UCBM ACADEMY

Master di I livello in Cybersecurity Management

III Edizione

Blended Edition: 50% delle lezioni fruibili in presenza, 50% delle lezioni fruibili in diretta streaming

Direzione Scientifica

Prof. Roberto Setola
Professore Ordinario
Facoltà di Ingegneria
Università Campus Bio-Medico di Roma

Comitato Scientifico

Dott. Giovanni Amato
Agenzia per l'Italia Digitale

Ing. Luigi Ballarano
Chief Information Security Officer Terna

Dott. Massimo Cottafavi
Director of Cyber Security & Resilience Snam

Dott.ssa Nicla Ivana Diomede
Direttore Dipartimento Cybersecurity
e Sicurezza Urbana Roma Capitale

Dott. Riccardo Fragomeni
Direttore IT Ospedale Israelitico
Coordinatore Osservatorio Cybersicurezza Sanità
Fondazione ICSA

Dott. Ivano Gabrielli
Direttore Servizio Polizia Postale e delle Comunicazioni

Ing. Corrado Giustozzi
Esperto Cyber Security strategist

Col. Vincenzo Ingrosso
Capo Ufficio Sviluppo Tecnologico
Arma dei Carabinieri

Avv. Alessandro Lazari
Fellow Centre for Interdisciplinary Research on Security and
Resilience of Critical Infrastructures
Università del Salento

Dott. Mirko Leanza
CISO e Direttore della Business Unit
Cybersecurity & Governance Teleconsys

Dott. Alessandro Luzzi
Responsabile per l'Infrastruttura,
la connettività e la cybersecurity
Ministero dell'istruzione e del merito

Dott. Matteo Macina
Direttore Cyber Security
Gruppo Telecom Italia

Ing. Rocco Mammoliti
Responsabile Sicurezza Informatica
Poste Italiane

Coordinamento Scientifico

Ing. Luca Faramondi
Ricercatore
Facoltà di Ingegneria
Università Campus Bio-Medico di Roma

Gen. B. Antonio Mancazzo
Comandante del Nucleo Speciale Tutela Privacy
e Frodi Tecnologiche, Guardia di Finanza

Dott. Alessandro Marzi
CISO – Head of Cyber Defence
Gruppo A2A

C.V. (CP) Massimiliano Mezzani
Comando generale del Corpo delle Capitanerie di porto

Ing. Francesco Morelli
Responsabile Cyber & Information Security
Gruppo Ferrovie dello Stato Italiane

Ing. Yuri Rassega
CISO, ENEL Group
Presidente Associso

Ing. Massimo Ravenna
Head of Cyber Security Acea

Dott.ssa Annita Larissa Sciacovelli
Advisory Group ENISA e Ricercatrice
Università degli Studi di Bari

Dott.ssa Maria Siclari
Direttore Generale
ISPRA - Istituto Superiore per la Protezione
e la Ricerca Ambientale

Dott.ssa Eva Spina
Dirigente Generale del Dipartimento per il digitale,
la connettività e le nuove tecnologie
Ministero delle Imprese e del Made in Italy

Ing. Marco Venditti
CIO Fondazione Policlinico Universitario
Campus Bio-Medico

Dott. Valerio Visconti
CISO Autostrade per l'Italia

Prof. Luca Vollero
Professore Associato Facoltà di Ingegneria
Università Campus Bio-Medico di Roma

Ing. Gianpaolo Zambonini
Servizio per la Sicurezza Cibernetica del Ministero dell'Interno

Cos'è un Master in Cybersecurity Management?

Il Master di I livello in Cybersecurity Management è un corso di formazione avanzata che risponde alla necessità di protezione delle strutture informatiche di aziende, enti e pubbliche amministrazioni.

L'obiettivo principale del Master è **formare sia profili tecnici che manageriali nel campo della cybersecurity** in accordo con le figure previste dall'European Cybersecurity Skills Framework dell'Agenzia Europea ENISA. Il programma offre **competenze di base** per affrontare le sfide moderne della sicurezza informatica **e approfondimenti per aggiornarsi sulle ultime tecnologie e tendenze**, ampliando e consolidando le proprie conoscenze.

Perché un Master in Cybersecurity Management?

Ogni efficace strategia di cybersecurity impone di integrare le competenze tecnologiche in senso stretto con conoscenze gestionali, giuridiche ed organizzative, al fine di poter contrastare le diverse minacce alla luce dell'importanza del fattore umano in ogni efficace strategia di cyber security. Per poter operare in questo settore è però necessario acquisire solide conoscenze e competenze, indispensabili per poter operare in un dominio fortemente caratterizzato da tecnologie eterogenee. A tal fine il master fornisce le competenze tecniche per individuare, comprendere e mitigare minacce informatiche. Inoltre saranno illustrate le basi necessarie per impostare politiche di prevenzione, protezione, contrasto delle minacce e recovery di infrastrutture IT ed OT. Infine verranno fornite le competenze utili a definire efficaci processi di analisi del rischio cyber, di audit e di awareness del personale.

A chi è rivolto?

Il Master si rivolge a coloro che, pur non avendo seguito un percorso di studio specificatamente orientato al dominio della cybersecurity, vogliono indirizzare la propria carriera verso questo dominio con una operazione di re-skilling che consenta loro di arricchire le proprie competenze di base, innestandovi elementi utili a poter gestire i processi di cybersecurity.

In particolare è destinato a:

- Neo-laureati, interessati e motivati a intraprendere un percorso di crescita professionale nel settore cybersecurity.
- Professionisti con esperienza lavorativa, che intendono approfondire le tematiche più rilevanti e innovative del settore.

Titolo di accesso

Laurea Triennale o Laurea Vecchio Ordinamento. Coloro che non sono in possesso di tale titolo potranno essere ammessi come uditori secondo i limiti dell'apposito Decreto Rettorale.

L'iscrizione al Master è compatibile con l'iscrizione ad altro percorso universitario secondo quanto stabilito dalla Legge n. 33 del 12/04/2022 e dal D.M. 930 del 29/07/2022. L'iscrizione al master è aperta anche a laureandi triennali, purché il titolo di laurea venga conseguito entro 90 giorni dalla data di inizio Master.

Quota di partecipazione, quote agevolate e promozioni a tempo

La quota di partecipazione al Master è di euro 6.500,00. Sono previste le seguenti quote agevolate:

- Quota agevolata di euro 5.000,00 per laureati, laureandi e personale dell'Università Campus Bio-Medico di Roma e per il personale della Fondazione Policinico Universitario Campus Bio-Medico.

Il percorso si propone di fornire ai partecipanti le competenze necessarie per ricoprire diversi ruoli tecnici e manageriali in ambito cybersecurity. I profili tecnici formati avranno le capacità di:

- Fornire supporto nella risposta agli incidenti informatici, analizzando e mitigando le minacce.
- Progettare e implementare architetture di sicurezza per proteggere reti e sistemi informatici.
- Definire e aggiornare le misure di sicurezza informatica all'interno delle organizzazioni.
- Organizzare ed effettuare attività di vulnerability assessment e penetration testing.

Le competenze relative agli aspetti manageriali permetteranno ai discenti di:

- Gestire gli aspetti legali e normativi della cybersecurity, assicurando la conformità alle leggi e alle policy aziendali.
- Valutare e gestire i rischi legati alla sicurezza informatica, sviluppando strategie per mitigare le minacce e proteggere le risorse aziendali.

Il Master è organizzato partendo dalle indicazioni dell'**European Cybersecurity Skills Framework** (ECSF) dell'**Agenzia Europea ENISA**, per la formazione di figure tecniche **quali ad esempio cyber incident responder, cyber security architect, cyber security implementer, penetration tester**; e di figure manageriali **come il cyber legal, policy e compliance officer e il cyber security risk manager**.

L'iscrizione al master permette l'accesso gratuito a percorsi di certificazione nel campo della cybersecurity tra cui:

- il percorso **Network Security Expert** di **Fortinet**;
- i **Google Certificates** (tra cui AI Essentials, Cybersecurity, Data Anaytics, IT Support, Project Management, Advanced Daat Analystics, Business Intelligence, IT Automation with Python);
- il percorso **Certified Stormshield Network Administrator**.

KEY FACTS

Destinatari

Il Master è rivolto a coloro che, pur non avendo seguito un percorso di studio specificatamente orientato al dominio della cybersecurity, vogliono indirizzare la propria carriera verso un ruolo tecnico o manageriale in questo dominio.

Modalità didattica, organizzazione e durata

Il Master, con un approccio orientato al learning by-doing, consentirà al partecipante di impratichirsi dei principali strumenti in uso nell'ambito della cybersecurity, sia sul piano gestionale che per ciò che riguarda i principali applicativi in uso. Il percorso è organizzato in modalità **blended** e **part-time** consentendo ai partecipanti, soprattutto ai fuori regione, di conciliare la frequenza con il lavoro, con il 50% delle lezioni organizzate in presenza e il 50% delle lezioni in diretta streaming. La **durata** è di **1 anno (60 CFU) - 1500 ore**.

Borse di studio e rateizzazione

L'Università Campus Bio-Medico di Roma partecipa a bandi Inps per l'assegnazione di borse di studio a favore di partecipanti afferenti a specifiche categorie. Inoltre, è possibile rateizzare la quota di partecipazione contattando UCBM Academy ai seguenti recapiti 06.225419300 oppure ucbmacademy@unicampus.it.

Titolo di studio rilasciato

A coloro che completeranno il Master e saranno in regola con gli adempimenti amministrativi, verrà rilasciato il titolo di "Master Universitario di I livello in Cybersecurity Management".
Agli uditori e ai partecipanti ai singoli moduli verrà rilasciato l'attestato di partecipazione.

Sedi

Università Campus Bio-Medico di Roma

Via Álvaro del Portillo, 21 – 00128 – Roma | Via Giacomo Dina, 36 – 00128 – Roma

Modalità di ammissione

La domanda di ammissione al Master va presentata utilizzando la procedura online disponibile sulla pagina dedicata al Master nella sezione **https://ucbmacademy.unicampus.it/master/** e prevede l'inserimento di:

- dati anagrafici;
- Curriculum Vitae;
- dichiarazione sostitutiva titolo di studi;
- versamento della quota di ammissione di € 60,00.

La selezione si baserà su valutazione del curriculum vitae e colloquio tecnico-motivazionale.

L'iscrizione al Master è compatibile con l'iscrizione ad altro percorso universitario secondo quanto stabilito dalla Legge n. 33 del 1204/2022 e dal D.M. 930 del 29/07/2022.

Save the dates

Scadenza ammissioni:	Colloquio di ammissione:	Data di avvio:
28 settembre 2025	**2 ottobre 2025**	**14 ottobre 2025**

Struttura del Master

Il Master universitario di I livello in Cybersecurity Management conferisce 60 CFU e ha durata complessiva di **un anno**. I **60 CFU**, pari a **1.500 ore** di attività formative, sono così suddivisi:

- attività didattica: in presenza  e in diretta streaming  ;
- percorso di certificazione;
- tirocinio
- Project Work

Le attività saranno organizzate in **5 aree tematiche**:

1. **COMPETENZE DI BASE: L'allineamento delle competenze di base sarà orientato a fornire tutti gli strumenti utili a massimizzare l'apprendimento dei discenti nel corso del Master.** Rientrano in questo modulo sia nozioni di base su sistemi di elaborazione delle informazioni, che competenze gestionali utili per gestire con efficacia le problematiche relative alla sicurezza informatica nelle organizzazioni. Questo approccio interdisciplinare permette di sviluppare competenze sia tecniche sia manageriali, fondamentali per operare efficacemente nel campo della cybersecurity.
2. **PERSONA: Circa il 90% degli incidenti informatici deriva da una qualche forma di errore umano.** Il master propone un'accurata analisi degli aspetti legati alla social engineering e all'Open Source Intelligence Analysis. Il modulo contiene inoltre aspetti relativi a tutti gli strumenti di sicurezza informatica di utilizzo comune centrati sulla persona.
3. **TECNOLOGIA:** L'obiettivo principale del master è quello del re-skilling del discente fornendo nozioni, ma soprattutto strumenti professionali, che permettano un rapido inserimento nel mondo lavorativo del settore della cybersecurity. Attraverso un approccio pratico, il master si focalizza su casi di studio reali, simulazioni e laboratori, per garantire che i partecipanti acquisiscano non solo conoscenze teoriche, ma anche competenze pratiche immediatamente applicabili in contesti di **network security, software and hardware security e web security.** Completa il modulo un approfondimento sul tema dell'IA applicata sia come strumento di attacco che di difesa nella cybersecurity.
4. **PROCESSI:** La cybersecurity non è una soluzione unica e definitiva, ma piuttosto un processo continuo e dinamico. Il modulo fornisce gli elementi gestionali che permettono una corretta impostazione dei piani di mitigazione del rischio cyber in una organizzazione, affrontando temi legati ad analisi del rischio e best practice, anche attraverso le testimonianze di esperti del settore, con riferimento ai principali standard internazionali, quali la ISO/IEC 27001 per la gestione della sicurezza delle informazioni e la ISO 9001 per la gestione della qualità dei processi organizzativi della cybersecurity.
5. **ASPETTI GIURIDICI:** Completano la preparazione del discente le nozioni relative agli aspetti giuridici rispetto all'accesso illecito a sistemi informatici, fenomeni di databreach o data leak ed una comprensione dell'organizzazione nazionale ed internazionale in termini di gestione giuridica degli incidenti cyber, con un focus sul recepimento della normativa NIS2 e sul quadro normativo europeo in materia di sicurezza dei prodotti digitali introdotto dal Cyber Resilience Act.

Tirocinio

Il **tirocinio** avrà una durata di **320 ore**. La finalità del tirocinio curriculare è il completamento delle conoscenze teoriche acquisite durante il Master con una concreta esperienza operativa da svolgersi presso una delle aziende che supportano il Master o presso le sedi lavorative dei partecipanti per coloro che sono già assunti presso un Ente o una Azienda.

Modalità di frequenza

Le lezioni si svolgeranno, di norma, tutte le settimane, alternando la seguente strutturazione:

Settimana 1

- il lunedì dalle ore 17:00 alle ore 19:30: lezione in diretta streaming  ;
- il martedì dalle ore 17:00 alle ore 19:30: lezione in diretta streaming  ;
- il venerdì dalle ore 9:00 alle ore 13:00 e dalle ore 14:00 alle ore 19:00: lezione in presenza  ;
- il sabato dalle ore 9:00 alle ore 13:00 e dalle ore 14:00 alle ore 17:00: lezione in presenza  ;

Settimana 2

- il martedì dalle ore 17:00 alle ore 19:30: lezione in diretta streaming  ;
- il mercoledì dalle ore 17:00 alle ore 19:30: lezione in diretta streaming  ;
- il giovedì dalle ore 17:00 alle ore 19:30: lezione in diretta streaming  ;

Nell'arco di 2 settimane sono previste:

- 13 ore di lezioni in diretta streaming;
- 16 ore di lezioni in presenza.

La frequenza alle attività formative è obbligatoria per un minimo dell'80% delle ore di lezione e del 100% delle attività di tirocinio.

Finanziamenti con fondi interprofessionali

Se sei un'azienda interessata al nostro percorso formativo e sei iscritta a uno o più fondi interprofessionali (Fondimpresa, Forte, Fonter, Fondirigenti, Fondir, etc.), puoi finanziare il Master tramite il fondo stesso.

Contattaci telefonicamente allo 06.22541.9300 o via email a ucbmacademy@unicampus.it per maggiori informazioni e per valutare insieme i requisiti necessari.

I PARTNER DEL MASTER

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Teleconsys
Sharing Innovation

PATROCINI DEL MASTER

MARINA MILITARE

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

ASIS Italy Chapter

aipsa
ASSOCIAZIONE ITALIANA PROFESSIONISTI SECURITY AZIENDALE

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
ITALY

ASSOCISO
Associazione Nazionale
Chief Information Security Officer

UCBM ACADEMY

Università Campus Bio-Medico di Roma

Via Giacomo Dina, 36 - 00128 Roma
Email: ucbmacademy@unicampus.it
Telefono: 06.22541.9300
https://ucbmacademy.unicampus.it/