

Master universitario I livello

INTELLIGENCE, INVESTIGATION AND SECURITY

Anno Accademico 2025-2026

VI Edizione

Accordi e collaborazioni:



DIRETTORI

Prof. Dott. Nicolò Marcello D'Angelo
Dott. Francesco Di Maio

DIRETTORE ORGANIZZATIVO

Dott. Antonio Attianese

COMITATO SCIENTIFICO

Prof. 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

Il Master in Intelligence e Cyber Security, organizzato dal Consorzio Universitario Humanitas in collaborazione con l'Università San Raffaele, nasce per rispondere alla crescente domanda di professionisti altamente qualificati nella gestione della sicurezza digitale e delle investigazioni tecnologiche.

In un'epoca in cui la criminalità informatica, le violazioni della riservatezza e gli attacchi cibernetici rappresentano minacce sempre più diffuse e sofisticate, diventa fondamentale formare figure capaci di integrare competenze **tecniche, giuridiche e investigative**.

Il percorso formativo fornisce agli studenti:

- **Conoscenze avanzate in intelligence e cyber security**, per la prevenzione e la gestione delle minacce digitali.
- Competenze per analizzare, ricostruire e interpretare eventi criminosi complessi.
- **Capacità di utilizzare strumenti** fondamentali per raccogliere prove digitali valide in sede giudiziaria.
- **Approfondimenti giuridici a livello nazionale e internazionale**, indispensabili per comprendere la normativa in continua evoluzione.

Il Master si rivolge a professionisti che desiderano aggiornarsi o specializzarsi in un settore strategico per la tutela di individui, imprese e istituzioni, offrendo una visione integrata che coniuga **aspetti tecnici, legali e operativi**.

Grazie a questo percorso, i partecipanti potranno sviluppare competenze immediatamente spendibili in ambiti come la sicurezza aziendale, le istituzioni pubbliche, le società di consulenza e tutte le realtà che necessitano di esperti nella difesa da crimini informatici e nella protezione dei dati sensibili.

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, oltretutto normative e interpretative legate ai ruoli tecnici e legali.

Le conoscenze/competenze acquisite potranno essere utilizzate nel mondo del lavoro secondo le prescrizioni e le indicazioni dell'Ordine Professionale di appartenenza e/o della Laurea posseduta.

STRUTTURA E MODALITÀ DI EROGAZIONE

FAD asincrona

- 300 ore (videolezioni, coaching online, project work, tutoring, etc.)
- 200 ore (tirocinio virtuale)
- 900 ore (studio individuale)
- 100 ore (verifiche e tesi finale)

DURATA

Il Master dura un anno ed ha un monte ore di 1500.

TIROCINIO

Modalità FAD asincrona

Il tirocinio sarà svolto a distanza attraverso la realizzazione di project work individuali o di gruppo supervisionati dal corpo docente del Master.

REQUISITI DI AMMISSIONE

Possesso di uno dei seguenti requisiti:

- 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.

TITOLO RILASCIATO E CFU

- Diploma di Master universitario di I livello "*Intelligence, Investigation e Security*";
- 60 CFU.



PROGRAMMA

GIUR-09/A Intelligence: scenari politici-economici-giuridici, globalizzazione, 6 CFU

- 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 (Risk 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.

GIUR-01/A Security (aspetti giuridici/normativi), 6 CFU

- 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 GDPR (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 Sistemasanzionatorio
- 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 analysis
- 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

INFO-01/A Security (aspetti tecnico/tecnologici e data), 6 CFU

- Security management: Definizione,
- Security management: Definizione, Evoluzione storica, Compiti e attività, Organizzazione e Relazioni interne ed esterne della security, Chi e Cosa proteggere: 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

GIUR-13/A Criminalistica e Digital forensics, 6 CFU

- 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.

GIUR-14/A Discipline Legali ed Internazionali – Tutela Dati Personali, 6 CFU

- 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

PSIC-04/B Psicologia, Sociologia e Antropologia Applicate – Gestione Della Comunicazione, 6 CFU

- Antropologia della sicurezza;
- Scenario & Contesto Psicologia etnica;
- Cross-culture Bias ed errori 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

GIUR-09/A Sistemi Globali e Diplomazia, 6 CFU

- Le organizzazioni internazionali impegnate nella sicurezza;
- Sistema NATO;
- Diplomazia, nella teoria e nella pratica;
- Diplomazia parallela;
- Peacekeeping intelligence

COSTO

Modalità FAD asincrona: € 2.700,00

Per info su rateizzazione, modalità di pagamento e agevolazioni consultare il sito www.consorziohumanitas.com

INFORMAZIONI

Consorzio Universitario Humanitas

Telefono: 06 3224818

Università Telematica San Raffaele Roma

Telefono: 800 12 86 06

