

A.A. 2026/2027

# MaSCAI Cybersecurity e Compliance Aziendale Integrata.

Master di II livello.

60 CFU

Ottobre 2026 – Ottobre 2027



**Università  
di Brescia**

SMAE · School of Management  
and Advanced Education



### Informazioni e candidature

Visitare la pagina ufficiale del master

Per informazioni amministrative o problemi tecnici  
relativi all'iscrizione on line:

segreteria.smae@unibs.it

030 2988835 - 2988761

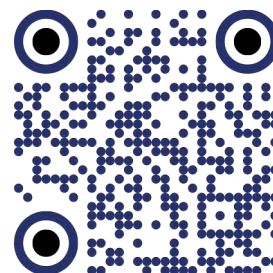


### Nodo di Brescia del CINI National Cybersecurity Lab

<https://cyberseclab.unibs.it/>

Per informazioni relative all'attività didattica:

master-cybersecurity@unibs.it



### Collaborazioni

Il master vede la collaborazione di soggetti che hanno manifestato il proprio interesse per il progetto formativo:

A2A

Camera Civile di Brescia

Camera di Commercio di Brescia

Cavagna Group / Parteca S.p.A.

CINI Cybersecurity National Lab

CLUSIT - Associazione Italiana per la  
Sicurezza Informatica

Confindustria Brescia

Errecom S.p.A.

Feralpi Group

Nemesi Italia S.r.l.

ONIF - Osservatorio Nazionale per  
l'Informatica Forense

Ordine Avvocati della Provincia di Brescia

Ordine Ingegneri della Provincia di Brescia

PersonalData

Verxo S.r.l.

# Sintesi

Un Master universitario di II livello per integrare cybersecurity, compliance, governance e gestione del rischio

MaSCAI fornisce un titolo riconosciuto dal sistema universitario italiano e amplia l'accesso alla cultura della cybersecurity a professionisti di diversa formazione, promuovendo una visione trasversale della sicurezza.

Forma figure intermedie capaci di integrare competenze tecniche e di compliance, traducendo i requisiti normativi in soluzioni operative.

## Ambiti Professionali

Cybersecurity e compliance management

Sicurezza delle informazioni e governance IT

Supporto a CISO, SOC e system integration

Risk management, compliance e audit interno

Adeguamento normativo

Gestione integrata dei rischi tecnologici e organizzativi





# I tre pilastri

## **01 · Accesso multidisciplinare**

Il MaSCAI è aperto a laureati di diversa formazione e affronta la cybersecurity come ambito trasversale, integrando diritto, gestione dei sistemi informativi, programmazione, intelligenza artificiale e LLMs. Sono previsti laboratori pratici e l'adozione di framework raccomandati a livello nazionale e internazionale.

## **02 · Profilo integrato tecnico-compliance**

Il MaSCAI forma professionisti capaci di collegare aspetti tecnologici, normativi e organizzativi. Vi è ampio spazio a lezioni dedicate a governance, rischio, privacy e sicurezza della supply chain, così come a tematiche tecniche come attacchi, difese e sicurezza di sistemi, software e infrastrutture.

## **03 · Innovazione digitale e applicazione pratica**

Il MaSCAI si concentra su minacce attuali e tecnologie emergenti, con particolare attenzione all'intelligenza artificiale generativa, alle attività di laboratorio, e alle attività di tirocinio e tesi.

# Organizzazione

**1 anno**

**1500 ore**

## Ripartizione delle ore

|         |                     |
|---------|---------------------|
| 300 ore | Lezioni frontali    |
| 875 ore | Studio individuale  |
| 250 ore | Tirocinio formativo |
| 75 ore  | Preparazione tesi   |

Il tirocinio comprende attività preparatorie, tra cui analisi di standard, framework e normative tecniche.

## Calendario e modalità

|             |   |
|-------------|---|
| Periodo     | Ottobre 26 — Ottobre 27                           |
| Lezioni     | Venerdì pomeriggio<br>Sabato mattina e pomeriggio |
| Sospensione | Gennaio e prima metà di Febbraio                  |
| Modalità    | In presenza e online sincrona                     |

# Programma didattico

|   |                 |   |
|---|-----------------|---|
| <b>Elementi di Ingegneria dell'Informazione</b>           | 60 ore frontali | Fondamenti di sistemi digitali (calcolatori, reti, basi di dati) e sviluppo software, con introduzione all'AI e ai relativi rischi, per comprendere architetture, flussi informativi e impatti organizzativi. |
| <b>Diritto della Sicurezza</b>                            | 72 ore frontali | Quadro giuridico e normativo integrato per analizzare responsabilità, compliance e impatti legali della sicurezza informatica, con casi applicativi e riflessione etica.                                      |
| <b>Sicurezza delle Reti</b>                               | 48 ore frontali | Progettazione e valutazione della sicurezza di infrastrutture di rete, con crittografia, autenticazione e monitoraggio, supportate da laboratori.   |
| <b>Sicurezza dei Sistemi di Elaborazione Tradizionali</b> | 84 ore frontali | Protezione dei sistemi informativi, gestione degli incidenti, digital forensics e threat intelligence, con focus su attacchi, malware, e contesti IT/OT.  |
| <b>Sicurezza dei Sistemi di Intelligenza Artificiale</b>  | 36 ore frontali | Analisi dei rischi e delle vulnerabilità dei sistemi AI, modelli di governance e mitigazione, con laboratori e studio di casi reali.  |



# Elementi di ingegneria dell'informazione

SSD: IINF-05/A

Ore: 60

## Descrizione:

Fondamenti di sistemi digitali (calcolatori, reti, basi di dati) e sviluppo software, con introduzione all'intelligenza artificiale e ai relativi rischi, per comprendere architetture, flussi informativi e impatti organizzativi.

## Argomenti trattati

Architettura dei calcolatori, sistemi operativi

Basi di dati e sistemi informativi

Reti di telecomunicazione

Programmazione, sviluppo web, e interazione mobile

Sistemi industriali

Fondamenti di intelligenza artificiale (AI) e sistemi conversazionali

Agentic AI



# Diritto della sicurezza

**SSD:** GIUR-11/A

**Ore:** 72

## **Descrizione:**

Quadro giuridico e normativo integrato per analizzare responsabilità, compliance e impatti legali della sicurezza informatica, con casi applicativi e riflessione etica.

## **Argomenti trattati**

Fondamenti di diritto europeo, comparato e internazionale

Fondamenti di diritto pubblico, privato, penale, commerciale e del lavoro

Normativa in materia di cyberspazio, cybersicurezza, intelligenza artificiale

Sistemi di compliance e catene del valore

Responsabilità e governance dei sistemi tecnologici

Criminologia e profili investigativi

Analisi dei rischi legali e reputazionali



# Sicurezza delle reti

SSD: IINF-03/A

Ore: 48

## Descrizione:

Progettazione e valutazione della sicurezza di infrastrutture di rete, con crittografia, autenticazione e monitoraggio, supportate da laboratori.

## Argomenti trattati

Sicurezza delle reti e segmentazione

Controllo accessi, autenticazione e identità digitali

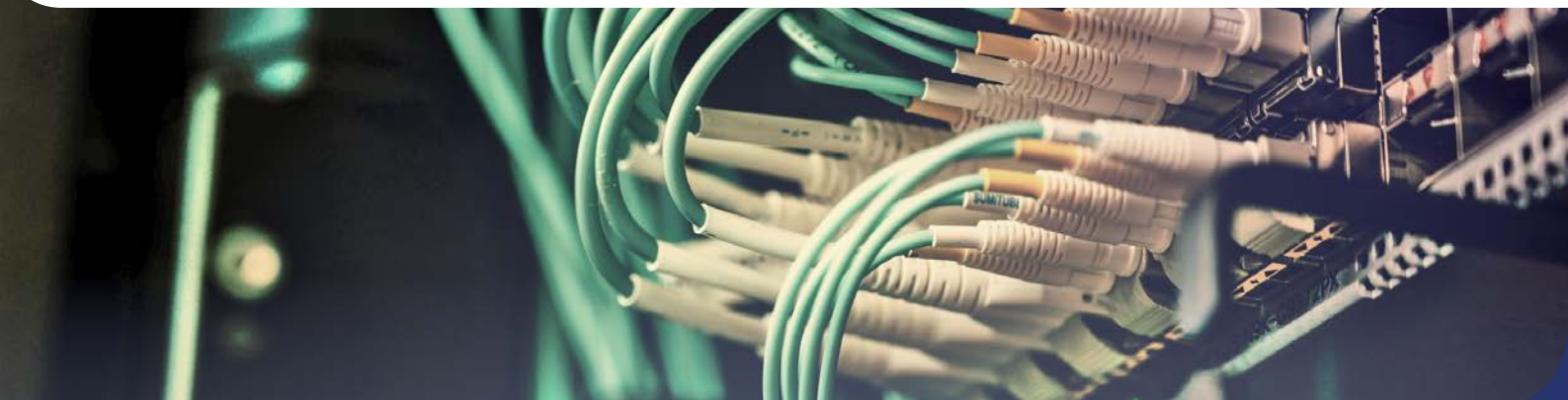
Crittografia e sicurezza delle comunicazioni

Monitoraggio del traffico e difesa operativa

Laboratori su piattaforme di sicurezza

Principi di penetration testing e analisi delle vulnerabilità

Principali minacce nelle reti moderne



# Sicurezza dei sistemi di elaborazione tradizionali

SSD: IINF-05/A

Ore: 84

## Descrizione:

Protezione dei sistemi informativi, gestione degli incidenti, digital forensics e threat intelligence, con focus su attacchi, malware e contesti IT/OT.

## Argomenti trattati

Strategie di cybersecurity

Tecniche di attacco, malware e compromissione

Gestione degli incidenti informatici

Digital forensics e analisi delle evidenze

Compliance e modelli organizzativi

Convergenza IT/OT

Intelligence analysis e cyber threat intelligence

# Sicurezza dei sistemi di intelligenza artificiale

SSD: IINF-05/A

Ore: 36

## Descrizione:

Analisi dei rischi e delle vulnerabilità dei sistemi di intelligenza artificiale, modelli di governance e mitigazione, con laboratori e studio di casi reali.

## Argomenti trattati

AI nella cybersecurity

Rischi dei sistemi di AI predittiva

Rischi dei sistemi di AI generativa

Rischi dei sistemi agentici

Mitigazione e modelli di governance

Conoscenza operativa aziendale e strumenti di AI



# Consiglio direttivo



**Prof. Federico Cerutti**, Direttore del Master.  
Direttore del nodo di Brescia del CINI National Cybersecurity Lab.  
AI, incertezza e cyber-threat intelligence.



**Dott. Antonio Fiorentino**  
Ispettore della Sezione Distrettuale Operativa Sicurezza Cibernetica di  
Brescia, Polizia Postale.



**Prof. Matteo Frau**  
Sicurezza nazionale, guerra cibernetica e regolazione delle tecnologie.



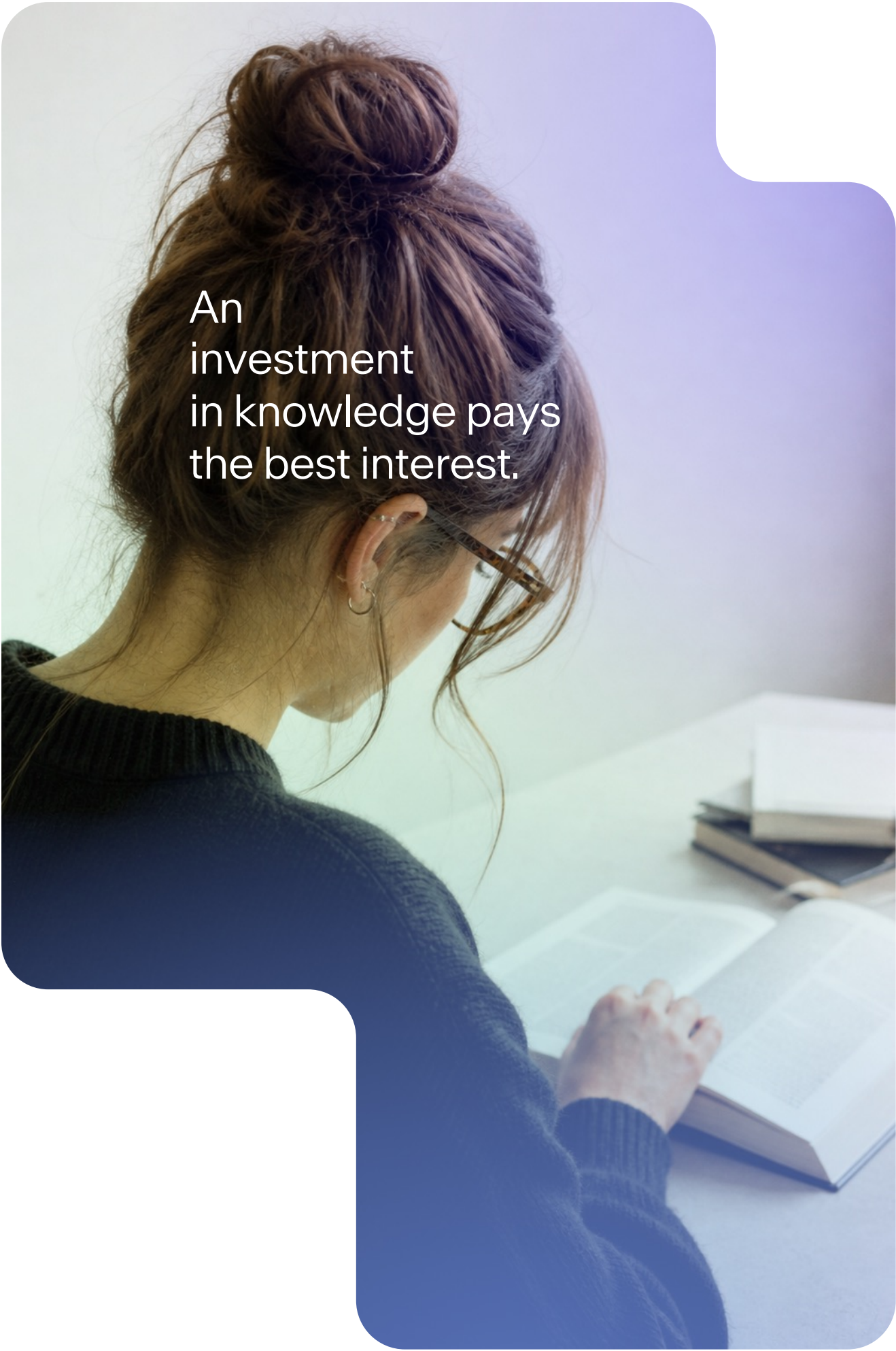
**Prof. Francesco Gringoli**  
Sicurezza e prestazioni delle reti wireless, packet processing e analisi del  
traffico.



**Prof. Giorgio Pedrazzi**  
Privacy, protezione dei dati e trasformazione digitale.



**Prof.ssa Francesca Romanin Jacur**  
Diritto internazionale, transizione energetica e tutela dei diritti  
fondamentali.

A photograph of a woman with her hair in a bun, wearing glasses and a dark sweater, sitting at a desk and reading a book. The image has a purple-to-blue gradient overlay. The text is centered over the woman's head and shoulders.

An  
investment  
in knowledge pays  
the best interest.