D.R. n. 377 del 15/07/2024

L'UNIVERSITA' TELEMATICA SAN RAFFAELE ROMA

e il CONSORZIO UNIVERSITARIO HUMANITAS

organizzano il
Master di I° livello in

"INTELLIGENCE, INVESTIGATION AND SECURITY"

(V edizione)

Partners: ICI Istituto Clinico Interuniversitario, Consorzio Universitario Universalus, Istituto Universalus, Humanitas Edizioni, Unindustria Perform S.r.l, Confedersicurezza

(A.A. 2024/2025)

Titolo	INTELLIGENCE, INVESTIGATION AND SECURITY
Direttore	Pref. Dott. Nicolò Marcello D'Angelo - Dott. Francesco Di Maio
Comitato scientifico	Pref. Dott. Nicolò Marcello D'Angelo Prof. Aniello Castiglione Prof. Francesco Orciuoli Prof. Angelo Gaeta Avv. Alessandro Bracci Dott. Francesco Di Maio Dott. Bruno Valensise Dott. Luigi Mone Dott. Giovanni Bonzano
Obiettivi e finalità	Il Master risponde alla richiesta di professionisti esperti in intelligence, cyber security, crimini informatici, violazione della riservatezza, criminalistica e indagini con strumenti tecnologicamente avanzati, per una visione completa dell'evento criminoso, inclusi gli aspetti tecnici e legali. Il master fornisce conoscenze e competenze per affrontare le richieste di settore, affrontando tematiche specifiche nell'ambito giuridico, nazionale ed internazionale, necessarie per l' aggiornamento dei professionisti del settore.
Articolazione e Metodologia del corso	Il Master ha una durata di 1500 ore (12 mesi), pari a 60 CFU (Crediti Formativi Universitari) ed è erogato in modalità FAD (asincrona) Durata: 12 mesi *Modalità FAD asincrona/sincrona* Metodologie Didattiche: – lezione: 300 ore – coaching online: 50 ore. Sono ore previste in sincrono con il tutor disciplinare esperto del modulo didattico – project work, prove di verifica: 200 ore – studio individuale: 500 ore – tirocinio: 250 ore – esercitazioni e prova finale: 200 ore I crediti formativi Universitari (CFU) si maturano con il superamento dell'esame finale di profitto, che consiste nella redazione e discussione di una tesina, davanti ad una Commissione appositamente nominata, frutto dello studio e dell'interpretazione personale del percorso formativo intrapreso e relativo alle attività svolte. La Commissione, nominata dal Rettore, è composta dai docenti del Corso. Al termine del Corso, a quanti abbiano osservato tutte le condizioni richieste e superato con esito positivo la prove finale sarà rilasciato un Diploma di Master di I° livello in

	"INTELLIGENCE, INVESTIGATION AND SECURITY"

Programma didattico

INSEGNAMENTO	SSD	CFU
Mod.1: Intelligence: scenari politici- economici -giuridici, globalizzazione Contesto istituzionale e normativo; • Analisi scenari di riferimento (geopolitici, sociali, economici, ambientali, tecnologici); • Rischi e terrorismo in trasformazione nell'area mediterranea. Estremismi; • L'Islam; • Intelligence e fonti aperte; • Metodologia della previsione. Il metodo, archiviazione e carteggio; • Analista e analisi previsionali (Risck Management); • Intelligence economico-finanziaria; • Intelligence e sicurezza psicologica. La comunicazione interpersonale; • Diritto Internazionale e Intelligence. Gli interessi nazionali: la sicurezza nei campi energetici, finanziari, chimici, dei trasporti e delle telecomunicazioni; • Intelligence e security intelligence: definizioni, metodologie e tecniche, Ambiti di utilizzo. Elementi di protezione delle infrastrutture critiche e del cyberspace	IUS/13	5
Mod.2: Security (aspetti giuridici/normativi) Legislazione: Sicurezza nella costituzione e sicurezza pubblica (ruoli e responsabilità); • Responsabilità giuridiche (penali, civili e amministrative) e aziendali; Elementi di diritto penale; • Responsabilità amministrativa degli enti; • Sicurezza sul lavoro; • Sicurezza privata.; • Elementi di sicurezza delle informazioni; • Codice la tutela della proprietà Industriale; • Tutela del know-how e del segreto industriale; Statuto dei Lavoratori; • Elementi di protezione dei dati personali; • Sicurezza nazionale, privacy e regolamento UE. Sicurezza nella PA, dalle normative alla governance: il sistema pubblico di sicurezza; Standard internazionali; • Normativa sulla privacy e sicurezza dei dati; Il codice dell'amministrazione digitale e la sicurezza; • Governance: principi generali sul GDRP (reg. UE 679/2016); codice protezione dei dati personali e D. Lgs. 101/2018 di modifica Delitti contro la riservatezza dei dati personali e dei dati sensibili Sistema sanzionatorio Sicurezza informatica nelle aziende (legislazione e giurisprudenza su diverse tematiche) Legislazione e compliance Direttiva NIS e legislazione sulla cybersecurity – obblighi di comunicazione Premesse sistematiche e dogmatiche sul cybercrime I reati informatici, reati commessi a mezzo di sistemi informatici e telematici e social network analisys Aspetti e principi di procedura penale in tema di indagini informatiche e telematiche (giurisprudenza) Lgs. 231/2001, modelli organizzativi e prevenzione del cybercrime in azienda; • Analisi organizzativa interna: struttura organizzativa, processi critici e operativi, risorse e aree critiche, vision, mission, strategia aziendale, policy, linee guida e procedure aziendali, codice di condotta, valore e azienda (economico,mercato e sociale), principi di sostenibilità, responsabilità sociale, tutela dei diritti umani ed etica; • Attività investigative ed indagini in Azienda	IUS/01	8
Mod.3: Security (aspetti tecnico/tecnologici e data) Security management: Definizione, • Security management: Definizione, Evoluzione storica, Compiti e attività, Organizzazione e Relazioni interne ed esterne della security, Chi e Cosa proteggere:	INF/01	8

	persone, risorse materiali, risorse immateriali, strutture, infrastrutture e infrastrutture critiche, siti e obiettivi sensibili, processi, Focus su: Sicurezza di luoghi ad alta frequentazione, Sicurezza di porti e aeroporti, Sicurezza di eventi e grandi eventi; • Analisi delle minacce e dei rischi: analisi delle minacce, vulnerabilità e rischi che possono gravare sul patrimonio informativo di una organizzazione Sicurezza OT Sicurezza delle reti radio mobili (Attività di penetration test e di malware analysis) Social engineering Il fenomeno dei virus, evoluzione e risposte Attacchi ad infrastrutture critiche Cybercrime Social media Architettura e sicurezza: Infrastrutture critiche Sicurezza delle reti Sicurezza IT Risk management Aspetti economici della sicurezza Computer forensics Crittografia; • Gestione del rischio (enterprise risk management): Rischi nelle organizzazioni, Metodologie di analisi, Politiche di gestione, Struttura di riferimento per la gestione dei rischi e normativa correlata, Strumenti di trasferimento a terzi (es. strumenti tecnici e assicurativi); • Il sistema di gestione dei rischi per la security (security risk management). Strumenti di sicurezza: Tecnologie e sistemi di sicurezza passiva, Tecnologie e sistemi di sicurezza attiva, Strumenti organizzativi di security (policy, procedure, organizzazione, ecc…). Servizi di sicurezza e altri servizi: Servizi di sicurezza privata Vigilanza privata: servizi, contratti e normativa di riferimento. Conoscenze Investigazione privata: servizi, contratti e normativa di riferimento Servizi di guardiania (portierato, accoglienza, ecc.); • Continuità operativa e gestione delle emergenze (business continuity & emergency management): Business Continuity e Disaster Recovery: definizione, metodologia e normativa di riferimento; Emergency Management: definizione, metodologia, attori coinvolti, comportamento individuale e delle masse, elementi di psicologia delle emergenze, comunicazione in caso di crisi		
	Mod.4: Criminalistica e Digital forensics Sopralluogo, repertamento e catena di custodia; • Genetica forense e banca dati del DNA (casi pratici); • BPA (casi pratici); • Dattiloscopia forense; • Tossicologia forense; • Antropologia forense; • Grafologia forense; • Medicina legale (casi pratici); • Truffa alle assicurazioni e falsi sinistri; • Analisi di fascicoli processuali (casi pratici); • Psicologia forense e Autopsia psicologica; • Consulenza tecnica; • Violenza di genere e vittimologia; • Fotodocumentazione delle tracce sulla scena del crimine;• Crime Training.	IUS/16	6
	Mod.5: Discipline Legali ed Internazionali – Tutela Dati Personali Cenni procedura penale e diritto penale; • Diritto penale internazionale; • Tutela dei Diritti Umani; • Le collaborazioni Internazionali; • Gestione internazionale dei testimoni; • Cooperazione Italiana allo sviluppo in paesi terzi; • Il regime di tutela dei dati personali, in ambito nazionale, europeo ed internazionale; • Antropologia Generale; • Sociologia della Criminalità	IUS/17	4
	Mod.6: Psicologia, Sociologia e Antropologia Applicate – Gestione Della Comunicazione Antropologia della sicurezza; • Scenario & Contesto Psicologia	M-PSI/01	5

	etnica; •Cross-culture Bias ederrori di percezione nell'analisi e attività di intelligence; • Basi neuro-fisio-psicologiche del comportamento; • Etica e approccio psicologico alla professione; • Criminologia applicata: Criminologia applicata e profiling criminale. Criminalità e sicurezza nei contesti urbani (CPTED); • Elementi di management: Elementi di strategia, pianificazione e controllo aziendale di organizzazione del lavoro e gestione delle risorse, di budgeting e finanza aziendale (es. strumenti di valutazione degli investimenti), di leadership, di project management, di time management, di comunicazione e negoziazione, di gestione dei conflitti, dello stress e del sé nei momenti critici.		
	Mod.7: Sistemi Globali e Diplomazia Le organizzazioni internazionali impegnate nella sicurezza; • Sistema NATO; • Diplomazia, nella teoria e nella pratica; • Diplomazia parallela; • Peacekeeping intelligence	IUS/13	4
	Laboratori: formazione on the job e redazioni progetti (casi)	-	2
	TIROCINIO		10
	ESERCITAZIONI E PROVA FINALE		8
	Tot. CFU		**60**
Docenti	Pref. Dott. Nicolò Marcello D'Angelo, già Vice Direttore Generale della Pubblica Sicurezza, Amministratore "Integrated Security Management Company srl" Avv. Prof. Francesco Di Maio, senior security consultant, Nato Cybersecurity Expert Prof.ssa Avv. Antonella Minieri, avvocato Cassazionista. Fondatrice dello Studio Legale Minieri & Partners Prof. Mario Morcellini, Professore ordinario, designato dal coordinamento Nazionale della Conferenza dei Presidi di Facoltà Dott. Renato Biondo, Direttore della Banca dati nazionale del Dna. Servizio sistema informativo interforze – Direzione centrale polizia criminale Dott. Giovanni Bonzano, Generale di Corpo d'Armata (c) nei Carabinieri, già rappresentante Agenzia Informazioni per la Sicurezza Esterna Dott. Genseric Cantournet, Presidente KELONY®, First Risk Rating Agency Dott. Marco Iaconis, Coordinatore di OSSIF, il Centro di Ricerca ABI sulla Sicurezza Anticrimine Dott.ssa Mihaela Gavrila, Università degli Studi "La Sapienza" di Roma, Comunicazione e Ricerca Sociale, Faculty Member Cap. Ludovica Glorioso, Legal Advisor presso NATO Security Force Assistance Dott. Pier Luigi Martusciello, Head of corporate security – BNL Gruppo BNP Paribas Avv. Pietro Mazzei, avvocato cassazionista, Vice Procuratore presso la Procura della Repubblica di Civitavecchia Dott. Francesco Modafferi, Dirigente del Garante per la protezione dati personali Dott. Luigi Mone, già Prefetto Dipartimento Pubblica Sicurezza Dott.ssa Lucia Muscari, Dirigente Polizia di Stato Gen. Nicolò Pollari, Consigliere di Stato, Generale di Corpo d'Armata della Guardia di Finanza in congedo, già Direttore del SISMI Dott. Carlo Parolisi, è stato Capo della Divisione Controspionaggio dell'AISE, e in precedenza Vice-Capo del Centro Operativo del SISDE di Roma dedicato al controterrorismo e alla contro-eversione Dott. Sergio Santoro, Presidente dell'Associazione Nazionale Magistrati della Giustizia Amministrativa		

	Dott. Bruno Valensise, Vice Direttore del DIS (Dipartimento delle Informazioni per la Sicurezza Dott. Nicola Zupo, Dirigente Polizia di Stato Dott.ssa Roberta Monni, Vice-Prefetto
Tirocinio	*Modalità FAD* Il Tirocinio potrà essere svolto in modalità virtuale e/o simulata con i docenti del Master (elaborazione di un project work, analisi e problem solving riguardante filmati e case study consegnati dai docenti, supervisione su casi presentati dagli allievi), elaborati da svolgere.in supervisione con i docenti del master.
Profilo Professionale Requisiti di ammissione	*Profilo Professionale* Lo specialista in Intelligence, Investigation and Security attraverso le conoscenze/competenze acquisite durante il Master, è in grado di affrontare questioni nell'ambito dell'intelligence e della cybersecurity, legate ai crimini informatici, alla violazione della riservatezza e alle moderne indagini con strumenti tecnologicamente molto avanzati, oltreché normative e interpretative legate ai ruoli tecnici e legali. *Requisiti di ammissione* Laurea triennale, Laurea magistrale oppure Laurea specialistica oppure Laurea ante DM 509/1999 (vecchio ordinamento) o altro titolo di studio universitario conseguito all'estero riconosciuto idoneo in base alla normativa vigente.
Attività e adempimenti	Gli insegnamenti nel loro complesso prevedono: – videolezioni sulla piattaforma didattica e in presenza – tirocinio Agli studenti vengono richiesti i seguenti adempimenti: – studio individuale del materiale didattico, prove di verifica e project work – attività di tirocinio – superamento dell'esame finale che si svolgerà in presenza della commissione.
Modalità di iscrizione	Per iscriversi al Master si dovrà seguire la procedura indicata nel sito ufficiale di Ateneo, www.uniroma5.it. L'iscrizione dovrà essere perfezionata entro 1 settimana prima dell'avvio del corso salvo eventuali proroghe. I cittadini non comunitari residenti all'estero potranno presentare la domanda tramite le Rappresentanze diplomatiche italiane competenti per territorio che, a loro volta, provvederanno ad inviarla all'Università Telematica San Raffaele Roma, allegando il titolo di studio straniero corredato di traduzione ufficiale in lingua italiana, legalizzazione e dichiarazione di valore. Oltre alla suddetta documentazione, i cittadini non comunitari residenti all'estero, dovranno presentare all'Università il permesso di soggiorno rilasciato dalla Questura in unica soluzione per il periodo di almeno un anno; i cittadini non comunitari residenti in Italia dovranno presentare il permesso di soggiorno rilasciato per uno dei motivi indicati all'articolo 39, quinto comma, del D.L.vo n. 286 del 25.7.1998 (ossia per lavoro autonomo, lavoro subordinato, per motivi familiari, per asilo politico, per asilo umanitario o per motivi religiosi). Non saranno ammesse iscrizioni con riserva per documentazione incompleta o per errata trascrizione dei dati sul sito dell'Ateneo. Il mancato pagamento delle rate nei termini prestabiliti comporta la sospensione dell'accesso alla piattaforma e la non ammissione all'esame finale.
Durata del corso e modalità di erogazione	Il master ha durata annuale pari a 1500 ore di impegno complessivo per il corsista, corrispondenti a 60 CFU (Crediti Formativi Universitari). L'insegnamento viene erogato sia in presenza sia in modalità e-learning sulla piattaforma didattica 24/24 ore con materiale didattico integrativo e in presenza laddove previsto (Blended) secondo la modalità scelta.

Quote di iscrizione	La quota di iscrizione è di: **Modalità FAD: € 2.600,00 (duemilaseicento/00)** I pagamenti possono essere effettuati secondo le modalità specificate sul sito internet dell'Ateneo, in rate così ripartite: – quota pre-iscrizione: € 100,00 da versare al Consorzio Universitario Humanitas – quota immatricolazione: € 520,00 da versare all'Università San Raffaele – I rata di € 1000,00, entro il entro il 1 mese dall'attivazione del master, da versare al Consorzio Universitario Humanitas – II e ultima rata di € 980,00, entro il entro il 2 mese dall'attivazione del master, da versare al Consorzio Universitario Humanitas Eventuali informazioni potranno essere richieste all'indirizzo e-mail: master@consorziohumanitas.com e al numero telefonico Tel. +39 06 3224818 dal lunedì al venerdì dalle 09:00 alle 19:00 Il mancato pagamento delle rate nei termini prestabiliti comporta la sospensione dell'accesso alla piattaforma e la non ammissione all'esame finale. Il discente potrà esercitare il diritto di recesso entro il termine di 14 giorni lavorativi dalla data di iscrizione, mediante invio, entro i termini sopra indicati, di una raccomandata A.R. all'Università Telematica San Raffaele Roma, via di Val Cannuta 247, 00166 Roma o di una pec all'indirizzo amministrazione@pec.uniroma5.it. In tale ipotesi il relativo rimborso sarà effettuato entro 90 giorni dalla comunicazione, da parte del discente, dell'esercizio del diritto di recesso e sarà trattenuto il 10% del corrispettivo versato a titolo di penale. L'attivazione del master è subordinata al raggiungimento di: Modalità FAD: minimo 30 - a tassa piena e minimo 50 - a tassa in convenzione (scontata) Modalità Blended: minimo 20 - a tassa piena e minimo 30 - a tassa in convenzione (scontata)
Scadenze	Il termine ultimo per la raccolta delle iscrizioni è la settimana prima dell'avvio del corso, salvo eventuali proroghe. Inizio Gennaio 2025 - Fine Marzo 2026 Le iscrizioni ai Master saranno aperte fino al 30 Giugno 2025 La prova d'esame potrebbe essere posticipata per effetto dell'eventuale proroga della data inizio corso.

Roma, 15/07/2024

IL RETTORE
(Prof. Vilberto Stocchi)