

Sicurezza digitale e intelligenza artificiale

PARTE I - INFORMAZIONI GENERALI

Tipologia di corso

Master di secondo livello

Titolo del corso

Sicurezza digitale e intelligenza artificiale

PARTE II - REGOLAMENTO DIDATTICO ORGANIZZATIVO

Indirizzo web del corso

<https://giurisprudenza.uniroma3.it/didattica/post-lauream/>

Il Corso di Studio in breve

Il Master universitario di secondo livello in "Sicurezza digitale e intelligenza artificiale" propone una formazione specialistica post lauream sulle varie implicazioni della sicurezza digitale e dell'intelligenza artificiale. Per sicurezza digitale si intende quel dispositivo sempre più complesso che unisce tra loro sicurezza nazionale digitale, cybersecurity, sviluppo e impiego dell'intelligenza artificiale, intelligence, ruolo delle imprese e dello Stato, attraverso l'impiego di poteri speciali quali il Golden Power, sempre più ricadenti nell'alveo dell'alta tecnologia, ecosistema della difesa. L'obiettivo è quello di far acquisire adeguati strumenti metodologici e competenze, teoriche e pratiche a chi, nel settore pubblico o privato, deve essere in grado di affrontare le sfide poste dalle nuove tecnologie, per comprendere, definire e risolvere questioni in tema di sicurezza e tutela tanto della dimensione aziendale, quanto di quella statale. La convergenza tra intelligenza artificiale, mondo delle imprese, interesse nazionale, sicurezza informatica e intelligenza artificiale impone sfide strategiche e geopolitiche sempre più articolate e complesse, sia sul versante della multidisciplinarietà sia nel senso, interno al mondo del diritto, di andare oltre i confini di una singola materia o di un singolo ambito, riuscendo così a sviluppare competenze trasversali. Per tale ragione, la proposta didattica si fonda sull'interdisciplinarietà dei saperi, a fronte della eterogeneità delle conoscenze indispensabili per la prevenzione di eventuali situazioni di crisi, per la gestione di eventuali attacchi informatici e delle loro implicazioni nel contesto del sistema nazionale e internazionale, per il monitoraggio dei flussi economico-finanziari, per il contrasto al cybercrime, per l'indispensabile conoscenza dei paradigmi di analisi geopolitica e di cyber-intelligence e degli strumenti ordinamentali posti a tutela del nostro Paese. Il Corso si articola in due parti. La prima, dal taglio teorico, è connotata da attività di docenza e seminariale, organizzata dal Dipartimento di Giurisprudenza e da quello di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche dell'Università degli Studi Roma Tre, per analizzare questioni giuridiche, sotto diversi profili - sovranazionali, penalistici, pubblicistici, amministrativistici e di management-aziendale - e per approfondire le più delicate questioni relative agli algoritmi, ai sistemi informativi, all'internet delle cose, alle infrastrutture critiche e alla loro sicurezza, all'applicazione dell'IA in chiave di geopolitica, sicurezza nazionale e di difesa, all'utilizzo dei poteri speciali in chiave digitale (Golden Power). La seconda parte del corso, invece, ha un taglio eminentemente pratico-operativo, grazie al coinvolgimento nell'attività di docenza di esperti della Guardia di Finanza, per l'esame delle questioni in materia economico-finanziaria, relative al contrasto al riciclaggio e al finanziamento del terrorismo e della Polizia postale, per lo studio dei modelli teorici e delle prassi operative in tema di investigazione proattiva in rete, di contrasto al cybercrime, al cyberterrorismo, in tema di digital forensics. L'obiettivo è quello di incrementare conoscenze e sviluppare competenze avanzate sul diritto delle nuove tecnologie esaminando, in particolare, il bilanciamento tra protezione delle banche dati e tutela dei diritti, con un focus sulle problematiche di più stringente attualità, relative al crescente potere dei c.d. attori del capitalismo della sorveglianza e al rapporto tra sovranità statale e digitale. Il Corso vuole offrire un bagaglio di strumenti indispensabili per la specializzazione nel campo della sicurezza digitale e dell'IA di funzionari e dirigenti delle Pubbliche Amministrazioni, di operatori delle Forze dell'ordine e delle forze armate, di operatori nell'ambito della sicurezza economico-finanziaria o del settore bancario e creditizio, di esperti di crimini informatici, di professionisti e consulenti, in considerazione anche della sempre maggiore importanza della figura del Chief Information Security Officer (CISO) nell'organigramma aziendale.

Obiettivi formativi specifici del Corso

Il percorso formativo del Master è in grado di assicurare una preparazione adeguata sia dal punto di vista del quadro teorico di riferimento, che delle conoscenze pratico-applicative in materia di intelligenza artificiale, geopolitica digitale, cybersecurity e sicurezza nazionale digitale, al fine di specializzare analisti, operatori delle forze dell'ordine, professionisti e consulenti, tanto libero-professionali quanto interni a realtà aziendali, esperti in crimini informatici, avvocati e funzionari amministrativi nel campo della cybersicurezza, nonché Referenti per la cybersicurezza delle amministrazioni pubbliche di cui alla legge n.90/2024 e i futuri Chief Information Security Officer (CISO). Lo scopo del Master è quello di fornire gli strumenti adeguati a implementare le conoscenze dei partecipanti, tanto da un punto di vista teorico, quanto pratico-operativo, tenuto conto dell'apporto che in tal senso sarà fornito dalla Guardia di Finanza e dalla Polizia Postale e per la Sicurezza Cibernetica, al fine di offrire una formazione che consenta di affrontare le sfide, anche professionali, del settore della sicurezza nazionale digitale, dell'intelligenza artificiale, dell'analisi geopolitica legata alle nuove tecnologie e alla cybersecurity nella realtà contemporanea, ove ai rischi tradizionali si aggiungono le numerose e sempre crescenti minacce cyber, con evidenti ripercussioni sul sistema nazionale.

Sbocchi occupazionali e professionali previsti per i laureati

Consulente di impresa, esperto in crimini informatici, informatico forense (digital forensics) avvocato specializzato, operatori delle Forze dell'ordine, operatori dei servizi di Intelligence, funzionari e dirigenti nel campo della sicurezza digitale e della cybersecurity, appartenenti alle Forze Armate specializzati in chiave IA e cyber, esperti di Golden Power con specifico riguardo all'alta tecnologia, analisti geopolitici in tema di IA e alta tecnologia, Referente per la cybersicurezza delle amministrazioni pubbliche di cui alla legge n.90/2024 Chief Information Security Officer (CISO).

Obiettivi formativi specifici

Il percorso formativo del Master è in grado di assicurare una preparazione adeguata sia dal punto di vista del quadro teorico di riferimento, che delle conoscenze pratico-applicative in materia di intelligenza artificiale, geopolitica digitale, cybersecurity e sicurezza nazionale digitale, al fine di specializzare analisti, operatori delle forze dell'ordine, professionisti e consulenti, tanto libero-professionali quanto interni a realtà aziendali, esperti in crimini informatici, avvocati e funzionari amministrativi nel campo della cybersicurezza, nonché Referenti per la cybersicurezza delle amministrazioni pubbliche di cui alla legge n.90/2024 e i futuri Chief Information Security Officer (CISO). Lo scopo del Master è quello di fornire gli strumenti adeguati a implementare le conoscenze dei partecipanti, tanto da un punto di vista teorico, quanto pratico-operativo, tenuto conto dell'apporto che in tal senso sarà fornito dalla Guardia di Finanza e dalla Polizia Postale e per la Sicurezza Cibernetica, al fine di offrire una formazione che consenta di affrontare le sfide, anche professionali, del settore della sicurezza nazionale digitale, dell'intelligenza artificiale, dell'analisi geopolitica legata alle nuove tecnologie e alla cybersecurity nella realtà contemporanea, ove ai rischi tradizionali si aggiungono le numerose e sempre crescenti minacce cyber, con evidenti ripercussioni sul sistema nazionale.

Informazioni utili agli studenti

-

Descrizione modalità di svolgimento

Possono essere ammessi al Master, in qualità di uditori, soggetti non in possesso del diploma di laurea, per venire incontro alle esigenze di numerose figure professionali che si misurano quotidianamente con problemi relativi alla cybersecurity o più in generale alla sicurezza digitale, ma che non hanno conseguito il titolo necessario all'iscrizione al Master. Tali uditori – selezionati anch'essi in base al curriculum vitae – potranno partecipare alle lezioni e alle attività didattiche organizzate nell'ambito del Master, senza sostenere le prove di verifica e la prova finale. Al termine verrà consegnato loro un attestato di partecipazione, senza riconoscimento di crediti formativi. Agli uditori si riconosce la riduzione del 25% della quota di iscrizione all'intero Master. Opportunità formativa stage extracurriculare cybersecurity

Requisiti di ammissione

Scadenza delle domande di ammissione: Domande di ammissione entro il 20 gennaio 2027. Iscrizione entro il 31 gennaio 2027. Classi di laurea dei titoli di accesso e ogni altro requisito specifico: Laurea magistrale, specialistica o titolo di studio equipollente in Giurisprudenza, Scienze politiche, Economia, Ingegneria. In presenza di posti disponibili, si valuteranno, ai fini della ammissione, lauree conseguite presso Dipartimenti diversi da quelli sopra indicati, sulla base del percorso formativo dell'interessato. Criteri di selezione nel caso in cui le domande di ammissione superino il numero massimo di ammessi: Curriculum vitae ed eventuale

colloquio. Procedure e criteri per il riconoscimento di crediti maturati dagli studenti nel corso degli studi universitari precedenti ai fini di una eventuale riduzione del percorso formativo e delle tasse d'iscrizione: Nessuno.

Numero di posti

50

Durata prevista

1 Anno

Crediti previsti

60

Lingua di insegnamento

ITA

Modalità didattica

Convenzionale

Tasse di iscrizione ed eventuali esoneri

La tassa d'iscrizione all'intero Corso di Master è stabilita in Euro 5.000,00 (Euro 3.000 per i soggetti che beneficiano della Convenzione PA 110 e lode - solo nel caso in cui il DFP selezioni il corso nell'anno di riferimento), da versare in due rate: la prima con scadenza 31 gennaio 2027 e la seconda con scadenza il 31 maggio 2027.

All'importo della prima rata sono aggiunti l'imposta fissa di bollo e il contributo per il rilascio del diploma o dell'attestato.

Le quote di iscrizione non sono rimborsate in caso di volontaria rinuncia, ovvero in caso di non perfezionamento della documentazione prevista per l'iscrizione al Corso.

*Tassa di iscrizione per gli appartenenti alle Forze dell'Ordine e all'Agenzia delle Dogane e dei Monopoli.
Euro 2.500.*

Esonero dalle tasse di iscrizione

Coloro i quali si trovino in condizioni di disabilità, con riconoscimento di handicap ai sensi dell'articolo 3, commi 1 e 3, della legge 5 febbraio 1992, n. 104, o con un'invalidità pari o superiore al 66% sono tenuti in ogni caso al pagamento della prima rata di iscrizione al Corso.

Per usufruire dell'esonero è necessario allegare alla domanda di ammissione un certificato di invalidità rilasciato dalla struttura sanitaria competente indicante la percentuale riconosciuta.

Tassa di iscrizione per uditori

La tassa di iscrizione ai Corsi in qualità di uditori è fissata in euro 3.750.

Rilascio titolo congiunto

Titolo normale

Direttore del Corso

Pistorio Giovanna

PIANO DELLE ATTIVITA' FORMATIVE

(Insegnamenti, Seminari di studio e di ricerca, Stage, Prova finale)

Anno	Denominazione	SSD	CFU	Ore	Tipo Att.	Lingua
1	20111012 - Cybersecurity, intelligenza artificiale e diritto penale	GIUR-14/A	2	-	AP	ITA
1	20111009 - Cybersecurity: assetto normativo e istituzionale	GIUR-10/A	4	20	AP	ITA
1	20111011 - Management della cybersecurity e dell'intelligenza artificiale	GIUR-01/A	2	10	AP	ITA
1	20111013 - Sicurezza digitale e nuove tecnologie	IINF-05/A	6	30	AP	ITA
1	20111010 - Sicurezza digitale, intelligenza artificiale e diritti	GIUR-05/A	5	30	AP	ITA

OBIETTIVI FORMATIVI