



UCBM
ACADEMY

In collaborazione con



nitel

Consorzio Nazionale
Interuniversitario
per i Trasporti
e la Logistica

Master di I livello in Cybersecurity Management

IV 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

Magg. Maria Antonietta Silvia Di Bacco

Responsabile del Nucleo Tattico Operativo del CERT-MEF

Dott.ssa Nicola Ivana Diomede

Direttore Dipartimento Cybersecurity e Privacy Roma Capitale

Dott. Riccardo Fragoneri

Direttore IT Ospedale Israelitico, Coordinatore Osservatorio
Cybersicurezza Sanità, Fondazione ICSSA

Dott. Ivano Gabrielli

Direttore Servizio Polizia Postale e delle Comunicazioni

CV Mario Gaudino

Vice Capo Dipartimento C4 e Sicurezza presso lo Stato
Maggiore Marina, Comandante del Comando C4 e Sicurezza
Marina Militare

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 Telecomsys

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

Gen. B. Antonio Mancazzo

Comandante del Nucleo Speciale Tutela Privacy
e Frodi Tecnologiche, Guardia di Finanza



Coordinamento Scientifico

Ing. Luca Faramondi

Ricercatore
Facoltà di Ingegneria
Università Campus Bio-Medico di Roma

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

Dott.ssa Laura Petrillo

Direttore Sicurezza Informatica
Ministero Ambiente e Sicurezza Energetica

Col. t. SPEF Marco Querqui

Capo Ufficio Coordinamento IT e Data Protection
Guardia di Finanza

Ing. Yuri Rassegà

CISO, ENEL GroupPresidente Associato

Ing. Massimo Ravenna

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. Nicola Sotira

Responsabile CERT di Poste Italiane
Vice Presidente Associato

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

Perché scegliere il Master in Cybersecurity Management

Il Master è un percorso di alta formazione progettato per rispondere alla **crescente esigenza di protezione delle infrastrutture digitali di aziende, enti e pubbliche amministrazioni**. In linea con le figure professionali previste dall'**European Cybersecurity Skills Framework (ECSF)** dell'**Agenzia Europea ENISA**, il programma forma professionisti in grado di integrare competenze tecniche, manageriali, organizzative e giuridiche per affrontare le sfide della sicurezza informatica.

Il Master fornisce le conoscenze necessarie per individuare, comprendere e mitigare le minacce cyber, definire strategie di prevenzione e protezione, gestire la sicurezza di infrastrutture IT e OT e sviluppare processi di analisi del rischio, audit e awareness. Il percorso consente inoltre di approfondire le tecnologie e le tendenze più recenti del settore, consolidando competenze immediatamente spendibili nel contesto professionale.

A chi è rivolto?

Il Master si rivolge a coloro che vogliono indirizzare la propria carriera verso il dominio della cybersecurity con un'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. È possibile l'iscrizione per laureandi triennali, purché conseguano il titolo entro 90 giorni dall'avvio del Master.

L'iscrizione al master è compatibile con altri percorsi universitari, infatti **il master può essere integrato con la Laurea Magistrale in Ingegneria dei Sistemi Intelligenti (LM-32) UCBM** come percorso parallelo o successivo, con possibilità di riconoscimento crediti.

Coloro che non sono in possesso del titolo di accesso potranno essere ammessi come uditori.



Quota di partecipazione e quote agevolate

La quota di partecipazione al Master è di euro 6.500,00.

È prevista una quota agevolata di €5.000 per: laureati, laureandi e personale dell'Università Campus Bio-Medico di Roma, partecipanti al Cybersecurity Seminars Program UCBM, diplomati in altri Master o Corsi di Perfezionamento erogati da UCBM Academy, personale della Fondazione Policlinico Universitario Campus Bio-Medico.

Sono inoltre previste agevolazioni per il personale dell'Arma dei Carabinieri, Polizia di Stato, Guardia di Finanza, Marina Militare, Forze Armate, Capitaneria di Porto - Guardia Costiera, Corpo Nazionale dei Vigili del Fuoco nonché per i dipendenti di enti e associazioni partner e patrocinanti del Master.

Per maggiori dettagli: ucbmacademy@unicampus.it.



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 Analytics, IT Support, Project Management, Advanced Data Analytics, Business Intelligence, IT Automation with Python);
- il percorso **Certified Stormshield Network Administrator**.

KEY FACTS



Destinatari

Il titolo di accesso richiesto è la Laurea Triennale o la Laurea Vecchio Ordinamento.



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 va presentata utilizzando la procedura online disponibile sulla [pagina dedicata al Master](#). 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.

Save the dates



Scadenza ammissioni:

24/09/2026

Colloqui di selezione:

01/10/2026

Data di avvio:

23/10/2026

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 sui 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 DELLE PRECEDENTI EDIZIONI DEL MASTER



I PATROCINI DEL MASTER

Patrocini attuali e delle precedenti edizioni



UCBM ACADEMY

Università Campus Bio-Medico di Roma

Via Amsterdam, 125 - 00144

Email: ucbmacademy@unicampus.it

Telefono: 06.22541.9300

<https://ucbmacademy.unicampus.it/>