Master Specialistico

Secure Information Management

tech università tecnologica

tech università tecnologica

Master Specialistico

Secure Information Management

- Modalità: **online**
- Durata: **2 anni**
- Titolo: **TECH Università Tecnologica**
- Dedizione: **16 ore/settimana**
- Orario: **a scelta**
- Esami: **online**

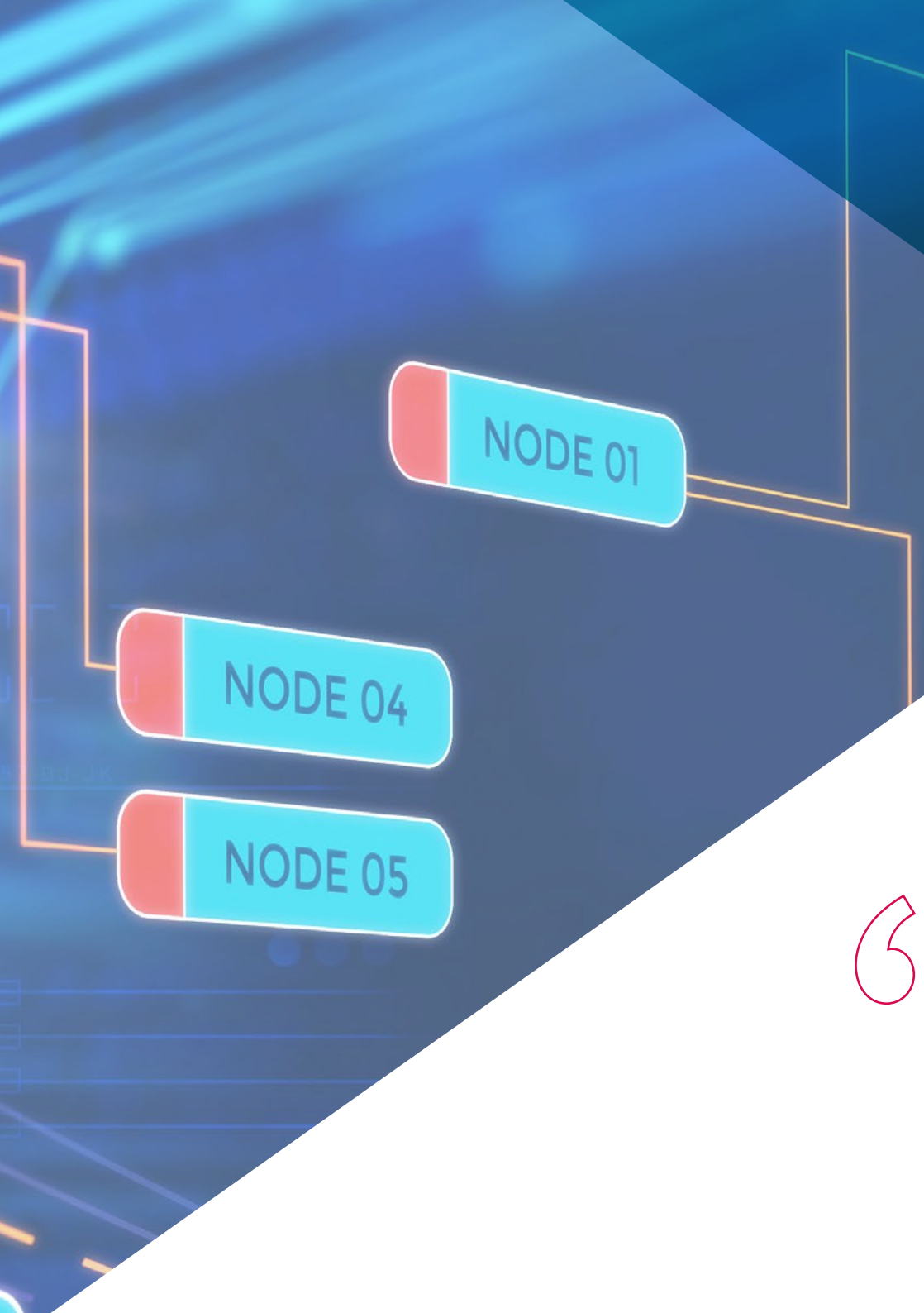
Accesso al sito web: www.techtitute.com/it/informatica/master-specialistico/master-specialistico-secure-information-management

Indice

01

Presentazione

Il mondo di oggi è dominato dall'ambiente digitale. Al suo interno vengono gestite numerose attività in diversi settori. Il tempo libero, il lavoro o i contatti con amici e familiari non sono più pensabili senza Internet e tutti gli strumenti online esistenti. Per questo motivo, ogni giorno vengono trasferite enormi quantità di informazioni, dai dati innocui delle conversazioni sui social network e le applicazioni di messaggistica alle informazioni personali e professionali altamente sensibili riportate sui siti web bancari o aziendali. In questo panorama complesso, sono necessari specialisti in grado di gestire tutti i tipi di informazioni relative a queste aree con un'adeguata attenzione alla sicurezza. Molte aziende cercano persone con questo profilo per proteggere le loro informazioni.



Ogni giorno individui malintenzionati tentano di compromettere la sicurezza delle aziende e delle istituzioni che gestiscono dati sensibili: tu potresti essere la figura che protegge queste informazioni"

Ogni giorno, milioni di persone svolgono ogni tipo di attività su Internet. Consultano notizie, chattano con amici e familiari, condividono opinioni sui social network, espletano compiti amministrativi in diverse aziende e istituzioni, condividono ogni tipo di file o svolgono attività lavorative. In tutto il mondo vengono create e trasferite innumerevoli quantità di dati in ogni momento.

Gestirli con un'adeguata sicurezza non è un compito facile, poiché richiede una serie di conoscenze specifiche provenienti da vari settori che normalmente non entrano in contatto tra loro. Per questo motivo, il Master Specialistico in Secure Information Management rappresenta un'opportunità straordinaria per tutti gli ingegneri e i professionisti IT che desiderano integrare la gestione delle informazioni e la cybersecurity e diventare specialisti di primo piano in entrambi i settori.

Molte aziende e istituzioni gestiscono dati altamente sensibili e preziosi che devono essere gestiti, conservati e monitorati correttamente. Non ci sono ancora molti esperti in entrambe le discipline in grado di gestirle correttamente. Pertanto, gli studenti che completano questa qualifica si troveranno nella miglior posizione per raggiungere incarichi di massima importanza nelle aziende che cercano di proteggere le loro informazioni digitali.

Per questo, TECH ha progettato i migliori contenuti e ha riunito i migliori docenti, con una vasta esperienza professionale in questi settori, in modo che gli studenti ricevano la preparazione più completa possibile e possano progredire nella loro carriera.

Questo **Master Specialistico in Secure Information Management** possiede il programma più completo e aggiornato del mercato. Le caratteristiche principali del corso sono:

- Lo sviluppo di casi di studio presentati da esperti in informatica
- Contenuti grafici, schematici ed eminentemente pratici forniscono informazioni scientifiche e pratiche sulle discipline mediche essenziali per l'esercizio della professione
- Esercizi pratici che offrono un processo di autovalutazione per migliorare l'apprendimento
- Si porrà speciale enfasi sulle metodologie innovative di sicurezza e dati digitali
- Lezioni teoriche, domande all'esperto, forum di discussione su questioni controverse e lavoro di riflessione individuale
- La disponibilità di accesso ai contenuti da qualsiasi dispositivo, fisso o portatile, con una connessione internet

Tutto ciò che compiamo nella sfera digitale viene registrato. Rendi Internet un luogo più sicuro grazie a questo Master Specialistico"

Una volta terminato il programma, le migliori aziende del Paese ti affideranno la gestione e la sicurezza dei loro dati”

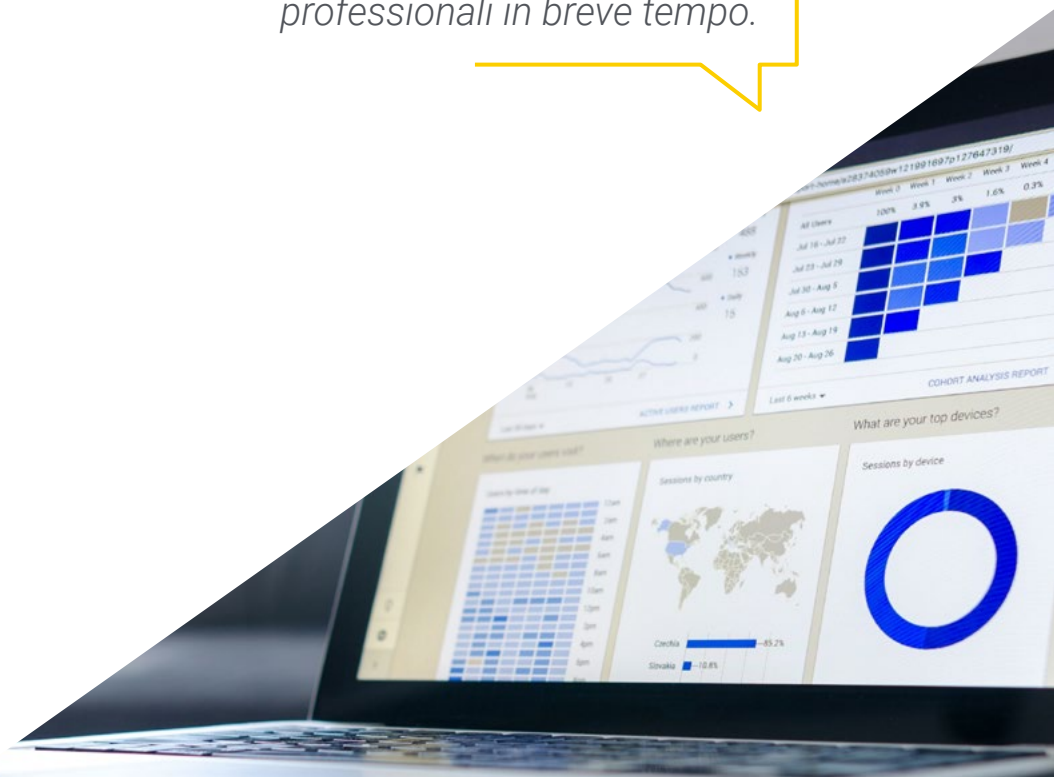
Questo Master Specialistico combina due discipline essenziali per il futuro della tua carriera. Iscriviti ora e raggiungi tutti i tuoi obiettivi.

Impara tutti gli aspetti della gestione e della sicurezza dei dati e ammira i tuoi progressi professionali in breve tempo.

Il personale docente del programma comprende un team di professionisti informatici di prestigio, che apportano a questo corso la propria esperienza professionale, nonché riconosciuti specialisti appartenenti a società scientifiche rilevanti.

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 progettazione 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. Per farlo, il professionista sarà assistito da un innovativo sistema di video interattivo creato da riconosciuti esperti.



02

Obiettivi

L'obiettivo principale di questo Master Specialistico in Secure Information Management è quello di fornire agli studenti le migliori conoscenze in due rami diversi ma interconnessi dell'informatica e dell'ingegneria: la gestione dei dati nell'ambiente digitale e la cybersecurity. Combinando queste due aree, gli informatici e i professionisti che seguono questo programma saranno in grado di applicare le soluzioni migliori in ogni situazione, offrendo alle loro aziende gli strumenti più appropriati per gestire e proteggere ogni tipo di informazione sensibile.

Il tuo obiettivo è quello di essere il miglior specialista della tua azienda e TECH ti fornisce gli strumenti per raggiungerlo"

Obiettivi generali

- Analizzare i vantaggi dell'applicazione delle tecniche di analisi dei dati in ogni area dell'azienda
- Sviluppare le basi per comprendere le esigenze e le applicazioni di ogni area
- Generare conoscenze specialistiche per selezionare gli strumenti giusti
- Proporre tecniche e obiettivi per essere il più produttivi possibile in base all'area
- Analizzare il ruolo dell'analista di cybersecurity
- Approfondire la comprensione dell'ingegneria sociale e dei suoi metodi
- Esaminare le metodologie OSINT, HUMINT, OWASP, PTEC, OSSTM e OWISAM
- Condurre un'analisi dei rischi e comprendere le metriche di rischio
- Determinare l'uso appropriato dell'anonimizzazione e l'uso di reti come TOR, I2P e Freenet
- Riassumere le normative vigenti in materia di cybersecurity
- Sviluppare conoscenze specialistiche per condurre un controllo di sicurezza
- Sviluppare politiche di utilizzo appropriate
- Esaminare i sistemi di rilevamento e prevenzione delle principali minacce
- Valutare i nuovi sistemi di rilevamento delle minacce e la loro evoluzione rispetto alle soluzioni più tradizionali
- Analizzare le principali piattaforme mobili attuali, le loro caratteristiche e il loro utilizzo
- Identificare, analizzare e valutare i rischi per la sicurezza delle parti di un progetto IoT
- Valutare le informazioni ottenute e sviluppare meccanismi di prevenzione e *hacking*
- Applicare il reverse engineering all'ambiente della cybersecurity
- Specificare i test da effettuare sul software sviluppato
- Riassumere 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 nuove tecnologie emergenti
- Conoscere le diverse tecnologie in relazione alla sicurezza informatica

La sicurezza informatica e la gestione dei dati sono discipline in rapida evoluzione. Porta a termine questo Master Specialistico e ottieni le conoscenze più aggiornate"

Obiettivi specifici

- Sviluppare capacità analitiche per prendere decisioni di qualità
- Esaminare campagne di marketing e comunicazione efficaci
- Determinare la creazione di dashboard e KPI a livello di area
- Generare conoscenze specialistiche per sviluppare analisi predittive
- Proporre piani commerciali e di fidelizzazione basati su studi di mercato
- Sviluppare la capacità di ascoltare il cliente
- Applicare le conoscenze statistiche, quantitative e tecniche a situazioni reali
- Eseguire l'analisi dei dati
- Unificare dati diversi: ottenere la coerenza delle informazioni
- Produrre informazioni rilevanti ed efficaci per il processo decisionale
- Determinare le migliori pratiche per la gestione dei dati in base alla loro tipologia e ai loro usi
- Stabilire politiche di accesso e riutilizzo dei dati
- Garantire la sicurezza e la disponibilità: disponibilità, integrità e riservatezza delle informazioni
- Esaminare gli strumenti di gestione dei dati utilizzando i linguaggi di programmazione
- Identificare cosa si intende per IoT (*Internet of Things*) e IIoT (*Industrial Internet of Things*)
- Esaminare il consorzio internet industriale
- Analizzare l'architettura di riferimento dell'IoT
- Indirizzare i sensori e i dispositivi IoT e la loro classificazione
- Identificare i protocolli e le tecnologie di comunicazione utilizzati nell'IoT
- Esaminare le diverse piattaforme *Cloud* nell'IoT: general purpose, industriale e open source

- Sviluppare meccanismi di scambio di dati
- Stabilire i requisiti e le strategie di sicurezza
- Introdurre le diverse aree di applicazione dell'IoT e dell'IIoT
- Generare competenze nella rappresentazione e nell'analisi dei dati
- Esaminare i diversi tipi di dati aggregati
- Stabilire le rappresentazioni grafiche più comunemente utilizzate in diversi ambiti
- Determinare i principi di progettazione nella visualizzazione dei dati
- Introdurre la narrazione grafica come strumento
- Analizzare i diversi strumenti software per la creazione di grafici e l'analisi esplorativa dei dati
- Sviluppare competenze per convertire i dati in informazioni da cui estrarre la conoscenza
- Determinare le caratteristiche principali di un *dataset*, la sua struttura, i suoi componenti e le implicazioni della sua distribuzione sulla modellazione
- Supportare il processo decisionale eseguendo un'analisi preventiva completa dei dati
- Sviluppare competenze per risolvere casi di studio utilizzando tecniche di scienza dei dati
- Stabilire gli strumenti e i metodi generali più appropriati modellare ogni dataset rispetto alla pre-elaborazione effettuata
- Valutare i risultati in modo analitico, compreso l'impatto della strategia scelta sulle diverse metriche
- Dimostrare una capacità critica rispetto ai risultati ottenuti dopo l'applicazione di metodi di preelaborazione o modellazione
- Generare conoscenze specialistiche sui prerequisiti statistici per l'analisi e la valutazione dei dati
- Sviluppare le competenze necessarie per l'identificazione, la preparazione e la trasformazione dei dati
- Valutare le diverse metodologie presentate e identificare vantaggi e svantaggi
- Esaminare i problemi in ambienti di dati ad alta dimensionalità
- Sviluppare l'implementazione degli algoritmi utilizzati per la pre-elaborazione dei dati
- Dimostrare la capacità di interpretare le visualizzazioni dei dati per l'analisi descrittiva
- Sviluppare una conoscenza avanzata delle diverse tecniche di preparazione dei dati esistenti per la pulizia, la normalizzazione e la trasformazione dei dati
- Analizzare le serie numeriche
- Sviluppare la formulazione e le proprietà di base dei modelli di serie numeriche univariate
- Esaminare la metodologia di modellazione e previsione delle serie numeriche reali
- Determinare i modelli univariati includendo gli outlier
- Applicare modelli di regressione dinamica e la metodologia di costruzione di tali modelli a partire da serie osservate
- Affrontare l'analisi spettrale delle serie temporali univariate, nonché i fondamenti dell'inferenza basata sui periodogrammi e la loro interpretazione
- Stimare la probabilità e il trend di una serie numerica per un determinato orizzonte temporale
- Analizzare il passaggio dall'informazione alla conoscenza
- Sviluppare i diversi tipi di tecniche di apprendimento automatico
- Esaminare metriche e punteggi per quantificare la qualità dei modelli
- Implementare i diversi algoritmi di apprendimento automatico
- Identificare modelli di ragionamento probabilistico
- Gettare le basi dell'apprendimento profondo
- Dimostrare le competenze acquisite per comprendere i diversi algoritmi di apprendimento automatico
- Determinare i requisiti dei sistemi di big data
- Esaminare diversi modelli di dati e analizzare i database

- Analizzare le funzionalità chiave dei sistemi distribuiti e la loro importanza in diversi tipi di sistemi
- Valutare quali applicazioni diffuse utilizzano i fondamenti dei sistemi distribuiti per la progettazione dei propri sistemi
- Analizzare il modo in cui i database memorizzano e recuperano le informazioni
- Identificare i diversi modelli di replica e i problemi ad essi associati
- Sviluppare modalità di partizionamento e transazioni distribuite
- Identificare i sistemi batch e i sistemi (quasi) in tempo reale
- Analizzare lo stato dell'arte dell'intelligenza artificiale (AI) e dell'analisi dei dati
- Sviluppare una conoscenza specialistica delle tecnologie più diffuse
- Generare una migliore comprensione della tecnologia mediante la casistica
- Analizzare le strategie scelte per selezionare le migliori tecnologie da implementare
- Determinare le aree di applicazione
- Esaminare i rischi reali e potenziali della tecnologia applicata
- Proporre i benefici che ne derivano dall'utilizzo
- Identificare le tendenze future in settori specifici
- Sviluppare le metodologie utilizzate nella cybersecurity
- Esaminare il ciclo dell'intelligence e stabilirne l'applicazione alla cyber intelligence
- Determinare il ruolo dell'analista di intelligence e gli ostacoli all'attività di evacuazione
- Stabilire gli strumenti più comuni per la produzione di intelligence
- Condurre un'analisi dei rischi e comprendere le metriche utilizzate
- Specificare le opzioni di anonimizzazione e l'uso di reti come TOR, I2P, FreeNet
- Illustrare le norme di cybersecurity attualmente in vigore
- Specificare le politiche di backup per i dati personali e professionali
- Valutare i diversi strumenti per fornire soluzioni a problemi di sicurezza specifici
- Stabilire meccanismi per mantenere il sistema aggiornato
- Analizzare le apparecchiature per rilevare gli intrusi
- Determinare le regole di accesso al sistema
- Esaminare e classificare la posta elettronica per evitare frodi
- Generare elenchi di software consentiti
- 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
- Compilare le soluzioni 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*
- Determinare gli strumenti per la protezione della rete e dimostrare perché sono fondamentali per una difesa su più livelli
- 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 attuali per stabilire una configurazione più sicura
- Specificare i passaggi principali per eseguire un test di penetrazione su entrambe le piattaforme iOS e Android
- Sviluppare una conoscenza specialistica dei diversi strumenti di protezione e sicurezza
- Stabilire le migliori pratiche di programmazione per i dispositivi mobili
- Analizzare le principali architetture IoT
- Esaminare le tecnologie di connettività
- Sviluppare i principali protocolli applicativi
- Identificare 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
- Esaminare i metodi IOSINT
- Acquisire le informazioni disponibili dai media pubblici
- Scansionare le reti per ottenere informazioni sulla modalità attiva
- Sviluppare laboratori di prova
- Analizzare gli strumenti per le prestazioni del pentesting
- Catalogare e valutare le diverse vulnerabilità dei sistemi
- Definire concretamente le diverse metodologie di *hacking*
- Analizzare le fasi di un compilatore
- Esaminare l'architettura dei processori x86 e l'architettura dei processori ARM
- Determinare i diversi tipi di analisi
- Applicare il *sandboxing* in diversi ambienti
- Sviluppare diverse tecniche di analisi dei *malware*
- Creare strumenti orientati all'analisi dei *malware*
- 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 conservare nei log
- Generare codice sanificato, facilmente verificabile e di qualità
- Valutare la documentazione appropriata per ogni fase di sviluppo
- Definire concretamente il comportamento del server per ottimizzare il sistema
- Sviluppare codice modulare, riutilizzabile e manutenibile
- Identificare i diversi elementi di prova di un reato
- Generare conoscenze specializzate per ottenere dati da diversi supporti prima che vadano persi
- Recuperare i dati che sono stati cancellati intenzionalmente
- Analizzare i log e i record del sistema
- Determinare il modo in cui i dati vengono duplicati per non alterare gli originali
- Sostanziare le prove di coerenza
- Generare un rapporto robusto e continuo
- Presentare i risultati in modo coerente
- Stabilire come difendere la relazione dinanzi all'autorità competente
- Specificare le strategie per rendere il telelavoro sicuro e protetto
- Esaminare l'uso delle criptovalute, l'impatto sull'economia e sulla sicurezza
- Analizzare la situazione degli utenti e il grado di analfabetismo digitale
- Determinare l'ambito di utilizzo della blockchain
- Presentare le alternative all'IPv4 nell'indirizzamento di rete
- Sviluppare strategie per educare la popolazione all'uso corretto delle tecnologie
- Generare conoscenze specialistiche per affrontare le nuove sfide della sicurezza e prevenire i furti di identità
- Specificare le strategie per rendere il telelavoro sicuro e protetto

03

Competenze

Gli studenti che completano il Master Specialistico in Secure Information Management saranno in grado di svolgere un gran numero di compiti altamente specializzati nei settori della gestione dei dati e della cybersecurity. Questa qualifica fonde entrambi i rami per offrire conoscenze complementari che possono essere incrociate e utilizzate in situazioni e ambienti professionali diversi. In questo modo, gli studenti intraprenderanno un processo di apprendimento completo che li porterà a diventare veri specialisti del settore.

Le tue nuove competenze ti renderanno il più grande specialista del tuo ambiente"

Competenze generali

- Sviluppare una prospettiva tecnica e commerciale dell'analisi dei dati
- Comprendere i più recenti algoritmi, piattaforme e strumenti per l'esplorazione, la visualizzazione, la manipolazione, l'elaborazione e l'analisi dei dati
- Implementare una visione aziendale necessaria per il valore aggiunto come elemento chiave per il processo decisionale
- Essere in grado di affrontare problemi specifici dell'analisi dei dati
- Conoscere le metodologie utilizzate in materia di cybersecurity
- Valutare ogni tipo di minaccia per offrire una soluzione ottimale a seconda dei casi
- Generare soluzioni intelligenti e complete per automatizzare il comportamento in caso di incidenti
- Saper valutare i rischi associati alle vulnerabilità interne ed esterne all'azienda
- Comprendere l'evoluzione e l'impatto dell'IoT nel tempo
- Dimostrare che un sistema è vulnerabile, attaccarlo in modo proattivo e risolvere questi problemi
- Applicare il *sandboxing* in diversi ambienti
- Conoscere le linee guida che deve seguire un buon sviluppatore per rispettare la sicurezza richiesta

Competenze specifiche

- Specializzarsi in *data science* da un punto di vista tecnico e commerciale
- Visualizzare i dati nel modo più appropriato per favorirne la condivisione e la comprensione da parte di diversi profili
- Indirizzare le aree funzionali chiave dell'organizzazione in cui la scienza dei dati può apportare il massimo valore
- Sviluppare il ciclo di vita dei dati, la sua tipologia e le tecnologie e le fasi necessarie per la sua gestione
- Elaborare e manipolare i dati utilizzando linguaggi e librerie specifiche
- Sviluppare una conoscenza avanzata delle tecniche fondamentali di data mining per la selezione, la pre-elaborazione e la trasformazione dei dati
- Specializzati nei principali algoritmi di *machine learning* per l'estrazione di conoscenza nascosta dai dati
- Generare competenze specifiche sulle architetture software e sui sistemi necessari per l'uso intensivo dei dati
- Determinare come l'IoT possa essere una fonte di generazione di dati e informazioni chiave su cui applicare la scienza dei dati per l'estrazione della conoscenza
- Analizzare i diversi modi di applicare la scienza dei dati in diversi settori o verticali, imparando da esempi reali
- Condurre operazioni di sicurezza difensiva
- Avere una percezione approfondita e specializzata della sicurezza informatica
- Possedere conoscenze specialistiche nel campo della cybersecurity e della cyber intelligence
- Conoscere a fondo aspetti fondamentali quali il ciclo dell'intelligence, le fonti di intelligence, l'ingegneria sociale, la metodologia OSINT, HUMINT, l'anonimizzazione e l'analisi del rischio, le metodologie esistenti (OWASP, OWISAM, OSSTM, PTES) e le normative vigenti in materia di cybersecurity
- Comprendere l'importanza di concepire una difesa a più livelli, nota anche come *defense in depth*, che copra tutti gli aspetti di una rete aziendale, dove alcuni dei concetti e dei sistemi che vedremo possono essere utilizzati e applicati anche in un ambiente domestico
- Saper applicare i processi di sicurezza per smartphone e dispositivi portatili
- Conoscere i mezzi per eseguire il cosiddetto *hacking* etico e proteggere un'azienda da un attacco informatico
- Indagare su un incidente di cybersecurity
- Comprendere le diverse tecniche di attacco e di difesa disponibili
- Analizzare il ruolo dell'analista di cybersecurity e capire come funziona l'ingegneria sociale e i suoi metodi

Vuoi distinguerti dagli altri specialisti, ma non sai come fare? Questo Master Specialistico fa al caso tuo"

04

Direzione del corso

Questo programma è impartito dai migliori docenti nel campo della cybersecurity e della gestione dei dati digitali. La loro esperienza garantisce che gli studenti ricevano i contenuti più completi e aggiornati, in modo da poterli applicare direttamente alle loro carriere professionali. I docenti di questo Master Specialistico in Secure Information Management trasmetteranno tutte le loro conoscenze agli studenti, al fine di assicurare che diventino specialisti altamente qualificati e richiesti dalle grandi aziende dei loro paesi.

I migliori specialisti ti insegnano come diventare un professionista di spicco del settore"

Direttore Ospite Internazionale

Il Dott. Frederic Lemieux è riconosciuto a livello internazionale come esperto innovativo e leader ispiratore nei settori dell'**Intelligence, della Sicurezza Nazionale, della Sicurezza Interna, Cybersecurity** e delle **Tecnologie Dirompenti**. La sua dedizione costante e i suoi contributi rilevanti alla ricerca e all'istruzione lo posizionano come figura chiave nella promozione della sicurezza e della comprensione delle tecnologie emergenti di oggi. Nel corso della sua carriera professionale, ha ideato e condotto programmi accademici all'avanguardia presso diverse istituzioni rinomate, come l'**Università di Montreal,** la **George Washington University** e la **Georgetown University**.

Nel corso della sua vasta esperienza, ha pubblicato molti libri importanti, tutti relativi all'**intelligence criminale, alla polizia, alle minacce informatiche e alla sicurezza internazionale**. Ha anche contribuito in modo significativo al campo della cybersecurity pubblicando numerosi articoli su riviste accademiche che esaminano il controllo del crimine durante i grandi disastri, l'antiterrorismo, le agenzie di intelligence e la cooperazione di polizia. Inoltre, ha partecipato come relatore a diverse conferenze nazionali e internazionali, affermandosi come un importante accademico e professionista.

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. La sua prestigiosa carriera accademica lo ha portato a ricoprire il ruolo di Professore di Pratica e Direttore di Facoltà dei programmi MPS in **Intelligence Applicata, Gestione del Rischio di Cybersecurity, Gestione della Tecnologia e Gestione della Tecnologia dell'Informazione** presso la Georgetown University.

Dott. Lemieux, Frederic

- Ricercatore in Intelligence, Cybersecurity e Tecnologie dirompenti presso la Georgetown University
- Direttore del Master in Information Technology Management della Georgetown University
- Direttore del Master in Technology Management presso la Georgetown University
- Direttore del Master in Cybersecurity Risk Management dell'Università di Georgetow
- Direttore del Master in Applied Intelligence presso la Georgetown University
- Professore di Tirocini presso la Georgetown University
- Laurea in Sociologia, Minor Degree in Psicologia, Università Laval
- Dottorato di ricerca in Criminologia presso la School of Criminology dell'Università di Montreal
- Membro di: New Program Roundtable Committee, presso la Georgetown University

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

Direzione

Dott. Peralta Martín-Palomino, Arturo

- CEO e CTO presso Prometeus Global Solutions
- CTO presso Korporate Technologies
- CTO presso AI Shephers GmbH
- Dottore in Ingegneria Informatica presso l'Università di Castilla La Mancha
- Dottore in Economia Aziendale e Finanze presso l'Università Camilo José Cela Premio di Eccellenza del Dottorato
- Laurea in Psicologia presso l'università di Castilla La Mancha
- Master in Tecnologie Informatiche Avanzate presso l'Università di Castilla La Mancha
- Master MBA+E (Master in Amministrazione Aziendale e Ingegneria Organizzativa) presso l'Università di Castilla La Mancha
- Professore associato, docente della Laurea triennale e Master in Ingegneria Informatica presso l'Università di Castilla La Mancha
- Professore del Master in Big Data e Data Science presso l'Università Internazionale di Valencia
- Professore del Master in Industria 4.0 e Master in Disegno Industriale e Sviluppo di Prodotti
- Membro del Gruppo di Ricerca SMIL dell'Università di Castilla La Mancha

Dott.ssa Fernández Sapena, Sonia

- Formatrice in Sicurezza Informatica e Hacking Etico Centro di Riferimento Nazionale per l'Informatica e le Telecomunicazioni di Getafe Madrid
- Istruttrice certificata E-Council Madrid
- Formatrice nelle seguenti certificazioni: EXIN Ethical Hacking Foundation e EXIN Cyber & IT Security Foundation Madrid
- Formatrice certificata dal CAM per i seguenti certificati di professionalità: Sicurezza Informatica (IFCT0190), Gestione di Reti di Voce e Dati (IFCM0310), Amministrazione di Reti Dipartimentali (IFCT0410), Gestione degli Allarmi nelle Reti di Telecomunicazioni (IFCM0410), Operatore di Reti di Voce e Dati (IFCM0110) e Amministrazione di Servizi Internet (IFCT0509)
- Collaboratrice esterna CSO/SSA (*Chief Security Officer/Senior Security Architect*). Università delle Isole Baleari
- Ingegnere Informatico Università di Alcalá de Henares. Madrid
- Master in DevOps: Docker and Kubernetes Cas-Training Madrid
- Microsoft Azure Security Techonologies E-Council Madrid

Personale docente

Dott. Armero Fernández, Rafael

- Business Intelligence Consultant presso SDG Group
- Digital Engineer presso Mi-GSO
- Logistic Engineer presso Torrecid S.A
- Quality Intern presso INDRA
- Laurea in Ingegneria Aerospaziale presso l'Università Politecnica di Valencia
- Master in Professional Development 4.0 presso l'Università di Alcalá de Henares

Dott. Peris Morillo, Luis Javier

- Technical Lead presso Capitole Consulting
- Senior Technical Lead e Delivery Lead Support presso HCL
- Agile Coach e Direttore di Operazioni presso Mirai Advisory
- Sviluppatore, Team Lead, Scrum Master, Agile Coach, Product Manager presso DocPath
- Ingegneria Superiore in Informatica presso la ESI di Ciudad Real (UCLM)
- Laurea Magistrale in Gestione di Progetti presso la CEOE - Confederazione Spagnola di Organizzazioni Aziendali
- +50 MOOC corsi, impartiti da Università riconosciute come l'Università di Stanford, del Michigan, del Yonsei, l'Università Politecnice di Madrid ecc.

Dott. Montoro Montarroso, Andrés

- Membro del Gruppo di Ricerca SMIL dell'Università di Castilla La Mancha
- Scientifico di Dati presso Prometeus Global Solutions
- Laurea in Ingegneria Informatica presso l'Università di Castilla - La Mancha Specializzazione in Scienze Informatiche
- Master in Scienze dei Dati e Ingegneria dei Computer presso l'Università di Granada

Dott.ssa Fernández Meléndez, Galina

- Analista Dati presso ADN Mobile Solution
- Processi ETL, estrazione di dati, analisi e visualizzazione dei dati, creazione di KPI, progettazione e implementazione di Dashboard, controllo di gestione Sviluppo in R, gestione di SQL e altro
- Determinazione dei modelli, modellazione predittiva, apprendimento automatico
- Laurea in Amministrazione Aziendale Università Bicentenaria di Aragua (Caracas) - Laurea in Progettazione e Finanze Pubbliche Scuola Venezuelana di Progettazione - Scuola di Finanza
- Master in Analisi dei dati e Intelligenza di Commercio Università di Oviedo
- MBA in Amministrazione e Direzione Aziendale presso la Scuola di Commercio Europea di Barcellona
- Master in Big Data e Business Intelligence presso la Scuola di Commercio Europea di Barcellona

Dott.ssa Pedrajas Parabás, Elena

- Business Analyst in Management Solutions a Madrid
- Ricercatrice presso il Dipartimento di Informatica e Analisi Numerica dell'Università di Cordoba
- Ricercatrice presso il Centro Singolare di Ricerca in Tecnologie Intelligenti di Santiago de Compostela
- Laureata in Ingegneria informatica Master in Data Science e Ingegneria Informatica e Intelligence (Scuola Europea di Business di Barcellona)

Dott.ssa Martínez Cerrato, Yésica

- Tecnico di prodotti di sicurezza elettronica presso Securitas Seguridad España
- Analista di intelligenza Aziendale presso Ricopia Technologies (Alcalá de Henares) Laurea in Ingegneria Elettronica delle Comunicazioni presso la Scuola Politecnica Superiore, Università di Alcalá
- Responsabile delle nuove incorporazioni dei software di gestione commerciale (CRM, ERP, INTRANET), prodotti e procedure presso Ricopia Technologies (Alcalá de Henares)
- Responsabile dei nuovi tirocinanti incorporati alle Aule di Informatica dell'Università di Alcalá
- Responsabile di progetti nell'area dell'Integrazione di Grandi Account presso Correos y Telégrafos (Madrid)
- Tecnico Informatico - Responsabile delle aule informatiche OTEC presso l'Università di Alcalá (Alcalá de Henares)
- Professoressa di lezioni di Informatica presso l'Associazione ASALUMA (Alcalá de Henares)
- Tirocinio formativo come Tecnico Informatico presso OTEC, Università di Alcalá (Alcalá de Henares)

Dott. Fondón Alcalde, Rubén

- Analista aziendale in gestione del valore del cliente presso Vodafone Spagna
- Responsabile dell'integrazione dei servizi di Entelgy per Telefónica Global Solutions
- Responsabile dell'account Clone Server Online presso EDM Electronics
- Analista Aziendale per il Sud Europa presso Vodafone Global Enterprise
- Ingegnere delle Telecomunicazioni presso l'Università Europea di Madrid
- Master in Big Data e Analytics presso l'Università Internazionale di Valencia

Dott. Díaz Díaz-Chirón, Tobías

- Ricercatore nel laboratorio ArCO dell'Università di Castilla La Mancha, gruppo dedicato a progetti relazionati con l'architettura e reti di computer
- Consulente presso Blue Telecom, compagnia dedicata al settore delle telecomunicazioni
- Laurea in Ingegneria Informatica presso l'Università di Castilla - La Mancha

Dott. Tato Sánchez, Rafael

- Gestione di progetti presso INDRA SISTEMAS S.A. Gestione del contratto di manutenzione per le installazioni dei sistemi di trasporto intelligenti dipendenti dal Centro di Controllo e Gestione del Traffico della Direzione Generale del Traffico di Madrid
- Direttore tecnico presso INDRA SISTEMAS S.A., responsabile del Centro di Controllo e Gestione del Traffico della Direzione Generale del Traffico di Madrid
- Ingegnere di sistemi ENA TRÁFICO SAU
- Ingegnere Tecnico Industriale in Elettricità presso l'Università Politecnica di Madrid
- Laurea in Elettronica Industriale e Ingegneria dell'Automazione presso l'Università Europea di Madrid
- Certificazione professionale SSCE0110: Docenza per la formazione professionale per il lavoro
- Master in Industria 4.0 presso l'Università Internazionale di La Rioja (UNIR)

Dott. Catalá Barba, José Francisco

- Middle management nel MINISDEF Diversi compiti e responsabilità all'interno del GOE III, come l'amministrazione e la gestione degli incidenti della rete interna, lo sviluppo di programmi personalizzati per le diverse aree, i corsi di formazione per gli utenti della rete e per il personale del gruppo in generale
- Tecnico elettronico nella Fabbrica Ford di Almusafes, Valencia, programmazione di robot, PLC, riparazione e manutenzione
- Tecnico di Elettronica
- Sviluppatore di applicazioni per dispositivi mobili

Dott. Jiménez Ramos, Álvaro

- Analista di Sicurezza presso Capgemini
- Analista di Cybersecurity L1 presso Axians
- Analista di Cybersecurity L2 presso Axians
- Analista di Cybersecurity presso SACYR S.A.
- Laurea in Ingegneria Telematica presso l'Università Politecnica di Madrid
- Master in Cybersecurity e Hacking Etico presso il CICE
- Corso Avanzato di Cybersecurity presso Deusto Formación

Dott.ssa Marcos Sbarbaro, Victoria Alicia

- Sviluppatrice di Applicazioni Mobili Native Android presso B60 UK
- Analista Programmatrice per la gestione, il coordinamento e la documentazione di un ambiente di allarme di sicurezza virtualizzato
- Analista programmatrice di applicazioni Java per ATM
- Professionista dello Sviluppo Software per la convalida della firma e l'applicazione di gestione dei documenti
- Tecnico di Siistemi per la migrazione delle apparecchiature e per la gestione, la manutenzione e la formazione dei palmari
- Ingegneria Tecnica dei Sistemi Informatici Universitat Oberta de Catalunya
- Master in Cyber Security e Hacking Etico Ufficiale EC- Council e CompTIA

Dott. Peralta Alonso, Jon

- Avvocato / DPO Altia Consultores S.A.
- Docente del Master in Protezione dei Dati Personali, Cybersecurity e Diritto delle TIC Università pubblica dei Paesi Baschi (UPV-EHU)
- Avvocato / Consulente legale Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Consulente legale / Tirocinante Studio professionale: Oscar Padura
- Laurea in Giurisprudenza Università pubblica dei Paesi Baschi
- Master in Delegato della Protezione dei Dati Delegati. EIS Innovative School
- Master Universitario in Legge Università pubblica dei Paesi Baschi
- Master Specialistico in Pratica del Contenzioso Civile Università Internazionale Isabella I di Castiglia

Dott. Redondo, Jesús Serrano

- Sviluppatore FrontEnd Junior e Tecnico di Cybersecurity Junior
- Sviluppatore FrontEnd presso Telefónica, Madrid
- Sviluppatore FrontEnd. Best Pro Consulting SL, Madrid
- Installatore di apparecchiature e servizi di Telecomunicazione Gruppo Zener, Castilla y León
- Installatore di apparecchiature e servizi di Telecomunicazione Lican Comunicaciones SL, Castilla y León
- Certificato in Sicurezza Informatica. CFTIC Getafe, Madrid
- Tecnico Senior: Telecomunicazioni e Sistemi Informatici IES Trinidad Arroyo, Palencia
- Tecnico Senior: Impianti Elettrotecnici MT e BT. IES Trinidad Arroyo, Palencia
- Formazione in Reverse Engineering, stenografia, crittografia Accademia Hacker Incibe (Talenti Incibe)

I principali professionisti del settore si sono uniti per fornirti le conoscenze più ampie in questo campo, così da poter crescere con tutte le garanzie di successo"

05

Struttura e contenuti

I contenuti di questo Master Specialistico in Secure Information Management sono stati concepiti in base allo stato attuale della professione, in modo che gli studenti ricevano le migliori conoscenze possibili e possano applicarle al loro settore. Nel corso dei 20 moduli che compongono questa qualifica, gli studenti potranno apprendere tutto ciò che riguarda la gestione e la sicurezza dei dati e delle informazioni digitali, diventando veri e propri specialisti del settore.

Non esiste un programma migliore. Questo Master Specialistico fornisce tutto ciò di cui hai bisogno per diventare un massimo esperto in queste aree"

Modulo 1. Analisi dei dati nell'organizzazione aziendale

1.1. Analisi aziendale
- 1.1.1. Analisi aziendale
- 1.1.2. Struttura dei dati
- 1.1.3. Fasi ed elementi

1.2. L'analisi dei dati nell'impresa
- 1.2.1. Dashboard e Kpi per aree
- 1.2.2. Reporting operativo, tattico e strategico
- 1.2.3. Analisi dei dati applicata a ciascuna area
  - 1.2.3.1. Marketing e comunicazione
  - 1.2.3.2. Commerciale
  - 1.2.3.3. Servizio clienti
  - 1.2.3.4. Acquisti
  - 1.2.3.5. Amministrazione
  - 1.2.3.6. HR
  - 1.2.3.7. Produzione
  - 1.2.3.8. IT

1.3. Marketing e comunicazione
- 1.3.1. Kpi da misurare, applicazioni e benefici
- 1.3.2. Sistemi di marketing e *data warehouse*
- 1.3.3. Implementazione di una struttura di analisi dei dati nel Marketing
- 1.3.4. Piano di marketing e comunicazione
- 1.3.5. Strategie, previsioni e gestione delle campagne

1.4. Commerciale e vendite
- 1.4.1. Contributi dell'analisi dei dati nell'area commerciale
- 1.4.2. Esigenze del reparto Vendite
- 1.4.3. Studi di mercato

1.5. Servizio clienti
- 1.5.1. Fidelizzazione
- 1.5.2. Qualità del personale e intelligenza emozionale
- 1.5.3. Soddisfazione del cliente

1.6. Acquisti
- 1.6.1. Analisi dei dati per le ricerche di mercato
- 1.6.2. Analisi dei dati per la ricerca competitiva
- 1.6.3. Altre applicazioni

1.7. Amministrazione
- 1.7.1. Esigenze nel settore amministrativo
- 1.7.2. *Data Warehouse* e analisi dei rischi finanziari
- 1.7.3. *Data Warehouse* e analisi del rischio di credito

1.8. Risorse umane
- 1.8.1. HR e vantaggi dell'analisi dei dati
- 1.8.2. Strumenti di analisi dei dati nel dipartimento HR
- 1.8.3. Applicazioni di analisi dei dati nel dipartimento HR

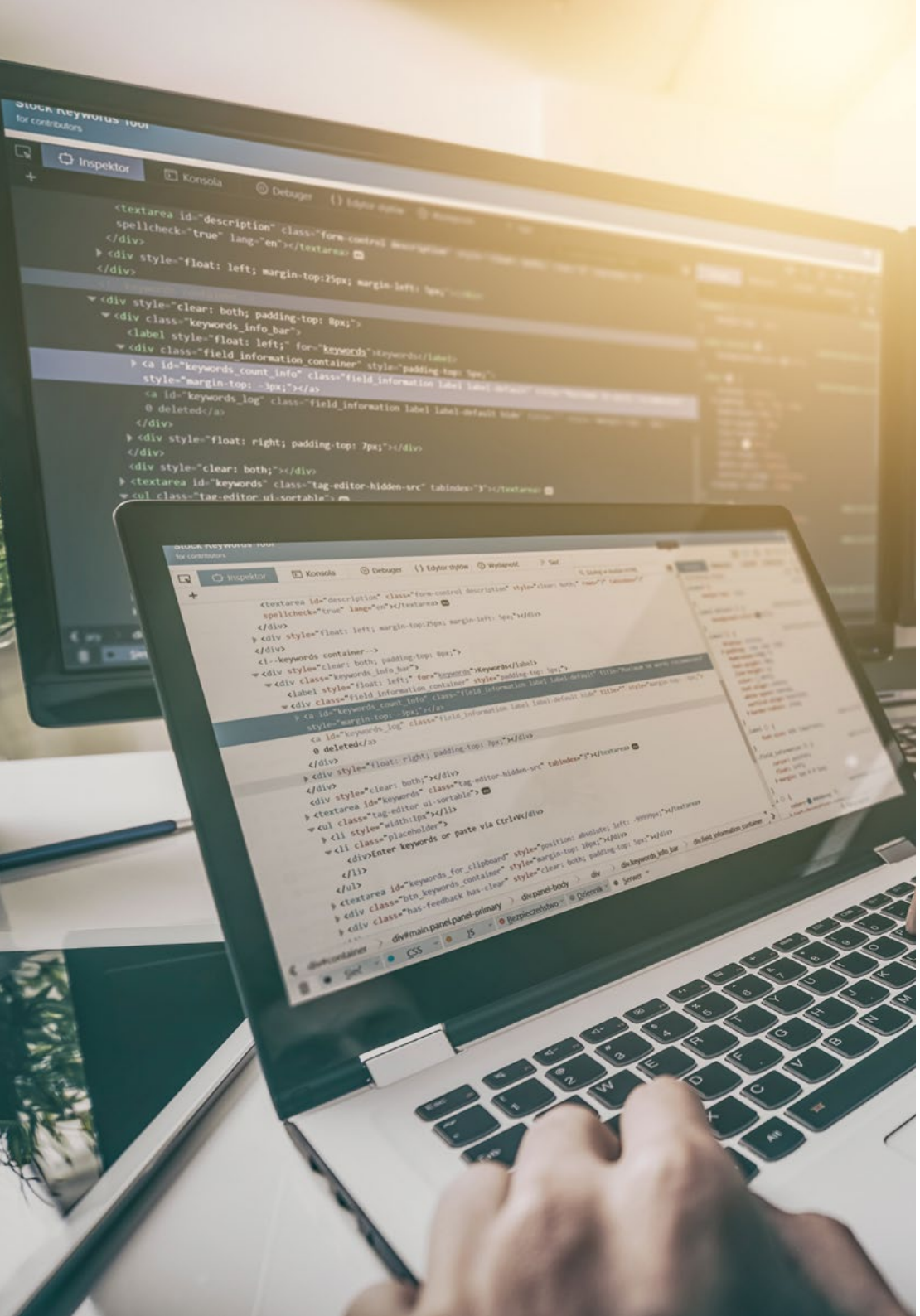
1.9. Produzione
- 1.9.1. Analisi dei dati nell'area di produzione
- 1.9.2. Applicazioni
- 1.9.3. Benefici

1.10. IT
- 1.10.1. Dipartimento di IT
- 1.10.2. Analisi dei dati e trasformazione digitale
- 1.10.3. Innovazione e produttività

Modulo 2. Gestione, elaborazione dei dati e informazioni per la scienza dei dati

2.1. Statistica. Variabili, indici e rapporti
- 2.1.1. La statistica
- 2.1.2. Dimensioni statistiche
- 2.1.3. Variabili, indici e rapporti

2.2. Tipologia di dati
- 2.2.1. Qualitativi
- 2.2.2. Quantitativi
- 2.2.3. Caratterizzazione e categorie



2.3. Conoscenza dei dati delle misurazioni
- 2.3.1. Misure di centralizzazione
- 2.3.2. Misure di dispersione
- 2.3.3. Correlazione

2.4. Conoscenza dei dati dai grafici
- 2.4.1. Visualizzazione in base al tipo di dati
- 2.4.2. Interpretazione di informazioni grafiche
- 2.4.3. Personalizzazione della grafica con R

2.5. Probabilità
- 2.5.1. Probabilità
- 2.5.2. Funzione di probabilità
- 2.5.3. Distribuzioni

2.6. Raccolta di dati
- 2.6.1. Metodologia di raccolta
- 2.6.2. Strumenti di raccolta
- 2.6.3. Canali di raccolta

2.7. Pulizia del dato
- 2.7.1. Fasi di pulizia dei dati
- 2.7.2. Qualità del dato
- 2.7.3. Elaborazione dei dati (con R)

2.8. Analisi dei dati, interpretazione e valutazione dei risultati
- 2.8.1. Misure statistiche
- 2.8.2. Indici di relazione
- 2.8.3. Estrazione di dati

2.9. Magazzino dati (*Data Warehouse*)
- 2.9.1. Elementi
- 2.9.2. Design

2.10. Disponibilità del dato
- 2.10.1. Accesso
- 2.10.2. Utilità
- 2.10.3. Sicurezza

Modulo 3. Dispositivi e piattaforme IoT come base per la scienza dei dati

3.1. *Internet of Things*
- 3.1.1. Internet del futuro, *Internet of Things*
- 3.1.2. Il consorzio di internet industriale

3.2. Architettura di riferimento
- 3.2.1. Architettura di riferimento
- 3.2.2. Livelli
- 3.2.3. Componenti

3.3. Sensori e dispositivi IoT
- 3.3.1. Componenti principali
- 3.3.2. Sensori e attuatori

3.4. Comunicazioni e protocolli
- 3.4.1. Protocolli Modello OSI
- 3.4.2. Tecnologie di comunicazione

3.5. Piattaforme *cloud* per IoT e IIoT
- 3.5.1. Piattaforme con proposito generale
- 3.5.2. Piattaforme industriali
- 3.5.3. Piattaforme con codice aperto

3.6. Gestione dei dati in piattaforme IoT
- 3.6.1. Meccanismi di gestione dei dati. Dati aperti
- 3.6.2. Scambio e visualizzazione dei dati

3.7. Sicurezza in IoT
- 3.7.1. Requisiti di sicurezza e aree di sicurezza
- 3.7.2. Strategie di sicurezza IIoT

3.8. Applicazioni IoT
- 3.8.1. Cure intelligenti
- 3.8.2. Salute e condizione fisica
- 3.8.3. Casa intelligente
- 3.8.4. Altre applicazioni

3.9. Applicazioni IIoT
- 3.9.1. Fabbricazione
- 3.9.2. Trasporto
- 3.9.3. Energia
- 3.9.4. Agricoltura e allevamento
- 3.9.5. Altri settori

3.10. Industria 4.0
- 3.10.1. IoRT *(Internet of Robotics Things)*
- 3.10.2. Fabbricazione additiva 3D
- 3.10.3. *Big Data Analytics*

Modulo 4. Rappresentazione grafica per l'analisi dei dati

4.1. Analisi esplorativa
- 4.1.1. Rappresentazione per l'analisi dei dati
- 4.1.2. Il valore della rappresentazione grafica
- 4.1.3. Nuovi paradigmi di rappresentazione grafica

4.2. Ottimizzazione per la scienza dei dati
- 4.2.1. Gamma di colori e design
- 4.2.2. Gestalt nella rappresentazione grafica
- 4.2.3. Errori da evitare e suggerimenti

4.3. Fonti di dati di base
- 4.3.1. Per una rappresentazione di qualità
- 4.3.2. Per una rappresentazione di quantità
- 4.3.3. Per una rappresentazione di tempo

4.4. Fonti di dati di complessi
- 4.4.1. File, elenchi e DB
- 4.4.2. Dati aperti
- 4.4.3. Dati generati in modo continuo

4.5. Tipi di grafici
- 4.5.1. Rappresentazioni di base
- 4.5.2. Rappresentazione a blocchi
- 4.5.3. Rappresentazione per l'analisi della dispersione
- 4.5.4. Rappresentazioni circolari
- 4.5.5. Rappresentazioni a bolla
- 4.5.6. Rappresentazioni geografiche

4.6. Tipi di visualizzazione
- 4.6.1. Comparative e relazionali
- 4.6.2. Distribuzione
- 4.6.3. Gerarchia

4.7. Progettazione di report con rappresentazione grafica
- 4.7.1. Applicazione dei grafici nei rapporti di marketing
- 4.7.2. Applicazione dei grafici nei dashboard e nei Kpi
- 4.7.3. Applicazione dei grafici nei piani strategici
- 4.7.4. Altri usi: scienza, salute, affari

4.8. Narrazione grafica
- 4.8.1. Narrazione grafica
- 4.8.2. Evoluzione
- 4.8.3. Utilità

4.9. Strumenti orientati alla visualizzazione
- 4.9.1. Strumenti avanzati
- 4.9.2. Software online
- 4.9.3. *Open Source*

4.10. Nuove tecnologie di visualizzazione dei dati
- 4.10.1. Sistemi per la virtualizzazione della realtà
- 4.10.2. Sistemi per l'aumento e il potenziamento della realtà
- 4.10.3. Sistemi intelligenti

Modulo 5. Strumenti di gestione dei dati

5.1. Scienza dei dati
- 5.1.1. Scienza dei dati
- 5.1.2. Strumenti avanzati per i data scientist

5.2. Dati, informazioni e conoscenze
- 5.2.1. Dati, informazioni e conoscenze
- 5.2.2. Tipi di dati
- 5.2.3. Fonti di dati

5.3. Dai dati alle informazioni
- 5.3.1. Analisi dei dati
- 5.3.2. Tipi di analisi
- 5.3.3. Estrazione di informazioni da un *Dataset*

5.4. Estrazione di informazioni tramite visualizzazione
- 5.4.1. La visualizzazione come strumento di analisi
- 5.4.2. Metodi di visualizzazione
- 5.4.3. Visualizzazione di un set di dati

5.5. Qualità dei dati
- 5.5.1. Dati di qualità
- 5.5.2. Pulizia dei dati
- 5.5.3. Pre-elaborazione dei dati di base

5.6. *Dataset*
- 5.6.1. Arricchimento del *dataset*
- 5.6.2. La maledizione della dimensionalità
- 5.6.3. Modificare il nostro set di dati

5.7. Sbilanciamento
- 5.7.1. Sbilanciamento delle classi
- 5.7.2. Tecniche di mitigazione dello sbilanciamento
- 5.7.3. Bilanciamento di un *dataset*

5.8. Modelli non supervisionati
- 5.8.1. Modello non supervisionato
- 5.8.2. Metodi
- 5.8.3. Classificazione con modelli non supervisionati

5.9. Modelli supervisionati
- 5.9.1. Modello supervisionato
- 5.9.2. Metodi
- 5.9.3. Classificazione con modelli supervisionati

5.10. Strumenti e buone pratiche
- 5.10.1. Le migliori pratiche per un data scientist
- 5.10.2. Il modello migliore
- 5.10.3. Strumenti utili

Modulo 6. Estrazione di dati. Selezione, pre-elaborazione e trasformazione

6.1. Inferenza statistica
- 6.1.1. Statistica descrittiva vs. Inferenza statistica
- 6.1.2. Procedure parametriche
- 6.1.3. Procedure non parametriche

6.2. Analisi esplorativa
- 6.2.1. Analisi descrittiva
- 6.2.2. Visualizzazione
- 6.2.3. Preparazione dei dati

6.3. Preparazione dei dati
- 6.3.1. Integrazione e pulizia dei dati
- 6.3.2. Normalizzazione dei dati
- 6.3.3. Trasformazione degli attributi

6.4. Valori mancanti
- 6.4.1. Gestione dei valori mancanti
- 6.4.2. Metodi di imputazione a massima verosimiglianza
- 6.4.3. Imputazione dei valori mancanti con l'apprendimento automatico

6.5. Rumore nei dati
- 6.5.1. Classi e attributi di rumore
- 6.5.2. Filtraggio del rumore
- 6.5.3. Effetto del rumore

6.6. La maledizione della dimensionalità
- 6.6.1. *Oversampling*
- 6.6.2. *Undersampling*
- 6.6.3. Riduzione multidimensionale dei dati

6.7. Da attributi continui a discreti
- 6.7.1. Dati continui e dati discreti
- 6.7.2. Processo di discretizzazione

6.8. I dati
- 6.8.1. Selezione dei dati
- 6.8.2. Prospettive e criteri di selezione
- 6.8.3. Metodi di selezione

6.9. Selezione di istanze
- 6.9.1. Metodi per la selezione delle istanze
- 6.9.2. Selezione di prototipi
- 6.9.3. Metodi avanzati per la selezione delle istanze

6.10. Pre-elaborazione dei dati in ambienti *Big Data*
- 6.10.1. *Big Data*
- 6.10.2. Pre-elaborazione "classica" contro pre-elaborazione massiva
- 6.10.3. *Smart Data*

Modulo 7. Prevedibilità e analisi dei fenomeni stocastici

7.1. Serie temporali
- 7.1.1. Serie temporali
- 7.1.2. Utilità e applicabilità
- 7.1.3. Casi di studio correlati

7.2. La serie temporale
- 7.2.1. Trend Stagionalità di ST
- 7.2.2. Variazioni tipiche
- 7.2.3. Analisi dei residui

7.3. Tipologie
- 7.3.1. Stazionarie
- 7.3.2. Non stazionarie
- 7.3.3. Trasformazioni e adattamenti

7.4. Schemi per le serie temporali
- 7.4.1. Schema additivo (modello)
- 7.4.2. Schema moltiplicativo (modello)
- 7.4.3. Procedure per determinare il tipo di modello

7.5. Metodi base di *forecast*
- 7.5.1. Media
- 7.5.2. *Naïve*
- 7.5.3. *Naïve* stagionale
- 7.5.4. Confronto tra i metodi

7.6. Analisi dei residui
- 7.6.1. Autocorrelazione
- 7.6.2. ACF dei residui
- 7.6.3. Test di correlazione

7.7. Regressione nel contesto delle serie temporali
- 7.7.1. ANOVA
- 7.7.2. Fondamenti
- 7.7.3. Applicazione pratica

7.8. Modelli predittivi di serie temporali
- 7.8.1. ARIMA
- 7.8.2. Smoothing esponenziale

7.9. Manipolazione e analisi delle serie temporali con R
- 7.9.1. Preparazione dei dati
- 7.9.2. Identificazione di modelli
- 7.9.3. Analisi del modello
- 7.9.4. Previsione

7.10. Analisi grafica combinata con R
- 7.10.1. Situazioni tipiche
- 7.10.2. Applicazione pratica per la risoluzione di problemi semplici
- 7.10.3. Applicazione pratica per la risoluzione di problemi avanzati

Modulo 8. Progettazione e sviluppo di sistemi intelligenti

8.1. Pre-elaborazione dei dati
- 8.1.1. Pre-elaborazione dei dati
- 8.1.2. Trasformazione dei dati
- 8.1.3. Estrazione di dati

8.2. Apprendimento automatico
- 8.2.1. Apprendimento supervisionato e non supervisionato
- 8.2.2. Apprendimento forzato
- 8.2.3. Altri modelli di apprendimento

8.3. Algoritmi di classificazione
- 8.3.1. Apprendimento Automatico Induttivo
- 8.3.2. SVM y KNN
- 8.3.3. Metriche e punteggi per la classificazione

8.4. Algoritmi di Regressione
- 8.4.1. Regressione lineare, regressione logistica e modelli non lineari
- 8.4.2. Serie temporali
- 8.4.3. Metriche e punteggi di regressione

8.5. Algoritmi di Clustering
- 8.5.1. Tecniche di clustering gerarchico
- 8.5.2. Tecniche di clustering partizionale
- 8.5.3. Metriche e punteggi di *clustering*

8.6. Tecniche di regole di associazione
- 8.6.1. Metodi per l'estrazione delle regole
- 8.6.2. Metriche e punteggi per gli algoritmi di regole di associazione

8.7. Tecniche di classificazione avanzate. Multi classificatori
- 8.7.1. Algoritmi di *Bagging*
- 8.7.2. Classificatore "*Random Forests*"
- 8.7.3. "*Boosting*" per alberi decisionali

8.8. Modelli grafici probabilistici
- 8.8.1. Modelli probabilistici
- 8.8.2. Reti bayesiane. Proprietà, rappresentazione e parametrizzazione
- 8.8.3. Altro modelli grafici probabilistici

8.9. Reti Neuronali
- 8.9.1. Apprendimento automatico con reti neuronali artificiali
- 8.9.2. Reti *feedforward*

8.10. Apprendimento profondo
- 8.10.1. Reti *feedforward* profonde
- 8.10.2. Reti neurali convoluzionali e modelli di sequenza
- 8.10.3. Strumenti per l'implementazione di reti neurali profonde

Modulo 9. Architetture e sistemi a uso intensivo di dati

9.1. Requisiti non funzionali. Pilastri delle applicazioni dei big data
- 9.1.1. Affidabilità
- 9.1.2. Adattamento
- 9.1.3. Mantenimento

9.2. Modelli di dati
- 9.2.1. Modello relazionale
- 9.2.2. Modello documentario
- 9.2.3. Modello di dati di rete

9.3. Database. Gestione dell'archiviazione e del recupero dei dati
- 9.3.1. Indici hash
- 9.3.2. Archiviazione strutturata in log
- 9.3.3. Alberi B

9.4. Formati di codifica dei dati
- 9.4.1. Formati specifici del linguaggio
- 9.4.2. Formati standardizzati
- 9.4.3. Formati di codifica binaria
- 9.4.4. Flusso di dati interprocessi

9.5. Replica
- 9.5.1. Obiettivi della replica
- 9.5.2. Modelli di replica
- 9.5.3. Problemi con la replica

9.6. Transazioni distribuite
- 9.6.1. Transazione
- 9.6.2. Protocolli per le transazioni distribuite
- 9.6.3. Transazioni serializzabili

9.7. Suddivisione
- 9.7.1. Moduli di partizionamento
- 9.7.2. Interazione tra indice secondario e partizionamento
- 9.7.3. Bilanciamento delle partizioni

9.8. Elaborazione dati *offline*
- 9.8.1. Elaborazione di lotti
- 9.8.2. Sistemi di file distribuite
- 9.8.3. *MapReduce*

9.9. Elaborazione dei dati in tempo reale
- 9.9.1. Tipi di *broker* di messaggi
- 9.9.2. Rappresentazione dei database come flussi di dati
- 9.9.3. Processo dei flussi di dati

9.10. Applicazioni pratiche in azienda
- 9.10.1. Coerenza nelle letture
- 9.10.2. Approccio olistico ai dati
- 9.10.3. Scalabilità di un servizio distribuito

Modulo 10. Applicazione pratica della scienza dei dati nei settori di attività imprenditoriale

10.1. Settore sanitario
- 10.1.1. Implicazioni dell'IA e dell'analisi dei dati nel settore sanitario
- 10.1.2. Opportunità e sfide

10.2. Rischi e tendenze nell'assistenza sanitaria
- 10.2.1. Utilizzo nel settore sanitario
- 10.2.2. Rischi potenziali legati all'uso dell'IA

10.3. Servizi finanziari
- 10.3.1. Implicazioni dell'IA e dell'analisi dei dati nel settore dei servizi finanziari
- 10.3.2. Utilizzo nei servizi finanziari
- 10.3.3. Rischi potenziali legati all'uso dell'IA

10.4. Retail
- 10.4.1. Implicazioni dell'IA e dell'analisi dei dati nel settore del retail
- 10.4.2. Uso in retail
- 10.4.3. Rischi potenziali legati all'uso dell'IA

10.5. Industria 4.0
- 10.5.1. Implicazioni dell'IA e dell'analisi dei dati per l'Industria 4.0
- 10.5.2. Utilizzo nell'Industria 4.0

10.6. Rischi e tendenze dell'Industria 4.0
- 10.6.1. Rischi potenziali legati all'uso dell'IA

10.7. Amministrazione pubblica
- 10.7.1. Implicazioni dell'IA e dell'analisi dei dati nella pubblica amministrazione
- 10.7.2. Utilizzo nella pubblica amministrazione
- 10.7.3. Rischi potenziali legati all'uso dell'IA

10.8. Istruzione
- 10.8.1. Implicazioni dell'IA e dell'analisi dei dati per l'istruzione
- 10.8.2. Rischi potenziali legati all'uso dell'IA

10.9. Silvicoltura e agricoltura
- 10.9.1. Implicazioni dell'intelligenza artificiale e dell'analisi dei dati per la silvicoltura e l'agricoltura
- 10.9.2. Utilizzo in silvicoltura e agricoltura
- 10.9.3. Rischi potenziali legati all'uso dell'IA

10.10. Risorse umane
- 10.10.1. Implicazioni dell'IA e dell'analisi dei dati per la gestione delle risorse umane
- 10.10.2. Applicazioni pratiche nel mondo degli affari
- 10.10.3. Rischi potenziali legati all'uso dell'IA

Modulo 11. Cyber intelligence e sicurezza informatica

11.1. Cyber Intelligence
- 11.1.1. Cyber Intelligence
  - 11.1.1.1. Intelligenza
    - Ciclo dell'intelligenza Cyber Intelligence
  - 11.1.1.2. Cyber Intelligence
  - 11.1.1.3. Cyber intelligence e sicurezza informatica
- 11.1.2. L'Analista di Intelligence
  - 11.1.2.1. Il ruolo dell'analista di intelligence
  - 11.1.2.2. I pregiudizi dell'analista di intelligence nell'attività di valutazione

11.2. Cybersecurity
- 11.2.1. Livelli di sicurezza
- 11.2.2. Identificazione delle minacce informatiche
  - 11.2.2.1. Minacce esterne
  - 11.2.2.2. Minacce interne
- 11.2.3. Azioni avverse
  - 11.2.3.1. Ingegneria sociale
  - 11.2.3.2. Metodi comunemente utilizzati

11.3. Strumenti e tecniche di intelligence
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Distribuzioni e strumenti Linux
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Metodologie di valutazione
- 11.4.1. Analisi di intelligence
- 11.4.2. Tecniche di organizzazione delle informazioni acquisite
- 11.4.3. Affidabilità e credibilità delle fonti di informazione
- 11.4.4. Metodologie di analisi
- 11.4.5. Presentazione dei risultati dell'intelligence

11.5. Controlli e documentazione
- 11.5.1. Controllo della sicurezza informatica
- 11.5.2. Documentazione e autorizzazioni di controllo
- 11.5.3. Tipi di controllo
- 11.5.4. Consegne
  - 11.5.4.1. Rapporto tecnico
  - 11.5.4.2. Rapporto esecutivo

11.6. Anonimato in rete
- 11.6.1. Uso dell'anonimato
- 11.6.2. Tecniche di anonimizzazione (Proxy, VPN)
- 11.6.3. Reti TOR, Freenet e IP2

11.7. Minacce e tipi di sicurezza
- 11.7.1. Tipi di minacce
- 11.7.2. Sicurezza fisica
- 11.7.3. Sicurezza di rete
- 11.7.4. Sicurezza logica
- 11.7.5. Sicurezza delle applicazioni web
- 11.7.6. Sicurezza dei dispositivi mobili

11.8. Normativa e *compliance*
- 11.8.1. RGPD
- 11.8.2. La strategia nazionale per la sicurezza informatica 2011
- 11.8.3. Famiglia ISO 27000
- 11.8.4. Quadro di sicurezza informatica NIST
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. Normative *cloud*
- 11.8.8. SOX
- 11.8.9. PCI

11.9. Analisi del rischio e metriche
- 11.9.1. Portata dei rischi
- 11.9.2. Attivi
- 11.9.3. Minacce
- 11.9.4. Vulnerabilità
- 11.9.5. Valutazione dei rischi
- 11.9.6. Trattamento dei rischi

11.10. Organi competenti in materia di sicurezza informatica
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Modulo 12. Sicurezza dell'host

12.1. Copie di backup
- 12.1.1. Strategie di backup
- 12.1.2. Strumenti per Windows
- 12.1.3. Strumenti per Linux
- 12.1.4. Strumenti per MacOS

12.2. Antivirus utente
- 12.2.1. Tipi di antivirus
- 12.2.2. Antivirus per Windows
- 12.2.3. Antivirus per Linux
- 12.2.4. Antivirus per MacOS
- 12.2.5. Antivirus per smartphone

12.3. Rivelatori di intrusione - HIDS
- 12.3.1. Metodi di rilevamento delle intrusioni
- 12.3.2. *Sagan*
- 12.3.3. *Aide*
- 12.3.4. *Rkhunter*

12.4. *Firewall* locale
- 12.4.1. *Firewalls* per Windows
- 12.4.2. *Firewalls* per Linux
- 12.4.3. *Firewalls* per MacOS

12.5. Gestori di password
- 12.5.1. *Password*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *Sticky Password*
- 12.5.5. *RoboForm*

12.6. Rilevatori di *phishing*
- 12.6.1. Rilevamento manuale del *phishing*
- 12.6.2. Strumenti *antiphishing*

12.7. *Spyware*
- 12.7.1. Meccanismi di evitamento
- 12.7.2. Strumenti *antispyware*

12.8. Tracker
- 12.8.1. Misure di protezione del sistema
- 12.8.2. Strumenti anti-tracker

12.9. EDR- *End Point Detection and Response*
- 12.9.1. Comportamento del sistema EDR
- 12.9.2. Differenze tra EDR e antivirus
- 12.9.3. Il futuro dei sistemi EDR

12.10. Controllo dell'installazione del software
- 12.10.1. Repository e store di software
- 12.10.2. Elenchi di software consentiti e vietati
- 12.10.3. Criteri di aggiornamento
- 12.10.4. Privilegi di installazione del software

Modulo 13. Sicurezza di rete (Perimetrale)

13.1. Sistemi di rilevamento e prevenzione delle minacce
- 13.1.1. Quadro generale per gli incidenti di sicurezza
- 13.1.2. Sistemi di difesa attuali: *Defense in Depth* e SOC
- 13.1.3. Architetture di rete attuali
- 13.1.4. Tipi di strumenti per il rilevamento e la prevenzione degli incidenti
  - 13.1.4.1. Sistemi basati sulla rete
  - 13.1.4.2. Sistemi basati su host
  - 13.1.4.3. Sistemi centralizzati
- 13.1.5. Comunicazione e scoperta di istanze/*hosts*, contenitori e *serverless*

13.2. *Firewall*
- 13.2.1. Tipi di *firewall*
- 13.2.2. Attacchi e mitigazione
- 13.2.3. *Firewall* comuni in kernel Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables e iptables
  - 13.2.3.3. *Firewall*
- 13.2.4. Sistemi di rilevamento basati sui log di sistema
  - 13.2.4.1. TCP *Wrappers*
  - 13.2.4.2. *BlockHosts* e *DenyHosts*
  - 13.2.4.3. Fai2ban

13.3. Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)
- 13.3.1. Attacchi agli IDS/IPS
- 13.3.2. Sistemi IDS/IPS
  - 13.3.2.1. *Snort*
  - 13.3.2.2. Suricata

13.4. *Firewall* di nuova generazione (NGFW)
- 13.4.1. Differenze tra NGFW e firewall tradizionali
- 13.4.2. Capacità principali
- 13.4.3. Soluzioni commerciali
- 13.4.4. Firewall per servizi *Cloud*
  - 13.4.4.1. Architettura *Cloud* VPC
  - 13.4.4.2. *Cloud* ACLs
  - 13.4.4.3. *Security Group*

13.5. Proxy
- 13.5.1. Tipi di Proxy
- 13.5.2. Utilizzo del Proxy. Vantaggi e svantaggi

13.6. Motori antivirus
- 13.6.1. Contesto generale di *Malware* e CIO
- 13.6.2. Problemi del motore antivirus

13.7. Sistemi di protezione della posta
- 13.7.1. Antispam
  - 13.7.1.1. Whitelist e blacklist
  - 13.7.1.2. Filtri bayesiani
- 13.7.2. *Mail Gateway* (MGW)

13.8. SIEM
- 13.8.1. Componenti e architettura
- 13.8.2. Regole di correlazione e casi d'uso
- 13.8.3. Le sfide attuali dei sistemi SIEM

13.9. SOAR
- 13.9.1. SOAR e SIEM: nemici o alleati?
- 13.9.2. Il futuro dei sistemi SOAR

13.10. Altri sistemi basati sulla rete
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots e HoneyNets
- 13.10.4. CASB

Modulo 14. Sicurezza degli smartphone

14.1. Il mondo dei dispositivi mobili
- 14.1.1. Tipi di piattaforme mobili
- 14.1.2. Dispositivi iOS
- 14.1.3. Dispositivi Android

14.2. Gestione della Sicurezza Mobile
- 14.2.1. Progetto OWASP sulla Sicurezza Mobile
  - 14.2.1.1. Le 10 principali vulnerabilità
- 14.2.2. Comunicazioni, reti e modalità di connessione

14.3. Il dispositivo mobile nell'ambiente aziendale
- 14.3.1. Rischi
- 14.3.2. Politiche di sicurezza
- 14.3.3. Monitoraggio del dispositivo
- 14.3.4. Gestione dei dispositivi mobili (MDM)

14.4. Privacy degli utenti e sicurezza dei dati
- 14.4.1. Stati di informazione
- 14.4.2. Protezione dei dati e riservatezza
  - 14.4.2.1. Permessi
  - 14.4.2.2. Crittografia
- 14.4.3. Archiviazione sicura dei dati
  - 14.4.3.1. Archiviazione sicura su iOS
  - 14.4.3.2. Archiviazione sicura su Android
- 14.4.4. Le migliori pratiche di sviluppo delle applicazioni

14.5. Vulnerabilità e vettori di attacco
- 14.5.1. Vulnerabilità
- 14.5.2. Vettori di attacco
  - 14.5.2.1. *Malware*
  - 14.5.2.2. Esfiltrazione di dati
  - 14.5.2.3. Manipolazione dei dati

14.6. Principali minacce
- 14.6.1. Utente non obbligato
- 14.6.2. *Malware*
  - 14.6.2.1. Tipi di *Malware*
- 14.6.3. Ingegneria sociale
- 14.6.4. Fuga di dati
- 14.6.5. Furto di dati
- 14.6.6. Reti *Wi-Fi* non protette
- 14.6.7. Software obsoleto
- 14.6.8. Applicazioni dannose
- 14.6.9. Password insicure
- 14.6.10. Impostazioni di sicurezza deboli o inesistenti
- 14.6.11. Accesso fisico
- 14.6.12. Perdita o furto del dispositivo
- 14.6.13. Impersonificazione (Integrità)
- 14.6.14. Crittografia debole o danneggiata
- 14.6.15. Negazione del servizio (DoS)

14.7. Principali attacchi
- 14.7.1. Attacchi di *phishing*
- 14.7.2. Attacchi relativi alle modalità di comunicazione
- 14.7.3. Attacchi di *Smishing*
- 14.7.4. Attacchi di *Criptojacking*
- 14.7.5. *Man in The Middle*

14.8. *Hacking*
- 14.8.1. *Rooting e Jailbreaking*
- 14.8.2. Anatomia di un attacco mobile
  - 14.8.2.1. Propagazione della minaccia
  - 14.8.2.2. Installazione di *malware* sul dispositivo
  - 14.8.2.3. Persistenza
  - 14.8.2.4. Esecuzione *Payload* ed estrazione delle informazioni
- 14.8.3. *Hacking* su dispositivi iOS: meccanismi e strumenti
- 14.8.4. *Hacking* su dispositivi Android: meccanismi e strumenti

14.9. Test di penetrazione
- 14.9.1. *iOS PenTesting*
- 14.9.2. *Android PenTesting*
- 14.9.3. Strumenti

14.10. Protezione e sicurezza
- 14.10.1. Impostazioni di sicurezza
  - 14.10.1.1. Su dispositivi iOS
  - 14.10.1.2. Su dispositivi Android
- 14.10.2. Misure di sicurezza
- 14.10.3. Strumenti di protezione

Modulo 15. Sicurezza in IoT

15.1. Dispositivi
- 15.1.1. Tipi di dispositivi
- 15.1.2. Architetture standardizzate
  - 15.1.2.1. ONEM2M
  - 15.1.2.2. IoTWF
- 15.1.3. Protocolli applicativi
- 15.1.4. Tecnologie di connettività

15.2. Dispositivi IoT Aree di applicazione
- 15.2.1. *SmartHome*
- 15.2.2. *SmartCity*
- 15.2.3. Trasporti
- 15.2.4. *Wearables*
- 15.2.5. Settore sanitario
- 15.2.6. IioT

15.3. Protocolli di comunicazione
- 15.3.1. MQTT
- 15.3.2. LWM2M
- 15.3.3. OMA-DM
- 15.3.4. TR-069

15.4. *SmartHome*
- 15.4.1. Domotica
- 15.4.2. Reti
- 15.4.3. Elettrodomestici
- 15.4.4. Sorveglianza e sicurezza

15.5. *SmartCity*
- 15.5.1. Illuminazione
- 15.5.2. Meteo
- 15.5.3. Sicurezza

15.6. Trasporti
- 15.6.1. Localizzazione
- 15.6.2. Effettuare pagamenti e ottenere servizi
- 15.6.3. Connettività

15.7. *Wearables*
- 15.7.1. Vestiti intelligenti
- 15.7.2. Gioielli intelligenti
- 15.7.3. Orologi intelligenti

15.8. Settore sanitario
- 15.8.1. Monitoraggio dell'esercizio e della frequenza cardiaca
- 15.8.2. Monitoraggio dei pazienti e degli anziani
- 15.8.3. Impiantabili
- 15.8.4. Robot chirurgici

15.9. Connettività
- 15.9.1. *Wi-Fi/Gateway*
- 15.9.2. *Bluetooth*
- 15.9.3. Connettività integrata

15.10. Securizzazione
- 15.10.1. Reti dedicate
- 15.10.2. Gestori di password
- 15.10.3. Utilizzo di protocolli criptati
- 15.10.4. Suggerimenti per l'uso

Modulo 16. *Hacking* etico

16.1. Ambiente di lavoro
- 16.1.1. Distribuzioni di Linux
  - 16.1.1.1. Kali Linux - Offensive Security
  - 16.1.1.2. Parrot OS
  - 16.1.1.3. Ubuntu
- 16.1.2. Sistemi di virtualizzazione
- 16.1.3. *Sandbox*
- 16.1.4. Utilizzo di laboratori

16.2. Metodologie
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. NIST
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. *Footprinting*
- 16.3.1. Intelligence Open Source (OSINT)
- 16.3.2. Ricerca di violazioni di dati e vulnerabilità
- 16.3.3. Utilizzo di strumenti passivi

16.4. Scansione di rete
- 16.4.1. Strumenti di scansione
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Altri strumenti di scansione
- 16.4.2. Tecniche di scansione
- 16.4.3. Tecniche di elusione di *Firewall* e IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Diagrammi di rete

16.5. Enumerazione
- 16.5.1. Enumerazione SMTP
- 16.5.2. Enumerazione DNS
- 16.5.3. Enumerazione NetBIOS e Samba
- 16.5.4. Enumerazione LDAP
- 16.5.5. Enumerazione SNMP
- 16.5.6. Altre tecniche di enumerazione

16.6. Scansione delle vulnerabilità
- 16.6.1. Soluzioni di scansione delle vulnerabilità
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. Sistemi di valutazione delle vulnerabilità
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Attacchi alle reti *wireless*
- 16.7.1. Metodologia di hacking delle reti wireless
  - 16.7.1.1. Wi-Fi Discovery
  - 16.7.1.2. Analisi del traffico
  - 16.7.1.3. Attacchi *aircrack*
    - 16.7.1.3.1. Attacchi WEP
    - 16.7.1.3.2. Attacchi WPA/WPA2
  - 16.7.1.4. Attacchi di *Evil Twin*
  - 16.7.1.5. Attacchi WPS
  - 16.7.1.6. *Jamming*
- 16.7.2. Strumenti di sicurezza wireless

16.8. Hacking di server web
- 16.8.1. *Cross site Scripting*
- 16.8.2. CSRF
- 16.8.3. *Session Hijacking*
- 16.8.4. *SQLinjection*

16.9. Sfruttamento delle vulnerabilità
- 16.9.1. Utilizzo di *exploit* noti
- 16.9.2. Uso di *metasploit*
- 16.9.3. Uso di *malware*
  - 16.9.3.1. Definizione e portata
  - 16.9.3.2. Generazione di *malware*
  - 16.9.3.3. Bypassare le soluzioni antivirus

16.10. Persistenza
- 16.10.1. Installazione di rootkit
- 16.10.2. Utilizzo di ncat
- 16.10.3. Utilizzo delle attività pianificate per le backdoor
- 16.10.4. Creazione di utenti
- 16.10.5. Rilevamento di HIDS

Modulo 17. Reverse engineering

17.1. Compilatori
- 17.1.1. Tipi di codici
- 17.1.2. Fasi del compilatore
- 17.1.3. Tabella dei simboli
- 17.1.4. Gestore degli errori
- 17.1.5. Compilatore GCC

17.2. Tipi di analisi del compilatore
- 17.2.1. Analisi lessicale
  - 17.2.1.1. Terminologia
  - 17.2.1.2. Componenti lessicali
  - 17.2.1.3. Analizzatore lessicale LEX
- 17.2.2. Analisi sintattica
  - 17.2.2.1. Grammatiche libere dal contesto
  - 17.2.2.2. Tipi di analisi sintattiche
    - 17.2.2.2.1. Analisi discendente
    - 17.2.2.2.2. Analisi ascendente
  - 17.2.2.3. Alberi sintattici e derivazioni
  - 17.2.2.4. Tipi di analizzatori sintattici
    - 17.2.2.4.1. Analizzatori LR (*Left To Right*)
    - 17.2.2.4.2. Analizzatori LALR
- 17.2.3. Analisi semantica
  - 17.2.3.1. Grammatiche degli attributi
  - 17.2.3.2. S-Atribuidas
  - 17.2.3.3. L-Atribuidas

17.3. Strutture dati dell'assemblaggio
- 17.3.1. Variabili
- 17.3.2. Arrays
- 17.3.3. Puntatori
- 17.3.4. Struttura
- 17.3.5. Obiettivi

17.4. Strutture del codice di assemblaggio
- 17.4.1. Strutture di selezione
  - 17.4.1.1. If, else if, Else
  - 17.4.1.2. Switch
- 17.4.2. Strutture di iterazione
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Uso del break
- 17.4.3. Funzioni

17.5. Architettura hardware x86
- 17.5.1. Architettura del processore x86
- 17.5.2. Strutture dati x86
- 17.5.3. Strutture di codice x86

17.6. Architettura hardware ARM
- 17.6.1. Architettura del processore ARM
- 17.6.2. Strutture dati ARM
- 17.6.3. Strutture di codice ARM

17.7. Analisi del codice statico
- 17.7.1. Disassemblatori
- 17.7.2. IDA
- 17.7.3. Ricostruttori di codici

17.8. Analisi del codice dinamico
- 17.8.1. Analisi comportamentale
  - 17.8.1.1. Comunicazioni
  - 17.8.1.2. Monitoraggio
- 17.8.2. Debugger di codice per Linux
- 17.8.3. Debugger di codice per Windows

17.9. *Sandbox*
- 17.9.1. Architettura *Sandbox*
- 17.9.2. Evasione della *Sandbox*
- 17.9.3. Tecniche di rilevamento
- 17.9.4. Tecniche di evasione
- 17.9.5. Contromisure
- 17.9.6. *Sandbox* su Linux
- 17.9.7. *Sandbox* su Windows
- 17.9.8. *Sandox* su MacOS
- 17.9.9. *Sandbox* su Android

17.10. Analisi del malware
- 17.10.1. Metodi di analisi del *malware*
- 17.10.2. Tecniche di offuscamento del *malware*
  - 17.10.2.1. Offuscamento degli eseguibili
  - 17.10.2.2. Limitazione degli ambienti di esecuzione
- 17.10.3. Strumenti di analisi del *malware*

Modulo 18. Sviluppo sicuro

18.1. Sviluppo sicuro
- 18.1.1. Qualità, funzionalità e sicurezza
- 18.1.2. Riservatezza, integrità e disponibilità
- 18.1.3. Ciclo di vita dello sviluppo del software

18.2. Fase dei Requisiti
- 18.2.1. Controllo dell'autenticazione
- 18.2.2. Controllo dei ruoli e dei privilegi
- 18.2.3. Requisiti orientati al rischio
- 18.2.4. Approvazione dei privilegi

18.3. Fasi di analisi e progettazione
- 18.3.1. Accesso ai componenti e amministrazione del sistema
- 18.3.2. Tracce di controllo
- 18.3.3. Gestione delle sessioni
- 18.3.4. Dati storici
- 18.3.5. Gestione appropriata degli errori
- 18.3.6. Separazione delle funzioni

18.4. Fase di implementazione e codifica
- 18.4.1. Protezione dell'ambiente di sviluppo
- 18.4.2. Elaborazione della documentazione tecnica
- 18.4.3. Codifica sicura
- 18.4.4. Comunicazioni sicure

18.5. Buone pratiche di codifica sicura
- 18.5.1. Convalida dei dati di ingresso
- 18.5.2. Crittografia dei dati in uscita
- 18.5.3. Stile di programmazione
- 18.5.4. Gestione del registro delle modifiche
- 18.5.5. Pratiche crittografiche
- 18.5.6. Gestione degli errori e dei log
- 18.5.7. Gestione dei file
- 18.5.8. Gestione della memoria
- 18.5.9. Standardizzazione e riutilizzo delle funzioni di sicurezza

18.6. Preparazione del server e *Hardening*
- 18.6.1. Gestione di utenti, gruppi e ruoli sul server
- 18.6.2. Installazione del software
- 18.6.3. *Hardening* del server
- 18.6.4. Configurazione robusta dell'ambiente applicativo

18.7. Preparazione del DB y *Hardening*
- 18.7.1. Ottimizzazione del motore DB
- 18.7.2. Creazione di un proprio utente per l'applicazione
- 18.7.3. Assegnazione dei privilegi richiesti all'utente
- 18.7.4. *Hardening* del DB

18.8. Fase di test
- 18.8.1. Controllo di qualità nei controlli di sicurezza
- 18.8.2. Ispezione del codice per fasi
- 18.8.3. Controllo della gestione della configurazione
- 18.8.4. Test a scatola nera

18.9. Preparare il passaggio alla produzione
- 18.9.1. Eseguire il controllo delle modifiche
- 18.9.2. Eseguire la procedura di cambio a produzione
- 18.9.3. Eseguire la procedura di *rollback*
- 18.9.4. Test di pre-produzione

18.10. Fase di mantenimento
- 18.10.1. Garanzia basata sul rischio
- 18.10.2. Test di manutenzione della sicurezza della scatola bianca
- 18.10.3. Test di manutenzione della sicurezza della scatola nera

Modulo 19. Analisi forense

19.1. Acquisizione e replica dei dati
- 19.1.1. Acquisizione dati volatili
  - 19.1.1.1. Informazioni sul sistema
  - 19.1.1.2. Informazioni sulla rete
  - 19.1.1.3. Ordine di volatilità
- 19.1.2. Acquisizione statica dei dati
  - 19.1.2.1. Creazione di un'immagine duplicata
  - 19.1.2.2. Preparazione di un documento di catena di custodia
- 19.1.3. Metodi di validazione dei dati acquisiti
  - 19.1.3.1. Metodi per Linux
  - 19.1.3.2. Metodi per Windows

19.2. Valutazione e sconfitta delle tecniche anti-forensi
- 19.2.1. Obiettivi delle tecniche anti-forensi
- 19.2.2. Cancellazione dei dati
  - 19.2.2.1. Cancellazione di dati e file
  - 19.2.2.2. Recupero dei file
  - 19.2.2.3. Recupero di partizioni eliminate
- 19.2.3. Protezione con password
- 19.2.4. Steganografia
- 19.2.5. Cancellazione sicura del dispositivo
- 19.2.6. Crittografia

19.3. Analisi forense del sistema operativo
- 19.3.1. Analisi forense di Windows
- 19.3.2. Analisi forense di Linux
- 19.3.3. Analisi forense di Mac

19.4. Analisi Forense della rete
- 19.4.1. Analisi dei log
- 19.4.2. Correlazione dei dati
- 19.4.3. Indagine di rete
- 19.4.4. Passi da seguire nell'analisi forense della rete

19.5. Analisi forense del Web
- 19.5.1. Indagine sugli attacchi web
- 19.5.2. Rilevamento degli attacchi
- 19.5.3. Localizzazione dell'indirizzo IP

19.6. Analisi forense dei database
- 19.6.1. Analisi forense del MSSQL
- 19.6.2. Analisi forense del MySQL
- 19.6.3. Analisi forense del PostgreSQL
- 19.6.4. Analisi forense del MongoDB

19.7. Analisi forense del *cloud*
- 19.7.1. Tipi di crimini sul *cloud*
  - 19.7.1.1. *Cloud* come soggetto
  - 19.7.1.2. *Cloud* come oggetto
  - 19.7.1.3. *Cloud* come strumento
- 19.7.2. Sfide dell'analisi forense del *cloud*
- 19.7.3. Indagine sui servizi di *cloud storage*
- 19.7.4. Strumenti di analisi forense sul *cloud*

19.8. Indagine sui reati di posta elettronica
- 19.8.1. Sistemi di posta elettronica
  - 19.8.1.1. Clienti di posta elettronica
  - 19.8.1.2. Server di posta elettronica
  - 19.8.1.3. Server SMTP
  - 19.8.1.4. Server POP3
  - 19.8.1.5. Server IMAP4
- 19.8.2. Crimini postali
- 19.8.3. Messaggio di posta elettronica
  - 19.8.3.1. Intestazioni standard
  - 19.8.3.2. Intestazioni estese
- 19.8.4. Passi per l'investigazione di questi crimini
- 19.8.5. Strumenti forensi per la posta elettronica

19.9. Analisi forense mobile
- 19.9.1. Reti cellulari
  - 19.9.1.1. Tipi di reti
  - 19.9.1.2. Contenuti del CDR
- 19.9.2. *Subscriber Identity Module* (SIM)
- 19.9.3. Acquisizione logica
- 19.9.4. Acquisizione fisica
- 19.9.5. Acquisizione del file system

19.10. Stesura e presentazione di rapporti forensi
- 19.10.1. Aspetti importanti di un rapporto forense
- 19.10.2. Classificazione e tipi di rapporti
- 19.10.3. Guida alla stesura di un rapporto
- 19.10.4. Presentazione del rapporto
  - 19.10.4.1. Preparazione preventiva alla testimonianza
  - 19.10.4.2. Deposizione
  - 19.10.4.3. Rapporti con i media

Modulo 20. Sfide attuali e future nella sicurezza informatica

20.1. Tecnologia *blockchain*
- 20.1.2. Ambiti di applicazione
- 20.1.3. Garanzia di riservatezza
- 20.1.4. Garanzia di non ripudio

20.2. Denaro digitale
- 20.2.1. Bitcoin
- 20.2.2. Criptovalute
- 20.2.3. Mining di criptovalute
- 20.2.4. Schemi piramidali
- 20.2.5. Altri potenziali reati e problemi

20.3. *Deepfake*
- 20.3.2. Impatto mediatico
- 20.3.3. Pericoli per la società
- 20.3.4. Meccanismi di rilevamento

20.4. Il futuro dell'intelligenza artificiale
- 20.4.1. Intelligenza artificiale e informatica cognitiva
- 20.4.2. Utilizzi per semplificare il servizio clienti

20.5. Privacy digitale
- 20.5.1. Valore dei dati in rete
- 20.5.2. Utilizzo dei dati in rete
- 20.5.3. Gestione della privacy e dell'identità digitale

20.6. Conflitti informatici, criminali informatici e attacchi informatici
- 20.6.1. Impatto della sicurezza informatica sui conflitti internazionali
- 20.6.2. Conseguenze degli attacchi informatici sulla popolazione generale
- 20.6.3. Tipi di criminali informatici. Misure di protezione

20.7. Telelavoro
- 20.7.1. Rivoluzione del telelavoro durante e dopo Covid19
- 20.7.2. Colli di bottiglia di accesso
- 20.7.3. Variazione della superficie di attacco
- 20.7.4. Requisiti dei lavoratori

20.8. Tecnologie *wireless* emergenti
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Onde millimetriche
- 20.8.4. Tendenza *"Get Smart"* invece di *"Get more"*

20.9. L'indirizzamento futuro nelle reti
- 20.9.1. Problemi attuali con l'indirizzamento IP
- 20.9.2. IPv6
- 20.9.2. IPv4+
- 20.9.3. Vantaggi dell'IPv4+ rispetto all'IPv4
- 20.9.4. Vantaggi dell'IPv6 rispetto all'IPv4

20.10. La sfida della sensibilizzazione all'educazione precoce e continua della popolazione
- 20.10.1. Le attuali strategie governative
- 20.10.2. Resistenza della popolazione all'apprendimento
- 20.10.3. Piani di formazione da adottare da parte delle imprese

Non esitare oltre, sai che con questo Master Specialistico andrai lontano"

06

Metodologia

Questo programma ti offre un modo differente di imparare. La nostra metodologia si sviluppa in una modalità di apprendimento ciclico: ***il Relearning***.

Questo sistema di insegnamento viene applicato nelle più prestigiose facoltà di medicina del mondo ed è considerato uno dei più efficaci da importanti pubblicazioni come il ***New England Journal of Medicine.***

Scopri il Relearning, un sistema che abbandona l'apprendimento lineare convenzionale, per guidarti attraverso dei sistemi di insegnamento ciclici: una modalità di apprendimento che ha dimostrato la sua enorme efficacia, soprattutto nelle materie che richiedono la memorizzazione"

Caso di Studio per contestualizzare tutti i contenuti

Il nostro programma offre un metodo rivoluzionario per sviluppare le abilità e le conoscenze. Il nostro obiettivo è quello di rafforzare le competenze in un contesto mutevole, competitivo e altamente esigente.

Con TECH potrai sperimentare un modo di imparare che sta scuotendo le fondamenta delle università tradizionali in tutto il mondo"

Avrai accesso a un sistema di apprendimento basato sulla ripetizione, con un insegnamento naturale e progressivo durante tutto il programma.

Imparerai, attraverso attività collaborative e casi reali, la risoluzione di situazioni complesse in ambienti aziendali reali.

Un metodo di apprendimento innovativo e differente

Questo programma di TECH consiste in un insegnamento intensivo, creato ex novo, che propone le sfide e le decisioni più impegnative in questo campo, sia a livello nazionale che internazionale. Grazie a questa metodologia, la crescita personale e professionale viene potenziata, effettuando un passo decisivo verso il successo. Il metodo casistico, la tecnica che sta alla base di questi contenuti, garantisce il rispetto della realtà economica, sociale e professionale più attuali.

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

Il Metodo Casistico è stato il sistema di apprendimento più usato nelle migliori Scuole di Informatica del mondo da quando esistono. Sviluppato nel 1912 affinché gli studenti di Diritto non imparassero la legge solo sulla base del contenuto teorico, il metodo casistico consisteva nel presentare loro situazioni reali e complesse per prendere decisioni informate e giudizi di valore su come risolverle. Nel 1924 fu stabilito come metodo di insegnamento standard ad Harvard.

Cosa dovrebbe fare un professionista per affrontare una determinata situazione? Questa è la domanda con cui ti confrontiamo nel metodo dei casi, un metodo di apprendimento orientato all'azione. Durante il corso, gli studenti si confronteranno con diversi casi di vita reale. Dovranno integrare tutte le loro conoscenze, effettuare ricerche, argomentare e difendere le proprie idee e decisioni.

Metodologia Relearning

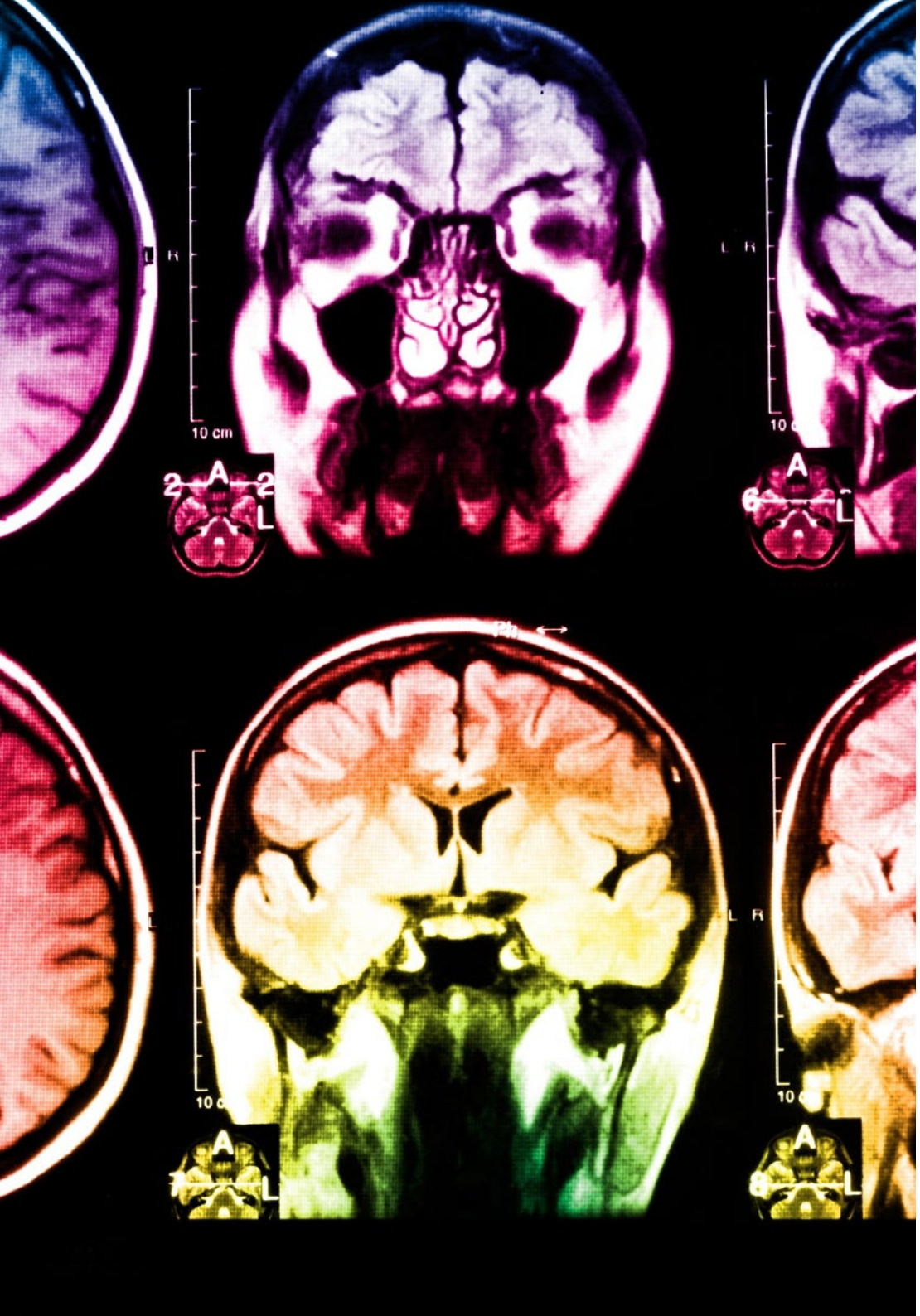
TECH coniuga efficacemente la metodologia del Caso di Studio con un sistema di apprendimento 100% online basato sulla ripetizione, che combina diversi elementi didattici in ogni lezione.

Potenziamo il Caso di Studio con il miglior metodo di insegnamento 100% online: il Relearning.

Nel 2019 abbiamo ottenuto i migliori risultati di apprendimento di tutte le università online del mondo.

In TECH imparerai con una metodologia all'avanguardia progettata per formare i manager del futuro. Questo metodo, all'avanguardia della pedagogia mondiale, si chiama Relearning.

La nostra università è l'unica autorizzata a utilizzare questo metodo di successo. Nel 2019, siamo riusciti a migliorare il livello di soddisfazione generale dei nostri studenti (qualità dell'insegnamento, qualità dei materiali, struttura del corso, obiettivi...) rispetto agli indicatori della migliore università online.



Nel nostro programma, l'apprendimento non è un processo lineare, ma avviene in una spirale (impariamo, disimpariamo, dimentichiamo e re-impariamo). Pertanto, combiniamo ciascuno di questi elementi in modo concentrico. Questa metodologia ha formato più di 650.000 laureati con un successo senza precedenti in campi diversi come la biochimica, la genetica, la chirurgia, il diritto internazionale, le competenze manageriali, le scienze sportive, la filosofia, il diritto, l'ingegneria, il giornalismo, la storia, i mercati e gli strumenti finanziari. Tutto questo in un ambiente molto esigente, con un corpo di studenti universitari con un alto profilo socio-economico e un'età media di 43,5 anni.

Il Relearning ti permetterà di apprendere con meno sforzo e più performance, impegnandoti maggiormente nella tua specializzazione, sviluppando uno spirito critico, difendendo gli argomenti e contrastando le opinioni: un'equazione diretta al successo.

Dalle ultime evidenze scientifiche nel campo delle neuroscienze, non solo sappiamo come organizzare le informazioni, le idee, le immagini e i ricordi, ma sappiamo che il luogo e il contesto in cui abbiamo imparato qualcosa è fondamentale per la nostra capacità di ricordarlo e immagazzinarlo nell'ippocampo, per conservarlo nella nostra memoria a lungo termine.

In questo modo, e in quello che si chiama Neurocognitive Context-dependent E-learning, i diversi elementi del nostro programma sono collegati al contesto in cui il partecipante sviluppa la sua pratica professionale.

Questo programma offre i migliori materiali didattici, preparati appositamente per i professionisti:

Materiale di studio

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

Questi contenuti sono poi applicati al formato audiovisivo che supporterà la modalità di lavoro online di TECH. Tutto questo, con le ultime tecniche che offrono componenti di alta qualità in ognuno dei materiali che vengono messi a disposizione dello studente.

Master class

Esistono evidenze scientifiche sull'utilità dell'osservazione di esperti terzi.

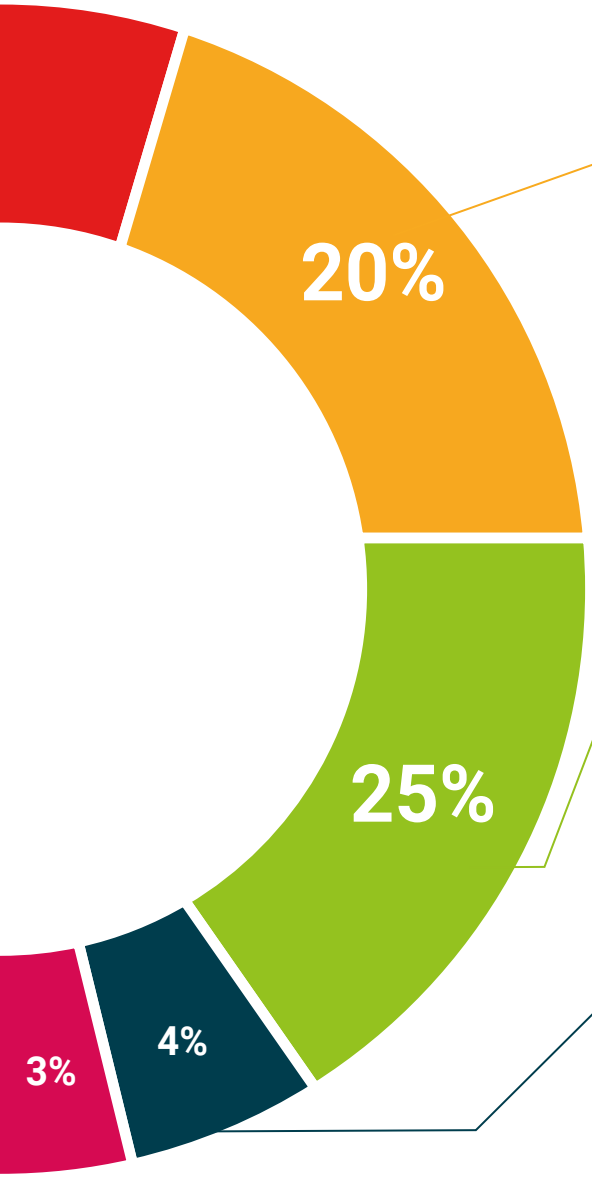
Imparare da un esperto rafforza la conoscenza e la memoria, costruisce la fiducia nelle nostre future decisioni difficili.

Pratiche di competenze e competenze

Svolgerai attività per sviluppare competenze e capacità specifiche in ogni area tematica. Pratiche e dinamiche per acquisire e sviluppare le competenze e le abilità che uno specialista deve sviluppare nel quadro della globalizzazione in cui viviamo.

Letture complementari

Articoli recenti, documenti di consenso e linee guida internazionali, tra gli altri. Nella biblioteca virtuale di TECH potrai accedere a tutto il materiale necessario per completare la tua specializzazione.



Casi di Studio

Completerai una selezione dei migliori casi di studio scelti appositamente per questo corso. Casi presentati, analizzati e monitorati dai migliori specialisti del panorama internazionale.

Riepiloghi interattivi

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

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

Testing & Retesting

Valutiamo e rivalutiamo periodicamente le tue conoscenze durante tutto il programma con attività ed esercizi di valutazione e autovalutazione, affinché tu possa verificare come raggiungi progressivamente i tuoi obiettivi.

07

Titolo

Il Master Specialistico in Secure Information Management ti garantisce, oltre alla formazione più rigorosa e aggiornata, l'accesso al Master Privato rilasciato dalla TECH Università Tecnologica.

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

Questo **Master Specialistico in Secure Information Management** possiede il programma più completo e aggiornato presente sul mercato.

Dopo aver superato le valutazioni, lo studente riceverà, mediante lettera certificata* con ricevuta di ritorno, il suo corrispondente titolo **Master Specialistico** rilasciato da **TECH Università Tecnologica.**

Il titolo rilasciato da **TECH Università Tecnologica** indica 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 Secure Information Management**
Nº Ore Ufficiali: **3.000 O.**

tech università tecnologica

Conferisce il presente

DIPLOMA

a

Dott./Dott.ssa _____, con documento d'identità nº_____

Per aver completato con esito positivo e accreditato il programma di

MASTER SPECIALISTICO

in

Secure Information Management

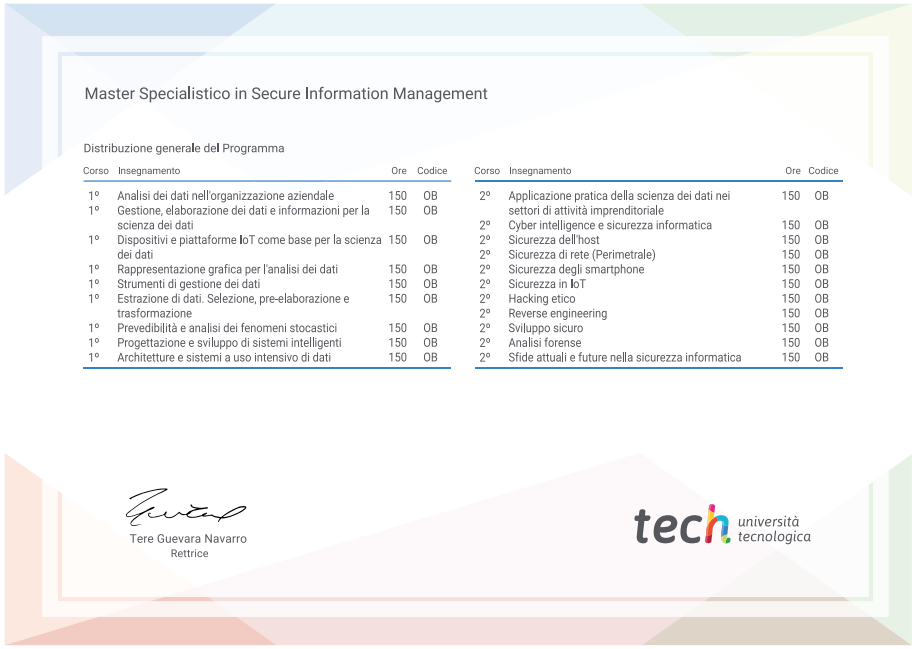
Si tratta di un titolo rilasciato da questa Università ed equivalente a 3.000 ore, con data di inizio gg/mm/aaaa e con data di fine gg/mm/aaaa.

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

Questo titolo deve essere sempre accompagnato da un titolo universitario rilasciato dall'autorità competente per l'esercizio della pratica professionale in ogni paese. codice unico TECH: AFWORD23S techtitute.com/titulos



Master Specialistico in Secure Information Management

Distribuzione generale del Programma

Corso	Insegnamento	Ore	Codice
1º	Analisi dei dati nell'organizzazione aziendale	150	OB
1º	Gestione, elaborazione dei dati e informazioni per la scienza dei dati	150	OB
1º	Dispositivi e piattaforme IoT come base per la scienza dei dati	150	OB
1º	Rappresentazione grafica per l'analisi dei dati	150	OB
1º	Strumenti di gestione dei dati	150	OB
1º	Estrazione di dati. Selezione, pre-elaborazione e trasformazione	150	OB
1º	Prevedibilità e analisi dei fenomeni stocastici	150	OB
1º	Progettazione e sviluppo di sistemi intelligenti	150	OB
1º	Architetture e sistemi a uso intensivo di dati	150	OB
2º	Applicazione pratica della scienza dei dati nei settori di attività imprenditoriale	150	OB
2º	Cyber intelligence e sicurezza informatica	150	OB
2º	Sicurezza dell'host	150	OB
2º	Sicurezza di rete (Perimetrale)	150	OB
2º	Sicurezza degli smartphone	150	OB
2º	Sicurezza in IoT	150	OB
2º	Hacking etico	150	OB
2º	Reverse engineering	150	OB
2º	Sviluppo sicuro	150	OB
2º	Analisi forense	150	OB
2º	Sfide attuali e future nella sicurezza informatica	150	OB

Tere Guevara Navarro
Rettrice

tech università tecnologica

*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

Secure Information Management

- Modalità: **online**
- Durata: **2 anni**
- Titolo: **TECH Università Tecnologica**
- Dedizione: **16 ore/settimana**
- Orario: **a scelta**
- Esami: **online**

Master Specialistico

Secure Information Management

tech universidad tecnológica