.10.1. Aspetti importanti di un rapporto forense
- 10.10.2. Classificazione e tipi di rapporti
- 10.10.3. Guida per scrivere un rapporto
- 10.10.4. Presentazione del rapporto
  - 10.10.4.1. Preparazione preventiva alla testimonianza
  - 10.10.4.2. Deposizione
  - 10.10.4.3. Rapporti con i media

Modulo 11. Sicurezza nella progettazione e nello sviluppo dei sistemi

11.1. Sistemi di informazioni
- 11.1.1. Ambiti di applicazione di un sistema di informazione
- 11.1.2. Componenti di un sistema di informazione
- 11.1.3. Attività di un sistema di informazione
- 11.1.4. Ciclo di vita di applicazione di un sistema di informazione
- 11.1.5. Risorse di un sistema di informazione

11.2. Sistemi di informazioni: Tipologia
- 11.2.1. Tipi di sistema di informazione
  - 11.2.1.1. Aziendale
  - 11.2.1.2. Strategici
  - 11.2.1.3. In base all'ambito di applicazione
  - 11.2.1.4. Specifici
- 11.2.2. Sistemi di informazioni: Esempi reali
- 11.2.3. Evoluzione del sistema di informazione: Fasi
- 11.2.4. Metodologie del sistema di informazione

11.3. Sicurezza del sistema di informazione: Implicazioni giuridiche
- 11.3.1. Accesso ai dati
- 11.3.2. Minacce alla sicurezza: Vulnerabilità
- 11.3.3. Implicazioni giuridiche: Reati
- 11.3.4. Procedure di mantenimento di un sistema di informazione

11.4. Sicurezza del sistema di informazione: Protocolli di sicurezza
- 11.4.1. Sicurezza di un sistema di informazione
  - 11.4.1.1. Integrità
  - 11.4.1.2. Riservatezza
  - 11.4.1.3. Disponibilità
  - 11.4.1.4. Autenticazione
- 11.4.2. Servizi di sicurezza
- 11.4.3. Protocolli di sicurezza delle informazioni: Tipologia
- 11.4.4. Sensibilità di un sistema di informazione

11.5. Sicurezza in sistema di informazione: Misure e sistemi di controllo degli accessi
- 11.5.1. Misure di sicurezza
- 11.5.2. Tipo di misure di sicurezza
  - 11.5.2.1. Prevenzione
  - 11.5.2.2. Screening
  - 11.5.2.3. Correzione
- 11.5.3. Sistema di controllo degli accessi: Tipologia
- 11.5.4. Crittografia

11.6. Sicurezza di rete e Internet
- 11.6.1. Firewall
- 11.6.2. Identificazione digitale
- 11.6.3. Virus e worm
- 11.6.4. Hacking
- 11.6.5. Esempi e casi reali

11.7. Reati informatici
- 11.7.1. Reato informatico
- 11.7.2. Reati informatici: Tipologia
- 11.7.3. Reati informatici: Attacco. Tipologie
- 11.7.4. Il caso della realtà virtuale
- 11.7.5. Profili degli colpevoli e delle vittime. Penalizzazione del reato
- 11.7.6. Reati informatici: Esempi e casi reali

11.8. Piano di sicurezza in sistema di informazione
- 11.8.1. Piano di sicurezza: Obiettivi
- 11.8.2. Piano di sicurezza: Pianificazione
- 11.8.3. Piano di rischio: Analisi
- 11.8.4. Politica di sicurezza: Implementazione nell'organizzazione
- 11.8.5. Piano di sicurezza: Implementazione nell'organizzazione
- 11.8.6. Procedure di sicurezza: Tipologie
- 11.8.7. Piani di sicurezza: Esempi

11.9. Piano di contingenza
- 11.9.1. Piano di contingenza: Funzioni
- 11.9.2. Piano di emergenza: Elementi e obiettivi
- 11.9.3. Piani di contingenza all'interno dell'organizzazione: Implementazione
- 11.9.4. Piano di contingenza: Esempi

11.10. Governance della sicurezza dei sistemi informazione
- 11.10.1. Normativa legale
- 11.10.2. Standard
- 11.10.3. Certificazioni
- 11.10.4. Tecnologie

Modulo 12. Strutture e modelli per la sicurezza delle informazioni

12.1. Architettura di sicurezza delle informazioni
- 12.1.1. ISMS/PDS
- 12.1.2. Allineamento strategico
- 12.1.3. Gestione del rischio
- 12.1.4. Misurazione della performance

12.2. Modelli di sicurezza delle informazioni
- 12.2.1. In base alle politiche di sicurezza
- 12.2.2. In base agli strumenti di protezione
- 12.2.3. In base alle apparecchiature di lavoro

12.3. Modello di sicurezza. Componenti chiave
- 12.3.1. Identificazione dei rischi
- 12.3.2. Definizione dei controlli
- 12.3.3. Valutazione continua dei livelli di rischio
- 12.3.4. Piano di sensibilizzazione per dipendenti, fornitori, partner, ecc.

12.4. Processo di gestione dei rischi
- 12.4.1. Identificazione delle risorse
- 12.4.2. Identificazione delle minacce
- 12.4.3. Valutazione dei rischi
- 12.4.4. Priorità dei controlli
- 12.4.5. Rivalutazione e rischio residuo

12.5. Processi di business e sicurezza delle informazioni
- 12.5.1. Processi aziendali
- 12.5.2. Valutazione del rischio in base ai parametri aziendali
- 12.5.3. Analisi dell'impatto aziendale
- 12.5.4. Operazioni aziendali e sicurezza delle informazioni

12.6. Processo di miglioramento continuo
- 12.6.1. Il ciclo di Deming
  - 12.6.1.1. Pianificare
  - 12.6.1.2. Fare
  - 12.6.1.3. Verificare
  - 12.6.1.4. Agire

12.7. Architetture di sicurezza
- 12.7.1. Selezione e omogeneizzazione delle tecnologie
- 12.7.2. Gestione dell'identità. Autenticazione
- 12.7.3. Gestione degli accessi. Autorizzazione
- 12.7.4. Sicurezza dell'infrastruttura di rete
- 12.7.5. Tecnologie e soluzioni di crittografia
- 12.7.6. Sicurezza delle apparecchiature terminali (EDR)

12.8. Quadro normativo
- 12.8.1. Regolamenti settoriali
- 12.8.2. Certificazioni
- 12.8.3. Legislazione

12.9. Standard ISO 27001
- 12.9.1. Implementazione
- 12.9.2. Certificazione
- 12.9.3. Verifiche e penetration test
- 12.9.4. Gestione continua del rischio
- 12.9.5. Classificazione di Sicurezza delle Informazioni

12.10. Legislazione sulla privacy: RGPD (GDPR)
- 12.10.1. Ambito di applicazione del Regolamento generale sulla protezione dei dati (RGPD)
- 12.10.2. Dati personali
- 12.10.3. Ruoli nel trattamento dei dati personali
- 12.10.4. Diritti ARCO
- 12.10.5. Il DPO: Funzioni

Modulo 13. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

13.1. Sicurezza di Sicurezza delle Informazioni: Aspetti fondamentali
- 13.1.1. Sicurezza di Sicurezza delle Informazioni
  - 13.1.1.1. Riservatezza
  - 13.1.1.2. Integrità
  - 13.1.1.3. Disponibilità
  - 13.1.1.4. Misure di sicurezza delle informazioni

13.2. Sistema di Gestione della Sicurezza delle Informazioni (SGSI)
- 13.2.1. Modelli di gestione di sicurezza delle informazioni
- 13.2.2. Documenti per l'implementazione di un SGSI
- 13.2.3. Documenti per l'implementazione di un SGSI

13.3. Norme e standard internazionali
- 13.3.1. Standard internazionali di Sicurezza delle Informazioni
- 13.3.2. Origine ed evoluzione dello standard
- 13.3.3. Standard internazionali di Sicurezza delle Informazioni
- 13.3.4. Altri standard di riferimento

13.4. Norme ISO/IEC 27.000
- 13.4.1. Scopo e campo di applicazione
- 13.4.2. Struttura della norma
- 13.4.3. Certificazione
- 13.4.4. Fasi dell'accreditamento
- 13.4.5. Vantaggi delle norme ISO/IEC 27.000

13.5. Progettazione e implementazione di un Sistema Generale di Sicurezza delle informazioni
- 13.5.1. Fasi di implementazione di un Sistema Generale di Sicurezza delle informazioni
- 13.5.2. Piano di continuità operativa

13.6. Fase I: diagnosi
- 13.6.1. Diagnosi preliminare
- 13.6.2. Identificazione del livello di stratificazione
- 13.6.3. Livello di conformità agli standard/norme

13.7. Fase II: Preparazione
- 13.7.1. Contesto dell'Organizzazione
- 13.7.2. Analisi delle norme di sicurezza applicabili
- 13.7.3. Ambito di applicazione del Sistema Generale di Sicurezza delle Informazioni
- 13.7.4. Politica del Sistema Generale di Sicurezza delle informazioni
- 13.7.5. Obiettivi del Sistema Generale di Sicurezza delle informazioni

13.8. Fase III: Pianificazione
- 13.8.1. Classificazione degli asset
- 13.8.2. Valutazione del rischio
- 13.8.3. Identificazione delle minacce e dei rischi

13.9. Fase IV: Attuazione e monitoraggio
- 13.9.1. Analisi dei risultati
- 13.9.2. Assegnazione di responsabilità
- 13.9.3. Tempistica del piano d'azione
- 13.9.4. Monitoraggio e audit

13.10. Politiche di sicurezza per la gestione degli incidenti
- 13.10.1. Fasi
- 13.10.2. Categorizzazione degli incidenti
- 13.10.3. Gestione degli incidenti e procedure

Modulo 14. Gestione della sicurezza IT

14.1. Gestione della sicurezza
- 14.1.1. Operazioni di sicurezza
- 14.1.2. Aspetti giuridici e normativi
- 14.1.3. Abilitazione all'esercizio dell'attività
- 14.1.4. Gestione dei rischi
- 14.1.5. Gestione dell'identità e degli accessi

14.2. Struttura dell'area di sicurezza. L'ufficio del CISO
- 14.2.1. Struttura organizzativa. Posizione del CISO nella struttura
- 14.2.2. Linee di difesa
- 14.2.3. Organigramma dell'ufficio del CISO
- 14.2.4. Gestione del bilancio

14.3. Governance della sicurezza
- 14.3.1. Comitato per la sicurezza
- 14.3.2. Comitato per il monitoraggio dei rischi
- 14.3.3. Comitato per il controllo
- 14.3.4. Comitato per le crisi

14.4. Governance della sicurezza. Funzioni
- 14.4.1. Politiche e standard
- 14.4.2. Piano generale di sicurezza
- 14.4.3. Quadro di controllo
- 14.4.4. Consapevolezza e formazione
- 14.4.5. Sicurezza della catena di approvvigionamento

14.5. Operazioni di sicurezza
- 14.5.1. Gestione dell'identità e degli accessi
- 14.5.2. Configurazione delle regole di sicurezza della rete. Firewall
- 14.5.3. Gestione di piattaforme IDS/IPS
- 14.5.4. Analisi dei punti deboli

14.6. Quadro di riferimento per la cybersecurity. NIST CSF
- 14.6.1. Metodologia NIST
  - 14.6.1.1. Identificare
  - 14.6.1.2. Proteggere
  - 14.6.1.3. Rilevare
  - 14.6.1.4. Rispondere
  - 14.6.1.5. Recuperare

14.7. Centro operativo di sicurezza (SOC). Funzioni
- 14.7.1. Protezione. *Red Team, pentesting, threat intelligence*
- 14.7.2. Rilevamento. SIEM, *user behavior analytics, fraud prevention*
- 14.7.3. Risposta

14.8. Audit di sicurezza
- 14.8.1. Penetration test
- 14.8.2. Esercizi di red *team*
- 14.8.3. Verifiche del codice sorgente: Sviluppo sicuro
- 14.8.4. Sicurezza dei componenti (*software supply chain*)
- 14.8.5. Analisi forense

14.9. Risposta agli incidenti
- 14.9.1. Preparazione
- 14.9.2. Rilevamento, analisi e reporting
- 14.9.3. Contenimento, eliminazione e recupero
- 14.9.4. Attività in seguito all'incidente
  - 14.9.4.1. Conservazione delle prove
  - 14.9.4.2. Analisi forense
  - 14.9.4.3. Gestire una violazione dei dati
- 14.9.5. Guide ufficiali per la gestione degli incidenti informatici

14.10. Gestione delle vulnerabilità
- 14.10.1. Analisi dei punti deboli
- 14.10.2. Valutazione della vulnerabilità
- 14.10.3. Base di sistema
- 14.10.4. Vulnerabilità 0-day. Zero-day

Modulo 15. Politiche di gestione degli incidenti di sicurezza

15.1. Politiche e miglioramenti per la gestione degli incidenti di sicurezza delle informazioni
- 15.1.1. Gestione degli imprevisti
- 15.1.2. Responsabilità e procedure
- 15.1.3. Notifica dell'evento

15.2. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 15.2.1. Dati di funzionamento del sistema
- 15.2.2. Tipi di sistemi di rilevamento delle intrusioni
- 15.2.3. Criteri di posizionamento degli IDS/IPS

15.3. Risposta agli incidenti di sicurezza
- 15.3.1. Procedura di sistema di informazione
- 15.3.2. Processo di verifica dell'intrusione
- 15.3.3. Organi del CERT

15.4. Processo di notifica e gestione dei tentativi di intrusione
- 15.4.1. Responsabilità nel processo di notifica
- 15.4.2. Classificazione degli incidenti
- 15.4.3. Processo di risoluzione e recupero

15.5. L'analisi forense come politica di sicurezza
- 15.5.1. Prove volatili e non volatili
- 15.5.2. Analisi e raccolta di prove elettroniche
  - 15.5.2.1. Analisi delle prove elettroniche
  - 15.5.2.2. Raccolta di prove elettroniche

15.6. Strumenti di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 15.6.1. Snort
- 15.6.2. Suricata
- 15.6.3. Solar-Winds

15.7. Strumenti di centralizzazione degli eventi
- 15.7.1. SIM
- 15.7.2. SEM
- 15.7.3. SIEM

15.8. Guida alla sicurezza CCN-STIC
- 15.8.1. Gestione degli incidenti informatici
- 15.8.2. Metriche e Indicatori

15.9. NIST SP800-61
- 15.9.1. Capacità di risposta agli incidenti di sicurezza informatica
- 15.9.2. Gestione degli incidenti
- 15.9.3. Coordinamento e informazione condivisa

15.10. Norma ISO 27035
- 15.10.1. Norma ISO 27035. Principi di gestione degli incidenti
- 15.10.2. Linee guida per lo sviluppo di un piano di gestione degli incidenti
- 15.10.3. Linee guida per le operazioni di risposta agli incidenti

Modulo 16. Analisi dei rischi e ambiente di sicurezza IT

16.1. Analisi del contesto
- 16.1.1. Analisi della situazione economica
  - 16.1.1.1. Ambienti VUCA
    - 16.1.1.1.1. Volatilità
    - 16.1.1.1.2. Incertezza
    - 16.1.1.1.3. Complessità
    - 16.1.1.1.4. Ambiguità
  - 16.1.1.2. Ambienti BANI
    - 16.1.1.2.1. Fragilità
    - 16.1.1.2.2. Ansia
    - 16.1.1.2.3. Non linearità
    - 16.1.1.2.4. Incomprensibilità
- 16.1.2. Analisi del contesto generale PESTEL
  - 16.1.2.1. Politico
  - 16.1.2.2. Economico
  - 16.1.2.3. Sociale
  - 16.1.2.4. Tecnologica
  - 16.1.2.5. Ecologica/Ambientale
  - 16.1.2.6. Giuridica
- 16.1.3. Analisi della situazione interna. SWOT
  - 16.1.3.1. Obiettivi
  - 16.1.3.2. Minacce
  - 16.1.3.3. Opportunità
  - 16.1.3.4. Punti di forza

16.2. Rischio e incertezza
- 16.2.1. Rischio
- 16.2.2. Gestione del rischio
- 16.2.3. Standard di gestione del rischio

16.3. Linee guida per la gestione del rischio ISO 31.000:2018
- 16.3.1. Oggetto
- 16.3.2. Principi
- 16.3.3. Quadro di riferimento
- 16.3.4. Processo

16.4. Metodologia per l'analisi e la gestione dei rischi dei sistemi di informazione (MAGERIT)
- 16.4.1. Metodologia MAGERIT
  - 16.4.1.1. Obiettivi
  - 16.4.1.2. Metodologia
  - 16.4.1.3. Elementi
  - 16.4.1.4. Tecniche
  - 16.4.1.5. Strumenti disponibili (PILAR)

16.5. Trasferimento del rischio informatico
- 16.5.1. Trasferimento del rischio
- 16.5.2. Rischi informatici. Tipologia
- 16.5.3. Assicurazione contro i rischi informatici

16.6. Metodologie agili per la gestione del rischio
- 16.6.1. Metodologie agili
- 16.6.2. Scrum per la gestione del rischio
- 16.6.3. *Agile risk management*

16.7. Tecnologie per la gestione del rischio
- 16.7.1. Intelligenza artificiale applicata alla gestione del rischio
- 16.7.2. *Blockchain* e crittografia. Metodi di conservazione del valore
- 16.7.3. Computazione quantistica Opportunità o minaccia

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

16.9. *Risk-Driven* nella gestione del rischio
- 16.9.1. *Risk driven*
- 16.9.2. *Risk-Driven* nella gestione del rischio
- 16.9.3. Sviluppo di un modello di gestione aziendale orientato al rischio

16.10. Innovazione e trasformazione digitale nella gestione del rischio IT
- 16.10.1. La gestione del rischio agile come fonte di innovazione aziendale
- 16.10.2. Trasformazione di dati informazione utile per il processo decisionale
- 16.10.3. Visione olistica dell'impresa tramite il rischio

Modulo 17. Politiche di Sicurezza per l'Analisi delle Minacce dei Sistemi Informatici

17.1. Gestione delle minacce nelle politiche di sicurezza
- 17.1.1. Gestione del rischio
- 17.1.2. Rischio per la sicurezza
- 17.1.3. Metodologie di gestione delle minacce
- 17.1.4. Implementazione delle metodologie

17.2. Fasi della gestione delle minacce
- 17.2.1. Identificazione
- 17.2.2. Analisi
- 17.2.3. Localizzazione
- 17.2.4. Misure di salvaguardia

17.3. Sistemi di audit per la localizzazione delle minacce
- 17.3.1. Classificazione e flusso di informazione
- 17.3.2. Analisi dei processi vulnerabili

17.4. Classificazione del rischio
- 17.4.1. Tipi di rischio
- 17.4.2. Calcolo della probabilità di rischio
- 17.4.3. Rischio residuo

17.5. Trattamento del rischio
- 17.5.1. Attuazione delle misure di salvaguardia
- 17.5.2. Trasferimento o assunzione

17.6. Controllo del rischio
- 17.6.1. Processo continuo di gestione del rischio
- 17.6.2. Implementazione di metriche di sicurezza
- 17.6.3. Modello strategico delle metriche di sicurezza delle informazioni

17.7. Metodologie pratiche per l'analisi e il controllo delle minacce
- 17.7.1. Catalogo delle minacce
- 17.7.2. Catalogo delle misure di controllo
- 17.7.3. Catalogo delle misure di sicurezza

17.8. Norma ISO 27005
- 17.8.1. Identificazione del rischio
- 17.8.2. Analisi del rischio
- 17.8.3. Valutazione del rischio

17.9. Matrice dei rischi, degli impatti e delle minacce
- 17.9.1. Dati, sistemi e personale
- 17.9.2. Probabilità di minaccia
- 17.9.3. Entità del danno

17.10. Progettazione di fasi e processi nell'analisi dei pericoli
- 17.10.1. Identificazione degli elementi critici dell'organizzazione
- 17.10.2. Determinazione delle minacce e degli impatti
- 17.10.3. Analisi degli impatti e dei rischi
- 17.10.4. Metodologie

Modulo 18. Implementazione Pratica di Politiche di Sicurezza contro gli Attacchi

18.1. *System Hacking*
- 18.1.1. Rischi e vulnerabilità
- 18.1.2. Contromisure

18.2. DoS nei servizi
- 18.2.1. Rischi e vulnerabilità
- 18.2.2. Contromisure

18.3. *Session Hijacking*
- 18.3.1. Il processo di Hijacking
- 18.3.2. Contromisure al Hijacking

18.4. Evasione di IDS *Firewalls and Honeypots*
- 18.4.1. Tecniche di evasione
- 18.4.2. Implementazione di contromisure

18.5. *Hacking Web Servers*
- 18.5.1. Attacchi ai server Web
- 18.5.2. Implementazione delle misure di difesa

18.6. *Hacking Web Applications*
- 18.6.1. Attacchi alle applicazioni web
- 18.6.2. Implementazione delle misure di difesa

18.7. *Hacking Wireless Networks*
- 18.7.1. Vulnerabilità nelle reti wifi
- 18.7.2. Implementazione delle misure di difesa

18.8. *Hacking Mobile Platforms*
- 18.8.1. Punti deboli di piattaforme mobili
- 18.8.2. Implementazione di contromisure

18.9. *Ransomware*
- 18.9.1. Vulnerabilità che causano *Ransomware*
- 18.9.2. Implementazione di contromisure

18.10. Ingegneria sociale
- 18.10.1. Tipi di ingegneria sociale
- 18.10.2. Contromisure per l'ingegneria sociale

Modulo 19. La crittografia nell'IT

19.1. Crittografia
- 19.1.1. Crittografia
- 19.1.2. Fondamenti matematici

19.2. Criptologia
- 19.2.1. Criptologia
- 19.2.2. Crittoanalisi
- 19.2.3. Steganografia e stegoanalisi

19.3. Protocolli crittografici
- 19.3.1. Blocchi di base
- 19.3.2. Protocolli di base
- 19.3.3. Protocolli intermedi
- 19.3.4. Protocolli avanzati
- 19.3.5. Protocolli esoterici

19.4. Tecniche crittografiche
- 19.4.1. Lunghezza della chiave di crittografia
- 19.4.2. Gestione delle chiavi
- 19.4.3. Tipi di algoritmi
- 19.4.4. Funzioni di riepilogo. *Hash*
- 19.4.5. Generatori di numeri pseudocasuali
- 19.4.6. Uso degli algoritmi

19.5. Crittografia simmetrica
- 19.5.1. Cifrari a blocchi
- 19.5.2. DES (*Data Encryption Standard*)
- 19.5.3. Algoritmo RC4
- 19.5.4. AES (*Advanced Encryption Standard*)
- 19.5.5. Combinazione di cifrari a blocchi
- 19.5.6. Derivazione delle chiavi

19.6. Crittografia asimmetrica
- 19.6.1. Diffie-Hellman
- 19.6.2. DSA (D*igital Signature Algorithm*)
- 19.6.3. RSA (Rivest, Shamir e Adleman)
- 19.6.4. Curva ellittica
- 19.6.5. Crittografia asimmetrica. Tipologia

19.7. Certificati digitali
- 19.7.1. Firma digitale
- 19.7.2. Certificati X509
- 19.7.3. Infrastruttura a chiave pubblica (PKI)

19.8. Implementazione
- 19.8.1. Kerberos
- 19.8.2. IBM CCA
- 19.8.3. *Pretty Good Privacy* (PGP)
- 19.8.4. ISO *Authentication Framework*
- 19.8.5. SSL e TLS
- 19.8.6. Smart card nei mezzi di pagamento (EMV)
- 19.8.7. Protocolli di telefonia mobile
- 19.8.8. *Blockchain*

19.9. Steganografia
- 19.9.1. Steganografia
- 19.9.2. Stegoanalisi
- 19.9.3. Applicazioni e usi

19.10. Crittografia quantistica
- 19.10.1. Algoritmi quantistici
- 19.10.2. Protezione degli algoritmi dalla computazione quantistica
- 19.10.3. Distribuzione quantistica delle chiavi

Modulo 20. Gestione dell'identità e degli accessi nella sicurezza informatica

20.1. Gestione dell'identità e degli accessi (IAM)
- 20.1.1. Identità digitale
- 20.1.2. Gestione dell'identità
- 20.1.3. Federazione di identità

20.2. Controllo degli accessi fisici
- 20.2.1. Sistemi di protezione
- 20.2.2. Sicurezza delle aree
- 20.2.3. Strutture di recupero

20.3. Controllo logico degli accessi
- 20.1.1. Autenticazione: Tipologia
- 20.1.2. Protocolli di autenticazione
- 20.1.3. Attacchi di autenticazione

20.4. Controllo logico degli accessi. Autenticazione MFA
- 20.4.1. Controllo logico degli accessi. Autenticazione MFA
- 20.4.2. Password. Importanza
- 20.4.3. Attacchi di autenticazione

20.5. Controllo logico degli accessi. Autenticazione biometrica
- 20.5.1. Controllo logico degli accessi. Autenticazione biometrica
  - 20.5.1.1. Autenticazione biometrica. Requisiti
- 20.5.2. Funzionamento
- 20.5.3. Modelli e tecniche

20.6. Sistemi di gestione dell'autenticazione
- 20.6.1. *Single sign on*
- 20.6.2. Kerberos
- 20.6.3. Sistemi AAA

20.7. Sistemi di gestione dell'autenticazione: Sistemi AAA
- 20.7.1. TACACS
- 20.7.2. RADIUS
- 20.7.3. DIAMETER

20.8. Servizi per il controllo degli accessi
- 20.8.1. FW - Firewall
- 20.8.2. VPN - Reti private virtuali
- 20.8.3. IDS - Sistema di rilevamento delle intrusioni

20.9. Sistemi di controllo degli accessi alla rete
- 20.9.1. NAC
- 20.9.2. Architettura ed elementi
- 20.9.3. Funzionamento e standardizzazione

20.10. Accesso alle reti wireless
- 20.10.1. Tipi di reti wireless
- 20.10.2. Sicurezza nelle reti wireless
- 20.10.3. Attacchi alla rete wireless

Modulo 21. Sicurezza nelle comunicazioni e nel funzionamento del *software*

21.1. Sicurezza informatica nelle comunicazioni e nel funzionamento del *software*
- 21.1.1. Sicurezza informatica
- 21.1.2. Cibersicurezza
- 21.1.3. Sicurezza del cloud

21.2. Sicurezza informatica nelle comunicazioni e nel funzionamento del *software*: Tipologia
- 21.2.1. Sicurezza fisica
- 21.2.2. Sicurezza logica

21.3. Sicurezza nelle comunicazioni
- 21.3.1. Elementi principali
- 21.3.2. Sicurezza di rete
- 21.3.3. Best practice

21.4. Cyberintelligence
- 21.4.1. Ingegneria sociale
- 21.4.2. *Deep web*
- 21.4.3. *Phishing*
- 21.4.4. *Malware*

21.5. Sviluppo sicuro nelle comunicazioni e nel funzionamento del *software*
- 21.5.1. Sviluppo sicuro. Protocollo HTTP
- 21.5.2. Sviluppo sicuro. Ciclo di vita
- 21.5.3. Sviluppo sicuro. Sicurezza PHP
- 21.5.4. Sviluppo sicuro. Sicurezza NET
- 21.5.5. Sviluppo sicuro. Best practice

21.6. Sistemi di gestione della sicurezza delle informazioni nelle comunicazioni e nel controllo del *software*
- 21.6.1. GDPR
- 21.6.2. ISO 27021
- 21.6.3. ISO 27017/18

21.7. Tecnologie SIEM
- 21.7.1. Tecnologie SIEM
- 21.7.2. Operazioni SOC
- 21.7.3. SIEM *vendors*

21.8. Il ruolo della sicurezza nelle organizzazioni
- 21.8.1. Ruoli nelle organizzazioni
- 21.8.2. Il ruolo degli specialisti IoT nelle aziende
- 21.8.3. Certificazioni riconosciute dal mercato

21.9. Analisi forense
- 21.9.1. Analisi forense
- 21.9.2. Analisi forense: Metodologia
- 21.9.3. Analisi forense: Strumenti e implementazione

21.10. Cybersecurity oggi
- 21.10.1. Principalli attacchi informatici
- 21.10.2. Previsioni di impiego
- 21.10.3. Sfide

Modulo 22. Sicurezza negli ambienti *Cloud*

22.1. Sicurezza negli ambienti *cloud computing*
- 22.1.1. Sicurezza negli ambienti *cloud computing*
- 22.1.2. Sicurezza negli ambienti *cloud computing*: Minacce e rischi per la sicurezza
- 22.1.3. Sicurezza negli ambienti *cloud computing*: Aspetti chiave della sicurezza

22.2. Tipi di infrastruttura *cloud*
- 22.2.1. Pubblico
- 22.2.2. Privato
- 22.2.3. Ibrido

22.3. Modello di gestione condivisa
- 22.3.1. Caratteristiche di sicurezza gestite dal fornitore
- 22.3.2. Elementi gestiti dal cliente
- 22.3.3. Definizione della strategia di sicurezza

22.4. Meccanismi di prevenzione
- 22.4.1. Sistemi di gestione dell'autenticazione
- 22.4.2. Sistemi di gestione dell'autenticazione: Politiche di accesso
- 22.4.3. Sistemi di gestione delle chiavi

22.5. Protezione dei sistemi
- 22.5.1. Protezione dei sistemi di archiviazione
- 22.5.2. Protezione dei sistemi di database
- 22.5.3. Protezione dei dati in transito

22.6. Protezione dell'infrastruttura
- 22.6.1. Progettazione e implementazione di reti sicure
- 22.6.2. Sicurezza delle risorse informatiche
- 22.6.3. Strumenti e risorse per la protezione delle infrastrutture

22.7. Rilevamento di minacce e attacchi
- 22.7.1. Sistemi di audit, *logging* e monitoraggio
- 22.7.2. Sistemi di eventi e allarmi
- 22.7.3. Sistemi SIEM

22.8. Risposta agli incidenti
- 22.8.1. Piano di risposta agli incidenti
- 22.8.2. La continuità operativa
- 22.8.3. Analisi forense e correzione di incidenti della stessa natura

22.9. Sicurezza nei *clouds* pubblici
- 22.9.1. AWS (Amazon Web Services)
- 22.9.2. Microsoft Azure
- 22.9.3. Google GCP
- 22.9.4. Oracle *Cloud*

22.10. Regolamenti e conformità
- 22.10.1. Conformità alle norme di sicurezza
- 22.10.2. Gestione dei rischi
- 22.10.3. Personale e procedure nelle organizzazioni

Modulo 23. Strumenti di monitoraggio nelle Politiche di Sicurezza dei Sistemi di Informazione

23.1. Politiche di monitoraggio dei sistemi informazione
- 23.1.1. Monitoraggio del sistema
- 23.1.2. Parametri
- 23.1.3. Tipi di parametri

23.2. Audit e registrazione nei sistemi
- 23.2.1. Audit e registrazione di Windows
- 23.2.2. Audit e registrazione su Linux

23.3. Protocollo SNMP. *Simple Network Management Protocol*
- 23.3.1. Protocollo SNMP
- 23.3.2. Funzionamento SNMP
- 23.3.3. Strumenti SNMP

23.4. Monitoraggio della rete
- 23.4.1. Monitoraggio della rete nei sistemi di controllo
- 23.4.2. Strumenti di monitoraggio per i sistemi di controllo

23.5. Nagios. Sistema di monitoraggio della rete
- 23.5.1. Nagios
- 23.5.2. Funzionamento di Nagios
- 23.5.3. Installazione di Nagios

23.6. Zabbix. Sistema di monitoraggio della rete
- 23.6.1. Zabbix.
- 23.6.2. Funzionamento di Zabbix
- 23.6.3. Installazione di Zabbix

23.7. Cacti. Sistema di monitoraggio della rete
- 23.7.1. Cacti
- 23.7.2. Funzionamento di Cacti
- 23.7.3. Installazione dim Cacti

23.8. Pandora. Sistema di monitoraggio della rete
- 23.8.1. Pandora
- 23.8.2. Funzionamento di Pandora
- 23.8.3. Installazione di Pandora

23.9. SolarWinds. Sistema di monitoraggio della rete
- 23.9.1. SolarWinds
- 23.9.2. Funzionamento di SolarWinds
- 23.9.3. Installazione di SolarWinds

23.10. Monitoraggio dei regolamenti
- 23.10.1. Controlli CIS su auditing e logging
- 23.10.2. NIST 800-123 (Stati Uniti)

Modulo 24. Sicurezza delle comunicazioni nei *dispositivi* Iot

24.1. Dalla telemetria all'IoT
- 24.1.1. Telemetria
- 24.1.2. Connettività M2M
- 24.1.3. Democratizzazione della telemetria

24.2. Modelli di riferimento IoT
- 24.2.1. Modello di riferimento IoT
- 24.2.2. Architettura IoT semplificata

24.3. Vulnerabilità della sicurezza IoT
- 24.3.1. *Dispositivi* IoT
- 24.3.2. *Dispositivi* IoT: Casi di utilizzo
- 24.3.3. *Dispositivi* IoT: Vulnerabilità

24.4. Connettività IoT
- 24.4.1. Reti PAN, LAN, WAN
- 24.4.2. Tecnologie wireless non IoT
- 24.4.3. Tecnologie wireless LPWAN

24.5. Tecnologie LPWAN
- 24.5.1. Il triangolo di ferro delle reti LPWAN
- 24.5.2. Bande di frequenza libere vs. Bande con licenza
- 24.5.3. Opzioni tecnologiche LPWAN

24.6. Tecnologia LoRaWAN
- 24.6.1. Tecnologia LoRaWAN
- 24.6.2. Casi d'uso di LoRaWAN. Ecosistema
- 24.6.3. Sicurezza in LoRaWAN

24.7. Tecnologia Sigfox
- 24.7.1. Tecnologia Sigfox
- 24.7.2. Casi d'uso di Sigfox. Ecosistema
- 24.7.3. Sicurezza in Sigfox

24.8. Tecnologia cellulare IoT
- 24.8.1. Tecnologia cellulare IoT (NB-IoT e LTE-M)
- 24.8.2. Casi d'uso cellulare IoT. Ecosistema
- 24.8.3. Sicurezza cellulare IoT

24.9. Tecnologia WiSUN
- 24.9.1. Tecnologia WiSUN
- 24.9.2. Casi d'uso di WiSUN. Ecosistema
- 24.9.3. Sicurezza di WiSUN

24.10. Altre tecnologie IoT
- 24.10.1. Altre tecnologie IoT
- 24.10.2. Casi d'uso ed ecosistema di altre tecnologie IoT
- 24.10.3. Sicurezza in altre tecnologie IoT

Modulo 25. Piano di continuità operativa associato alla sicurezza

25.1. Piano di continuità operativa
- 25.1.1. I piani di continuità operativa (BCP)
- 25.1.2. Piano di continuità operativa (BCP). Aspetti chiave
- 25.1.3. Piano di continuità operativa (BCP) per la valutazione dell'azienda

25.2. Parametri in un piano di continuità operativa (BCP)
- 25.2.1. *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO)
- 25.2.2. Tempo massimo tollerabile (MTD)
- 25.2.3. Livelli minimi di recupero (ROL)
- 25.2.4. Obiettivo del punto di ripristino (RPO)

25.3. Progetti di continuità. Tipologia
- 25.3.1. Piano di continuità operativa (BCP)
- 25.3.2. Piano di continuità ICT
- 25.3.3. Piano di ripristino in caso di disastro (DRP)

25.4. Gestione dei rischi connessi al BCP
- 25.4.1. Analisi dell'impatto aziendale
- 25.4.2. Vantaggi dell'implementazione di un BCP
- 25.4.3. Mentalità basata sul rischio

25.5. Ciclo di vita di un piano di continuità operativa
- 25.5.1. Fase 1: Analisi dell'organizzazione
- 25.5.2. Fase 2: Determinazione della strategia di continuità
- 25.5.3. Fase 3: Risposta alla contingenza
- 25.5.4. Fase 4: Test, manutenzione e revisione

25.6. Fase di analisi organizzativa di un BCP
- 25.6.1. Identificazione dei processi che rientrano nell'ambito di applicazione del BCP
- 25.6.2. Identificazione delle aree aziendali critiche
- 25.6.3. Identificazione delle dipendenze tra aree e processi
- 25.6.4. Determinazione del MTD appropriato
- 25.6.5. Prodotti. Creazione di un piano

25.7. Fase di determinazione della strategia di continuità in un BCP
- 25.7.1. Ruoli nella fase di determinazione della strategia
- 25.7.2. Compiti nella fase di determinazione della strategia
- 25.7.3. Risultati

25.8. Fase di risposta alla contingenza di un BCP
- 25.8.1. Ruoli nella fase di risposta
- 25.8.2. Compiti di questa fase
- 25.8.3. Risultati

25.9. Fase di test, manutenzione e revisione di un BCP
- 25.9.1. Ruoli nella fase di test, manutenzione e revisione
- 25.9.2. Lavori nella fase di test, manutenzione e revisione
- 25.9.3. Risultati

25.10. Standard ISO associati ai piani di continuità operativa (BCP)
- 25.10.1. ISO 22301:2019
- 25.10.2. ISO 22313:2020
- 25.10.3. Altri standard ISO e internazionali correlati

Modulo 26. Politica di Ripristino pratico in caso di Disastri di Sicurezza

26.1. DRP. Piano di Disaster Recovery
- 26.1.1. Obiettivo di un DRP
- 26.1.2. Benefici di un DRP
- 26.1.3. Conseguenze della mancanza di un DRP e del suo mancato aggiornamento

26.2. Linee guida per la definizione di un DRP (Disaster Recovery Plan)
- 26.2.1. Ambito e obiettivi
- 26.2.2. Progettazione della strategia di ripristino
- 26.2.3. Assegnazione di ruoli e responsabilità
- 26.2.4. Inventario di hardware, *software* e servizi
- 26.2.5. Tolleranza ai tempi di inattività e alla perdita di dati
- 26.2.6. Stabilire i tipi specifici di DRP richiesti
- 26.2.7. Realizzazione di un Piano di Formazione, consapevolezza e comunicazione

26.3. Ambito e obiettivi di un DRP (Disaster Recovery Plan)
- 26.3.1. Garantire la risposta
- 26.3.2. Componenti tecnologiche
- 26.3.3. Ambito di applicazione della politica di continuità

26.4. Progettazione di una Strategia DRP (Disaster Recovery)
- 26.4.1. Strategia di Disaster Recovery
- 26.4.2. Budget
- 26.4.3. Risorse umane e Fisiche
- 26.4.4. Posizioni dirigenziali a rischio
- 26.4.5. Tecnologia
- 26.4.6. Dati

26.5. Continuità del Processi di informazione
- 26.5.1. Pianificazione della cntinuità
- 26.5.2. Attuazione della cntinuità
- 26.5.3. Verifica e valutazione della continuità

26.6. Ambito di applicazione di un BCP (Business Continuity Plan)
- 26.6.1. Determinazione dei processi più critici
- 26.6.2. Approccio basato sugli asset
- 26.6.3. Approccio per processi

26.7. Implementazione di processi aziendali protetti
- 26.7.1. Attività Prioritarie (AP)
- 26.7.2. Tempi di recupero ideali (IRT)
- 26.7.3. Strategie di sopravvivenza

26.8. Analisi dell'organizzazione
- 26.8.1. Raccolta di informazioni
- 26.8.2. Analisi dell'impatto aziendale (BIA)
- 26.8.3. Analisi del rischio organizzativo

26.9. Risposta alla contingenza
- 26.9.1. Piano di crisi
- 26.9.2. Piani di recupero dell'ambiente operativo
- 26.9.3. Piani di recupero dell'ambiente operativo

26.10. Standard internazionale ISO 27031 BCP
- 26.10.1. Obiettivi
- 26.10.2. Termini e definizioni
- 26.10.3. Operazione

Modulo 27. Implementare le politiche di sicurezza fisica e ambientale in azienda

27.1. Aree sicure
- 27.1.1. Perimetro di sicurezza fisica
- 27.1.2. Lavorare in aree sicure
- 27.1.3. Sicurezza di uffici, sedi e risorse

27.2. Controlli fisici all'ingresso
- 27.2.1. Politiche di controllo degli accessi fisici
- 27.2.2. Sistemi di controllo dell'ingresso fisico

27.3. Vulnerabilità dell'accesso fisico
- 27.3.1. Principali vulnerabilità fisiche
- 27.3.2. Implementazione delle misure di salvaguardia

27.4. Sistemi biometrici fisiologici
- 27.4.1. Impronte digitali
- 27.4.2. Riconoscimento facciale
- 27.4.3. Riconoscimento dell'iride e della retina
- 27.4.4. Altri sistemi biometrici fisiologici

27.5. Sistemi biometrici comportamentali
- 27.5.1. Riconoscimento della firma
- 27.5.2. Riconoscimento della scrittura
- 27.5.3. Riconoscimento vocale
- 27.5.4. Altri sistemi biometrici comportamentali

27.6. Gestione del rischio nella biometria
- 27.6.1. Implementazione dei sistemi biometrici
- 27.6.2. Vulnerabilità dei sistemi biometrici

27.7. Implementazione dei criteri negli *Hosts*
- 27.7.1. Installazione del cablaggio e della sicurezza
- 27.7.2. Posizionamento delle apparecchiature
- 27.7.3. Uscita delle apparecchiature all'esterno dei locali
- 27.7.4. Apparecchiature informatico incustodite e politica delle postazioni libere

27.8. Protezione dell'ambiente
- 27.8.1. Sistemi di protezione antincendio
- 27.8.2. Sistemi di protezione antisismica
- 27.8.3. Sistemi antisismici

27.9. Sicurezza dei centri di elaborazione dati
- 27.9.1. Porte di sicurezza
- 27.9.2. Sistemi di videosorveglianza (CCTV)
- 27.9.3. Controllo di sicurezza

27.10. Regolamenti internazionali sulla sicurezza fisica
- 27.10.1. IEC 62443- 62443- 1(europea)
- 27.10.2. NERC CIP-005-5 (USA)
- 27.10.3. NERC CIP-014-2 (USA)

Modulo 28. Politiche di Comunicazione Sicura in Azienda

28.1. Gestione della sicurezza nelle reti
- 28.1.1. Controllo e monitoraggio della rete
- 28.1.2. Segregazione della rete
- 28.1.3. Sistemi di sicurezza della rete

28.2. Protocolli di comunicazione sicuri
- 28.2.1. Modello TCP/IP
- 28.2.2. Protocollo IPSEC
- 28.2.3. Protocollo TLS

28.3. Protocollo TLS 1,3
- 28.3.1. Fasi di un processo TLS1.3
- 28.3.2. Protocollo *Handshake*
- 28.3.3. Protocollo di registrazione
- 28.3.4. Differenze con TLS 1.2

28.4. Algoritmi crittografici
- 28.4.1. Algoritmi crittografici utilizzati nelle comunicazioni
- 28.4.2. *Cipher-suites*
- 28.4.3. Algoritmi crittografici ammessi per TLS 1.3

28.5. Funzioni Digest
- 28.5.1. MD6
- 28.5.2. SHA

28.6. PKI. Infrastruttura a chiave pubblica
- 28.6.1. La PKI e le sue entità
- 28.6.2. Certificato digitale
- 28.6.3. Tipi di certificati digitali

28.7. Comunicazioni tunnel e trasporto
- 28.7.1. Comunicazioni a tunnel
- 28.7.2. Comunicazioni di trasporto
- 28.7.3. Implementazione del tunnel crittografato

28.8. SSH. *Secure Shell*
- 28.8.1. SSH. Capsula sicura
- 28.8.2. Funzionamento SSH
- 28.8.3. Strumenti SSH

28.9. Audit dei sistemi crittografici
- 28.9.1. Test di integrità
- 28.9.2. Test del sistema crittografico

28.10. Sistemi crittografici
- 28.10.1. Vulnerabilità dei sistemi crittografici
- 28.10.2. Salvaguardie crittografiche

Modulo 29. Aspetti organizzativi della Politica di Sicurezza delle informazioni

29.1. Organizzazione interna
- 29.1.1. Assegnazione di responsabilità
- 29.1.2. Segregazione dei compiti
- 29.1.3. Contatti con le autorità
- 29.1.4. Sicurezza delle informazione nella gestione dei progetti

29.2. Gestione delle risorse
- 29.2.1. Responsabilità per gli asset
- 29.2.2. Classificazione di Sicurezza delle Informazioni
- 29.2.3. Gestione dei supporti di memorizzazione

29.3. Politiche di sicurezza nei processi aziendali
- 29.3.1. Analisi dei processi aziendali vulnerabili
- 29.3.2. Analisi dell'impatto sul business
- 29.3.3. Classificazione dei processi in base all'impatto sul business

29.4. Politiche di sicurezza legate alle Risorse Umane
- 29.4.1. Prima della stipula del contratto
- 29.4.2. Durante la stipula del contratto
- 29.4.3. Cessazione o cambio di incarico

29.5. Politiche di sicurezza della gestione
- 29.5.1. Linee guida della direzione sulla sicurezza delle informazioni
- 29.5.2. BIA - analisi dell'impatto
- 29.5.3. Il piano di ripristino come politica di sicurezza

29.6. Acquisizione e manutenzione del sistema di informazione
- 29.6.1. Requisiti di Sicurezza del sistema di informazione
- 29.6.2. Sicurezza dei dati di sviluppo e supporto
- 29.6.3. Dati di prova

29.7. Sicurezza con i fornitori
- 29.7.1. Sicurezza informatica di approvvigionamento
- 29.7.2. Gestione della fornitura di servizi con garanzia
- 29.7.3. Sicurezza della catena di approvvigionamento

29.8. Sicurezza operativa
- 29.8.1. Responsabilità operative
- 29.8.2. Protezione contro il codice maligno
- 29.8.3. Copie di backup
- 29.8.4. Registri di attività e monitoraggio

29.9. Gestione e norme di sicurezza
- 29.9.1. Conformità ai requisiti di legge
- 29.9.2. Revisioni di Sicurezza delle Informazioni

29.10. Sicurezza nella gestione della continuità operativa
- 29.10.1. Continuità di sicurezza delle informazioni
- 29.10.2. Ridondanze

05

Metodologia di studio

TECH è la prima università al mondo che combina la metodologia dei ***case studies*** con il ***Relearning***, un sistema di apprendimento 100% online basato sulla ripetizione diretta.

Questa strategia dirompente è stata concepita per offrire ai professionisti l'opportunità di aggiornare le conoscenze e sviluppare competenze in modo intensivo e rigoroso. Un modello di apprendimento che pone lo studente al centro del processo accademico e gli conferisce tutto il protagonismo, adattandosi alle sue esigenze e lasciando da parte le metodologie più convenzionali.

TECH ti prepara ad affrontare nuove sfide in ambienti incerti e a raggiungere il successo nella tua carriera"

Lo studente: la priorità di tutti i programmi di TECH

Nella metodologia di studio di TECH lo studente è il protagonista assoluto.
Gli strumenti pedagogici di ogni programma sono stati selezionati tenendo conto delle esigenze di tempo, disponibilità e rigore accademico che, al giorno d'oggi, non solo gli studenti richiedono ma le posizioni più competitive del mercato.

Con il modello educativo asincrono di TECH, è lo studente che sceglie il tempo da dedicare allo studio, come decide di impostare le sue routine e tutto questo dalla comodità del dispositivo elettronico di sua scelta. Lo studente non deve frequentare lezioni presenziali, che spesso non può frequentare. Le attività di apprendimento saranno svolte quando si ritenga conveniente. È lo studente a decidere quando e da dove studiare.

"In TECH NON ci sono lezioni presenziali (che poi non potrai mai frequentare)"

I piani di studio più completi a livello internazionale

TECH si caratterizza per offrire i percorsi accademici più completi del panorama universitario. Questa completezza è raggiunta attraverso la creazione di piani di studio che non solo coprono le conoscenze essenziali, ma anche le più recenti innovazioni in ogni area.

Essendo in costante aggiornamento, questi programmi consentono agli studenti di stare al passo con i cambiamenti del mercato e acquisire le competenze più apprezzate dai datori di lavoro. In questo modo, coloro che completano gli studi presso TECH ricevono una preparazione completa che fornisce loro un notevole vantaggio competitivo per avanzare nelle loro carriere.

Inoltre, potranno farlo da qualsiasi dispositivo, pc, tablet o smartphone.

> *Il modello di TECH è asincrono, quindi ti permette di studiare con il tuo pc, tablet o smartphone dove, quando e per quanto tempo vuoi"*

Case studies o Metodo Casistico

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori facoltà del mondo. Sviluppato nel 1912 per consentire agli studenti di Giurisprudenza non solo di imparare le leggi sulla base di contenuti teorici, ma anche di esaminare situazioni complesse reali. In questo modo, potevano prendere decisioni e formulare giudizi di valore fondati su come risolverle. Nel 1924 fu stabilito come metodo di insegnamento standard ad Harvard.

Con questo modello di insegnamento, è lo studente stesso che costruisce la sua competenza professionale attraverso strategie come il *Learning by doing* o il *Design Thinking*, utilizzate da altre istituzioni rinomate come Yale o Stanford.

Questo metodo, orientato all'azione, sarà applicato lungo tutto il percorso accademico che lo studente intraprende insieme a TECH. In questo modo, affronterà molteplici situazioni reali e dovrà integrare le conoscenze, ricercare, argomentare e difendere le sue idee e decisioni. Tutto ciò con la premessa di rispondere al dubbio di come agirebbe nel posizionarsi di fronte a specifici eventi di complessità nel suo lavoro quotidiano.

Metodo *Relearning*

In TECH i *case studies* vengono potenziati con il miglior metodo di insegnamento 100% online: il *Relearning*.

Questo metodo rompe con le tecniche di insegnamento tradizionali per posizionare lo studente al centro dell'equazione, fornendo il miglior contenuto in diversi formati. In questo modo, riesce a ripassare e ripete i concetti chiave di ogni materia e impara ad applicarli in un ambiente reale.

In questa stessa linea, e secondo molteplici ricerche scientifiche, la ripetizione è il modo migliore per imparare. Ecco perché TECH offre da 8 a 16 ripetizioni di ogni concetto chiave in una stessa lezione, presentata in modo diverso, con l'obiettivo di garantire che la conoscenza sia completamente consolidata durante il processo di studio.

Il Relearning ti consentirà di apprendere con meno sforzo e più rendimento, coinvolgendoti maggiormente nella specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando opinioni: un'equazione diretta al successo.

Un Campus Virtuale 100% online con le migliori risorse didattiche

Per applicare efficacemente la sua metodologia, TECH si concentra sul fornire agli studenti materiali didattici in diversi formati: testi, video interattivi, illustrazioni, mappe della conoscenza, ecc. Tutto ciò progettato da insegnanti qualificati che concentrano il lavoro sulla combinazione di casi reali con la risoluzione di situazioni complesse attraverso la simulazione, lo studio dei contesti applicati a ogni carriera e l'apprendimento basato sulla ripetizione, attraverso audio, presentazioni, animazioni, immagini, ecc.

Le ultime prove scientifiche nel campo delle Neuroscienze indicano l'importanza di considerare il luogo e il contesto in cui si accede ai contenuti prima di iniziare un nuovo apprendimento. Poter regolare queste variabili in modo personalizzato favorisce che le persone possano ricordare e memorizzare nell'ippocampo le conoscenze per conservarle a lungo termine. Si tratta di un modello denominato *Neurocognitive context-dependent e-learning,* che viene applicato in modo consapevole in questa qualifica universitaria.

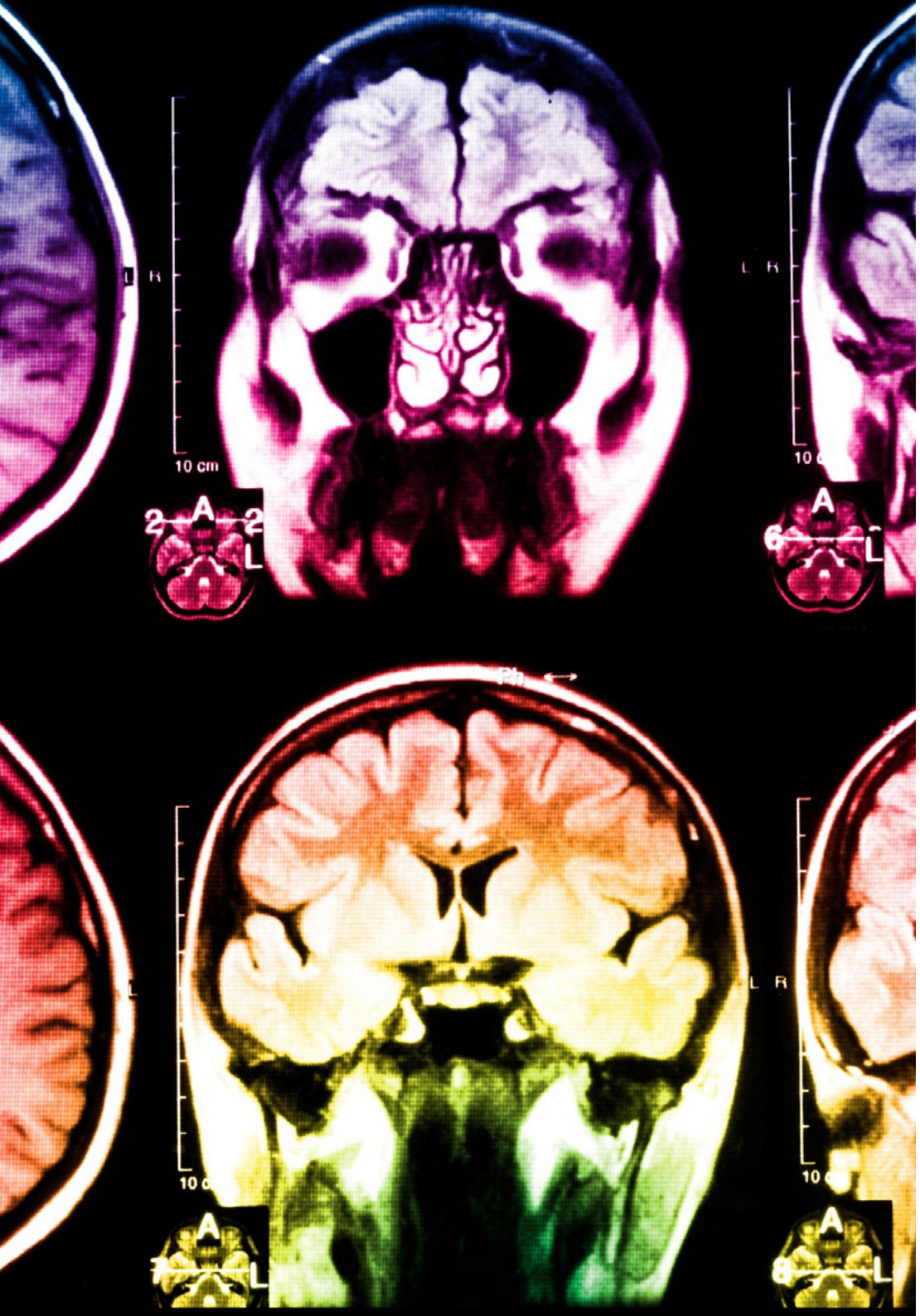
Inoltre, anche per favorire al massimo il contatto tra mentore e studente, viene fornita una vasta gamma di possibilità di comunicazione, sia in tempo reale che differita (messaggistica interna, forum di discussione, servizio di assistenza telefonica, e-mail di contatto con segreteria tecnica, chat e videoconferenza).

Inoltre, questo completo Campus Virtuale permetterà agli studenti di TECH di organizzare i loro orari di studio in base alla loro disponibilità personale o agli impegni lavorativi. In questo modo avranno un controllo globale dei contenuti accademici e dei loro strumenti didattici, il che attiva un rapido aggiornamento professionale.

La modalità di studio online di questo programma ti permetterà di organizzare il tuo tempo e il tuo ritmo di apprendimento, adattandolo ai tuoi orari"

L'efficacia del metodo è giustificata da quattro risultati chiave:

1. Gli studenti che seguono questo metodo non solo raggiungono l'assimilazione dei concetti, ma sviluppano anche la loro capacità mentale, attraverso esercizi che valutano situazioni reali e l'applicazione delle conoscenze.
2. L'apprendimento è solidamente fondato su competenze pratiche che permettono allo studente di integrarsi meglio nel mondo reale.
3. L'assimilazione di idee e concetti è resa più facile ed efficace, grazie all'uso di situazioni nate dalla realtà.
4. La sensazione di efficienza dello sforzo investito diventa uno stimolo molto importante per gli studenti, che si traduce in un maggiore interesse per l'apprendimento e in un aumento del tempo dedicato al corso.



La metodologia universitaria più apprezzata dagli studenti

I risultati di questo innovativo modello accademico sono riscontrabili nei livelli di soddisfazione globale degli studenti di TECH.

La valutazione degli studenti sulla qualità dell'insegnamento, la qualità dei materiali, la struttura del corso e i suoi obiettivi è eccellente. A conferma di ciò, l'istituto è diventato il migliore valutato dai suoi studenti sulla piattaforma di recensioni Trustpilot, ottenendo un punteggio di 4,9 su 5.

Accedi ai contenuti di studio da qualsiasi dispositivo con connessione a Internet (computer, tablet, smartphone) grazie al fatto che TECH è aggiornato sull'avanguardia tecnologica e pedagogica.

Potrai imparare dai vantaggi dell'accesso a ambienti di apprendimento simulati e dall'approccio di apprendimento per osservazione, ovvero Learning from an expert.

In questo modo, il miglior materiale didattico sarà disponibile, preparato con attenzione:

Materiale di studio

Tutti i contenuti didattici sono creati dagli specialisti che impartiranno il corso, appositamente per questo, in modo che lo sviluppo didattico sia realmente specifico e concreto.

Questi contenuti sono poi applicati al formato audiovisivo che supporterà la nostra modalità di lavoro online, impiegando le ultime tecnologie che ci permettono di offrirti una grande qualità per ogni elemento che metteremo al tuo servizio.

Capacità e competenze pratiche

I partecipanti svolgeranno attività per sviluppare competenze e abilità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve possedere nel mondo globalizzato in cui viviamo.

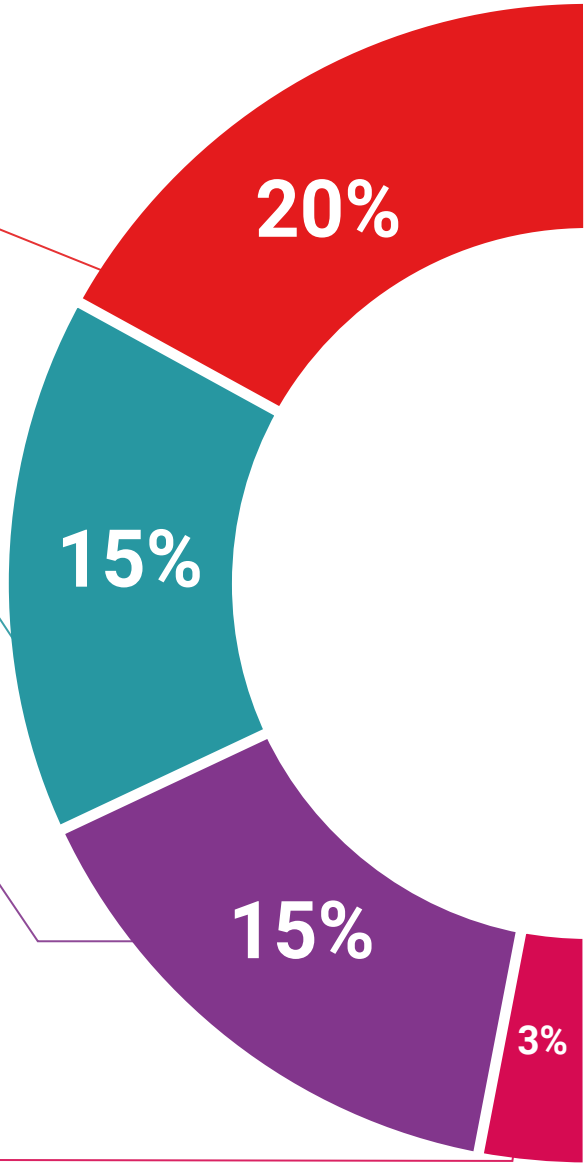
Riepiloghi interattivi

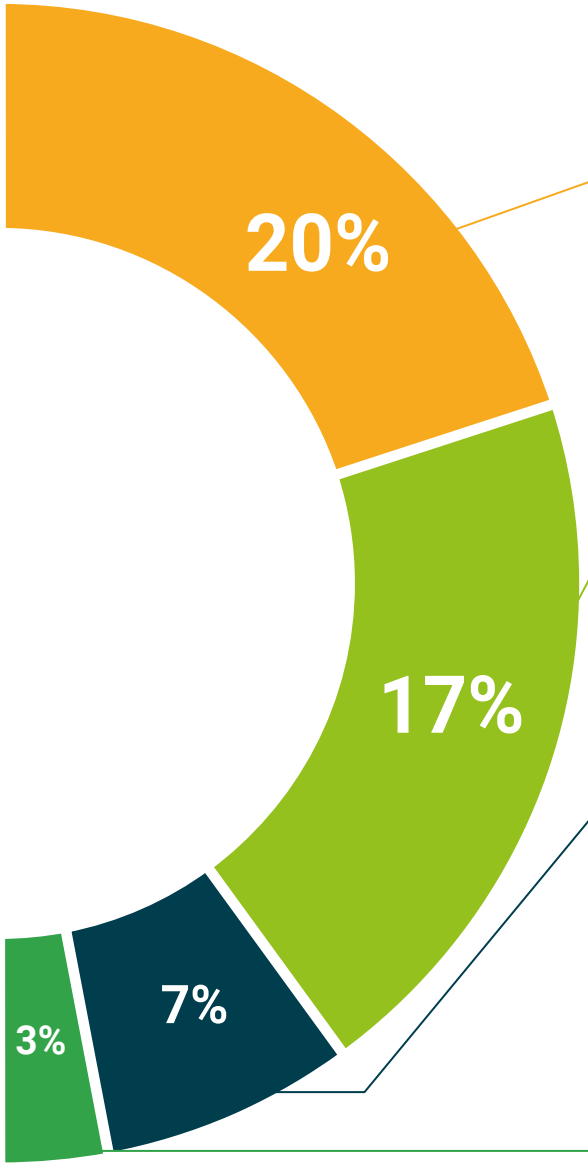
Presentiamo i contenuti in modo accattivante e dinamico tramite strumenti multimediali che includono audio, video, immagini, diagrammi e mappe concettuali per consolidare la conoscenza.

Questo esclusivo sistema di preparazione per la presentazione di contenuti multimediali è stato premiato da Microsoft come "Caso di successo in Europa".

Letture complementari

Articoli recenti, documenti di consenso, guide internazionali... Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua specializzazione.





Case Studies

Completerai una selezione dei migliori *case studies* in materia. Casi presentati, analizzati e monitorati dai migliori specialisti del panorama internazionale.

Testing & Retesting

Valutiamo e rivalutiamo periodicamente le tue conoscenze durante tutto il programma. Lo facciamo su 3 dei 4 livelli della Piramide di Miller.

Master class

Esistono prove scientifiche sull'utilità d'osservazione di terzi esperti.

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

Guide di consultazione veloce

TECH offre i contenuti più rilevanti del corso sotto forma di schede o guide rapide per l'azione. Un modo sintetico, pratico ed efficace per aiutare a progredire nel tuo apprendimento.

07

Titulación

Il Master Specialistico in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer) garantisce, oltre alla preparazione più rigorosa e aggiornata, il conseguimento di una qualifica di Master Specialistico rilasciata da TECH Università Tecnologica.

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

Questo programma ti consentirà di ottenere il titolo di studio privato di **Master Specialistico in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer)** possiede il programma più completo e aggiornato del mercato.

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

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

Titolo: **Master Specialistico in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer)**

Modalità: **online**

Durata: **2 anni**

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 SPECIALISTICO

in

Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer)

Si tratta di un titolo rilasciato da questa Università ed equivalente a 3.000 ore, con data di inizio gg/mm/aaaa e con data di fine gg/mm/aaaa.

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

In data 17 Giugno 2020

Tere Guevara Navarro
Rettrice

codice unico TECH: AFWORD23S techtitute.com/titulos

Master Specialistico in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer)

Distribuzione generale del Programma

Corso	Insegnamento	Ore	Codice
1°	Cyberintelligence e Cibersicurezza	100	OB
1°	Sicurezza in Host	100	OB
1°	Sicurezza di rete (perimetro)	100	OB
1°	Sicurezza degli smartphone	100	OB
1°	Sicurezza in IoT	100	OB
1°	Hacking etico	100	OB
1°	Ingegneria inversa	100	OB
1°	Sviluppo sicuro	100	OB
1°	Implementazione pratica delle politiche di sicurezza del software e dell'hardware	100	OB
1°	Analisi forense	100	OB
1°	Sicurezza nella progettazione e nello sviluppo dei sistemi	100	OB
1°	Strutture e modelli per la sicurezza delle informazioni	100	OB
1°	Sistema di Gestione della Sicurezza delle Informazioni (SGSI)	100	OB
1°	Gestione della sicurezza IT	100	OB
1°	Politiche di gestione degli incidenti di sicurezza	100	OB
2°	Analisi dei rischi e ambiente di sicurezza IT	100	OB
2°	Politiche di Sicurezza per l'Analisi delle Minacce dei Sistemi Informatici	100	OB
2°	Implementazione Pratica di Politiche di Sicurezza contro gli Attacchi	100	OB
2°	La crittografia nell'IT	100	OB
2°	Gestione dell'identità e degli accessi nella sicurezza informatica	100	OB
2°	Sicurezza nelle comunicazioni e nel funzionamento del software	100	OB
2°	Sicurezza negli ambienti Cloud	100	OB
2°	Strumenti di monitoraggio nelle Politiche di Sicurezza dei Sistemi di Informazione	100	OB
2°	Sicurezza delle comunicazioni nei dispositivi Iot	100	OB
2°	Piano di continuità operativa associato alla sicurezza	100	OB
2°	Politica di Ripristino pratico in caso di Disastri di Sicurezza	125	OB
2°	Implementare le politiche di sicurezza fisica e ambientale in azienda	125	OB
2°	Politiche di Comunicazione Sicura in Azienda	125	OB
2°	Aspetti organizzativi della Politica di Sicurezza delle informazioni	125	OB

Tere Guevara Navarro
Rettrice

tech università tecnologica

*Apostille dell'Aia. Se lo studente dovesse richiedere che il suo diploma cartaceo sia provvisto di Apostille dell'Aia, TECH EDUCATION effettuerà le gestioni opportune per ottenerla pagando un costo aggiuntivo.

tech università tecnologica

Master Specialistico in Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer)

- Modalità: **online**
- Durata: **2 anni**
- Titolo: **TECH Università Tecnologica**
- Orario: **a tua scelta**
- Esami: **online**

Master Specialistico

Alta Direzione di Cibersicurezza (CISO, Chief Information Security Officer)

tech università tecnologica