

■ MASTER UNICUSANO

CYBERCRIME MANAGEMENT
& IT INVESTIGATION FOR
DIGITAL DEFENCE

II LIVELLO



UNIVERSITÀ
CUSANO



Obiettivi e modalità

Il Master si propone di trasferire agli studenti le conoscenze, le competenze e i limiti necessari per fronteggiare questo nuovo fronte investigativo.

È cruciale esser pronti a cristallizzare le fonti di prova digitali a fronte di crimini interni ed esterni nell'ambito aziendale, privato o pubblico ed essere anche preparati a ricostruire gli accadimenti, tracciati dai dispositivi informatici, legati ad eventi criminosi di ogni genere, poiché ogni comportamento lascia tracce digitali, pertanto, sarà fondamentale imparare i metodi e gli strumenti necessari per le indagini informatiche, anche alla luce degli ultimi orientamenti giurisprudenziali.



Destinatari e ammissione

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

- laurea conseguita secondo gli ordinamenti didattici precedenti il decreto ministeriale 3 novembre 1999 n. 509;
- lauree specialistiche di I 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 al Comitato Scientifico 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; si svolgerà in modalità e-learning con piattaforma accessibile 24 h\24 ed è articolato in:

- lezioni video e materiale fad appositamente predisposto;
- congruo numero di ore destinate all'auto-apprendimento, allo studio individuale e domestico;
- eventuali verifiche intermedie per ogni materia.

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



Ordinamento didattico

TOTALE 60 CFU

4 CFU

Il Cybercrime: soggetto, oggetto e condotta

IUS/20

- La nascita del diritto penale dell'informatica
- La rilevanza internazionale del cyber crime
- La convenzione di Budapest
- La legge n.48/2008 di ratifica della Convenzione di Budapes
- La legge n.12/2012
- L'oggetto materiale e la condotta dei reati informatici
- I soggetti del reato informatico

7 CFU

I Cybercrimes nell'era digitale

IUS/17

- La diffamazione attraverso i social network
- La evoluzione della diffamazione con il mezzo digitale
- I problemi procedurali della diffamazione via web
- Il cyberbullismo
- I profili sovranazionali del cyberbullismo
- La normativa nazionale del cyberbullismo
- Il cyberstalking
- La raccolta delle prove nel cyberstalking
- Evoluzione giurisprudenziale e prassi



10 CFU I Sex Crimes nell'era digitale

IUS/20

- Internet e le fattispecie delittuose a sfondo sessuale
- Abuso sessuale sui minori: cenni descrittivi e normativi
- Pedofilia e pedopornografia nella rete
- Il fenomeno del child grooming
- Dalla pedopornografia al sexting
- Sextortion
- Revenge porn
- Le azioni di contrasto

7 CFU La cybersecurity come strumento per contrastare i crimini informatici

IUS/20

IUS/17

- Fondamenti di cybersecurity
- Evoluzioni della cybersecurity nel contesto normativo europeo e italiano
- Il fattore umano nell'ambito della sicurezza informatica
- La valutazione e gestione del Cyber risk
- Information Security Management System: lo Standard ISO/IEC 27001
- Cybersecurity e Responsabilità Amministrativa ex D.Lgs. 231/2001

8 CFU Le attività di digital forensics nel cybercrime

IUS/20

IUS/16

- L'informatica forense
- Il trattamento della prova digitale
- I mezzi di ricerca della prova digitale
- Le acquisizioni delle fonti di prova nell'ambiente informatico
- Il superamento della tradizionale distinzione tra rilievi e accertamenti tecnici
- La ripartizione dell'onere della prova digitale
- Violazione dei protocolli e conseguenze processuali
- Le acquisizioni digitali all'esterno ai sensi del nuovo articolo 234 - bis c.p.p.



4 CFU **La mobile Forensics e la Computer Forensics**

IUS/20

- Le fasi della mobile forensics
- Il mobile devices e procedimento penale
- Le best practices sulla computer forensics
- Il sopralluogo informatico

6 CFU **I risvolti processuali della prova digitale tra prova atipica e prova documentale**

IUS/16

- La prova atipica: profili generali
- Cenni sull'evoluzione del metodo di accertamento giudiziale dalla teoria della prova legale al libero convincimento del giudice
- Tassatività e libertà dei mezzi di prova
- La scelta di compromesso del Legislatore del 1988
- Prova documentale: profili sostanziali
- La prova documentale nell'era digitale

2 CFU **Prova informatica e diritti della persona**

IUS/16

- Diritti fondamentali e digital forensics
- La libertà personale e le sue manifestazioni
- Il diritto all'inviolabilità del domicilio
- Libertà e segretezza delle comunicazioni
- Libertà di circolazione
- Privacy e riservatezza
- Diritto alla vita privata e alla tutela dei dati personali nella Carta dei Diritti Fondamentali dell'Unione Europea
- Verso la creazione dei nuovi diritti



4 CFU Le incursioni digitali sulla vita privata

IUS/16

- Le tecniche di investigazione nel pedinamento elettronico
- Le investigazioni mediante celle telefoniche
- Acquisizioni dei contenuti e-mail
- Spionaggio digitale nell'ambito dei Social network
- Intrusioni segrete nel domicilio informatico
- Localizzazione mediante celle telefoniche
- Comunicazioni a distanza apprese dall'inquirente per volontà di un conversatore
- Approvvigionamento di flussi e dati tramite dispositivo telefonico altrui

8 CFU Intercettazioni telematiche

IUS/16

- Intercettazioni tramite virus informatico
- Intercettazioni ambientali
- Videoriprese
- Le operazioni digitali sotto copertura
- Acquisizione di dati custoditi in ambiente cloud



Consiglio didattico e scientifico

- Prof. Fabrizio Corona
- Avv. Enrico von Arx
- Avv. Alessia Del Pizzo
- Dott. Salvatore Pidota
- Dott.ssa Concetta Bottino
- Prof.ssa Vania Maffeo



Costi e agevolazioni

Il costo annuo del Master è di € 2.000,00 (duemila/00).

La quota verrà versata in quattro rate di pari importo.

E' prevista una quota d'iscrizione ridotta, pari a € 1.800,00 (milleottocento/00) per le seguenti categorie:

- Laureati Unicusano;
- Laureati da meno di 24 mesi.

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**