UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

DECRETO DEL RETTORE
Anno Accademico 2024/2025
N. 360 del 15/07/2025

MASTER UNIVERSITARIO DI I LIVELLO IN
CYBERSECURITY MANAGEMENT
III EDIZIONE

IL RETTORE

Visto lo Statuto vigente dell'Università Campus Bio-Medico di Roma;

Visto il Regolamento Didattico dell'Università Campus Bio-Medico di Roma;

Visto il Decreto Ministeriale n. 270 del 22 ottobre 2004 "Modifiche al Regolamento recante norme concernenti l'autonomia didattica degli atenei, approvato con decreto del Ministero dell'Università e della ricerca scientifica e tecnologica 3 novembre 1999, n. 509", pubblicato sulla G.U. n. 266 del 12 novembre 2004;

Visto il Decreto Interministeriale 9 luglio 2009 relativo alla equiparazione tra Lauree di vecchio ordinamento, Lauree Specialistiche e Lauree Magistrali;

Viste le disposizioni MIUR prot. n. 602 del 18 maggio 2011, aventi ad oggetto le immatricolazioni degli studenti stranieri e comunitari presso le Università italiane statali e non statali autorizzate a rilasciare titoli aventi valore legale;

Visto l'art. 15 della legge 12 novembre 2011, n. 183, "Norme in materia di certificati e dichiarazioni sostitutive";

Visto il D.P.R. del 28 dicembre 2000, n. 445, recante il "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";

Visto l'art. 32 della Legge 18 giugno 2009, n. 69, "Eliminazione degli sprechi relativi al mantenimento di documenti in forma cartacea";

Visto il Decreto Ministeriale n. 930 del 29 luglio 2022, "Disposizioni per consentire la contemporanea iscrizione a due corsi universitari";

Visto il Regolamento per la disciplina di Master Universitari e Corsi di Perfezionamento dell'Università Campus Bio-Medico di Roma;

Vista la delibera del Consiglio Scientifico UCBM Academy del 5 giugno 2025 concernente l'istituzione della III edizione del Master Universitario di I livello in "Cybersecurity Management";

Vista la delibera del Comitato Direttivo UCBM Academy del 6 giugno 2025 concernente l'istituzione della III edizione del Master Universitario di I livello in "Cybersecurity Management";

Vista la delibera del Senato Accademico del 25 giugno 2025 concernente l'istituzione della III edizione del Master Universitario di I livello in "Cybersecurity Management";

DECRETA

Articolo 1

l'attivazione del Master Universitario di I livello in "Cybersecurity Management" promosso dall'Università Campus Bio-Medico di Roma, per l'anno accademico 2025/2026 (III edizione), il cui bando di ammissione e il regolamento sono allegati al presente decreto e ne costituiscono parte integrante.

Roma, 15/07/2025

L'Amministratore Delegato
e Direttore Generale
(Dott. Andrea Rossi)

ROSSI ANDREA
2025.07.17 18:08:23
CN=ROSSI ANDREA
C=IT
2.5.4.4=ROSSI
2.5.4.42=ANDREA

Il Rettore

(Prof. Eugenio Guglielmelli)

GUGLIELMELLI EUGENIO
2025.07.17 18:51:28
CN=GUGLIELMELLI EUGENIO
C=IT
2.5.4.4=GUGLIELMELLI
2.5.4.42=EUGENIO
RSA/2048 bits

MASTER UNIVERSITARIO DI I LIVELLO IN CYBERSECURITY MANAGEMENT III EDIZIONE

Il Master Universitario di I livello in Cybersecurity Management è promosso dall'Area di Automatica della Facoltà Dipartimentale di Ingegneria dell'Università Campus Bio-Medico di Roma.

1. FINALITÀ

Il Master Universitario di I livello in Cybersecurity Management è un corso di formazione avanzata, che si propone di fornire ai partecipanti le competenze richieste per ricoprire diversi ruoli manageriali in ambito cyber security fra i quali i seguenti ruoli come definiti dal European Cybersecurity Skills Framework (ECSF) dell'Agenzia Europea ENISA:

- Cyber Legal, Policy & Compliance Officer
- Cybersecurity Auditor
- Cybersecurity Risk Manager

Il Master è specificatamente progettato per coloro che pur non avendo competenze tecniche desiderano operare nell'ambito della cyber security. A tal fine il master fornisce sia le competenze tecniche per comprendere le minacce, valutare il livello di esposizione al rischio cyber, definire adeguate politiche per la prevenzione, protezione, identificazione, contrasto, risposta e recovery in ambito di cybersecurity e per ciò che riguarda attività di audit e di awareness del personale.

Il Master, con un approccio orientato al learning by-doing, consentirà al partecipante di impratichirsi dei principali strumenti di uso nell'ambito della cybersecurity, sia sul piano gestionale che per ciò che riguarda i rudimenti tecnici, per ciò che fa riferimento al mondo Linux e agli ambienti Microsoft e per ciò che riguarda i principali applicativi in uso nell'ambito Cyber.

2. DIREZIONE E COORDINAMENTO DEL MASTER

Direzione Scientifica

Prof. Roberto Setola

Presidente del Corso di Laurea Magistrale in Ingegneria dei Sistemi Intelligenti - Università Campus Bio-Medico di Roma

Professore Ordinario, Facoltà Dipartimentale di Ingegneria - Università Campus Bio-Medico di Roma

Coordinamento Scientifico

Ing. Luca Faramondi

Ricercatore, Facoltà Dipartimentale di Ingegneria - Università Campus Bio-Medico di Roma

Comitato Scientifico[1]

CA (CP) Giuseppe Aulico

Ammiraglio Comando Generale Capitanerie di Porto-Guardia Costiera

Ing. Luigi Ballarano

Head of Cyber Security Governance Terna

[1] *L'elenco dei membri del Comitato Scientifico potrebbe subire delle variazioni. In caso di modifica, l'UCBM Academy provvederà a darne opportuna diffusione tramite Avviso pubblicato sulla pagina web del Master.*

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
Chief Information Security Officer 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
Ing. Rocco Mammoliti
Chief Information Security Officer Poste Italiane
Ing. Francesco Morelli
Responsabile Cyber & Information Security, Gruppo Ferrovie dello Stato Italiane
Ing. Massimo Ravenna
Head of Cyber Security Acea
Dott.ssa Annita Larissa Sciacovelli
Advisory Group ENISA e Ricercatrice Università degli Studi di Bari
Ing. Marco Venditti
CIO Fondazione Policlinico Universitario Campus Bio-Medico
Dott. Valerio Visconti
Chief Information Security Officer Autostrade per l'Italia
Prof. Luca Vollero
Professore Associato Facoltà Dipartimentale di Ingegneria, Università Campus Bio-Medico di Roma

Coordinamento Organizzativo
UCBM Academy
Università Campus Bio-Medico di Roma

Manager Didattico
Al fine di garantire un monitoraggio costante, affinché il percorso formativo sia in linea con gli obiettivi didattici definiti in fase di pianificazione, è prevista la figura del **manager didattico** che possa garantire una presenza continua per tutto il percorso del Master.

Tale ruolo di coordinamento, è affidato a un referente che verrà nominato a insindacabile giudizio della Direzione Scientifica del Master e che avrà il ruolo di gestire la logistica d'aula, gestire la piattaforma on-line di riferimento, gestire il flusso delle informazioni utili ai docenti e ai partecipanti.

3. PROFILO IN USCITA

Al termine del corso i partecipanti avranno le competenze richieste per ricoprire i seguenti ruoli definiti da ENISA:

Cyber Legal, Policy & Compliance Officer i cui compiti sono:
Supportare l'organizzazione nell'individuazione dei requisiti di cybersecurity, nella definizione delle strategie di sicurezza cibernetica, nella definizione dei processi di governance e per ciò che attiene le strategie e le soluzioni per la gestione e il ripristino in caso di eventi di cybersecurity.
Gestistire, supervisionare e assicurare la conformità alle normative nazionali e agli standard internazionali in tema di sicurezza cibernetica e di protezione dei dati.

Cybersecurity Auditor i cui compiti sono:
Eseguire audit di cybersecurity sull'organizzazione e sui suoi sistemi informatici al fine di garantire la conformità con le normative, gli standard internazionali e le policy aziendali.
Condurre revisioni indipendenti per valutare l'efficacia dei processi e dei controlli e la conformità delle iniziative di cybersecurity e delle modalità di gestione, archiviazione e manipolazione dei dati in tutto il loro ciclo di vita, con riferimento alle normative cogenti, agli standard internazionali ed alle policy aziendali.
Effettuare valutazioni, test e attività di verifica relative agli aspetti di cybersecurity dei prodotti (sistemi, hardware, software e servizi), al fine di garantirne la conformità alle normative, agli standard internazionali e alle policy aziendali.

Cybersecurity Risk Manager i cui compiti sono:
Gestire i rischi legati alla sicurezza informatica dell'organizzazione in linea con le normative di riferimento e le policy aziendali. Sviluppare, mantenere e comunicare i processi e i report di gestione del rischio.
Gestire il processo di analisi dei rischi legati alla cybersecurity (identificazione, analisi, valutazione, stima, e mitigazione) con riferimento alle infrastrutture, ai sistemi e ai servizi nei contesti dell'information technology (IT) e delle operational technologies (OT).
Contribuire alla redazione della strategia di gestione del rischio al fine di garantire che i rischi rimangano a un livello accettabile per l'organizzazione mediante l'adozione di adeguate azioni e controlli di mitigazione.

Le figure professionali formate dal Master, in accordo con la legislazione vigente, potranno collocarsi in aziende pubbliche e private.

4. STRUTTURA DEL MASTER

Il Master Universitario di I livello in Cybersecurity Management, conferisce 60 crediti formativi universitari (CFU) come previsto dall'Art. 7, comma 4 del D.M. 270/2004 e ha durata complessiva di un anno accademico. I 60 CFU, pari a 1.500 ore di attività formative, sono così suddivisi:

- 43 CFU di lezioni frontali in aula, lezioni in diretta streaming, esercitazioni di gruppo e individuali e studio individuale;
- 1 CFU di percorso di certificazione;
- 16 CFU tirocinio ed elaborazione Project Work finale.

Nell'ambito della didattica è previsto un modulo di orientamento al mondo del lavoro, nel quale vengono trattati nello specifico i seguenti argomenti:

- conoscenza del mercato della cyber security anche mediante incontri con responsabili della cyber security di rilevanti realtà pubbliche e private nazionali;
- evoluzione del mercato del lavoro giovanile e internazionale con particolare riferimento alle figure professionali a cui si rivolge il Master;
- orientamento al mercato del lavoro: strumenti legislativi di politiche attive, capacità imprenditoriali, innovazione e leadership. Sono inoltre previsti interventi sul personal-branding, come preparare un CV e gestire un colloquio di lavoro, ecc.;
- soft skills: team working e communication skills.

I **16 CFU** si riferiscono al tirocinio formativo e all'elaborazione del Project Work e corrispondono complessivamente a 400 ore d'attività di cui 320 dedicate al tirocinio formativo e 80 al Project Work.

Didattica d'aula
I corsi d'insegnamento, che costituiscono 43 CFU d'attività, introducono i partecipanti allo sviluppo di competenze necessarie ad affrontare e risolvere problemi gestionali e tecnici e a trasferire le conoscenze acquisite nei contesti operativi.
Ciascuna area prevede in molti casi un approccio multidisciplinare per l'individuazione e l'analisi di problemi nella gestione dei servizi di pertinenza. Tali problemi costituiscono la prima parte del contratto formativo.

Organizzazione della didattica
Le attività didattiche 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 infrastructure security, software and hardware security e web security.

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.

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.

I partecipanti che hanno frequentato il Cybersecurity Seminars Program o che hanno conseguito la Laurea Magistrale in Ingegneria dei Sistemi Intelligenti dell'Università Campus Bio-Medico di Roma, saranno esentati dalla partecipazione all'area tematica 1 "Competenze di base".

Attività di tirocinio curriculare
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.

L'attività di tirocinio potrà essere svolta, in funzione delle esigenze del partecipante e dell'ente ospitante, durante gli ultimi quattro mesi di docenza del Master oppure nei sei mesi successivi alla conclusione delle attività didattiche.

La fase di tirocinio curriculare si conclude con la dissertazione, davanti a una Commissione di valutazione appositamente istituita, del Project Work finale elaborato durante il tirocinio curriculare.

5. TITOLO RILASCIATO E CERTIFICAZIONE

Ai **discenti** 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".

Coloro che frequenteranno il Master in qualità di **uditori** non conseguiranno il titolo e a essi sarà rilasciato un certificato di frequenza.

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

1. Percorso Network Security Expert di Fortinet,
2. Google Certificates (AI Essentials, Prompting Essentials, Cybersecurity, Data Anaytics, Digital Marketing and E-commerce, IT Support, Project Management, UX Design, Advanced Dat Analystics, Business Intelligence, IT Automation with Python),
3. Certified Stormshield Network Administrator (NT-CSNA)

Agli studenti del Master che conseguiranno il titolo di Master e che nei successivi 3 anni si iscriveranno al Corso di Laurea Magistrale in Ingegneria dei Sistemi Intelligenti dell'Università Campus Bio-Medico di Roma verranno riconosciuti fino a 24 CFU, con relativo esonero dal sostenere i relativi esami, ed un'agevolazione del 24% sul costo della retta universitaria.

6. DESTINATARI E REQUISITI DI ACCESSO

Destinatari
Il Master si rivolge a coloro che pur non avendo seguito un percorso di studio specificatamente orientato al dominio della cybersecurity vogliono ri-orientare la propria dinamica formativa 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.

Il Master prevede, tra i suoi frequentatori, la figura dei **discenti**, riservata a coloro in possesso del titolo di studio di Laurea o Laurea vecchio ordinamento, e quella di **uditori**, riservata a coloro che sono privi di detto titolo purché abbiano una comprovata esperienza professionale.

Il titolo di studio deve essere posseduto dal candidato ammesso a frequentare il Master entro e non oltre **90 giorni dall'avvio del master**. I discenti ammessi al Master che, alla data delle selezioni, di cui al successivo paragrafo, non fossero in possesso di detto titolo di studio, saranno ammissibili al Master stesso come "discenti sub-condizione alla frequenza" con eventuale attribuzione alla categoria di uditori qualora non abbiano conseguito detto titolo di studio entro la scadenza specificata.

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.

Procedura di selezione

La partecipazione alla procedura selettiva per il conseguimento dell'idoneità di ammissione al Master prevede, a carico del candidato:

1) il versamento di una quota d'iscrizione alla procedura di selezione pari a € 60,00 attraverso bonifico sul C/C bancario IBAN: IT63Y0200805181000106877148, intestato a Università Campus Bio-Medico di Roma, presso Unicredit, specificando nella causale "Cognome, Nome, concorso Master Cybersecurity";
2) la compilazione della scheda d'iscrizione online alla procedura di selezione;
3) la presentazione, come file in formato .pdf del proprio Curriculum Vitae debitamente datato, firmato e completo dell'autorizzazione all'utilizzo dei dati personali ai fini della procedura di selezione ai sensi del Regolamento (UE) 2016/679;
4) la presentazione in formato .pdf di autocertificazione del possesso, ai sensi degli Artt. 46 e 47 del D.P.R. 445/2000, del titolo di Laurea o Laurea di vecchio ordinamento conseguito in Italia.

Le domande di amissione, pertanto i documenti di cui ai punti 2), 3) e 4) dovranno essere presentati esclusivamente per via telematica tramite la pagina dedicata del Master presente sul sito web https://ucbmacademy.unicampus.it/master, entro e non oltre le ore 23:59 del **28 settembre 2025.**

Non è ammessa la presentazione della domanda e dei relativi allegati via fax o via posta ordinaria. Per ogni eventuale problema tecnico e/o operativo, sarà a disposizione la casella di posta elettronica ucbmacademy@unicampus.it, la casella di posta elettronica certificata (PEC) postlauream@postasicura.unicampus.it e il recapito telefonico 06.22541.9300. Le domande di ammissione, presentate secondo le modalità sopraindicate, si considereranno prodotte in tempo utile solo se pervenute a questa Amministrazione entro il termine perentorio della scadenza indicata. Verranno, pertanto, escluse le domande presentate dopo i predetti termini, nonché quelle pervenute con modalità diverse da quella sopra indicata.
Nel corso della procedura telematica di presentazione della domanda il candidato dovrà dichiarare sotto la propria responsabilità:

- i propri dati anagrafici;
- i dati del versamento della quota d'iscrizione alla procedura di selezione;
- i recapiti telefonici e di posta elettronica;

- il/i titolo/i di studio posseduto/i con il voto conseguito.

Presentando la domanda di ammissione il candidato si impegna contestualmente:

- a comunicare tempestivamente ogni eventuale cambiamento della propria residenza o del recapito;
- nel caso di cittadino italiano o straniero in possesso di titolo accademico equipollente a quello italiano conseguito all'estero, a trasmettere il titolo stesso, con l'elenco degli esami sostenuti e corredato da traduzione in lingua italiana, legalizzazione e "dichiarazione di valore in loco" a cura della rappresentanza diplomatico-consolare italiana competente per territorio, nel rispetto delle norme vigenti in materia di ammissione degli studenti stranieri ai corsi di Laurea delle Università italiane, entro i termini sopraindicati.

Ai sensi dell'Art.15 della legge 12 novembre 2011, n. 183 si precisa che le certificazioni rilasciate dalla pubblica amministrazione in ordine a stati, qualità personali e fatti sono valide e utilizzabili solo nei rapporti tra privati. Nei rapporti con gli organi della pubblica amministrazione e i gestori di pubblici servizi, i certificati e gli atti di notorietà sono sempre sostituiti dalle dichiarazioni di cui agli Artt. 46 e 47 del D.P.R. 445/2000.

Le selezioni si svolgeranno il **2 ottobre 2025**, con comunicazione ufficiale ai candidati mediante posta elettronica e pubblicazione sul sito del Master.

I colloqui di selezione avverranno in modalità telematica tramite apposita piattaforma comunicata dall'Università Campus Bio-Medico di Roma. I Candidati dovranno dotarsi, nel momento dell'appuntamento telematico per sostenere il colloquio, di connessione ad Internet e di Web-cam.
Per la partecipazione alla selezione i candidati dovranno presentare il giorno del colloquio di selezione, un documento di identificazione personale in corso di validità.

Prova di selezione
I candidati per il ruolo sia di discenti, sia di uditori, per conseguire l'idoneità di ammissione al Master, dovranno superare le seguenti fasi di valutazione:

- valutazione del curriculum di studio scientifico/professionale;
- colloquio orale tecnico-motivazionale.

La valutazione verrà espletata da una Commissione Giudicatrice (detta Commissione) appositamente istituita dal Direttore Scientifico insieme al Coordinatore Scientifico avvalendosi della collaborazione del Comitato Scientifico del Master e di un membro dell'UCBM Academy. La Commissione Giudicatrice può essere suddivisa in Sub-Commissioni, costituite da almeno 3 membri ciascuna, in numero proporzionato alla numerosità dei candidati da esaminare.

La Commissione Giudicatrice ha a disposizione, per la valutazione di ogni singolo candidato, un punteggio totale massimo attribuibile pari a 60 punti così suddiviso:

- valutazione del curriculum di studio scientifico/professionale: punteggio massimo attribuibile 30/30, di cui 10 punti per il titolo di studio attribuiti sulla base del voto di laurea: voto da 66-70: 1 punto, voto da 71-75: 2 punti, voto da 76-80: 3 punti, voto da 81-90: 5 punti, voto da 91-100: 6 punti, voto da 101-105: 7 punti, voto da 106-109: 8 punti, voto 110: 9 punti; 110 e lode: 10 punti.

- colloquio finalizzato a verificare la preparazione, le motivazioni e le potenzialità di ogni singolo candidato allo svolgimento di funzioni di Cybersecurity Manager: punteggio massimo attribuibile 30/30.

Il giudizio espresso dalla Commissione Giudicatrice è insindacabile.

Il punteggio totale minimo per conseguire l'idoneità di ammissione al Master è di 30/60 punti. Al termine delle valutazioni la Commissione redige una graduatoria di merito dei candidati ordinandoli in ordine decrescente del punteggio totale conseguito. Il risultato delle valutazioni è comunicato ai candidati che hanno partecipato alla prova di selezione, tramite pubblicazione della graduatoria sulla pagina dedicata al Master presente sul sito web https://ucbmacademy.unicampus.it/master e a mezzo email a cura dell'UCBM Academy.

La graduatoria di ammissione degli ammessi al Master verrà pubblicata entro il giorno **6 ottobre 2025** tramite pubblicazione sull'apposita pagina web del Master.

Iscrizione
A pena di decadenza, i candidati che hanno conseguito l'idoneità di ammissione al Master che risultino utilmente collocati nella graduatoria di ammissione, dovranno completare l'iscrizione al Master entro il termine perentorio del **9 ottobre 2025.**

Subentro
Agli aventi diritto, nel caso di posti vacanti, sarà richiesto tramite e-mail di iscriversi, a pena di decadenza, entro il termine perentorio di cinque giorni lavorativi, a decorrere dal giorno successivo a quello di invio della email.
L'Università Campus Bio-Medico di Roma declina ogni responsabilità in caso di indirizzi errati indicati dal candidato idoneo all'ammissione o di variazione di indirizzi non comunicata tempestivamente agli uffici dell'UCBM Academy, email: ucbmacademy@unicampus.it.

7. NUMERO MASSIMO DI PARTECIPANTI

Il Master è a numero chiuso e il numero totale massimo di partecipanti, cioè discenti più uditori, è pari a 35. Il Master sarà attivato se e solo se, il numero di candidati che avranno conseguito l'idoneità di ammissione, sarà maggiore o uguale a 18. Al Master potranno partecipare in qualità di uditori al massimo 15 persone.

8. DURATA, DATA DI INIZIO E SEDE

Il Master ha durata di un anno.

Data d'inizio: **14 ottobre 2025.**
Didattica d'aula: da ottobre 2025 a maggio 2026.
Tirocinio curriculare: ha una durata di 320 ore per un periodo non superiore a 6 mesi.
Dissertazione del Project Work: a conclusione delle attività didattiche e di tirocinio.

Le attività di didattica frontale si svolgeranno presso le sedi dell'Università Campus Bio-Medico di Roma site in:

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

9. MODALITÀ DI FREQUENZA

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 09:00 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).

Eccezionalmente la giornata inaugurale del Master si terrà in presenza martedì 14 ottobre dalle ore 14:00.

Di norma ogni due settimane di lezione sono previste un totale di 13 ore di lezione in diretta streaming e 16 ore di lezione in presenza.

Il calendario delle lezioni è pubblicato nella pagina dedicata del Master presente sul sito web dell'Ateneo.

La frequenza alle attività formative è obbligatoria e i requisiti minimi per il rilascio del titolo ai discenti è subordinato a:

- aver frequentato con regolarità le attività didattiche. È, infatti, obbligatoria la:
  - partecipazione a non meno dell'80% delle ore di lezione;
  - partecipazione a non meno del 100% delle ore di attività di tirocinio formativo.
- superare con esito positivo tutte le prove di valutazione in itinere (es. esercitazioni, test ecc…);
- superare la prova finale che consiste nella dissertazione davanti ad una Commissione, appositamente istituita, del Project Work elaborato;
- essere in regola con il pagamento delle quote di iscrizione al Master.

Il rilascio del certificato di frequenza per gli uditori è subordinato a:

- aver frequentato non meno dell'80% delle ore di lezione frontale;
- essere in regola con il pagamento delle quote di iscrizione al Master.

L'uditore potrà, volontariamente sostenere le prove di valutazione in itinere e redigere e dissertare il project work.

È prevista inoltre la possibilità di partecipazione a singoli moduli del Master.

10. QUOTA DI ISCRIZIONE, BORSE DI STUDIO E QUOTE AGEVOLATE

La quota d'iscrizione al Master è pari a € 6.500,00 da versare in due rate:

- la I rata di € 3.250,00 da versare all'atto dell'iscrizione (**entro il 09/10/2025**);
- la II rata di € 3.250,00 da versare entro il **30/04/2026.**

Il mancato pagamento, almeno della I rata, della quota d'iscrizione al Master entro le scadenze specificate sarà considerata come rinuncia da parte del candidato a partecipare al Master e, pertanto, si provvederà a chiamare gli idonei seguendo la graduatoria.

Tutti i pagamenti dovranno essere effettuati attraverso bonifico sul C/C bancario intestato a:

Università Campus Bio-Medico di Roma
presso Banca Unicredit
IBAN: IT63Y0200805181000106877148

specificando nella causale: Cognome Nome Master Cybersecurity I rata, oppure II rata, oppure iscrizione totale.

In nessun caso le quote di partecipazione al Master versate saranno rimborsate.

Borse di Studio
L'Università Campus Bio-Medico di Roma partecipa a bandi Inps e di altri enti per l'assegnazione di borse di studio a favore di partecipanti afferenti a specifiche categorie.
La graduatoria dei vincitori di queste borse di studio eventualmente erogate, sarà comunicata nei modi e nei tempi specificati dai relativi bandi pubblicati dagli enti erogatori.

Quote agevolate
Sono previste quote agevolate a favore delle seguenti categorie:

- laureandi e laureati presso l'Università Campus Bio-Medico di Roma;
- partecipanti al Cybersecurity Seminars Program dell'Università Campus Bio-Medico di Roma;
- diplomati in altri Master o Corsi di Perfezionamento erogati dall' Università Campus Bio-Medico di Roma;
- personale dell'Università Campus Bio-Medico di Roma;
- personale della Fondazione Policlinico Universitario Campus Bio-Medico.

La quota agevolata è di € 5.000,00 anziché di € 6.500,00.

In base al contributo delle aziende partner del Master o ad altre opportunità di finanziamento si potranno prevedere ulteriori quote di agevolazione o delle gratuità.

11. EVENTUALI MODIFICHE E AVVISI

Ai sensi del Regolamento per la disciplina dei Master Universitari e dei Corsi di Perfezionamento dell'Università Campus Bio-Medico di Roma, qualora dovessero intervenire delle modifiche al presente regolamento l'UCBM Academy provvederà a darne opportuna diffusione tramite Avviso pubblicato sulla pagina web del Master.

ROSSI ANDREA
2025.07.17 18:08:43
CN=ROSSI ANDREA
C=IT
2.5.4.4=ROSSI
2.5.4.42=ANDREA

GUGLIELMELLI EUGENIO
2025.07.17 18:51:47
CN=GUGLIELMELLI EUGENIO
C=IT
2.5.4.4=GUGLIELMELLI
2.5.4.42=EUGENIO
RSA/2048 bits