PROTEZIONE STRATEGICA DEL SISTEMA PAESE. SICUREZZA FISICA E CYBER DELLE INFRASTRUTTURE CRITICHE

Master Universitario di I livello
a.a. 2026/2027
Con il patrocinio di:

UnitelmaSapienza.it

Indice

1 Finalità
2 Destinatari
3 Requisiti d'accesso
4 Modalità Didattica
5 Assistenza e Tutoraggio
6 Durata ed organizzazione del Master – Proroghe
7 Direzione e Docenti
8 Comitato Scientifico del Master
9 Prove intermedie, prova finale e Titolo
10 Domande di iscrizione e quote
11 Programma

1. Finalità

Il Master di I livello in *PROTEZIONE STRATEGICA DEL SISTEMA PAESE – SICUREZZA FISICA E CYBER DELLE INFRASTRUTTURE CRITICHE*, si propone di fornire a studenti e professionisti interessati, un percorso formativo avanzato e altamente specialistico nell'ambito della sicurezza fisica e logica, nella protezione delle infrastrutture critiche nazionali, per sviluppare capacità di analisi di modelli di simulazione e comprensione delle tecniche di sicurezza adottate nei vari settori delle infrastrutture critiche, gestione del rischio.
Il Master mira, inoltre, a:

- Fornire conoscenze sul sistema di sicurezza nazionale e sul ruolo delle infrastrutture critiche.
- Sviluppare competenze di analisi del rischio, prevenzione e gestione delle minacce (fisiche, cyber e ibride).
- Approfondire il quadro normativo e istituzionale nazionale ed europeo sulla protezione delle infrastrutture strategiche.
- Formare professionisti capaci di pianificare strategie di sicurezza, resilienza e gestione delle crisi a tutela del Sistema Paese.

Il Master è particolarmente innovativo perché coniuga la cyber intelligence della protezione con l'analisi geopolitica e previsionale e mira a fornire una conoscenza degli strumenti per l'attività di *cyber threat intelligence* nella rete e l'utilizzo di tecniche di *open source intelligence* per l'analisi del rischio, studiando gli strumenti per la navigazione e la ricerca anonima e affrontando il problema del *tracking* sul web.

2. Destinatari

Il Master è rivolto a tutti coloro che intendano formarsi in **Security Manager**, responsabili della sicurezza di infrastrutture pubbliche e private, e **Cyber Security Analyst** che possano operare in aziende pubbliche e private, nonché personale dei servizi di Intelligence e funzionari istituzionali.
In particolare il Master è rivolto a:

- Funzionari e dirigenti della Pubblica Amministrazione impegnati in ambiti di sicurezza, difesa e protezione civile.
- Personale delle Forze armate, forze di polizia e organismi di sicurezza.
- Professionisti e manager di aziende che gestiscono infrastrutture critiche (energia, trasporti, telecomunicazioni, finanza, sanità).
- Esperti e consulenti nei settori security, risk management e cyber security.

Laureati in qualsiasi facoltà interessati a specializzarsi nella protezione delle infrastrutture strategiche e nella sicurezza nazionale.

3. Requisiti di accesso

Possono accedere al master coloro che sono in possesso di:

i. laurea conseguita ai sensi del DM n. 270/2004;
ii. Laurea conseguita ai sensi del DM n. 509/1999;
iii. Laurea conseguita secondo gli ordinamenti previgenti;
iv. Titolo rilasciato all'estero, riconosciuto idoneo dalla normativa vigente.

4. Modalità Didattica

La metodologia didattica utilizzata per lo svolgimento del corso è in modalità blended, e prevede:

- una parte di formazione erogata in modalità e-learning (che prevede l'erogazione di video-lezioni, meta-datate ed indicizzate, integrate dai relativi materiali didattici scaricabili dalla piattaforma);
- una parte erogata in modalità sincrona, secondo una specifica calendarizzazione annuale – (2 volte al mese da gennaio a giugno 2027 (14 incontri da due ore);
- una parte in presenza secondo appuntamenti bimensili calendarizzati (il venerdì) (12 giornate ore 14 – 18 fino ad Aprile 2027);
- Seminari (secondo calendarizzazione).

5. Assistenza e Tutoraggio

L'Ateneo garantisce in via continuativa un'assistenza ed un sostegno al processo di apprendimento degli allievi mediante la presenza di un tutor esperto e qualificato.
Il tutor, oltre a prestare assistenza agli studenti dell'Università, gestisce in modo proattivo il rapporto con la classe virtuale degli studenti, predisponendo ogni strumento didattico ed informativo ritenuto utile per supportare gli studenti, utilizzando anche modalità sincrone ed asincrone, quali chat, forum etc.

6. Durata ed organizzazione del Master – Proroghe

La durata del Master è di norma di 12 (dodici) mesi dalla data di prima iscrizione.
Su apposita domanda, l'Ateneo può concedere una proroga per il completamento del Master entro il termine massimo di ulteriori 12 (dodici) mesi. La proroga comporta il rinnovo dell'iscrizione con pagamento contestuale di una tassa pari al 25% della tassa di iscrizione annuale originariamente corrisposta.
Il corsista che non consegua il titolo entro il termine di proroga può proseguire il percorso esclusivamente previo rinnovo dell'iscrizione, da perfezionarsi con il pagamento della tassa annuale originariamente corrisposta entro il termine perentorio di 120 (centoventi) giorni dalla scadenza della proroga.
In caso di mancato rinnovo entro il predetto termine perentorio, il corsista decade di diritto dalla qualità di iscritto al Master, con conseguente chiusura della carriera e perdita del diritto al conseguimento del titolo. La chiusura della carriera viene comunicata all'interessato tramite mail istituzionale o notifica nell'Area Riservata della piattaforma d'Ateneo.
In caso di disattivazione del Master, non si applicano le disposizioni sopra indicate relative alla concessione della proroga: a decorrere dal momento della disattivazione del corso, il corsista avrà a disposizione il termine massimo di un anno per concludere il Master e sostenere la prova finale, decorso il quale si darà luogo alla chiusura della carriera.

7. Direzione e Docenti

La direzione del Master è affidata all' Ing, **Luisa Franchina** (Presidente dell'Associazione Italiana Esperti in Infrastrutture Critiche – AIIC)

Sono docenti del Master:

- Ing. **Luisa Franchina** – Presidente AIIC; esperta in protezione e resilienza delle infrastrutture critiche.
- Prof. **Giorgio Spangher** - Professore Emerito di procedura penale presso la "Sapienza" Università degli Studi di Roma e Direttore Scuola ISI UnitelmaSapienza
- Dr. **Corrado Giustozzi** – Consiglio Direttivo CLUSIT; già esperto CERT-PA (AgID) e advisory ENISA.
- Dr. **Claudio Proietti** – Hermes Bay Srl, Senior Consultant; cybersecurity e sicurezza delle IC.
- Dr.ssa **Laura Teodonno** – Hermes Bay Srl, Senior Analyst/Security Manager; risk & security management.
- Dr. **Vittorio Calaprice** – Analista politico; focus su geopolitica e politiche UE.
- Dott. **Simone Botta**, avvocato.
- Dott. **Stefano Aterno**, avvocato.
- Dott. **Stefano Mele**, avvocato.
- Ing. **Carlotta Cosentino**, cyber security expert.
- Dott. **Filippo Vita**, 27001 auditor.
- Dott. **Matteo Lucchetti**, DG Cyber 4.0.
- Dott.ssa **Marianna Pedrazzi**, Ingegnere.
- Dott.ssa **Milena Antonella Rizzi**, Prefetto, Capo del Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale (ACN).

8. Comitato Scientifico del Master

Il Comitato Scientifico del Master è composto da:

- Prof. **Giorgio Spangher** – Direttore della Scuola I.S.I. UnitelmaSapienza
- Ing. **Luisa Franchina** – Presidente AIIC
- Dott.ssa **Milena Antonella Rizzi**, Prefetto, Capo del Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale (ACN)
- Dr. **Corrado Giustozzi** – Consiglio Direttivo CLUSIT
- Dr. **Claudio Proietti** – Hermes Bay Srl, Senior Consultant
- Dr.ssa **Laura Teodonno** – Hermes Bay Srl, Senior Analyst/Security Manager

9. Prove intermedie, prova finale e titolo

E' prevista una prova intermedia sotto forma di quiz a risposta multipla al termine del 3° modulo.
Al termine della componente didattica è previsto l'avvio della parte di approfondimento ed elaborazione, dedicata alla stesura del Project Work finale del master (tesina finale).
Il project work (studio, sperimentazione, ricerca) è un'attività complessa e strutturata che comprende la progettazione e la realizzazione di una ricerca sul campo finalizzata ad applicare le conoscenze acquisite su casi concreti.

La durata del project work corrisponde a 250 ore (per 10 CFU) di attività da parte dello studente, considerando il suo impegno complessivo ovvero l'attività di ricerca, studio, interazione con il docente ed il tutor, stesura e discussione finale.
La scelta dell'argomento dell'elaborato finale dovrà essere effettuata in coordinamento con il proprio docente di riferimento ed approvato dalla Direzione del Master, secondo le modalità definite.
L'elaborato finale sarà sottoposto alla valutazione della Commissione per il conseguimento del titolo di Master. Il voto verrà espresso in centodecimi.
A seguito della valutazione positiva dell'elaborato finale da parte della Commissione di Master, l'Università rilascerà il diploma di Master Universitario di I livello in "*PROTEZIONE STRATEGICA DEL SISTEMA PAESE – SICUREZZA FISICA E CYBER DELLE INFRASTRUTTURE CRITICHE*", con l'attribuzione di 60 crediti formativi universitari (CFU).

10. Domande di iscrizione e quote

Le iscrizioni al master saranno aperte dal **1° Novembre 2026 al 15 Dicembre 2026** esclusivamente attraverso l'apposita sezione "Iscriviti" del sito www.unitelmasapienza.it.
Il master avrà avvio nell'anno accademico 2026/2027.

La quota di iscrizione al Master è fissata in **3.500,00€** pagabili in due rate:

- la prima pari ad € 600,00 entro 30 gg dall'iscrizione;
- la seconda (€ 2.900,00) entro 60 gg dall'iscrizione.

Sono possibili riduzioni di quota per aziende o PA interessate a pacchetti di iscrizioni multiple.

Al termine del percorso è previsto il pagamento della tassa conseguimento titolo pari a € 200,00.
Si informa che il bollo per l'iscrizione (€ 16,00) e i due bolli per il conseguimento titolo (tot. € 32,00) sono previsti per normativa vigente dell'Agenzia dell'Entrate.
La proroga annuale (come da art. 6 del presente Bando) comporta il rinnovo dell'iscrizione con pagamento contestuale di una tassa pari al 25% della tassa di iscrizione annuale originariamente corrisposta.

11. Programma del corso

Il programma tiene conto del D.M. 639 del 2 maggio 2024 relativo alla Determinazione dei gruppi scientifico-disciplinari e delle relative declaratorie, nonché della razionalizzazione e l'aggiornamento dei settori scientifico-disciplinari e la riconduzione di questi ultimi ai gruppi scientifico-disciplinari.

Il programma prevede il conseguimento di 60 CFU, suddivisi in 50 CFU di didattica, secondo i 5 Moduli come di seguito indicati, e 10 CFU per il Project Work finale**.**

Modulo I (SSD GSPS-02/A; CFU 10)

TITOLO: Infrastrutture Critiche e protezione strategica

Il modulo analizza il ruolo delle infrastrutture critiche nella sicurezza nazionale e internazionale, con particolare attenzione ai settori energetico, dei trasporti, delle telecomunicazioni e delle reti digitali. Verranno esaminati i principali rischi e minacce, inclusi attacchi cyber, sabotaggi, disastri naturali e

instabilità geopolitica. Il corso introduce modelli di analisi del rischio, resilienza e continuità operativa applicati alla protezione delle infrastrutture strategiche. Saranno inoltre approfondite le politiche di sicurezza, i quadri normativi e i sistemi di governance multilivello. Il modulo prevede l'analisi di casi studio e strategie di prevenzione, risposta e recupero.

DOCENTI:

Luisa Franchina

Corrado Giustozzi

Stefano Mele

Vittorio Calaprice

Modulo II (SSD GSPS-02/A; CFU 10)

TITOLO: Minacce, analisi strategica e intelligence

Il modulo introduce le principali tipologie di minacce alla sicurezza nazionale e internazionale, includendo terrorismo, cyber threat, criminalità organizzata e instabilità geopolitica. Verranno presentati strumenti e metodologie di analisi strategica per valutare rischi, vulnerabilità e scenari futuri. Il corso approfondisce i principi dell'intelligence, dalle fonti aperte all'analisi dei dati sensibili, con focus su raccolta, elaborazione e sintesi informativa. Saranno discussi quadri normativi, etici e operativi relativi alle attività di intelligence. Il modulo include casi studio e simulazioni per applicare metodologie di valutazione e decision-making strategico.

DOCENTI:

Laura Teodonno

Claudio Proietti

Filippo Vita

Modulo III (SSD GIUR-13/A - IINF-05/A; CFU 15)

TITOLO: Risk assessment, impatti, normative e standard

Principi di valutazione del rischio applicati a contesti civili e industriali, con analisi di vulnerabilità e potenziali impatti. Verranno esaminati metodi quantitativi e qualitativi di risk assessment, inclusi scenari di criticità e mitigazione. Il corso approfondisce normative nazionali e internazionali, standard di sicurezza e linee guida operative. Saranno analizzati casi studio e best practice per l'implementazione efficace di sistemi di prevenzione e gestione del rischio.

DOCENTI:

Giorgio Spangher

Stefano Mele

Simone Botta

Vittorio Calaprice

Stefano Aterno

Modulo IV (SSD GSPS-02/A; CFU 5)

TITOLO: Strategie di protezione, negoziazione e gestione risorse

Il modulo esplora strategie operative per la protezione di persone, infrastrutture e asset critici in contesti complessi. Vengono analizzate tecniche di negoziazione, gestione di crisi e coordinamento tra team multidisciplinari. Il corso approfondisce l'allocazione efficiente delle risorse, pianificazione operativa e presa di decisioni strategiche. Attraverso casi studio e simulazioni, gli studenti applicano strumenti di gestione delle emergenze e di protezione preventiva.

DOCENTI:

Luisa Franchina

Claudio Proietti

Carlotta Cosentino

Marianna Pedrazzi

Filippo Vita

Modulo V (SSD IINF-05/A; CFU 10)

TITOLO: Business/Service Continuity, crisi e cyber intelligence
Il modulo introduce i principi di continuità operativa e gestione dei servizi in contesti critici, con focus su resilienza aziendale e infrastrutturale. Vengono analizzate strategie di gestione delle crisi, pianificazione del disaster recovery e risposta agli incidenti.
Il corso approfondisce strumenti e metodologie di cyber intelligence per identificare, prevenire e mitigare minacce digitali. Attraverso casi studio e simulazioni, gli studenti apprendono a integrare sicurezza informatica, continuità dei servizi e gestione del rischio.
DOCENTI:
Luisa Franchina
Laura Teodonno
Corrado Giustozzi
Claudio Proietti
Filippo Vita
Carlotta Cosentino
Marianna Pedrazzi
Matteo Lucchetti

Prova Finale (10 CFU)
Redazione project work e discussione

RIEPILOGO

- **Totale Moduli: 5 per un totale di 60 CFU**
- **Prova Intermedia: 1 prova (QUIZ Multiple choice alla fine del 3° modulo)**
- **Project work/tesi finale: 10 CFU**
- **Totale CFU: 60**

Formazione FAD e-learning	120 ore
Formazione sincrona	2 volte al mese da gennaio a giugno 2027 (14 incontri da 2 ore) - *(Secondo calendarizzazione)*
Formazione in presenza	(Venerdì) - 12 giornate: ore 14 – 18 fino ad aprile 2027 *(Secondo calendarizzazione)*
Seminari	Secondo calendarizzazione

INFORMAZIONI

Università degli Studi di Roma
UnitelmaSapienwww.unitelmasapienza.it
info@unitelmasapienza.it