Università di Brescia

A.A. 2026/2027

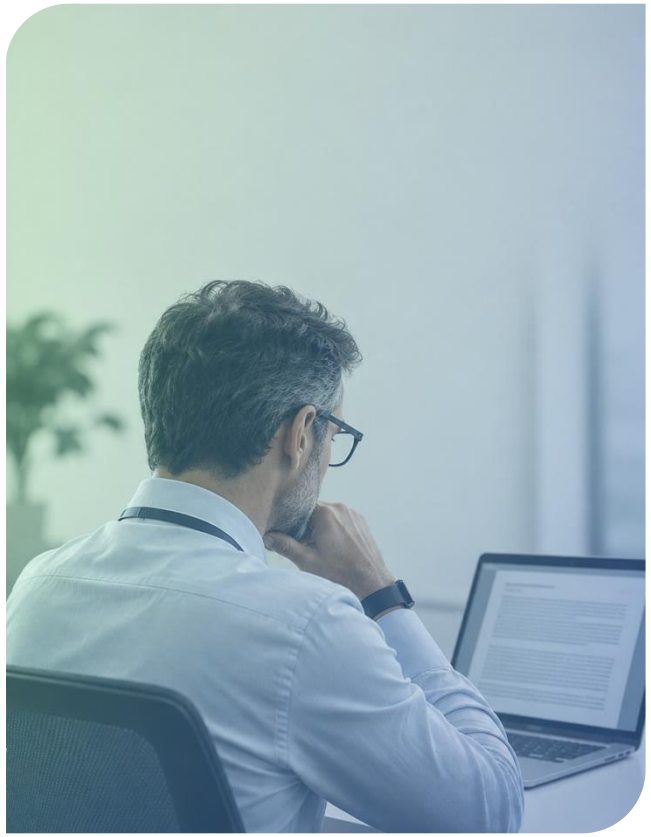
MaSCAI Cybersecurity e Compliance Aziendale Integrata.

Master *Executive* Universitario di II livello

60 CFU

Marzo 2027 – Marzo 2028

Executive summary



Cybersecurity e compliance oltre gli aspetti strettamente tecnologici

MaSCAI affronta la sicurezza informatica attraverso insegnamenti di carattere tecnologico, giuridico e organizzativo.

Per chi opera nei servizi ICT, l'impostazione multidisciplinare offre l'opportunità di approfondire, accanto agli aspetti tecnici, le implicazioni normative e organizzative della cybersecurity, temi che assumono rilevanza anche nelle relazioni tra fornitori tecnologici e organizzazioni clienti.

Ambiti di interesse

- Sicurezza delle reti e dei sistemi
- Gestione degli incidenti informatici
- Analisi delle minacce e delle vulnerabilità
- Diritto della sicurezza e compliance
- Governance e gestione dei rischi
- Sicurezza dei sistemi di intelligenza artificiale

Tecnologia, responsabilità e cybersecurity

Una prospettiva che affianca competenze tecniche, giuridiche e organizzative

Sicurezza delle reti

Segmentazione, autenticazione, crittografia, monitoraggio e principi di analisi delle vulnerabilità.

Sicurezza dei sistemi

Tecniche di attacco, malware, gestione degli incidenti, digital forensics e threat intelligence.

Diritto e compliance

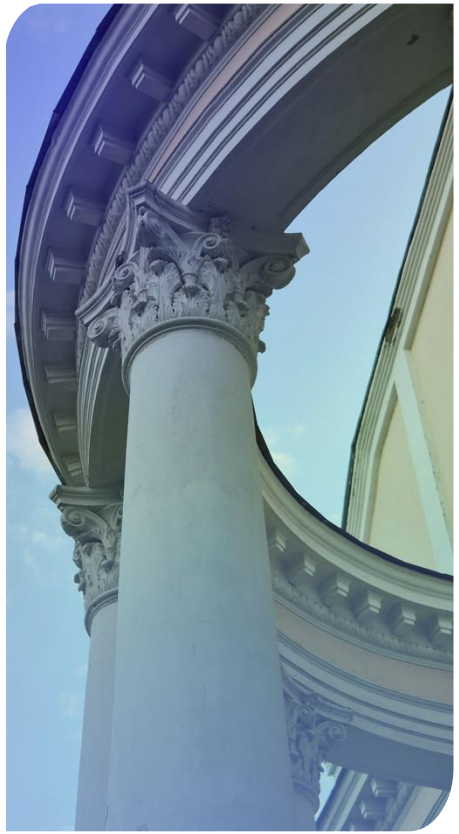
Normativa in materia di cybersecurity, governance dei sistemi tecnologici, compliance e catene del valore.

Sicurezza dell'AI

Rischi dei sistemi generativi e agentici, impiego dell'AI nella cybersecurity e modelli di governance.



I tre pilastri



01 · Formazione multidisciplinare

MaSCAI è aperto a laureati di diversa formazione e offre una preparazione che integra fondamenti di informatica, reti, sistemi informativi, diritto e intelligenza artificiale. Il percorso consente anche a professionisti non tecnici di acquisire gli strumenti necessari per comprendere le principali problematiche.

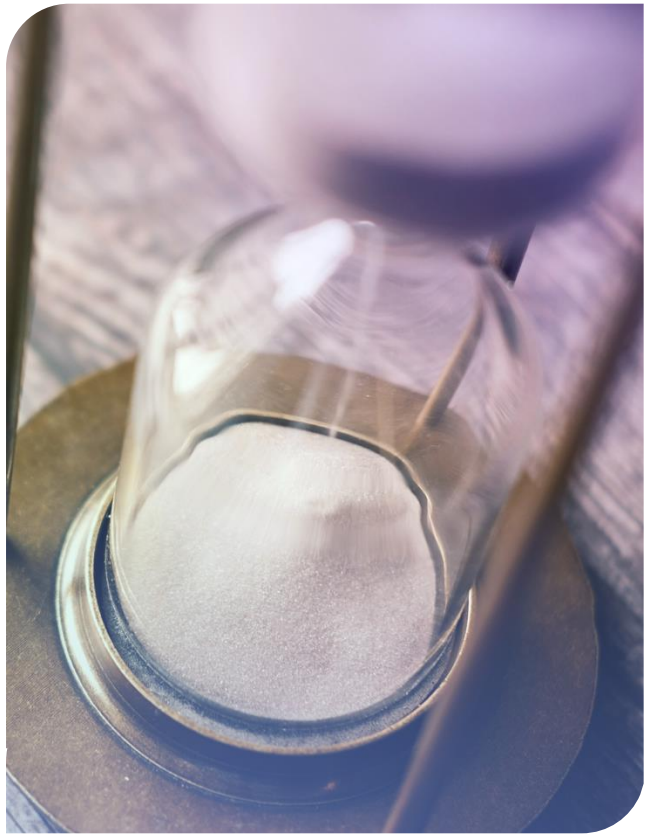
02 · Cybersecurity e compliance

Il Master affronta gli aspetti tecnologici, normativi e organizzativi della sicurezza, collegando la protezione dei sistemi informativi alla gestione del rischio, alle responsabilità giuridiche e ai processi aziendali. L'obiettivo è favorire il dialogo tra funzioni tecniche, legali e gestionali.

03 · Tecnologie emergenti e applicazione pratica

Il percorso approfondisce le minacce informatiche e la sicurezza delle tecnologie emergenti, con particolare attenzione all'intelligenza artificiale generativa e ai sistemi agentici. Laboratori, tirocinio e tesi permettono di applicare le conoscenze acquisite a problemi concreti.

Organizzazione



1 anno – 60 CFU – 1.500 ore complessive

Ripartizione delle ore

300 ore: Didattica
875 ore: Studio individuale
250 ore: Tirocinio formativo
75 ore: Preparazione tesi

Il tirocinio formativo comprende anche attività preparatorie e di approfondimento, tra cui l'analisi di standard, framework e requisiti normativi applicabili alla sicurezza informatica.

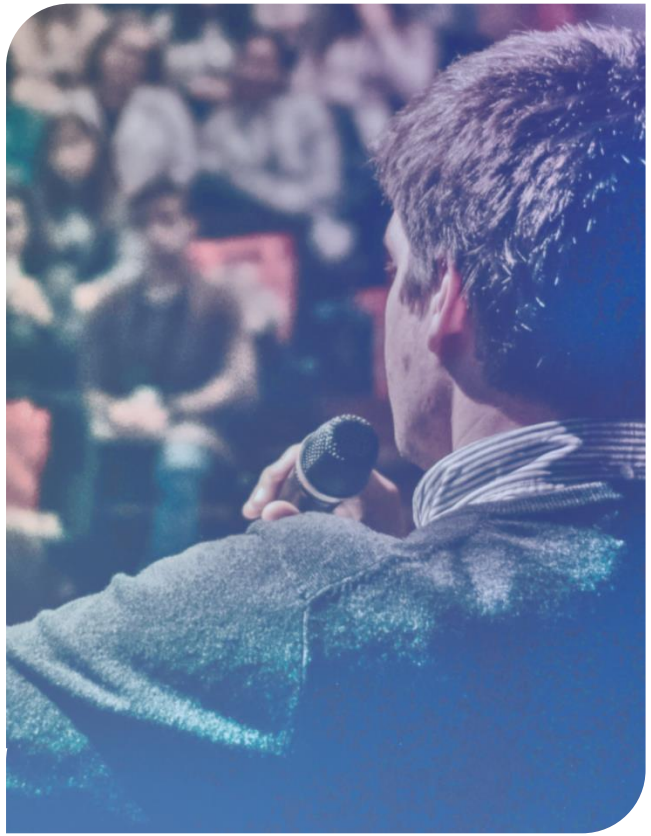
Calendario e modalità

Periodo
Marzo 27 — Marzo 28

Lezioni
Venerdì pomeriggio
Sabato mattina e pomeriggio

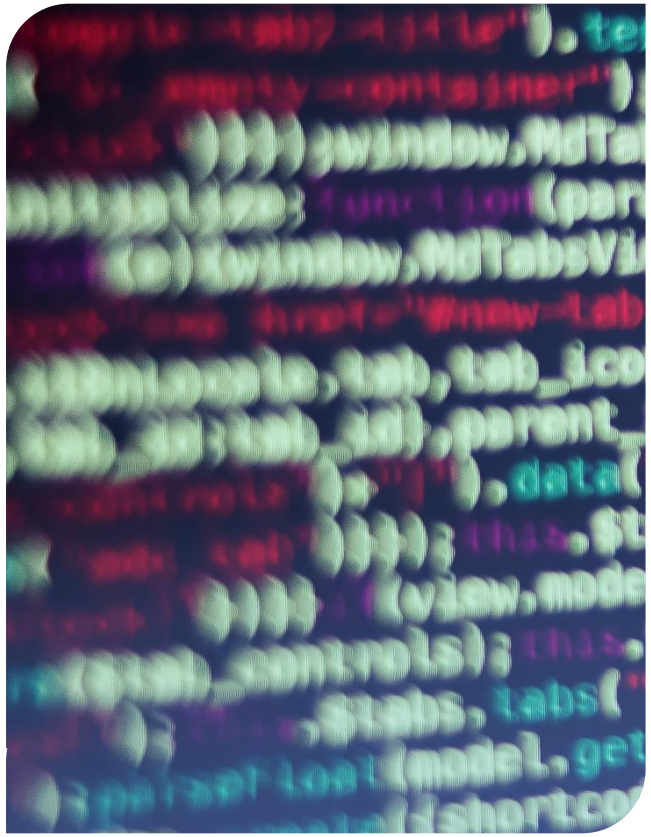
Modalità ibrida: in presenza oppure online in diretta

Programma didattico



Elementi di Ingegneria dell'Informazione	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.
Diritto della Sicurezza	72 ore frontali	Quadro giuridico e normativo integrato per analizzare responsabilità, compliance e impatti legali della sicurezza informatica, con casi applicativi e riflessione etica.
Sicurezza delle Reti	48 ore frontali	Progettazione e valutazione della sicurezza di infrastrutture di rete, con crittografia, autenticazione e monitoraggio, supportate da laboratori.
Sicurezza dei Sistemi di Elaborazione Tradizionali	84 ore frontali	Protezione dei sistemi informativi, gestione degli incidenti, digital forensics e threat intelligence, con focus su attacchi, malware, e contesti IT/OT.
Sicurezza dei Sistemi di Intelligenza Artificiale	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



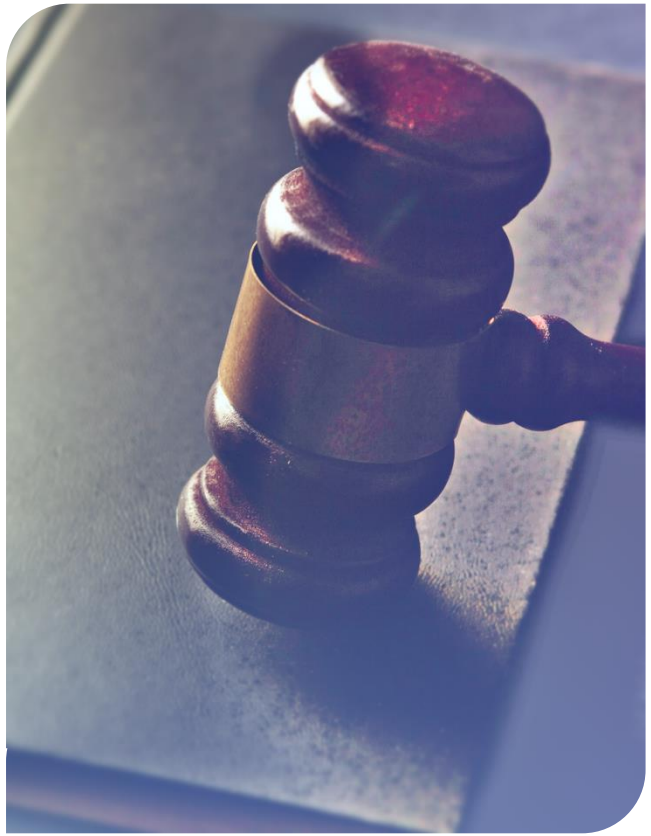
SSD: IINF-05/A
Ore: 60

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



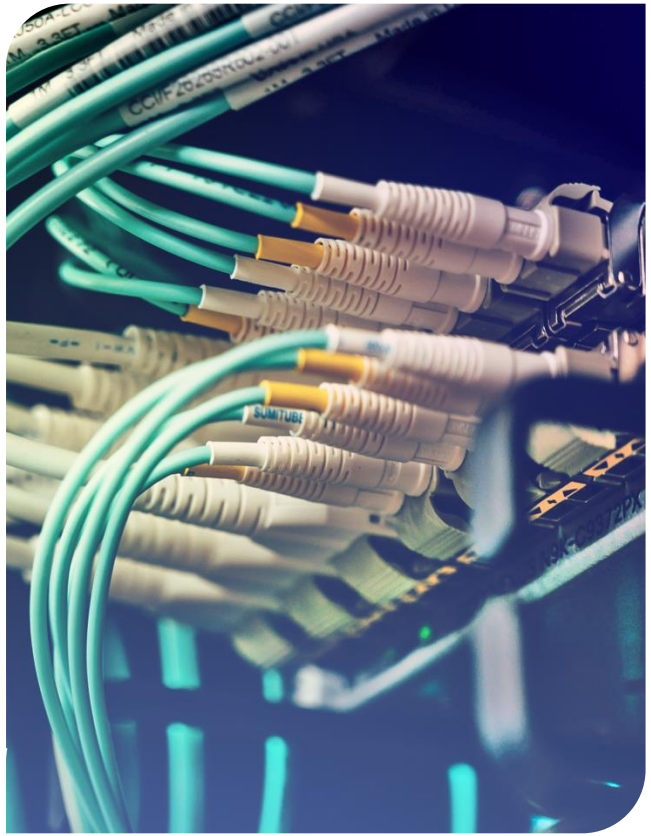
SSD: GIUR-11/A
Ore: 72

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

Sicurezza delle reti



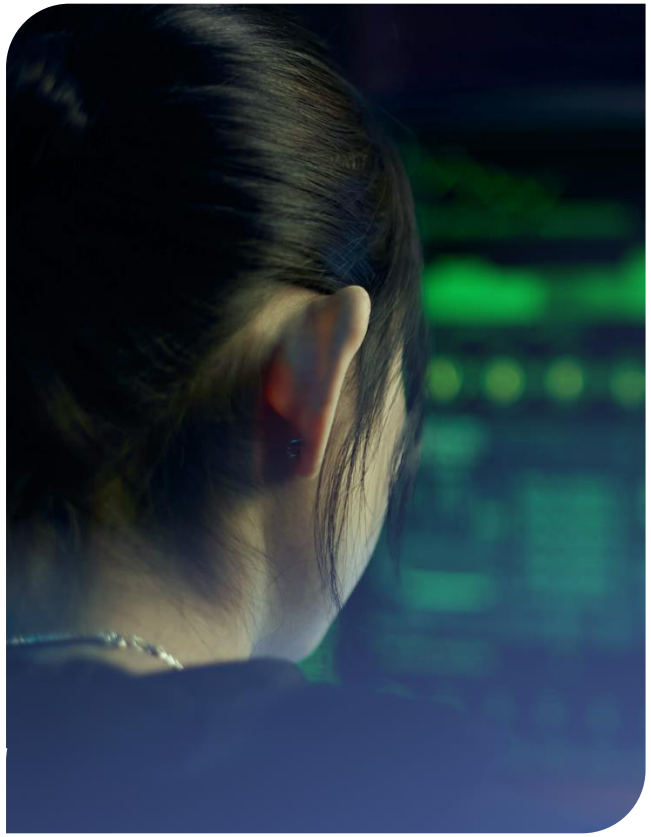
SSD: IINF-03/A
Ore: 48

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



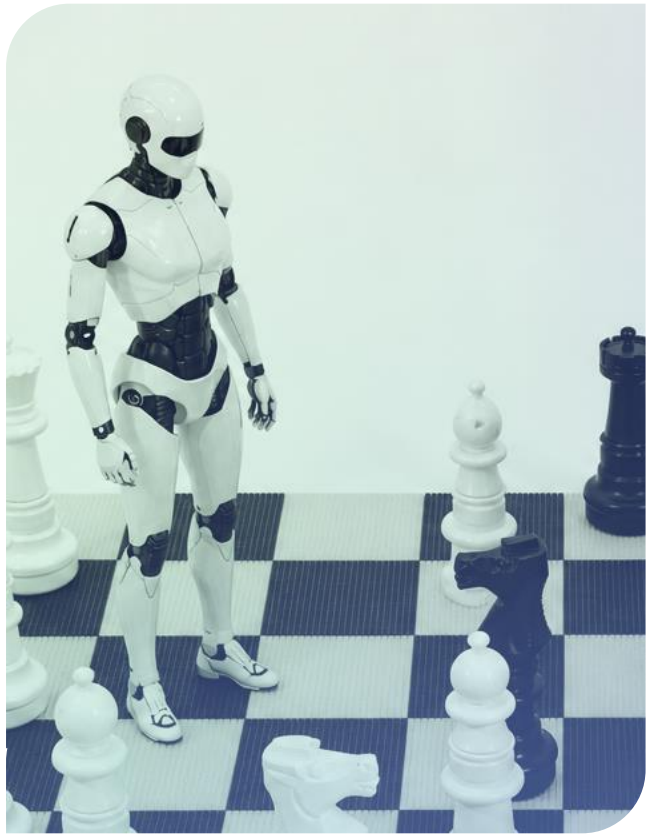
SSD: IINF-05/A
Ore: 84

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.



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



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



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



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



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

Informazioni e candidature

https://corsi.unibs.it/it/mascai26

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 progetto formativo ha raccolto l'interesse di organizzazioni e realtà professionali attive in diversi settori, tra cui industria, servizi ICT, cybersecurity e professioni giuridiche.

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.



MaSCAI
Cybersecurity e Compliance Aziendale Integrata

Master universitario executive di II livello

Marzo 2027 – Marzo 2028

Informazioni e candidature
https://corsi.unibs.it/it/mascai26
master-cybersecurity@unibs.it