



UNIVERSITÀ  
DEGLI STUDI  
DI SALERNO



CONSORZIO  
UNIVERSITARIO  
HUMANITAS

Master universitario I livello

# INTELLIGENCE, INVESTIGATION AND SECURITY

I Edizione

Anno Accademico 2023-2024

II classe

Master validato dal Consiglio Scientifico del Consorzio

Con il patrocinio di:

 **UNINDUSTRIA**  
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE  
ROMA • FROSINONE • LATINA • RIETI • VITERBO

## DIREZIONE

Prof. Francesco Orciuoli  
Avv. Prof. Francesco Di Maio

## COMITATO SCIENTIFICO

Pref. Dott. Nicolò Marcello D'angelo  
Dott. Bruno Valensise  
Prof. Francesco Orciuoli  
Avv. Prof. Francesco Di Maio  
Prof. Angelo Gaeta  
Prof. Aniello Castiglione  
Prof. Domenico Parente  
Avv. Alessandro Bracci  
Dott. Luigi Mone  
Prof. Vincenzo Loia  
Prof. Giuseppe Fenza  
Dott. Giovanni Bonzano

## PRESENTAZIONE

Il Master risponde alla richiesta di professionisti esperti in intelligence, cybersecurity, 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 percorso formativo, mirato a formare la figura professionale di specialista in Intelligence, Investigation and Security, fornisce conoscenze e competenze per affrontare le richieste di settore nell'ambito dell'Intelligence e della Cybersecurity, affrontando tematiche relative a crimini informatici e violazione della riservatezza, con prospettive specifiche nell'ambito giuridico, nazionale ed internazionale, necessarie per l'aggiornamento dei professionisti del settore. In sintesi, uno Specialista in Intelligence, Investigation and Security è responsabile di valutare e mitigare i rischi di sicurezza, raccogliere e analizzare informazioni di intelligence, condurre indagini e implementare misure di sicurezza per proteggere gli asset, le informazioni e il personale di un'organizzazione. Il suo ruolo è fondamentale nel mantenere la sicurezza e l'integrità di un'organizzazione in un mondo sempre più complesso e interconnesso.

## 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.

## MODALITÀ DI SVOLGIMENTO

### FAD (Formazione a distanza)

- Lezioni: 300 ore
- Studio individuale: 550 ore
- Tirocinio: 250 ore
- Verifiche intermedie e prova finale: 400 ore

Il Sistema di Didattica Integrata, garantisce agli allievi la continuità didattica e l'applicazione di metodologie attive per l'insegnamento/apprendimento. Il modello prevede approcci tecno/pedagogici necessari alla produzione di risultati didattici ottimali (cognitivismo, costruttivismo, apprendimento cooperativo, ecc.); impiego di molteplici forme di tecnologie didattiche e web (sincrone asincrone, collaborative, chat, forum, etc.); utilizzo di diverse forme di tutoring. I partecipanti al master fruiranno di materiale didattico costituito dalle lezioni, slide, documenti di approfondimento e articoli scientifici. Il calendario didattico si articolerà secondo lezioni in Formazione a distanza, distance learning, interattive e multimediali, erogate attraverso la Piattaforma eLearning del Consorzio Universitario Humanitas, Scorm compliant.

## 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, preferibilmente in Giurisprudenza, Informatica, Ingegneria, Data Science, Economia, Consulenza e Management Aziendale, Psicologia e altre discipline tecnico/scientifiche.

## DURATA

Il Master avrà una durata di studio di 1500 ore pari a 60 CFU.

## TITOLO RILASCIATO

Diploma di Master universitario di I livello  
*Intelligence, Investigation and Security*

## PROGRAMMA

**IUS/13: Intelligence, globalizzazione e diritto internazionale: scenari giuridici, politici, economici, 6 CFU**

*L'intelligence: definizioni, soggetti e contesto normativo nazionale, europeo e globale (il regime giuridico applicabile a informatori, spie, leakers e whistleblowers);*

*Le nuove minacce per la sicurezza comune nell'era della globalizzazione: il ruolo dell'intelligence nel contrasto ai crimini transnazionali;*



L'intelligence per la prevenzione e il contrasto di terrorismo, estremismo violento e radicalizzazione;

Criminalità transnazionale, intelligence e sicurezza nelle situazioni di emergenza globale (pandemie, disastri ambientali e conflitti armati);

Intelligence e sicurezza della comunicazione nel cyberspace: social media, persuasione, fake news;

Investigation, intelligence e nuove tecnologie nell'era della globalizzazione;

Intelligence economico-finanziaria e ruolo delle imprese per la tutela della sicurezza nazionale e delle relazioni internazionali;

Intelligence e diritti umani: il ruolo della giustizia penale nel bilanciamento tra sicurezza e garanzie individuali (libertà di espressione, privacy e data protection);

Cooperazione giudiziaria e digitalizzazione della giustizia penale per la sicurezza comune;

Intelligence, interessi nazionali e cross-border security (nei campi energetici, ambientali, sanitari, finanziari, chimici, dei trasporti e delle telecomunicazioni).

## IUS/01, Security (aspetti giuridici/normativi), 8 CFU

Tecnologie digitali e sistema ordinamentale. Complessità e dinamicità dell'ordinamento: sistema delle fonti del diritto 'multilivello'. Evoluzione del modello istituzionale: dallo Stato 'legislatore' allo Stato 'regolatore'. Soft law. Diritto giurisprudenziale e prassi. Principio di sussidiarietà e ruolo dell'autonomia privata: autodisciplina e autoregolazione. Fondamento assiologico unitario del sistema ordinamentale e superamento della distinzione 'interesse pubblico-interesse privato'. Paradigma privatistico e rapporto cittadino-amministrazione. Codice dell'Amministrazione Digitale. Interrelazione tra 'Penale' e 'Civile': causalità e colpa nella Società del Rischio. Big data, IA e nuovi rischi. Approccio proattivo della regola dell'accountability. Lex informatica tra "regolazione decentralizzata" e "costituzione civile". Regola algoritmica quale esplicitazione del potere di autonomia e limite di ordine pubblico della dignità umana.

Riservatezza e Sicurezza informatica nel quadro dei diritti di libertà e delle libertà economiche. Principi costituzionali e sovranazionali in materia di riservatezza. Riservatezza della persona e riservatezza dei dati come concetti speculari alla sicurezza. Dall'habeas corpus all'habeas data. L'habeas mentem come nuovo fulcro della libertà individuale e dei diritti connessi alla persona: i c.dd. neurodiritti. Cybersecurity come precondizione per esercitare i diritti di libertà (associazione, espressione ecc.). Sovranità digitale tra privacy e sicurezza.

Data governance. Principi generali sul GDPR (reg. UE 679/2016) e d.lgs. n. 101/2018 di modifica. Protezione dei dati personali: consenso al trattamento e controllo sulla circolazione dei propri dati. Concetto di 'dato personale'. I c.dd.

'dati sensibili'. Portabilità dei dati. Le figure del GDPR: responsabile del trattamento e DPO. Autoregolazione (Codicidi condotta, meccanismi di certificazione) e correttezza del trattamento. Informativa sul trattamento dei dati personali. Atti di nomina degli autorizzati. Contratti con i responsabili del trattamento ex art. 28, GDPR. Registro delle attività di trattamento. Policy sul trattamento dei dati personali. Valutazione di impatto (DPIA).

Security e social media. Identità Digitale, luoghi 'digitali' della persona (domicilio digitale), reputazione, diritto all'oblio, digital death. Phishing. Profilazione. Disinformazione. Social media e sicurezza del minore: la l. n. 71 del 2017 sul 'cyberbullismo'.

Cybersecurity del consumatore digitale. Ruolo del Notariato.

Gli obblighi di sicurezza a carico degli operatori economici. Dalla direttiva 'NIS' alla direttiva 'NIS 2'. Strategia cyber dell'UE. La dir. 'NIS 2' nella strategia nazionale di cyber security. Standard e Best practice. Servizi essenziali e critici. Soggetti essenziali e soggetti importanti. Normative settoriali specifiche: la resilienza operativa digitale per il settore finanziario (DORA) e la Direttiva sulla resilienza delle entità critiche (CER). Dalla sicurezza cyber alla resilienza. Rischi della supply chain compliance della catena di fornitura. Incident response.

Aspetti specifici. Tutela del know-how e del segreto industriale.

## INF/01 Security (aspetti tecnico/tecnologici e data), 8 CFU

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): Rischinelle 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 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.

### IUS/16 Criminalistica e Digital forensics, 8 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.

### IUS/17 Discipline Legali ed Internazionali – Tutela Dati Personali, 8 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.

### M-PSI/08, Psicologia strategica applicata, 6 CFU3

Approccio psicologico-strategico e agentività; Fondamenti neuro-psico-fisiologici del comportamento; Cross-cultural and socio-cognitive bias;

Psicologia strategica dello scenario e del contesto;

Previsione del comportamento e decision making nei contesti di emergenza e sicurezza;

Analisi e conduzione strategica delle dinamiche di gruppo;

Gestione e superamento della frustrazione e dello stress;

Prevenzione del burn-out promozione del benessere organizzativo;

Comunicazione efficace strategica; Strategie di leadership situata; Gestione dei conflitti, negoziazione e problemsolving.

### IUS/13 Organizzazioni e sistemi internazionali e ruolo della diplomazia, 6 CFU

Le organizzazioni internazionali impegnate nella sicurezza: International security e Human security; l'Organizzazione delle Nazioni Unite; le organizzazioni regionali;

Il sistema NATO: il nuovo Concetto strategico della NATO (2022); l'art. 5 del Trattato NATO nella più recente interpretazione;

La governance degli ecosistemi digitali, cybersicurezza e resilienza: cybersicurezza e protezione delle infrastrutture critiche; il quadro giuridico dell'Unione europea in materia di cybersicurezza (direttiva NIS2; direttiva CER; EU Cyber diplomacy toolbox); lo spazio quale nuova frontiera della sicurezza (tecnologie satellitari e cyber);

Diplomazia, nella teoria e nella pratica: evoluzione e connotazioni attuali delle relazioni diplomatiche (digital e soft diplomacy); il concetto di diplomazia parallela;

Peacekeeping and intelligence: Il peacekeeping nel sistema delle Nazioni Unite; Informazioni e spionaggio nel diritto internazionale; Le frontiere dell'intelligenza artificiale nei servizi di intelligence.

### COSTO

€ 2.500,00

Per info su rateizzazione, modalità di pagamento e iscrizioni consultare il sito [www.consorziohumanitas.com](http://www.consorziohumanitas.com)

### INFORMAZIONI

Consorzio Universitario Humanitas

Via della Conciliazione, 22

00166 Roma RM

Telefono: 06 3224818

Mail: [master@consorziohumanitas.com](mailto:master@consorziohumanitas.com)

Web: [www.consorziohumanitas.com](http://www.consorziohumanitas.com)



Il Consorzio Universitario Humanitas, ha tra i suoi associati l'Università degli Studi di Salerno, l'Università Cattolica del Sacro Cuore, l'Università Telematica San Raffaele Roma, la Pontificia Facoltà Teologica dell'Italia Meridionale – Sez. S. Luigi – Napoli, LUM – Libera Università Mediterranea “Giuseppe Degennaro”, Bari, l'Ospedale Pediatrico Bambino Gesù, l'IDI – Istituto Dermopatico dell'Immacolata, l'Istituto Universalus, il Consorzio Fortune, il C.I.R.P.S. – Centro Interuniversitario di Ricerca Per lo Sviluppo sostenibile, la Fondazione “Sapientia Mundi”, l'I.I.S.C.P.F. – Istituto Internazionale di Scienze Criminologiche e Psicopatologico Forensi.

Da oltre un decennio, svolge attività di ricerca scientifica e Alta Formazione a forte impatto professionalizzante, ha organizzato numerosi Master Universitari, Corsi di alta formazione e ha attivato Scuole di Specializzazione in Psicoterapia, diventando un centro di eccellenza e di riferimento nazionale, con diverse centinaia di studenti.

Il Consorzio è Provider accreditato all'Agenas per la formazione dei medici e delle professioni sanitarie ed è accreditato sulla piattaforma SOFIA per la formazione di docenti e dirigenti scolastici di ogni ordine e grado.

Il Consorzio ha una Casa editrice “Humanitas Edizioni” che realizza pubblicazioni editoriali anche in collaborazione con importanti case editrici come Franco Angeli e Armando editore.

**Direttore didattico:** Dott.ssa Carla Pampaloni

#### Partner e Associati



UNIVERSITÀ  
DEGLI STUDI  
DI SALERNO



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore



Università  
San Raffaele  
Roma



UNIVERSITÀ  
LUM  
GIUSEPPE  
DEGENNARO



Pontificia Facoltà Teologica  
dell'Italia Meridionale



OSPEDALE PEDIATRICO  
Bambino Gesù



ISTITUTO  
DERMOPATICO  
DELL'IMMACOLATA



LILT  
LEGA ITALIANA PER LA LOTTA CONTRO I TUMORI  
prevenire e vivere



ISTITUTO  
UNIVERSALUS



CONSORZIO  
FORTUNE



ISTITUTO  
CLINICO  
INTERUNIVERSITARIO



UNIVERSALUS  
CONSORZIO UNIVERSITARIO