MASTER

UNICUSANO

SPECIALISTA IN CYBERSECURITY, DIGITAL FORENSICS E DATA PROTECTION

II LIVELLO

Image by Freepik

UNIVERSITÀ CUSANO

L'Università degli Studi Niccolò Cusano attiva il Master di II livello in "Specialista in cybersecurity, digital forensics e data protection" di durata pari a 1500 h.

Agli iscritti che avranno superato le eventuali prove di verifica intermedie e la prova finale verrà rilasciato il Diploma di Master di II livello in "Specialista in cybersecurity, digital forensics e data protection".

Obiettivi e modalità

Il master si inserisce in un contesto, di livello europeo e nazionale, e si pone l'obiettivo di trasferire agli studenti le conoscenze, le competenze e le abilità necessarie ad individuare i sistemi, le infrastrutture informatiche e le reti da un parte, le informazioni riservate e i dati personali dall'altra, questi ultimi costituiscono l'asset informativo che deve essere protetto al pari di tutte le risorse critiche del sistema informativo.

Il master ha il pregio di affrontare non solo la tematica della cybersicurezza, attraverso un'approfondita analisi del "chi" e "come" deve compiere gli adempimenti necessari nell'ambito del perimetro nazionale sulla cybersicurezza, ma anche la conformità nornativa delle organizzazioni complesse, la conoscenza i modelli organizzativi relativi alla responsabilità amministrativa degli enti collettivi, la protezione dei dati personali e dell'identità digitali, la sicurezza informazioni.

Saranno anche affrontate tematiche connesse alle nuove sfide tecnologiche come le soluzioni di intelligenza artificiale, le criptovalute, le frodi informatiche più insidiose che colpiscono in prevalenza il settore privato e il settore pubblico, il cloud computing. Il master tratterà anche la digital forensics, informatica forense, ossia quella scienza forense dedicata alla prova digitale nei casi giudiziari.

Destinatari e requisiti di ammissione

Per l'iscrizione al Master è richiesto il possesso di almeno uno dei seguenti titoli:

1. laurea conseguita secondo gli ordinamenti didattici precedenti il decreto ministeriale 3 novembre 1999 n. 509;

2. lauree specialistiche di II livello ai sensi del D.M. 509/99 e lauree magistrali ai sensi del D.M. 270/2004;

I candidati in possesso di titolo di studio straniero non preventivamente dichiarato equipollente da parte di una autorità accademica italiana, potranno chiedere il riconoscimento del titolo ai soli limitati fini dell'iscrizione al Master. Il titolo di studio straniero dovrà essere corredato da traduzione ufficiale in lingua italiana, legalizzazione e dichiarazione di valore a cura delle Rappresentanze diplomatiche italiane nel Paese in cui il titolo è stato conseguito.

I candidati sono ammessi con riserva previo accertamento dei requisiti previsti dal bando.

I titoli di ammissione devono essere posseduti alla data di scadenza del termine utile per la presentazione per le domande di ammissione.

L'iscrizione al Master è compatibile con altre iscrizioni nel rispetto della nuova normativa in materia di iscrizione contemporanea a due corsi di istruzione superiore, così delineata ai sensi della Legge n. 33 del 12 aprile 2022.

Durata, organizzazione didattica, verifiche e prova finale

Il Master ha durata annuale pari a 1500 ore di impegno complessivo per il corsista, corrispondenti a 60 cfu.

Il Master si svolgerà in modalità e-learning con piattaforma accessibile 24h / 24h.

Il Master è articolato in :

- lezioni video e materiale fad appositamente predisposto;

- eventuali test di verifica di autoapprendimento

Tutti coloro che risulteranno regolarmente iscritti al Master dovranno sostenere un project work finale che accerti il conseguimento degli obiettivi proposti presso la sede dell'Università sita in Roma– Via Don Carlo Gnocchi 3.

Ordinamento didattico

10 CFU

IUS/13
IUS/14

Cyber crimes: quadro normativo internazionale, europeo ed italiano.

- I cyber crimes: la digitalizzazione della criminalità, anche organizzata.
- La normativa internazionale: analisi delle convenzioni internazionali rilevanti in materia di cybersicurezza , contrasto al terrorismo e criminalità informatica, la protezione dei dati
- Il direttiva e-privacy (Direttiva UE 2008/58) e le prospettive di riforma
- Unione Europea: normativa generale ed interventi nell'area UE: la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 (c.d. Direttiva NIS), Reg. UE 2016/679, Direttiva UE 2016/680 e Direttiva UE 2016/681
- Analisi dei criteri, principi e adempimenti previsti dalla normative europee sopra richiamate
- Il diritto italiano: analisi delle normative di recepimento nazionale, analisi di disposizioni rilevanti del codice penale, di procedura penale e della normativa speciale di settore
- Perimetro Sicurezza Il decreto-legge 21 settembre 2019, n. 105,
- CSIRT e CERT : l'importanza dell'iteroperabilità tra Stato Regioni e aziende nella gestione degli alert di sicurezza

Ordinamento didattico

20 CFU

Cyber crimes: imprese ed aziende private — IUS/14 ING-INF/01

Analisi del quadro normativo applicabile al settore privato: il Regolamento UE 2016/679 (c.d. GDPR) e la Direttiva UE 2015/2366 (c.d. PSD2): il livello di sicurezza adeguato al rischio e la sicurezza degli strumenti di pagamento – la nozione di indipendenza dei fattori di autenticazione
Analisi della giurisprudenza in tema di risarcimento dei danni da furto di identità e dati personali
Analisi della distribuzione dei ruoli e delle responsabilità nelle organizzazioni complesse: settore bancario e assicurativo e la complessa rete degli intermediari
Evoluzione della criminalità informatica in Italia: analisi statistica e statistiche
Evoluzione della criminalità informatica nel settore bancario:

- dal phishing tradizionale allo spear phishing
- pharming
- trashing
- Man in the middle e Man in the browser
- La Sim Swap Fraud, il Sim Hijacking, sicurezza ed investigazioni nel mobile
- Investigazioni tramite celle telefoniche e tabulati
- Banking App e la sicurezza informatica nel contesto italiano ed internazionale

Analisi di casi di studio relativi alla criminalità informatica in ambito bancario Criminalità informatica e protezione degli asset informativi nel settore sanitario:

- Le app mediche e la sicurezza informatica
- Criminalità informatica nel settore assicurativo.

Criminalità informatica e protezione degli asset informativi nei servizi essenziali
Il data breach (violazione dei dati) nelle imprese, il registro delle violazioni: procedure di indagine e gestione dei data breach
IoT overview (protocolli, standard e campi di applicazione)
cybersecurity IoT nel mondo industriale (ICS e SCADA) e nelle auto a guida autonoma
modelli di IoT Risk Assessment
Il sistema di gestione D.lgs 231 sulle responsabilità delle persone giuridiche: modelli organizzativi

Delitti informatici e trattamenti illeciti di dati
Il Monitoraggio e la prevenzione : le armi delle aziende contro gli attacchi Cyber
L'importanza del SOC (security operation Center)
L'analisi del "movimento laterale": l'utilizzo di honeypot
Vulnerability assessment e Test penetration
La gestione dell'incident
Quali i log fondamentali da mantenere ed analizzare
Le simulazioni e le procedure interne per il data breach

Ordinamento didattico

15 CFU

Cyber crimes: la Pubblica Amministrazione

IUS/10 IUS/14 IUS/17

- Analisi del quadro normativo applicabile nelle pubbliche amministrazioni
- Brevi cenni storci sulla criminalità informatica in Italia.
- Il caso Noi PA.
- La sicurezza della APP nella pubblica amministrazione
- Analisi delle APP nelle sanità pubblica: il caso di APP immuni
- Caso relativo alla truffa al CEO
- Analisi della APP Immuni: analisi del quadro normativo e le appdi contact tracing nel contesto internazionale
- Furti di identità in ambito sanitario pubblico e sanitario accreditato: come, quando e perché.

Trattamento dei dati personali in ambito lavorativo

IUS/10 IUS/14 IUS/17

- La disciplina privacy nei rapporti di lavoro pubblici e la nuova disciplina prevista dal Reg. UE 2016/679 I
- controlli a distanza sull'attività del lavoratore e riforma dell'art. 4 dopo il Jobs act: videosorveglianza, geolocalizzazione, dispositivi di riconoscimento biometrico
- Le soluzioni biometriche per il controllo accesso e per la rilevazione presenze nella PA:analisi del Decreto c.d. Concretezza ed il parere del Garante per la protezione dei dati personali
- Gestione della posta elettronica e dei dati di navigazione su internet nell'ambito del rapporto di lavoro
- Ambito di utilizzabilità delle prove per fini disciplinari
- Lo smart working e la tutela della protezione dei dati
- Lo smart working e gli illeciti penali

Analisi dei principali reati informatici e illeciti realizzati nelle imprese, le garanzie costituzionali:

- Reati posti a tutela dell'inviolabilità del domicilio
- Reati posti a tutela dell'inviolabilità dei segreti
- Delitti contro il patrimonio mediante violenza alle cose o persone
- Delitto contro il patrimonio mediante frode
- Illeciti penali in ambito protezione dei dati personali
- Illeciti penali in ambito legge sul diritto d'autore
- Illeciti presenti in diverse normative applicabili all'ambiente digitale

Le indagini a tutela della persona offesa del reato: analisi dei casi di studio

UNIVERSITÀ CUSANO

Ordinamento didattico

15 CFU

Cyber security e informatica forense

ING-INF/01
IUS/14

- 1. Panoramica sulle Best Practices Computer forensics;
- 1.1 – L'immodificabilità della fonte di prova ed il metodo scientifico;
- 1.1.1 - Il sopralluogo informatico;
- 1.2 - Analisi live e post mortem (i perché, pro e contro);
- 1.3 - Identicità della prova;
- 1.3.1 - hash, cosa sono ed il problema della collisione;
- 1.3.2 - catena custodia;
- 1.3.3 - ripetibilità delle operazioni;
- 1.4 – Digital profiling e social engineering.
- 2. Gli strumenti della C.F. - open source vs commerciale
- 3. Write blocker ed hardware forense;
- 3. 1 Le quattro fasi (Identificazione, acquisizione, analisi, reporting) in pratica.
- 4. GNU/Linux per la C.F. (uso della distro C.A.I.N.E. http://www.caine-live.net live distro forense);
- 5. Cenni su casi reali di cronaca.
- 6 Panoramica sulla mobile forensics: tecniche di acquisizione ed analisi sui cellulari/tablet.
- 7. Cenni sulla legge 48/2008, art. 359 e 360 c.p.p. e DPR 115/02.
- 8. Live analysis ed acquisizione su un sistema acceso.
- 10. Il futuro della D.F.
- 11. I miti e le leggende.
- 12. Elementi di OSINT (Open Source Intelligence).
- 13. Indagini sulle criptovalute.
- 13. Introduzione all'Intelligenza Artificiale applicata alla digital forensics.
- 14. Set-up di un Laboratorio di Digital Forensics.

Ordinamento didattico

CYBER SECURITY

Definizione

- Panoramica sui crimini informatici e la loro evoluzione e diffusione
- Malware e cracking
- Anatomia di un attacco informatico
- Le vulnerabilità
- I rischi e le minacce (ransomware, phishing, social engineering, MITM ecc.)
- La difesa (contromisure informatiche ed umane)
- La prevenzione e le regole
- Esempio di un protocollo SGSI (Sistema di Gestione della Sicurezza delle Informazioni)
- Il Dark Web e sistemi di anonimizzazione
- I vettori di malware (computer e mobile)
- I nuovi cybercriminali
- Semplici regole di protezione domestica
- La profilassi informatica
- Contromisure tecniche
- Incident Response
- La sicurezza come processo

Consiglio didattico scientifico

- **Fabio Di Resta** : Responsabile Scientifico, Avvocato, specializzato in Gran Bretagna in ICT and IP Law, ISO 27001 Lead Auditor, fondatore dello studio legale “Di Resta Lawyers”, Presidente del Centro europeo per la Privacy (EPCE)
- **Mauro Alovisio** : Avvocato presso Università degli Studi di Torino, già docente a contratto presso Università Statale di Milano, è specializzato nel diritto delle nuove tecnologie e nella protezione dei dati personali /privacy
- **Giovanni Grassucci** : Avvocato, esperto in tutela giudiziale in ambito protezione dei dati.
- **Silvano Sacchi:** Avvocato, esperto in tutela giudiziale in ambito protezione dei dati.
- **Antonio Mauro** : Dottorato in Ingegneria Informatica e Dottore in Filosofia, Comunicazione Elettronica e Cybercrime Security Governance Cloud, Computing per il governo degli Stati Uniti
- **Massimo Davi** : AMMD Law – Socio Fondatore - Avvocato Cassazionista - Penalista -Legal & 231 Compliance Consultant
- **Enzo Veiluva** : Dirigente Responsabile della nuova area DPO dedicata alla gestione delle problematiche privacy in azienda, inserita all'interno della Direzione Intemal Audit.
- **Paolo Reale** : Consulente, di Aziende e Privati, Polizia Giudiziaria e del Giudice (Consulenze d’Ufficio), esperto in ambito delle telecomunicazioni, dell’informatica e più in generale dei sistemi di Information and Communication Technology.
- **Giovanni Bassetti** : Esperto in Digital Forensics (Informatica forense) - Consulenze tecniche di parte e d'ufficio, perizie informatiche
- **Paolo Dal Checco** : Titolare di Studio Tecnico d’Informatica Forense, iscritto all’Albo dei CTU e dei Periti del Tribunale di Torino, Esperto della CCIAA di Torino, CTP (Consulente Tecnico di Parte) in ambito di perizia informatica forense per Perizia di Parte
- **Nadia Zabbeo** : Consulente e Formatore Privacy & Cybersecurity e Data Breach Protection Advisor
- **Alberto Culatina** : Esperto per il Dipartimento per la Trasformazione Digitale sotto la Presidenza del Consiglio dei ministri

Costi e agevolazioni

Il costo annuo del Master è di € 2.500,00 (duemilacinquecento/00).

Il pagamento verrà corrisposto in quattro rate di pari importo.

È prevista una quota d'iscrizione ridotta per determinate categorie.

Si invita a consultare il bando del Master.

CONTATTI

Ufficio consulenza orientamento didattico Master e

Corsi di Perfezionamento (pre-iscrizione):
Telefono: 06 45678363
dal Lunedì al Venerdì dalle 9:00 alle 18:00
Mail: infomaster@unicusano.it

Ufficio Assistenza Didattica (post-iscrizione):
Telefono: 06 89320000
dal Lunedì al Venerdì dalle 9:00 alle 22:00
Mail: master@unicusano.it
unicusano.it/master-universitari-online

UNIVERSITÀ CUSANO