

**BLENDED EDITION**  
67% delle lezioni fruibili in presenza  
33% delle lezioni fruibili in diretta streaming

MASTER UNIVERSITARIO DI II LIVELLO

## **HOMELAND SECURITY**

**SISTEMI, METODI E STRUMENTI PER LA  
SECURITY E IL CRISIS MANAGEMENT**

*XVIII EDIZIONE 2025-2026*

[www.MasterHomelandSecurity.eu](http://www.MasterHomelandSecurity.eu)



## Direzione Scientifica

**Prof. Roberto Setola**

Università Campus Bio-Medico di Roma

## Comitato Scientifico

**Dott. Gianluca Ansalone**

Esperto di strategia, sicurezza, intelligence

**Gen. B. Vincenzo Caci**

Capo Centrale Operativa del III Reparto Operazioni

Comando Generale della Guardia di Finanza

**Prof. Stefano Carrese**

Università degli Studi Roma Tre

**Dott. Andrea Chittaro**

Chief Security Officer Snam S.p.A.

**Dott.ssa Nunzia Ciardi**

Vicedirettore Agenzia nazionale per la Cyber Sicurezza

**Dott.ssa Isabella Corradini**

Presidente Themis

**Ing. Luigi D'Angelo**

Direttore vicario del Dipartimento della Protezione Civile

**Dott. Manuel Di Casoli**

Chief Security Officer Pan American Energy

**Dott. Francesco Di Maio**

Chief Security, Risk & Business Continuity Management ELT Group

**Ing. Roberto Emmanuele**

Direttore Vicedirigente Ufficio del Capo del Corpo Nazionale dei Vigili del Fuoco

**Dott. Maurizio Fiasco**

Sociologo

**Dott. Costantino Fiorillo**

Capo dell'Organo Centrale di Sicurezza

Ministero delle Infrastrutture e dei Trasporti

**Dott. Franco Fiumara**

Amministratore Unico Fiumara&Partners Srl

**Dott. Ivano Gabrielli**

Direttore Servizio Polizia Postale e delle Comunicazioni

**Gen. Valerio Giardina**

Head of Security – Enel

**Ing. Gioacchino Giomi**

Già Capo Corpo Nazionale Vigili del Fuoco

**Avv. Stefano Grassi**

Amministratore Delegato Leonardo Lgs

**Dott. Salvatore Iannicelli**

Chief Security Officer Gruppo FS



## Coordinamento Scientifico

**Prof.ssa Marcella Trombetta**

Università Campus Bio-Medico di Roma

**Ing. Francesco Lambiase**

Vice-presidente BCManager

**Dott. Giuseppe Lasco**

Direttore Generale Poste Italiane

**Dott. Marco Lisi**

Inviato Speciale del Ministero degli Affari Esteri e della Cooperazione Internazionale per lo Spazio

**Dott. Giuseppe Mancini**

Leonardo Security Vice President - Intelligence & International

**Dott. Alessandro Manfredini**

Direttore Group Security & Cyber Defence, A2A

**Dott. Pier Luigi Martusciello**

Head of Corporate Security Bnl, Bnp Paribas

**Dott. Roberto Massi**

Chief Risk Officer, Gruppo FS

**Capitano Massimiliano Mezzani**

Capitaneria di Porto

**Dott. Vanes Montanari**

Responsabile Tutela Aziendale Poste Italiane

**Col. Antonio Montanaro**

Ufficio Criminalità Organizzata, Eversione e Terrorismo

**Prof. Stefano Panzieri**

Università degli Studi Roma Tre

**Min. Matteo Piantedosi**

Ministro dell'Interno

**Dott. Alfio Rapisarda**

Responsabile Security Eni

**Dott. Paolo Spinelli**

Responsabile della Funzione IT, Facility, Safety & Security in La7

**Gen. Christian Tettamanti**

Direttore Generale Innovazione Tecnologica

presso il Ministero dell'Ambiente e della Sicurezza Energetica

**Dott. Nicola Vanin**

Responsabile Corporate Security, Cassa Depositi e Prestiti SpA

**Dott. Domenico Vozza**

Responsabile Tutela Aziendale di Acea

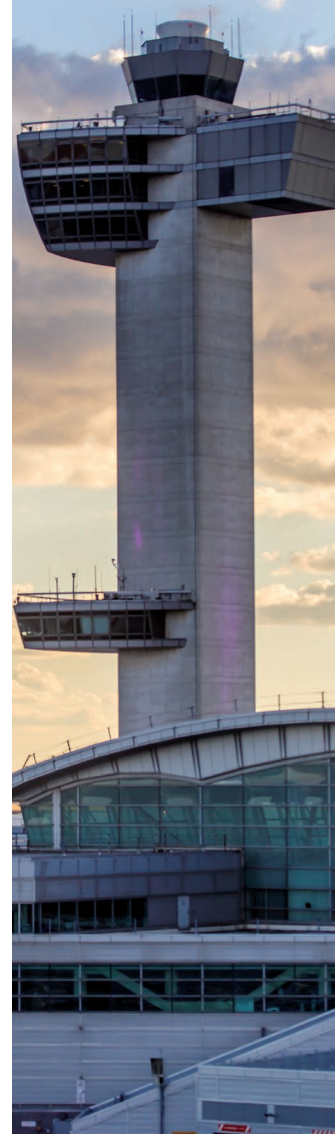
**Dott. Domenico Vulpiani**

Prefetto della Repubblica

**Dott. Francesco Zio**

Executive Director Corporate and Physical Security

Intesa Sanpaolo



## Obiettivi Formativi

Al termine del Master i partecipanti saranno in grado di:

- comprendere, caratterizzare e quantificare le minacce antropiche (sia di natura accidentale che dolosa), naturali e quelle tecnologiche;
- definire e mettere in pratica un sistema di governo della sicurezza basato su un processo di analisi e gestione dei rischi che integri soluzioni organizzative, procedurali e tecnologiche;
- concepire e progettare un sistema di sicurezza integrato capace di identificare, prevenire e contrastare le varie minacce in modo efficace, conforme alle normative e in linea con i risultati dell'analisi dei rischi;
- definire e gestire efficaci ed efficienti sistemi di crisis management, inclusi gli aspetti connessi con la comunicazione verso i media e i cittadini, con l'obiettivo di migliorare la resilienza e la capacità di service-continuity;
- analizzare le problematiche di sicurezza con una visione all-hazard in grado di contemplare e conciliare gli aspetti di safety con quelli di security considerando le minacce sia di natura fisica che cyber;
- comprendere la normativa nazionale ed internazionale di settore;
- interfacciarsi con i fornitori di tecnologie e sistemi per la sicurezza e/o i diversi end-user al fine di comprendere le caratteristiche e le potenzialità dell'offerta/richiesta di sicurezza;
- comprendere e formulare requisiti di sicurezza pertinenti agli scenari di interesse;
- avere una visione d'insieme delle principali tecnologie esistenti nell'ambito della security e del crisis management.

## Struttura e aree tematiche del Master

Il Master di II livello in Homeland Security 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:

- **44 CFU** di didattica d'aula;    ■ **16 CFU** tirocinio ed elaborazione del project work finale.

La didattica prevede 5 moduli tecnici più un modulo di orientamento al lavoro e soft skills.

Il Master sarà erogato in modalità blended, ovvero parte delle lezioni saranno in aula e parte in live streaming. La parte di Didattica Digitale Integrata costituirà il 40% del monte ore.

| Aree Tematiche                                                                                                                  | Argomenti                                                                                                                   | Parole chiave                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>01 - Risk Management</i><br><b>Analisi, qualificazione e quantificazione del contesto</b>                                    | Elementi normativi, gestionali e organizzativi.<br>Metodologia e strumenti per l'analisi del rischio e delle vulnerabilità. | <ul style="list-style-type: none"><li>• Rischio</li><li>• Minaccia</li><li>• Vulnerabilità</li><li>• All Hazard</li><li>• Geopolitica</li><li>• Terrorismo e criminalità organizzata</li><li>• Normativa tecnica</li></ul> |
| <i>02 - Business Continuity &amp; Crisis Management</i><br><b>Prevenzione, Pianificazione, Incident handling &amp; Recovery</b> | Prevenzione, gestione degli incidenti e delle situazioni di crisi.                                                          | <ul style="list-style-type: none"><li>• Sistemi e procedure di Business Continuity e Disaster Recovery</li><li>• La comunicazione in situazioni di emergenza</li><li>• Gestione grandi eventi</li></ul>                    |
| <i>03 - Le tecnologie di physical Security</i><br><b>Metodologie, strumenti e tecnologie</b>                                    | Illustrazione delle principali tecnologie impiegate nell'ambito della sicurezza fisica, logica e organizzativa.             | <ul style="list-style-type: none"><li>• Sicurezza fisica e perimetrale</li><li>• Safety &amp; Security</li><li>• Videosorveglianza</li><li>• Sistemi di supporto alle decisioni e di early warning</li></ul>               |
| <i>04 - Cyber security</i><br><b>Prevenire e contrastare la minaccia cyber</b>                                                  | Illustrazioni delle principali classi di minacce cyber e delle possibili contromisure.                                      | <ul style="list-style-type: none"><li>• Minacce cyber</li><li>• Social Engineering</li><li>• Principali contromisure cyber</li><li>• Scada, IoT, OT</li></ul>                                                              |
| <i>05 - Infrastrutture Critiche</i><br><b>Protezione, Robustezza e Resilienza</b>                                               | Soluzioni organizzative e tecnologiche per la protezione e resilienza cyber-physical di infrastrutture critiche.            | <ul style="list-style-type: none"><li>• Intelligence e Osint</li><li>• Aspetti giuridici e normativi</li><li>• Sicurezza partecipata</li><li>• Travel Security</li></ul>                                                   |
| <i>Soft skill</i><br><b>Come valorizzare le attività</b>                                                                        | Project management, soft skill ed etica.                                                                                    | <ul style="list-style-type: none"><li>• Project management</li><li>• Team Building</li><li>• Etica e deontologia</li><li>• Aspetti economici</li><li>• Privacy e statuto dei lavoratori</li></ul>                          |



## Destinatari e requisiti di accesso

Il Master prevede, tra i suoi frequentatori, la figura dei **di-  
scenti**, riservata a coloro in possesso del titolo di studio in  
Laurea Magistrale o equipollente, e quella di **uditori**, riser-  
vata a coloro che sono privi di detto titolo ma abbiano una  
comprovata esperienza professionale di almeno 3 anni.

I discenti possono provenire da percorsi di studio diversi,  
come ingegneria, giurisprudenza, economia, scienze cri-  
minologiche, informatica, scienze politiche, ecc.

Il Master si rivolge, tra gli altri, anche a funzionari della Pub-  
blica Amministrazione civile e militare, funzionari di Amba-  
sciate, giornalisti e dirigenti del settore privato.

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



## Modalità di ammissione

La domanda di ammissione al Master va presentata **entro  
il 19 febbraio 2026** utilizzando la procedura online dispo-  
nibile all'indirizzo internet:

**[www.MasterHomelandSecurity.eu](http://www.MasterHomelandSecurity.eu)** e prevede l'inseri-  
mento di:

- dati anagrafici e recapiti;
- informazioni relative al titolo di studio;
- curriculum vitae;
- documento d'identità;
- dichiarazione sostitutiva di certificazione;
- dati avvenuto bonifico della quota di ammissione (€ 60).

La selezione verrà effettuata mediante valutazione curricu-  
lare e colloquio orale che si svolgerà il **26 febbraio 2026**.

Il Master è a numero chiuso per un massimo di 40 parte-  
cipanti.

## Save the dates

Scadenza iscrizioni:  
**19 febbraio 2026**

Selezioni:  
**26 febbraio 2026**

Data di inizio:  
**12 marzo 2026**



## Frequenza

Le lezioni si svolgeranno  
a settimane alterne e nei  
seguenti giorni e orari:

**giovedì 10-19  
venerdì 09-18  
sabato 09-13**



## Immatricolazioni e quota di partecipazione

L'immatricolazione al Master dovrà essere effettuata entro il **7 marzo  
2026**. La mancata immatricolazione entro tale termine verrà conside-  
rata come rinuncia.

L'immatricolazione si ritiene perfezionata con l'invio, tramite mail, della  
scheda d'immatricolazione, unitamente a copia del bonifico che atte-  
sta l'avvenuto pagamento almeno della I rata.

Tutti i versamenti, compreso quello relativo alla domanda di ammissio-  
ne, vanno effettuati su c/c bancario intestato a:

Università Campus Bio-Medico di Roma, Unicredit SpA  
IBAN: IT63Y0200805181000106877148

La quota di iscrizione al Master è pari a € 8.000 da pagare in due rate.

L'Ateneo prevede agevolazioni per le quote di iscrizione e possibilità  
di finanziamenti.

Per ulteriori dettagli e per il Bando di Concorso del Master si rimanda  
al sito: **[www.MasterHomelandSecurity.eu](http://www.MasterHomelandSecurity.eu)**.

La spesa per la frequenza del Corso rientra tra quelle di istruzione uni-  
versitaria, di perfezionamento e/o di specializzazione che consentono  
la detrazione dalle imposte.



**Dott.ssa Alessandra Toma**  
Partecipante XVI edizione

*Credo che i punti di valore di questo Master siano sicuramente l'approccio olistico e sistemico del corpo docente, i quali affrontano il tema della sicurezza a 360°; dalla sicurezza fisica alla sicurezza informatica, dall'analisi del rischio fino ad arrivare anche agli aspetti di relazioni interpersonali.*

## Quote agevolate e borse di studio

L'Università Campus Bio-Medico di Roma mette a disposizione:

- fino a un massimo di **2 borse di studio a copertura totale** della quota di iscrizione per un importo di € 8.000,00 riservate ai laureati magistrali da meno di due anni che siano inoccupati o disoccupati;
- fino a un massimo di **6 borse di studio a copertura parziale** della quota di iscrizione per un importo di € 4.000,00 riservate a persone fisiche con l'esclusione di coloro che svolgono attività professionale abituale (titolari di P.IVA).

L'Università Campus Bio-Medico di Roma partecipa a bandi INPS, SNA e di altri enti per l'assegnazione di borse di studio a favore di partecipanti afferenti a specifiche categorie.

Per conoscere ulteriori agevolazioni, rate e opportunità di partecipazione a singoli moduli, contattare l'UCBM Academy:

06.22541.9300 oppure [ucbmacademy@unicampus.it](mailto:ucbmacademy@unicampus.it).

## Manager didattico

I partecipanti al Master potranno fare riferimento durante il percorso didattico, non solo alla Faculty, alla Direzione Scientifica e al Coordinamento organizzativo, ma anche al **Manager didattico dedicato**.

Questa figura è unica per ogni master e supporta il partecipante facendo da tramite per tutte le richieste di carattere didattico-organizzativo.

Il Manager didattico arricchisce l'esperienza offerta al partecipante consentendogli di essere seguito costantemente nell'apprendimento didattico, nella scelta del tirocinio curriculare e durante le attività del percorso formativo.

## Il piano didattico del Master soddisfa i requisiti per la certificazione professionale:

**UNI10459:2017** che definisce i requisiti relativi alla figura professionale del "Security Manager".



ICMQ



## 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 altre strutture che operano nel settore della “Homeland Security”.

Per coloro già assunti presso un Ente o una Azienda, il tirocinio curriculare potrà essere sviluppato all'interno della stessa con l'elaborazione di un progetto formativo da realizzarsi su un argomento attinente alla “Homeland Security”.

La fase di tirocinio curriculare si conclude con la dissertazione del Project Work davanti a una Commissione di Valutazione.

## Perché scegliere questo percorso?

Per i professionisti già occupati nel settore della sicurezza, il Master offre l'opportunità per arricchire il proprio Curriculum, ampliare il network di conoscenze in un settore in grande espansione e l'occasione per una crescita lavorativa e un avanzamento di carriera.



Conferimento Premio Sine Cura 2025:  
Direttore del Dipartimento delle Informazioni per la Sicurezza  
Vittorio Rizzi



Conferimento Premio Sine Cura 2023:  
Ministro dell'Interno Matteo Piantedosi

## Titolo rilasciato

Al termine del corso verrà rilasciato il titolo di Master Universitario di II livello in **“Homeland Security - sistemi, metodi e strumenti per la security e il crisis management”**. Il riconoscimento del credito formativo è legato alla regolare frequenza (obbligatoria per un monte ore non inferiore al 70% delle lezioni e al 90% delle attività di tirocinio), e al superamento delle prove in itinere e finale.

## Esonero crediti formativi professionali per ingegneri

La partecipazione al Master prevede l'esonero dai CFP, secondo le linee di indirizzo per l'aggiornamento della competenza professionale, testo unico 2018, in ottemperanza al D.P.R. 7 agosto 2012, n. 137 e successivi.

I nostri Partner delle ultime edizioni del Master



Hanno patrocinato il Master nelle ultime edizioni





## RESHAPE YOUR SKILLS

L'UCBM Academy promuove la formazione post-lauream dell'Università Campus Bio-Medico di Roma attraverso percorsi in linea con i più attuali scenari e le più rilevanti esigenze del mercato del lavoro, all'interno di programmi sviluppati anche in partnership con aziende, incubatori e acceleratori d'impresa.

UCBM Academy è un luogo, fisico e virtuale, dove la condivisione continua di conoscenza contribuisce a produrre valore e occupabilità nel mondo sanitario, tecnologico, nutrizionale, rispondendo alle sfide urgenti dell'innovazione e della sostenibilità.

### Master e Perfezionamento

Pensati per rispondere alle esigenze del mercato del lavoro, sono fruibili sia da neolaureati che vogliono perfezionare la propria formazione prima di inserirsi nel mondo lavorativo, sia da professionisti che desiderano specializzare le proprie competenze. La metodologia didattica è orientata alla

traduzione delle conoscenze in competenze professionali. I momenti d'aula sono arricchiti da testimonianze di manager del settore, dimostrazioni pratiche e simulazioni e sono sempre seguiti da un'attività di tirocinio curriculare presso aziende del settore di riferimento.



### Coordinamento Organizzativo

#### UCBM ACADEMY

Università Campus Bio-Medico di Roma

Tel.: (+39) 06.22541.9300

E-mail: [ucbmacademy@unicampus.it](mailto:ucbmacademy@unicampus.it) - [postlauream@postasicura.unicampus.it](mailto:postlauream@postasicura.unicampus.it)  
<https://ucbmacademy.unicampus.it/>

#### CONSORZIO NITEL

Tel.: (+39) 06.64003640 | E-mail: [presidenza@nitel.it](mailto:presidenza@nitel.it)

#### Sedi del Corso

Università Campus Bio-Medico di Roma

Via Álvaro del Portillo, 21 - 00128 Roma

Via Giacomo Dina, 36 - 00128 Roma

Copernico Repubblica

Via Antonio Salandra, 13 - 00187 Roma

Leggi il Bando di Concorso completo sul sito: [www.MasterHomelandSecurity.eu](http://www.MasterHomelandSecurity.eu)