FACOLTÀ DI INGEGNERIA INFORMATICA

MASTER EXECUTIVE IN PROTEZIONE AZIENDALE
Cybersecurity & Data Protection

Presentazione del Corso

Sebbene la cybersecurity rappresenti oggi una delle principali esigenze in tema di sicurezza, a causa della gravità e della frequenza degli attacchi, la protezione delle infrastrutture e dei dati aziendali non può basarsi solo alla prevenzione contro i cyber-attacchi. Le minacce ai dati e ai sistemi aziendali si manifestano anche con altre modalità (eventi naturali, attentati, ecc.) che richiedono al responsabile della protezione aziendale delle competenze che vanno ben al di là della sola cybersecurity.

La recente direttiva Europea NIS2 di prossima entrata in vigore e Il Regolamento Europeo 2016/679 per la protezione dei dati personali, solo per citare alcune delle normative in materia, hanno generato una profonda necessità di ripensare la gestione dei dati all'interno delle organizzazioni. Queste ultime hanno ora la responsabilità di integrare i propri sistemi e di definire un insieme di misure di mitigazione, tra cui la formazione del personale.

Il **Master Executive in Protezione Aziendale** – **Cybersecurity & Data Protection** è un percorso innovativo e di taglio pratico che risponde alla crescente esigenza di figure in grado di prevenire le minacce, tra cui i cyber attacchi e di organizzare l'azienda in una cultura della sicurezza, attraverso l'adozione di processi operativi in linea con le Best Practices internazionali e gli obblighi normativi.

Il **Master Executive in Protezione Aziendale – Cybersecurity e Data Protection,** progettato in collaborazione con **professionisti internazionali del settore**, è un percorso formativo di **100 ore** che offre una preparazione altamente specialistica utile ad acquisire gli strumenti tecnici e metodologici necessari per **valutare i maggiori rischi legati alla sicurezza dei dati e delle infrastrutture aziendali**. Un focus specifico sarà sui diversi aspetti che costituiscono una corretta gestione della sicurezza informatica: comprensione dei

Créée en vertu des articles 20 et 27 de la Constitution Fédérale
Dénomination enregistrée par le Registre du commerce de Genève: CH-660.6.638.023-1 | IDE: CHE-133.413.467

sistemi informativi, delle reti e delle moderne tecniche di crittografia, senza tuttavia trascurare gli altri aspetti, tra cui quello del rischio finanziario.

Una particolare enfasi è posta **agli aspetti pratici** dove i docenti, mediante l'utilizzo di **esercitazioni pratiche e attività di laboratorio**, portano in aula la propria esperienza e trasferiscono conoscenze e competenze in materia di sicurezza aziendale.

Obiettivi formativi

L' obiettivo è affrontare le sfide emergenti a livello nazionale e internazionale, offrendo ai partecipanti una formazione completa che comprenda conoscenze, competenze e abilità essenziali per identificare e proteggere non solo i sistemi e le infrastrutture informatiche, ma anche le informazioni sensibili e i dati personali.

Inoltre, ci impegniamo a esplorare le nuove frontiere rappresentate dall'Intelligenza Artificiale partendo dall'analisi delle frodi informatiche più sofisticate preparando i partecipanti ad affrontare in modo competente e proattivo le sfide in evoluzione nel campo della sicurezza informatica, fornendo loro una comprensione completa delle tecnologie emergenti e delle strategie per proteggere dati e risorse aziendali in un ambiente sempre più complesso e interconnesso.

Sbocchi occupazionali

Il Corso di Master Executive in Protezione Aziendale – Cybersecurity e Data Protection offre diverse possibilità di impiego nel mondo del lavoro. Al termine del corso, con le **competenze acquisite** e sarà possibile ricoprire diversi **ruoli manageriali** nei diversi ambiti della Cyber Security:

- Security Manager
- Security Administrator
- IT Auditor
- Project Manager
- Cybersecurity Consultant
- Cloud, Network & Security Specialist
- Blockchain Specialist

Requisiti di ammissione, esami di verifica e prova finale

Possono iscriversi i candidati in possesso di Diploma di Scuola Media Superiore e Laurea Triennale o Laurea Specialistica, Magistrale o Vecchio Ordinamento. In difetto dei titoli di studio richiesti, è possibile l'ammissione su dossier, sulla base di una valutazione dei titoli di studio conseguiti e dell'esperienza acquisita, nonché delle competenze sviluppate nel quadro dell'attività professionale.

Le lezioni verranno erogate a discrezione del Docente attraverso Tesine, commentari, manuali specialistici, dispense o lezioni tramite piattaforma in live streaming. La valutazione viene espressa in trentesimi.

La prova finale consiste in una Tesi di almeno 30 pagine su uno degli argomenti trattati durante il Master Executive.

MASTER EXECUTIVE IN
PROTEZIONE AZIENDALE – CYBERSECURITY E DATA PROTECTION

SSD	INSEGNAMENTO	ECTS
ING-INF/05	Fondamenti di sistemi informativi	1
INF/01	Reti di elaboratori e Internet	2
IUS/01	Tutela della privacy nel mondo digitale	2
IUS/01	I principi del GDPR	1
IUS/01	GDPR: Data breach	2
IUS/01	GDPR: Valutazione di impatto sulla protezione dei dati	2
INF/01	Fondamenti di sicurezza ICT	2
IUS/04	Privacy e proprietà intellettuale	2
INF/01	Laboratorio sicurezza cloud	1
INF/01	Crittografia	2
M-GGR/02	Introduzione alla geo-politica	1
INF/01	Applicazioni della crittografia	2
INF/01 IUS/04 IUS/13	Criptovalute	2
INF/01	Analisi e gestione del rischio cyber	2

INF/01	Internet of Things (IoT)	2
INF/01	Laboratorio criptovalute	1
INF/01	Laboratorio sicurezza dei sistemi	1
ING-INF/05	Computer forensic	2
ING-INF/05	Business intelligence e data mining	2
INF/01	Laboratorio sicurezza delle reti	1
INF/01	Tecniche di verifica della sicurezza dei sistemi e delle reti - Teoria e pratica	2
-	Case study	2
	Tesi finale	3

DURATA E STRUTTURA DEL MASTER EXECUTIVE	
Durata:	Aprile - luglio 2024 – 100 ore
Frequenza:	Formula fine settimana: 8 ore il venerdì e 4 ore il sabato
Docente:	Prof. Claudio Cilli
Iscrizioni:	Dal 1° marzo al 15 aprile 2024
Stage in presenza:	Presso aziende o università con cui sono stati stipulati specifici accordi
Crediti:	40 ECTS
Modalità:	**Lezioni sincrone in virtual room e laboratori pratici**: Le lezioni saranno condotte sia in aula virtuale sincrona, per favorire l'interazione e il coinvolgimento attivo degli studenti, sia attraverso laboratori pratici. Questo approccio garantisce una formazione completa e pratica.
Prezzo:	CHF/EUR 4.800,00 (comprensivo di Iscrizione, Diritti di Segreteria e eventuale **stage in presenza e/o online**)

PROGRAMMA

INSEGNAMENTO	PROGRAMMA
Fondamenti di sistemi informativi	Fornire le basi per comprendere, significato, scopo, struttura e funzionamento di un sistema informativo.
Reti di elaboratori e Internet	Far comprendere il funzionamento delle reti di elaboratori e la struttura di Internet
Tutela della privacy nel mondo digitale	Conoscere gli elementi tecnici rilevanti relativi alla protezione dei dati personali, all'anonimizzazione delle informazioni e alle valute digitali
I principi del GDPR	I principi fondamentali per garantire la protezione dei dati: liceità, correttezza, trasparenza, minimizzazione, esattezza, limitazione, integrità e riservatezza
GDPR: Data breach	Legislazione e definizione di Data Breach- Impatto sulle aziende - Data Breach Notification: responsabilità della notifica, contenuto della notifica, eccezioni alla notifica, registrazione delle violazioni - Integrità/Disponibilità/Riservatezza dei dati personali
GDPR: Valutazione di impatto sulla protezione dei dati	Come condurre la valutazione di impatto privacy sulla protezione dei dati in particolare che utilizzano le nuove tecnologie, tenuto conto della natura, dell'ambito, del contesto e delle finalità del trattamento che possa comportare un rischio elevato per i diritti e le libertà degli individui.
Fondamenti di sicurezza ICT	Conoscere gli elementi essenziali della sicurezza ICT in termini di malware, attacchi tipici, apt ecc.
Privacy e proprietà intellettuale	Avere capacità di valutare scenari reali utilizzando gli aspetti essenziali della normativa sulla privacy (GDRP) e sulla proprietà intellettuale
Laboratorio sicurezza cloud	Obiettivi: consentire di svolgere e verificare gli effetti della configurazione sicura di utenze, sistemi e infrastrutture cloud, se possibile mostrando configurazioni di servizi CASB. Illustrare e far utilizzare soluzioni e configurazioni avanzate di sicurezza dei servizi di almeno un grande cloud provider.
	Programma pratico di sicurezza cloud: Identity management (if the enterprise's identity management system is integrated with the cloud computing system), Security incident management (to interface with and manage cloud computing incidents), Network perimeter security (as an access point to the Internet), Systems development (in which the cloud is part of the application infrastructure), Project management, IT risk management, Data management (for data transmitted and stored on cloud systems), Vulnerability management
Crittografia	Avere conoscenze sulle moderne tecniche di crittografia, algoritmi e loro caratteristiche (inclusa la steganografia) e tecniche di crittoanalisi
Introduzione alla geo-politica	Avere un quadro che includa gli elementi essenziali della geo-politica, a partire dai fondamenti
Applicazioni della crittografia	Disporre di un riferimento pratico e diretto per applicare le tecniche di crittografia (firma digitale, funzioni hash)
Criptovalute	Introduzione alle Criptovalute - Sicurezza e normative
Analisi e gestione del rischio cyber	Conoscere ed applicare i modelli di analisi del rischio
Internet of Things (IoT)	Avere una panoramica della tecnologia alla base degli embedded device, loro costituzione e rischi connessi al loro utilizzo - NFT e applicazioni su Blockchain
Laboratorio criptovalute	Progettare una dapp su blockchain
Laboratorio sicurezza dei sistemi	Classificare gli eventi di compromissione usando i modelli Cyber Kill Chain ed il MITRE ATT&CK framework; Il database Mitre CVE; Massimizzare il rilevamento e la risposta ad attacchi avanzati durante una tipica kill chain; Il ruolo della Threat Intelligence; Microsoft CyberSecurity reference model. Esempi pratici di attacchi

Créée en vertu des articles 20 et 27 de la Constitution Fédérale
Dénomination enregistrée par le Registre du commerce de Genève: CH-660.6.638.023-1 | IDE: CHE-133.413.467

INSEGNAMENTO	PROGRAMMA
Computer forensic	Essere in grado di applicare le tecniche di analisi forense sui sistemi informatici a fini investigativi
Business intelligence e data mining	Conoscere gli strumenti fondamentali per analizzare i cosiddetti Big Data ed i principali utilizzi dell'intelligenza Artificiale
Laboratorio sicurezza delle reti	Obiettivi: consentire di svolgere attività di configurazione sicura degli apparati e delle principali tipologie di sistemi perimetrali e di monitoraggio della rete, progettare e/o rivedere la progettazione di reti per garantire adeguati livelli di sicurezza e disponibilità dei servizi. Esempi pratici: Network Cabling Attacks, Network Component Attacks, ICMP Attacks, DNS Attacks, Email Attacks, Wireless Attacks, Remote Attacks and Other Attacks
Tecniche di verifica della sicurezza dei sistemi e delle reti - Teoria e pratica	• Enumerazione di porte e servizi di un sistema (port-scanning con nmap, masscan, ecc.) • Identificazione di potenziali vulnerabilità (check risultati e ricerche online) • Verifica e exploitation di potenziali vulnerabilità (valutazione di possibili exploit e utilizzo degli stessi) • Enumerazione di un'applicazione web (directory e file enumeration con tool come gobuster, ffuf, ecc.) • Analisi e verifica di un'applicazione web (utilizzo di proxy web come Burpsuite)
Case study	Testimonianza società internazionale di cybersecurity
Tesi finale	Un elaborato su uno dei temi trattati di almeno 30 pagine.