MASTER EXECUTIVE IN

CYBER SECURITY E DATA PROTECTION

Presentazione del Corso

Questo Master Executive è progettato per fornire una formazione avanzata e completa in Cyber Security e Data Protection. Il corso si concentra su due aree chiave: la sicurezza informatica e la protezione dei dati.

1. **Cyber Security:**

   Fondamenti di Cyber Security: Introduzione ai concetti chiave della sicurezza informatica, compresi i tipi di minacce, le vulnerabilità e le misure di mitigazione.

   Sicurezza delle Reti e dei Sistemi: Approfondimento sulla sicurezza delle reti e dei sistemi, con particolare attenzione alla protezione contro gli attacchi informatici.

   Gestione delle Crisi e Risposta agli Incidenti: Formazione sulla gestione delle crisi e sulla risposta agli incidenti, inclusa la pianificazione della risposta agli incidenti e la gestione delle violazioni della sicurezza.

2. **Data Protection**

   Principi di Protezione dei Dati: Discussione sui principi fondamentali della protezione dei dati, compresi i diritti degli individui e le responsabilità delle organizzazioni.

   Regolamenti sulla Protezione dei Dati: Esame dei regolamenti sulla protezione dei dati a livello nazionale e internazionale, con un focus sul Regolamento Generale sulla Protezione dei Dati (GDPR).

   Implementazione della Protezione dei Dati: Guida pratica su come implementare efficacemente le politiche e le procedure di protezione dei dati in un'organizzazione.

In sintesi, Il Master Executive in Cyber Security e Data Protection mira a equipaggiare i partecipanti con le competenze necessarie per diventare leader nel campo della sicurezza informatica e della protezione dei dati. Alla fine del corso, i partecipanti saranno in grado di implementare strategie di sicurezza efficaci e di garantire la conformità alle leggi sulla protezione dei dati.

Obiettivi Formativi del Master Executive in Cyber Security e Data Protection

- **Capire i Fondamenti della Cyber Security**: Comprendere i concetti chiave della sicurezza informatica, tra cui i tipi di minacce, le vulnerabilità e le misure di mitigazione.
- **Sviluppare Competenze in Sicurezza delle Reti e dei Sistemi**: Acquisire competenze avanzate nella protezione delle reti e dei sistemi informatici contro vari tipi di attacchi.
- **Gestire Crisi e Rispondere agli Incidenti**: Sviluppare abilità nella gestione delle crisi e nella risposta agli incidenti di sicurezza, compresa la pianificazione e la gestione delle violazioni della sicurezza.
- **Comprendere i Principi di Protezione dei Dati**: Conoscere i principi fondamentali della protezione dei dati, compresi i diritti degli individui e le responsabilità delle organizzazioni.
- **Studiare i Regolamenti sulla Protezione dei Dati**: Familiarizzare con i regolamenti sulla protezione dei dati a livello nazionale e internazionale, con particolare attenzione al Regolamento Generale sulla Protezione dei Dati (GDPR).
- **Implementare la Protezione dei Dati**: Imparare a implementare efficacemente le politiche e le procedure di protezione dei dati in un'organizzazione.
- **Leadership nel Campo della Sicurezza Informatica e della Protezione dei Dati**: Sviluppare le competenze necessarie per diventare leader nel campo della sicurezza informatica e della protezione dei dati, compresa la capacità di implementare strategie di sicurezza efficaci e garantire la conformità alle leggi sulla protezione dei dati.

Sbocchi Occupazionali del Master Executive in Cyber Security e Data Protection

- **Consulente per la Sicurezza Informatica**: Gli studenti possono lavorare come consulenti, fornendo consigli strategici e tattici alle organizzazioni per proteggere i loro dati e le infrastrutture IT.
- **Analista della Sicurezza**: Questo ruolo implica la protezione dei sistemi informatici da minacce e vulnerabilità, monitorando le reti per rilevare eventuali attività sospette.
- **Responsabile della Protezione dei Dati (DPO)**: In conformità con il GDPR, molte organizzazioni richiedono un DPO per supervisionare le strategie di protezione dei dati e garantire la conformità.
- **Ingegnere della Sicurezza delle Reti**: Questo ruolo si concentra sulla protezione delle reti informatiche di un'organizzazione da minacce esterne e interne.
- **Responsabile della Sicurezza Informatica**: Questo ruolo di alto livello implica la supervisione di tutte le operazioni di sicurezza informatica e la definizione della strategia di sicurezza di un'organizzazione.
- **Ricercatore sulla Sicurezza**: Questi professionisti conducono ricerche per scoprire nuove minacce alla sicurezza e sviluppare metodi per mitigarle.
- **Esperto di Conformità IT**: Questi specialisti assicurano che le organizzazioni rispettino tutte le leggi e i regolamenti relativi alla sicurezza informatica e alla protezione dei dati.

- **Formatore in Sicurezza Informatica**: Gli studenti possono anche diventare formatori, insegnando ad altri le competenze necessarie per proteggere le informazioni e le reti.

Questi sono solo alcuni degli sbocchi occupazionali possibili. La domanda di professionisti della sicurezza informatica e della protezione dei dati è in costante crescita, offrendo molte opportunità di carriera in vari settori.

Requisiti di ammissione, esami di verifica e prova finale

L'iscrizione è aperta ai candidati che detengono un Diploma di Scuola Media Superiore, una Laurea Triennale, Specialistica, Magistrale o del Vecchio Ordinamento. In assenza dei titoli di studio specificati, l'ammissione può essere considerata su base di dossier. Questo implica una valutazione dei titoli di studio posseduti, dell'esperienza professionale maturata e delle competenze acquisite nel contesto lavorativo.

Il Docente ha la libertà di erogare le lezioni utilizzando vari strumenti, tra cui Tesine, commentari, manuali specialistici, dispense, o attraverso lezioni in diretta su una piattaforma di live streaming. Per quanto riguarda la valutazione, essa sarà espressa su una scala di trentesimi.

La prova conclusiva del Master Executive richiede la redazione di una Tesi. Questa deve essere di almeno 30 pagine e deve trattare uno degli argomenti studiati durante il corso.

MASTER EXECUTIVE IN

CYBER SECURITY E DATA PROTECTION

SSD	INSEGNAMENTO	ECTS
IUS/01	Diritto della Privacy e della Protezione dei Dati Personali	10
ING-INF/05	Business Intelligence e Big Data	6
ING-INF/05	Cyber Security	10
INF/01	IT Risk Analysis and Management	10
INF/01	Digital Forensics	6
INF/01	Deep Learning	6
ING-INF/05	Sistemi per la gestione di Database e Big Data	8
	Tesi finale	4

UNICAMPUS HETG
Facoltà di Scienze Giuridiche

DURATA E STRUTTURA DEL MASTER EXECUTIVE	
Durata:	Quadrimestrale 64 ore
Frequenza:	4 giornate al mese da 4 ore cad.
Docente:	Prof.ssa Stefania Pigati - Prof. Gabriele Mencarini
Iscrizioni:	Sempre aperte tutto l'anno
Stage in presenza:	Da concordare
Crediti:	60 ECTS
Modalità:	Online
Prezzo:	CHF/EUR 1.600,00 (comprensivo di Iscrizione, Diritti di Segreteria ed eventuale **stage in presenza e/o online**)

PROGRAMMA

INSEGNAMENTO	PROGRAMMA
Diritto della Privacy e della Protezione dei Dati Personali	1. Disciplina in materia di Protezione dei Dati Personali 2. Normativa nazionale ed Europea 3. GDPR (General Data Protection Regulation) Regolamento UE 2016/679 4. Principi e Soggetti del Trattamento 5. Categorie di Dati Personali 6. I Diritti e la Tutela degli Interessati 7. Big Data, Piattaforme digitali, Privacy by Design 8. Cybersecurity e Cyberisks 9. Intelligenza Artificiale 10. La figura del DPO TESTI CONSIGLIATI · G. MAGRI, S. MARTINELLI, S. THOBANI. Manuale di diritto privato delle nuove tecnologie. Giappichelli (18 marzo 2022). ISBN-13: 978-8892143098 · P. GUARDA, G. BINCOLETTO. Diritto comparato della privacy e della protezione dei dati personali. Ledizioni (19 aprile 2023). ISBN-13: 978-8855268868 · Compendio di normativa sulla privacy per il trattamento dei dati personali. Guida alla lettura del codice della privacy e del GDPR. Neldiritto Editore; 1° edizione (16 maggio 2022). ISBN-13: 979-1254700792

INSEGNAMENTO	PROGRAMMA
Business Intelligence e Big Data	1. La Business Intelligence all'interno dell'organizzazione aziendale 2. Data Warehousing 3. I Big Data 4. Data Science 5. Storage e Processo dei Dati nelle aziende 6. GDPR in relazione ai documenti informatici 7. Il decreto-legge Semplificazioni n. 76/2020. Art. 13-bis (codice di condotta tecnologica) del CAD (Codice dell'Amministrazione Digitale) 8. Responsabile per la Trasformazione digitale (RTD) TESTI CONSIGLIATI · REZZANI. Big Data Analytics. Il manuale del data scientist. Apogeo Education; I edizione (15 giugno 2017). ISBN-13: 978-8891621856 · S. OZDEMIR, P. POLI. Data science. Guida ai principi e alle tecniche base della scienza dei dati. Apogeo (15 giugno 2017). ISBN-13: 978-8850334193 · M. GOLFARELLI, S. RIZZI. Data Warehouse. Teoria e pratica della progettazione. McGraw-Hill Education; 2° edizione (1° gennaio 2006). ISBN-13: 978-8838662911 · F. BERGAMASCHI, D. BIANCONI, A. MATTAVELLI. Business intelligence per le PMI. Manuale per professionisti e imprenditori. Maggioli Editore (15 settembre 2022). ISBN-13: 978-8891659019
Cyber Security	1. Sicurezza Informatica 2. Analisi delle minacce informatiche 3. Gestione dei Rischi Informatici 4. Informatica Industriale 5. Data & System Security 6. Intelligenza Artificiale e Cyber Security 7. Ingegneria del Software Sicuro 8. Sicurezza Hardware e Software 9. Responsabilità delle Organizzazioni TESTI CONSIGLIATI · R. CERVELLI. Guida alla Cybersecurity: Manuale pratico di Sicurezza Informatica. Independently published, 2023. ISBN-13: 979-8397435857 · A. CONTALDO, D. MULA, G.BUSIA. Cybersecurity law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche. Pacini Giuridica, 2020. ISBN-13: 978-8833791548 · W. STALLINGS, A.DE PAOLA, G. LO RE. Sicurezza dei computer e delle reti. Pearson, 2022. ISBN-13: 978-8891915290 · I. CORRADINI, F. DI RESTA. Cybersecurity, digital forensics e data protection. Responsabilità delle organizzazioni, le prove digitali e il fattore umano. Themis, 2021. ISBN-13: 978-8896069448

INSEGNAMENTO	PROGRAMMA
IT Risk Analysis and Management	1. Introduzione alla protezione dei dati informatici 2. I sistemi e le reti informatiche: tipologie aziendali e rischi 3. Principi di analisi del rischio 4. Principi di gestione del rischio 5. Controlli di sicurezza ordinari 6. Controlli di sicurezza straordinari 7. Database dedicati per il monitoraggio di potenziali minacce TESTI CONSIGLIATI · A.C. WRIGHT, Manuale di business continuity e crisis management. La gestione dei rischi informatici e la continuità operativa, 2ª edizione, Franco Angeli, 2020. ISBN-13: 978-8891799098 · E. WHEELER, Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Syngress, 2011. ISBN-13: 978-1597496155 · F. ZUCCARI. IT Risk Management: Introduzione ai principali concetti e processi dell'IT Risk Management. Independently published, 2024. ISBN-13: 979-8873742899
Digital Forensics	1. Introduzione alla informatica forense 2. 2. Il profilo dell'informatico forense 3. 3. L'analisi dell'ambiente virtuale di un crimine informatico 4. 4. L'analisi dell'hardware utilizzato in un crimine informatico 5. Strumenti per l'analisi software 6. Strumenti per l'analisi hardware 7. Tecniche di recupero dati 8. Tecniche di recupero dati da hardware danneggiato 9. L'analisi dei cloud 10. Le indagini su servizi di posta elettronica 11. Le indagini su dispositivi mobili 12. Steganografia: riconoscimento e recupero di prove 13. L'acquisizione di prove durante un attacco informatico 14. La validazione e la presentazione delle prove raccolte 15. La stesura del report finale TESTI CONSIGLIATI · G. FAGGIOLI, A. GHIRARDINI. Digital Forensics: nuova edizione aggiornata (Hacking e Sicurezza Vol. 4). Apogeo; 3° edizione. ISBN-13: 978-8850331994 · R. MURENEC. Digital Forensics. Egaf, 2022. ISBN-13: 978-8835212706

INSEGNAMENTO	PROGRAMMA
Deep Learning	1. Introduzione al Deep Learning 2. Deep Learning e reti neurali 3. Metodologie di progettazione e di sviluppo 4. Le tecnologie del Deep Learning 5. Gli strumenti del Deep Learning 6. Panoramica sugli utilizzi del Deep Learning 7. Deep Learning applicato alla sicurezza informatica 8. Problemi e sfide nell'applicazione pratica del DP alla IT Security 9. Trend promettenti nello sviluppo del Deep Learning TESTI CONSIGLIATI · I.R.M.A., Deep Learning and Neural Networks: Concepts, Methodologies, Tools, and Applications, IGI Global, 2019. ISBN-13: 978-1799804147 · S. WEIDMAN. Deep learning. Dalle basi alle architetture avanzate con Python. Tecniche Nuove, 2020. ISBN-13: 978-8848141130
Sistemi per la gestione di Database e Big Data	1. Le norme europee sulla protezione dei dati 2. Norme sulla protezione dei dati di alcuni Stati extraeuropei 3. Tipologie di dati 4. Algoritmi di cifratura 5. Firme digitali 6. Sistemi biometrici di autenticazione 7. Sistemi di backup 8. La protezione fisica dei server dati 9. La protezione dei dati in ambiente cloud TESTI CONSIGLIATI P. DE GUISE, Programmazione e Controllo, Data Protection: Ensuring Data Availability, 2nd edition, Auerbach, 2020. ISBN-13: 978-0367256777 L. BROTHERSTON, A. BERLIN, R. VISCARDI. La sicurezza dei dati e delle reti aziendali. Tecniche e best practice per evitare intrusioni indesiderate. Tecniche Nuove, 2018. ISBN-13: 978-8848136150
Tesi finale	Un elaborato su uno dei temi trattati di almeno 30 pagine