Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 1 di 35

Ministero della Giustizia - m_dg.GDAP.12/10/2026.0459193.E pag. 1 di 1

3/4

Sez. I
12/10/26

m_dg.GAB.12/10/2026.0036340.U

m_dg.GAB.12/10/2026.0036340.U

PEC - Gabinetto del Ministro

INVIATO

Da: difealtistudi@postacert.difesa.it
Inviato: giovedì 8 ottobre 2026 11:12
A: ucm@mailbox.governo.it; protocollo_dfp@mailbox.governo.it; protezionecivile@pec.governo.it; acn@pec.acn.gov.it; asi@asi.postacert.it; ministero.affariesteri@cert.esteri.it; dgap.segreteria@cert.esteri.it; ministero.affarieuropeicoesionepnrr@pec.governo.it; affariregionali@pec.governo.it; urp@pec.politicheagricole.gov.it; recapito.postale@pec.politicheagricole.gov.it; statesercito@postacert.difesa.it; stamadifesa@postacert.difesa.it; MASE@pec.mase.gov.it; udcm@pec.cultura.gov.it; udcm@pec.cultura.gov.it; udc@postacert.difesa.it; sgd@postacert.difesa.it; ufficiodigabinetto@pec.mef.gov.it; gabinetto.ministro@giustiziacert.it; gabinetto.ministro@giustiziacert.it; gabinetto@pec.mise.gov.it; urp@pec.mise.gov.it; segreteria.nato-principale@pec.mit.gov.it; dipps001.0100@pecps.interno.it; for.logisticogestionale@cert.vigilfuoco.it; dippersciv.uff1capodip.prot@pec.interno.it; urp@postacert.istruzione.it; dginnovazione@pec.lavoro.gov.it; gabinettoministropa@pec.governo.it; protocollo_dfp@mailbox.governo.it; dgprev@postacert.sanita.it; gab@postacert.sanita.it; segretariatogenerale@pec.ministeroturismo.gov.it; segretariatogenerale@pec.ministeroturismo.gov.it; postdoc.pnrr@mur.gov.it; segretariatogenerale@pec.mur.gov.it; cor@postacert.difesa.it; cos@postacert.difesa.it; maripers@postacert.difesa.it; stataereo@postacert.difesa.it; carabinieri@pec.carabinieri.it; comando.generale@pec.gdf.it; cofs@postacert.difesa.it; covi@postacert.difesa.it; aiad@pec.it
Oggetto: [p: 7273-2026] Corso di Alta Formazione Senior Leader Cyber Anno Accademico 2026 2027
Allegati: Lineamenti_didattici_SENIOR_LEADER_CYBER_v2_completi_e_firmati.pdf; Elenco_indirizzi.pdf; Lettera_Corso_Senior_Leader_Cyber_A_A_2026_27.pdf; perstampa_Lettera_Corso_Senior_Leader_Cyber_A_A_2026_27.pdf; Segnatura.xml

Trasmissione messaggio da A349694 DIFEALTISTUDI.
Protocollo: M_D A349694 REG2026 0007273 08-10-2026.
Composto da 1 documento primario: Lettera_Corso_Senior_Leader_Cyber_A_A_2026_27.pdf e 4 Allegati.

m_dg.GAB.08/10/2026.0035875.E

m_dg.GDAP.15/10/2026.0039050.ID

AL DAP PER QUANTO DI EVENTUALE COMPETENZA E DIRETTO RISCONTRO

Visto
dlo DGF p.c

Roma 15/X/26

Il Capo del Dipartimento
Stefano Carmine De Michele

CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA A ORDINAMENTO SPECIALE
PROMOSSA DAL MINISTERO DELLA DIFESA

LINEAMENTI DIDATTICI
CORSO DI ALTA FORMAZIONE IN
"SENIOR LEADER CYBER"

A.A. 2026-2027

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 2 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 1 di 31

ATTO DI APPROVAZIONE

IL PRESIDENTE
CENTRO ALTI STUDI DIFESA
SCUOLA SUPERIORE UNIVERSITARIA A ORDINAMENTO SPECIALE

VISTO: il Decreto del Ministro della Difesa del 5 agosto 2021 che istituisce il "Polo formativo *cyber* della Difesa", retto dal Presidente del Centro Alti Studi Difesa (CASD) e costituito dal CASD, dalla Scuola Interforze delle Telecomunicazioni (STELMILIT) e dal Centro Interforze di Formazione Intelligence e Guerra Elettronica (CIFIGE) (inserire se applicabile);

VISTO: l'art. 1 del Decreto 4 luglio 2024 (G.U. n. 213 del 11.09.2024), che istituisce il Centro Alti Studi Difesa (CASD) quale Scuola Superiore Universitaria a Ordinamento Speciale (SSUOS) di alta qualificazione e di ricerca nel campo delle scienze della difesa e della sicurezza;

VISTO: l'art. 1, comma 4, dello Statuto del Centro Alti Studi Difesa (CASD), che attesta al Centro la competenza sull'istruzione universitaria per erogare corsi di formazione dottorale, alta formazione post-laurea e formazione continua nel campo delle Scienze della difesa e sicurezza, e comprende l'Istituto Alti Studi per la Difesa (IASD), l'Istituto Superiore di Stato Maggiore Interforze (ISSMI), l'Istituto di Ricerca e Analisi della Difesa (IRAD) e il Centro per la Formazione Logistica Interforze (CeFLI);

APPROVA

I Lineamenti didattici del corso di alta formazione "***Senior Leader Cyber***" per l'Anno Accademico 2026-2027.

Roma, li 07 ott. 2026

IL PRESIDENTE
Gen. C.A. Stefano MANNINO

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 3 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 2 di 31

RIFERIMENTI

a. Decreto interministeriale del 4 luglio 2024 (G.U. n. 213 del 11.09.2024);
b. Regolamento Didattico Generale del CASD/SSUOS, ed. 2025;
c. Regolamento dei Corsi di Master, Corsi di Alta Formazione e Corsi di Formazione, ed. 2026;
d. SMD-FORM-001 "Direttiva Interforze per la Formazione del Personale Militare", ed. 2025;
e. SMD-FORM-010 "Direttiva per la ricerca e la formazione della Difesa", ed. 2022;
f. Manifesto degli Studi A.A. 2026-2027.

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 4 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 3 di 31

INDICE

1.	GENERALITÀ	pag. 5
2.	DENOMINAZIONE DEL CORSO	pag. 5
3.	STRUTTURA ACCADEMICA DEL CORSO a. Struttura accademica proponente b. Struttura accademica responsabile per la progettazione didattica c. Struttura accademica responsabile per la gestione del corso	pag. 5
4.	SEDE E PERIODO DI SVOLGIMENTO a. Sede delle lezioni e periodo didattico b. Segreteria Studenti e Docenti	pag. 6
5.	OBIETTIVI FORMATIVI GENERALI DEL CORSO	pag. 6
6.	STRUTTURA DIDATTICA DEL CORSO	pag. 8
7.	PIANO FORMATIVO	pag. 8
8.	DESTINATARI DEL CORSO a. Frequentatori b. Uditori	pag. 10
9.	REQUISITI DI AMMISSIONE E SELEZIONE a. Requisiti di ammissione b. Numero dei posti disponibili c. Selezione	pag. 11
10.	ESIGENZE DI DOCENZA a. Docenti e formatori b. *Mentor* e *tutor*	pag. 12
11.	VALUTAZIONE E RICONOSCIMENTO TITOLI a. Valutazione e conseguimento titoli b. Attestati di frequenza	pag. 12
12.	PIANO GENERALE DEI COSTI E PROGRAMMAZIONE DELLA SPESA a. Piano generale dei costi b. Programmazione della spesa	pag. 13
13.	DISPOSIZIONI MATRICOLARI, AMMINISTRATIVE E LOGISTICHE a. Documentazione caratteristica per i discenti militari b. Obbligo di frequenza e cessazione dal corso c. Procedura di iscrizione, quota di iscrizione e modalità di pagamento d. Aspetti logistici e amministrativi	pag. 13
14.	NORME DI COMPORTAMENTO, PRESCRIZIONI E OBBLIGHI	pag. 14

ALLEGATI

A	Microstruttura e obiettivi
B	Calendario delle lezioni
C	Piano di impiego del tempo e CFU
D	Piano delle ammissioni
E	Fascicolo per la segnalazione del candidato

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 5 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 4 di 31

1. GENERALITÀ

Il Centro Alti Studi Difesa/Scuola Superiore Universitaria a Ordinamento Speciale (CASD/SSUOS) è una istituzione universitaria di vertice che promuove percorsi dottorali, programmi post-laurea di eccellenza e iniziative di aggiornamento continuo nei settori della difesa, della sicurezza nazionale e della governance strategica. La sua missione si fonda sulla costruzione di competenze avanzate, capaci di integrare dimensioni operative, tecnologiche, giuridiche e politico-strategiche in un quadro coerente con le esigenze del sistema-Paese.

In tale prospettiva, l'ecosistema digitale e la *cyber* security assumono un ruolo centrale e trasversale. Le loro peculiarità stanno ridefinendo le forme contemporanee della conflittualità, trasformando le tradizionali contrapposizioni belliche e di intelligence in dinamiche ibride, nelle quali il dominio cibernetico si interseca con quelli convenzionali (terra, mare, aria e spazio). Il cyberspazio si configura come teatro operativo a pieno titolo, nel quale attacchi informatici, campagne di disinformazione, manipolazioni cognitive e sabotaggi digitali possono compromettere la sicurezza nazionale con effetti paragonabili – e talvolta superiori – alle minacce fisiche.

In questo scenario, la figura del *Senior Leader Cyber* riveste un ruolo strategico. La crescente complessità del dominio digitale richiede decisori capaci di comprendere le interdipendenze tra tecnologia, operazioni, ***intelligence***, comunicazione strategica e *governance*, orientando processi, risorse e capacità in modo coerente con le priorità della Difesa e del sistema-Paese. Il *Senior Leader Cyber* deve essere in grado di interpretare gli scenari, valutare rischi e opportunità, guidare la trasformazione digitale, coordinare attori diversi e assicurare una postura di sicurezza proattiva, resiliente e multidominio.

La comprensione profonda dell'ecosistema digitale, delle sue vulnerabilità, delle tecniche di difesa, dei meccanismi di governance e delle dinamiche strategiche che regolano il dominio cibernetico è oggi una condizione imprescindibile per garantire la resilienza sistemica del Paese. Solo un approccio olistico, integrato e multidimensionale – che includa tecnologia, operazioni, intelligence, politica e comunicazione – consente di proteggere efficacemente gli asset strategici, assicurando una capacità decisionale matura e coerente con la complessità degli scenari contemporanei.

In questo quadro, il CASD/SSUOS si conferma come polo formativo e di pensiero strategico, capace di anticipare le evoluzioni del dominio digitale, promuovere cultura della sicurezza, sviluppare competenze critiche e contribuire alla definizione delle politiche e dei modelli nazionali di difesa e sicurezza in chiave multidominio.

2. DENOMINAZIONE DEL CORSO

Corso di alta formazione in "***Senior Leader Cyber***".

3. STRUTTURA ACCADEMICA DEL CORSO

a. Struttura accademica proponente

Direzione Alta Formazione e Ricerca (DiAFR) del CASD/SSUOS, unitamente al Polo Formativo *Cyber* della Difesa.

b. Struttura accademica responsabile per la progettazione didattica

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 6 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 5 di 31

Direzione Alta Formazione e Ricerca (DiAFR) del CASD/SSUOS, attraverso l'Ufficio Pianificazione e Progettazione Didattica.

c. Struttura accademica responsabile per la gestione del corso

Direzione Alta Formazione e Ricerca (DiAFR) del CASD/SSUOS. In particolare:

- Ufficio Pianificazione e Progettazione Didattica, unitamente al Polo Formativo Cyber della Difesa, sarà responsabile della fase di condotta del Corso, per gli aspetti sia tecnico-logistici sia amministrativi, incluse le attività connesse al coordinamento e controllo dello stesso;
- Segreteria Studenti sarà responsabile per la produzione e gestione della documentazione, inclusi la produzione degli elementi di informazione per i frequentatori nazionali militari, gli attestati di frequenza e il riconoscimento dei crediti universitari formativi.

Inoltre, sono nominati i seguenti Direttori:

- Direttore del Corso: **A.I. Gino MAZZEI**. È responsabile del Corso, avvalendosi delle sopra citate unità organizzative;
- Direttore Scientifico: **Dott.ssa Alessia VALENTINI**. È responsabile della micro-progettazione e dell'attività didattica.

4. SEDE E PERIODO DI SVOLGIMENTO

a. Sede delle lezioni e periodo didattico

Le lezioni si svolgeranno in presenza presso la sede del CASD/SSUOS, nello storico Palazzo Salviati, in Piazza della Rovere 83, 00165 Roma, sala Montezemolo, **dal 30.11.26 al 04.12.26**.

b. Segreteria Studenti e Segreteria Didattica

Le segreterie studenti e didattica sono site presso la sopracitata sede del CASD/SSUOS. Tutte le comunicazioni dovranno essere indirizzate al seguente indirizzo *e-mail*: segreteriastudenti@unicasd.it.

5. OBIETTIVI FORMATIVI GENERALI DEL CORSO

Il Corso "*Senior Leader Cyber*" ha l'obiettivo di sviluppare una *leadership* strategica capace di comprendere, indirizzare e governare le dinamiche operative, tecnologiche, organizzative e decisionali del dominio cibernetico, rafforzando le capacità di prevenzione, analisi, decisione e risposta alle minacce digitali in un quadro interforze, inter-agenzia e multidominio.

La progressione didattica accompagna il discente dalla comprensione dell'architettura di *governance* nazionale ed europea della cybersicurezza, attraverso la dimensione internazionale e la gestione del rischio, fino alle operazioni nel cyberspazio, alla cyber intelligence, alle attività di influenza e al rapporto con la base industriale e il mondo della ricerca. Ogni giornata combina inquadramenti concettuali, analisi di casi reali (da NotPetya a SolarWinds, dall'attacco Viasat alle frodi abilitate dall'intelligenza artificiale) ed esercitazioni decisionali che culminano in una *tabletop* finale multidominio, nella quale i partecipanti affrontano una crisi complessa che intreccia attacco a infrastrutture critiche, disinformazione e pressione sulla *supply chain*.

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 7 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 6 di 31

Il *Senior Leader* al termine del corso sa collocare decisioni nel dominio *cyber*, nel quadro istituzionale e normativo di riferimento, conosce ruoli e responsabilità di ACN, comparto intelligence e Difesa, padroneggia gli obblighi derivanti da NIS2, GDPR, Perimetro di Sicurezza Nazionale Cibernetica e dal quadro regolatorio europeo, ed è quindi in grado di definire *policy* di cybersicurezza coerenti con gli obiettivi della propria organizzazione e con gli indirizzi nazionali e alleati. Sa valutare il rischio cibernetico con criteri strutturati, orientare gli investimenti in protezione e resilienza, presidiare la continuità operativa e guidare personalmente la gestione di una crisi, dalla convocazione del comitato alle notifiche obbligatorie, fino alle scelte più delicate, come la decisione sul pagamento di un riscatto, e alla comunicazione verso l'interno, le autorità e l'opinione pubblica.

Sul piano operativo, il *leader* formato dal corso comprende la natura del cyberspazio come dominio di operazioni e il suo intreccio con spazio, spettro elettromagnetico e dimensione informativa; utilizza modelli come la *kill chain* e MITRE ATT&CK come linguaggio comune con gli esperti tecnici, ponendo le domande giuste e traducendo le informazioni in opzioni decisionali; valuta criticamente i prodotti di *cyber intelligence*, ne riconosce i livelli di confidenza e i limiti dell'attribuzione e li integra nei processi decisionali di vertice. Sa inoltre riconoscere e contrastare le operazioni di influenza e disinformazione, comprende le implicazioni dell'intelligenza artificiale e delle tecnologie emergenti sulla velocità e sulla qualità delle decisioni, mantenendo il principio del controllo umano significativo, e valuta la dipendenza tecnologica e la sicurezza della supply chain come fattori strategici, conoscendo gli strumenti nazionali disponibili, dal Golden Power alle certificazioni.

Ne risulta una figura capace di coordinare attori diversi in architetture interforze, interagenzia e internazionali, di dialogare con l'industria e con le università per lo sviluppo capacitivo e del capitale umano, e di promuovere all'interno della propria organizzazione una cultura della sicurezza duratura, guidando il cambiamento con autorevolezza. Un *Senior Leader Cyber* formato da questo corso non è un tecnico, ma un decisore consapevole: sa leggere gli scenari, valutarne le implicazioni strategiche, decidere in condizioni di incertezza e rendere la propria organizzazione, e con essa il sistema-Paese, più resiliente di fronte alle minacce digitali presenti e future.

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 8 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 7 di 31

6. STRUTTURA DIDATTICA DEL CORSO

ATTIVITÀ FORMATIVE	TIPOLOGIA DI EROGAZIONE	GSD/SSD	CFU
MODULO 1 **MA1 – Governance e strategia della cybersecurity in Italia**	Sincrona in presenza	01/INFO-01 INFO-01/A	
MODULO 2 **MA2 – Cenni sulla sicurezza informatica in un'organizzazione**	Sincrona in presenza	01/INFO-01 INFO-01/A	
MODULO 3 **MA3 – Overview sulle iniziative NATO/UE/estere**	Sincrona in presenza	01/INFO-01 INFO-01/A	
MODULO 4 **Gestione del rischio, business continuity e disaster recovery**	Sincrona in presenza	01/INFO-01 INFO-01/A	
MODULO 5 **MA5 – Overview sulle operazioni nel cyberspazio**	Sincrona in presenza	01/INFO-01 INFO-01/A	
MODULO 6 **MA6 – Overview sulla Cyber Intelligence**	Sincrona in presenza	01/INFO-01 INFO-01/A	**2**
MODULO 7 **MA7 – Overview sulle attività di Cyber Influence**	Sincrona in presenza	01/INFO-01 INFO-01/A	
MODULO 8 **MA8 – Capacità industriali nazionali nel settore cyber**	Sincrona in presenza	01/INFO-01 INFO-01/A	
MODULO 9 **MA9 – Collaborazione con le università nel settore cyber**	Sincrona in presenza	01/INFO-01 INFO-01/A	
Tabletop ex	Sincrona in presenza	01/INFO-01 INFO-01/A	
TOTALE **50 ore** (25 ore di lezione + 2 ore di ex + 4 integrative + 19 ore di studio e ricerca individuale)		01/INFO-01 INFO-01/A	**2**

7. PIANO FORMATIVO

a. Mappa concettuale

N.D.

b. Albero degli obiettivi[1]

Il percorso formativo mira a formare figure in grado di (microstruttura e obiettivi in **All. A**):

- S1 - Comprendere le *policy cyber*;
- S2 - Coordinare lo sviluppo e l'impiego della capacità *cyber* in coerenza con ruoli, compiti e responsabilità della Difesa, a livello nazionale e internazionale;
- S3 - Interpretare rischi e opportunità del dominio cibernetico;

[1] Livelli di complessità riferiti alla tassonomia di Bloom (Tassonomia di Bloom - Wikipedia).

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 9 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 8 di 31

- F1 - Interpretare gli scenari *cyber* e le implicazioni strategiche, operative e organizzative;
- F2 - Analizzare processi decisionali in contesti caratterizzati da incertezza, rapidità evolutiva e interdipendenze tecnologiche;
- F3 - Prioritizzare risorse e capacità per la protezione degli *asset* critici e la resilienza del sistema-Paese;
- F4 - Coordinare attori diversi in architetture interforze, inter-agenzia e internazionali;
- F5 - Comprendere il dominio *cyber* nel multidominio valorizzando le sinergie con spazio, elettromagnetico, informativo e domini convenzionali;
- F6 - Conoscere la cultura della sicurezza e la visione strategica all'interno delle organizzazioni;
- A1 - Conoscere l'architettura normativa nazionale ed europea (ACN, Perimetro, L.90/2024, NIS2, GDPR, DORA, CER, CRA, AI Act);
- A2 - Applicare i principi di *e-leadership* e *change management* alla trasformazione *cyber* delle organizzazioni;
- A3 - Comprendere logiche, vincoli giuridici ed effetti delle operazioni *cyber* offensive e difensive (compresi diritto internazionale e regole di ingaggio);
- A4 - Analizzare prodotti di *cyber intelligence* e integrarli nei processi decisionali di vertice;
- A5 - Riconoscere operazioni di influenza, disinformazione e minacce ibride nella dimensione cognitiva;
- A6 - Descrivere il ruolo dell'autonomia tecnologica, *supply chain* e base industriale nazionale come fattori strategici;
- A7 - Spiegare il valore dei partenariati ricerca-industria-Difesa per lo sviluppo capacitivo e del capitale umano;
- A8 - Applicare procedure per la gestione di crisi *cyber* a livello di vertice (comunicazione, escalation, continuità operativa).

Al termine del percorso, il discente sarà inoltre in grado di:

- B1 - Comprendere il linguaggio comune tra livello tecnico e livello decisionale, utilizzando correttamente modelli di riferimento quali *kill chain* e MITRE ATT&CK per dialogare con gli esperti, porre le domande giuste e tradurre le informazioni tecniche in opzioni decisionali;
- B2 – Controllare/presiedere un'esercitazione decisionale (*tabletop*), gestendo l'incertezza informativa, l'iniezione di eventi, la prioritizzazione sotto pressione temporale e il debriefing strutturato come strumento di apprendimento organizzativo;
- B3 - Analizzare un prodotto di *intelligence*, riconoscendo il linguaggio estimativo, i livelli di confidenza e i limiti dell'attribuzione, e produrre un *decision brief* sintetico (formato BLUF) per il vertice politico-militare;
- B4 - Applicare gli obblighi normativi nel processo decisionale in tempo di crisi, distinguendo notifiche obbligatorie (NIS2, GDPR, Perimetro/ACN), responsabilità del vertice e implicazioni giuridiche delle scelte, inclusa la decisione sul pagamento di un riscatto;
- B5 - Interpretare gli impatti delle tecnologie emergenti (intelligenza artificiale, agenti autonomi, tecnologie quantistiche) sulla velocità e sulla qualità delle decisioni;

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 10 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 9 di 31

- B6 - Riconoscere la dimensione cognitiva del conflitto, distinguendo disinformazione, misinformazione e malinformazione e analizzando gli effetti sulle campagne di influenza;
- B7 - Comprendere la dipendenza tecnologica e la sicurezza della *supply chain* come fattori di rischio strategico, utilizzando gli strumenti disponibili (Golden Power, CVCN, certificazioni, procurement) per orientare scelte di autonomia e resilienza del sistema-Paese;
- B8 - Comprendere l'importanza del capitale umano *cyber*, attivando partenariati con università e industria, valorizzando percorsi di reclutamento e ritenzione dei talenti e alimentando una cultura della sicurezza duratura nella propria organizzazione.

c. Schede formative

N.D.

d. Cronoprogramma

All. B.

e. Piano di impiego del tempo

All. C.

f. Livello EQF/QNQ-SQF/MILOF

Il CAF in argomento ha livello EQF 6 (SQF-MILOF non calcolato).

8. DESTINATARI DEL CORSO

a. Frequentatori

Nei limiti dei posti disponibili[2] (in conformità al "Piano delle ammissioni" posto in **All. D**), possono presentare la domanda di partecipazione ai Corsi in argomento, i seguenti candidati:

- gli Ufficiali Superiori o Generali delle Forze Armate, Arma dei Carabinieri e Guardia di Finanza, a titolo gratuito, segnalati dai rispettivi Organi di impiego/Comandi;
- gli Ufficiali Superiori o Generali di altri Corpi armati e non armati dello Stato, segnalati dai rispettivi Organi di impiego/Comandi;
- il personale di rango Ufficiale dei Corpi Ausiliari delle Forze Armate[3], segnalati dai rispettivi Organi di impiego/Comandi;
- i Funzionari e Dirigenti civili dell'Amministrazione Difesa, a titolo gratuito, designati dalla Direzione Generale del Personale Civile (PERSOCIV);
- Dirigenti/Funzionari civili appartenenti agli Organi e Agenzie di Stato, altre Amministrazioni Pubbliche, a livello centrale e periferico, Enti regionali e locali, segnalati dalle Amministrazioni di appartenenza;
- Dirigenti/Funzionari del mondo accademico e industriale.

Non saranno ammesse candidature a titolo privato.

[2] La Direzione del Corso si riserva la facoltà di variare le disponibilità di posti di cui trattasi sulla base delle esigenze segnalate e delle disponibilità logistiche del CASD/SSUOS.

[3] Ai sensi dell'art. 273 del DPR 15 marzo 2010 n. 90, il Corpo militare della Croce Rossa Italiana e il Corpo delle infermiere volontarie sono Corpi ausiliari delle Forze Armate.

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 11 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 10 di 31

Il personale – segnalato dall'Amministrazione o dall'Ente di appartenenza, nei numeri indicati in **All. D** – dovrà essere idoneo a ricoprire ruoli manageriali e di *governance* nel dominio digitale. I partecipanti dovranno essere motivati ad approfondire le opportunità, le responsabilità e le implicazioni strategiche connesse alla *cyber governance*, alla *cyber* difesa e, più in generale, alla protezione e alla resilienza degli enti pubblici. È inoltre richiesto un interesse verso la comprensione delle complessità del contesto digitale e della sua integrazione con gli ambienti operativi tradizionali, al fine di orientare processi decisionali, risorse e capacità in modo coerente con le priorità del sistema-Paese.

In tale quadro, il corso è rivolto a decisori capaci di interpretare gli scenari digitali, guidare la trasformazione tecnologica, coordinare attori diversi e assicurare una postura di sicurezza proattiva e multidominio. Il *Senior Leader Cyber* deve saper integrare tecnologia, operazioni, *intelligence*, comunicazione strategica e *governance*, orientando l'azione organizzativa verso la resilienza, la protezione degli asset critici e la competitività dell'Amministrazione o dell'Ente di appartenenza.

Il Corso consente di acquisire una comprensione aggiornata e allo stato dell'arte dell'ecosistema digitale, sia sotto il profilo tecnico-intrinseco, sia in relazione agli aspetti di sicurezza cibernetica, di gestione del rischio e di governance strategica. Tale conoscenza è finalizzata a migliorare la qualità dei processi decisionali interni, a rafforzare la capacità di operare in contesti interforze, inter-agenzia e internazionali e a consolidare il vantaggio competitivo dell'Amministrazione o dell'Ente di appartenenza nel dominio digitale, assicurando una postura di sicurezza proattiva, resiliente e multidominio.

b. Uditori

N.A.

9. REQUISITI DI AMMISSIONE E SELEZIONE

a. Requisiti di ammissione

Possono partecipare al CAF i candidati in possesso di uno dei seguenti requisiti:

- laurea conseguita secondo gli ordinamenti didattici precedenti il decreto ministeriale del 3 novembre 1999 n. 509;
- lauree specialistiche ai sensi del D.M. 509/99 e lauree triennali e magistrali ai sensi del D.M.270/2004;
- titolo accademico conseguito all'estero equiparabile per durata e contenuto al titolo accademico italiano richiesto per l'accesso al CAF. I titoli di studio conseguiti all'estero verranno valutati, ai soli fini dell'iscrizione al CAF, secondo la vigente normativa.

I requisiti per l'ammissione al CAF dovranno essere posseduti alla data di scadenza del termine utile per la presentazione delle domande di iscrizione. Saranno prese in considerazione esclusivamente le segnalazioni inoltrate tramite posta certificata a difealtistudi@postacert.difesa.it, per conoscenza a segreteriastudenti@unicasd.it, che perverranno **entro le ore 23.59 del 22 novembre 2026**, complete del "Fascicolo per la segnalazione del candidato" (fac-simile in **All. E**).

b. Numero dei posti disponibili

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 12 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 11 di 31

Il numero dei posti disponibili è di **62 unità**. Saranno prese in considerazione esclusivamente le segnalazioni che perverranno secondo le modalità rappresentate al precedente para a. e successivo para c., nei limiti dei posti disponibili per gli Enti di Organizzazione individuati, in accordo al piano delle ammissioni riportato **All. E**. La Direzione del Corso si riserva la facoltà di variare le disponibilità di posti sulla base delle esigenze segnalate dai Dicasteri/Agenzie/Enti invitati, nel limite delle disponibilità logistiche del CASD/SSUOS.

c. Selezione

Il CASD/SSUOS provvederà a inviare gli inviti per l'adesione al Corso agli Enti di Organizzazione elencati nel piano delle ammissioni (**cit. All. E**). Il personale interessato, militare o civile, potrà presentare la propria candidatura esclusivamente per via gerarchica e per il tramite dell'Amministrazione/Ente di appartenenza. Non saranno ammesse candidature a titolo privato.

La selezione dei candidati appartenetti all'Amministrazione Difesa sarà svolta dagli organi d'impiego per le F.A. ovvero dai Comandi di appartenenza, in accordo al piano delle ammissioni.

Laddove il totale delle adesioni sia inferiore al numero dei posti disponibili, si procederà ad ammettere le riserve indicate nelle comunicazioni, secondo il criterio dell'ordine cronologico di ricezione della segnalazione, dando comunque precedenza all'Agenzia per la *Cyber* sicurezza Nazionale (ACN).

All'atto della conferma di ammissione del candidato da parte del CASD/SSUOS, la locale Segreteria Studenti prenderà contatti diretti con gli interessati, al fine di fornire le istruzioni per la successiva registrazione/iscrizione sul portale ESSE3.

10. ESIGENZE DI DOCENZA

a. Docenti e formatori

Il CASD/SSUOS per esercitare le proprie funzioni nel settore di competenza, mantiene relazioni con istituti omologhi militari, civili, nazionali e internazionali, con i quali può stipulare accordi e convenzioni nel rispetto della normativa e delle linee guida vigenti. Il Centro si avvarrà, per lo svolgimento completo del programma del Corso, del contributo fornito da docenti selezionati sulla base delle motivazioni, delle esperienze e competenza specifica del settore.

b. Mentor e tutor

N.A.

11. VALUTAZIONE E RICONOSCIMENTO TITOLI

a. Valutazione e conseguimento titoli

I Corsi di Alta Formazione non attribuiscono titoli di studio. Il Corso prevede solo il riconoscimento di n. 2 (due) CFU, previa valutazione finale delle conoscenze acquisite, ambito GSD 01/INFO-01 Informatica / SSD INFO-01/A Informatica.

L'accertamento si svolgerà al termine del Corso nel giorno e ora indicati nel programma, secondo le modalità organizzative che saranno comunicate dal Direttore Scientifico. La

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 13 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 12 di 31

valutazione consisterà in un questionario a risposta multipla di 16 domande (risposta corretta 2 punti; risposta non data 0 punti; risposta errata 0 punti) da effettuarsi in un'ora e trenta. Il voto sarà espresso in trentesimi. Il voto minimo per conseguire il riconoscimento dei CFU è 18/30, mentre il voto massimo è 30/30 con lode (che potrà essere conseguito con 16 risposte esatte, mentre 30/30 senza lode con 15 risposte esatte). In caso di fallimento, sarà prevista una sola sessione di recupero da concordarsi con il frequentatore, unitamente al Direttore del Corso e il Direttore Scientifico. L'esito della verifica di profitto sarà comunicato dal Direttore Scientifico al termine delle operazioni di correzione.

b. Attestati di frequenza

Al termine del percorso didattico ai frequentatori, che abbiano conseguito i risultati di apprendimento attesi e accertati secondo le modalità su evidenziate, è rilasciato il "Certificato di frequenza con esito positivo" con indicazione della votazione finale espressa in trentesimi.

12. PIANO GENERALE DEI COSTI E PROGRAMMAZIONE DELLA SPESA

a. Piano generale dei costi

Numero di ore di lezione 25 + 2 di esercitazione.

Totale costi per docenza ed esercitazioni preventivati in circa € 1.800.

Rimborsi preventivati per spese di viaggio, vitto e alloggio circa € 5.000.

Totale spesa preventivata in circa € 6.800.

b. Programmazione della spesa

Spesa pianificata sul Capitolo 2265-6/57 dell'Esercizio Finanziario 2027.

13. DISPOSIZIONI MATRICOLARI, AMMINISTRATIVE E LOGISTICHE

a. Documentazione caratteristica per i discenti militari

Per il personale militare saranno redatti gli elementi di informazione con l'indicazione del superamento o meno del corso, dichiarazione del voto in trentesimi e posizione conseguita in graduatoria. La redazione sarà a cura della Segreteria Studenti.

b. Obbligo di frequenza e cessazione dal corso

I frequentatori sono tenuti a rispettare l'orario delle attività didattiche in accordo al programma (**All. B**). La presenza giornaliera verrà rilevata tramite il sistema informatico del CASD/SSUOS, laddove applicabile, in alternativa con registro cartaceo e firma autografa del frequentatore. Ai fini del riconoscimento dei CFU, è necessario che il frequentatore abbia seguito almeno 18 periodi di lezione. Il frequentatore che si assenti, anche in maniera non continuativa, per un periodo di tempo complessivo superiore a 7 periodi sarà esonerato dal Corso.

c. Procedura di iscrizione, quota di iscrizione e modalità di pagamento

A sensi della direttiva SMD-F-017 "Corsi di formazione in territorio nazionale – Tabelle di onerosità", ed. 2017, per costo della formazione si intende la valorizzazione monetaria delle

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 14 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 13 di 31

risorse impiegate per l'attività di formazione. La quota-costo della formazione, calcolata nella misura di 5 gg. è:

- gratuita per il personale militare e civile dell'Amministrazione Difesa e della Guardia di Finanza;
- € 136,25 per gli appartenenti alle Amministrazioni o Enti pubblici e della NATO;
- € 141,85 per gli Stati e le Organizzazioni Estere, Soggetti ed Enti privati. Per il trattamento amministrativo degli Ufficiali esteri, compresa la quota-costo della formazione, si procede secondo quanto previsto dal piano annuale delle ammissioni del personale militare straniero alla frequenza di corsi in Italia redatto dallo Stato Maggiore della Difesa.

Il versamento della quota-costo della formazione perfeziona l'iscrizione al Corso. Il mancato pagamento della predetta quota entro 5 giorni calendariali antecedenti la data di inizio della fase residenziale dello specifico Corso di Alta Formazione è causa di esclusione dal corso.

La procedura per l'iscrizione e il pagamento della quota di iscrizione prevede:

- E.O./E.d.O. invia la domanda di segnalazione per la frequenza del proprio personale (**All. E**);
- Segreteria Studenti, in caso di accoglimento della domanda, invia l'elenco degli iscritti a Difesa Servizi spa e chiede agli E.O./E.d.O. di procedere al pagamento della quota di iscrizione, ove dovuta, tramite bonifico in favore di Difesa Servizi spa sul Conto Corrente: Banca Intesa Sanpaolo / IBAN: IT13K0306905020100000064354 / BIC: BCITITMM, con causale la denominazione del CAF seguito dal nominativo del frequentatore;
- E.O./E.d.O. provvede al versamento della quota di iscrizione dandone comunicazione alla Segreteria Studenti e Direzione del Corso (segreteriastudenti@unicasd.it; difealtistudi@postacert.difesa.it) e Difesa Servizi spa (areats@difesa.servizi.it).
- Difesa Servizi spa rilascia, ove richiesto dall'E.O./E.d.O. (a seguito di *e-mail* a areats@difesa.servizi.it), apposita attestazione di pagamento senza valore fiscale in favore del versante.

Durante la procedura di registrazione sul sistema ESSE3, dovranno essere caricati i seguenti documenti, esclusivamente in formato pdf:

- scheda di pre-iscrizione e autocertificazione del titolo universitario con indicazione del voto finale (**All. E**).
- copia di un documento di riconoscimento in corso di validità;
- copia del codice fiscale;

È possibile rinunciare alla partecipazione al Corso facendo pervenire alla Direzione del Corso all'indirizzo di posta certificata difealtistudi@postacert.difesa.it e segreteriastudenti@unicasd.it una richiesta in tal senso sottoscritta dal rinunciatario. In caso di rinuncia scritta pervenuta cinque giorni calendariali prima dell'inizio della fase

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 15 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 14 di 31

residenziale si avrà diritto al rimborso della quota-costo della formazione. Qualora la rinuncia firmata pervenga oltre i limiti su citati non si avrà diritto ad alcun rimborso.

In ogni caso non è ammessa la sostituzione del frequentatore rinunciatario qualora la rinuncia pervenga dopo l'inizio della Fase propedeutica e-learning asincrono. A tal fine fa fede la data di arrivo dell'*e-mail* certificata di rinuncia al corso.

d. Aspetti logistici e amministrativi

Per quanto attiene al **vitto**, i frequentatori possono accedere alla mensa del CASD/SSUOS per la consumazione del pasto meridiano, previa prenotazione giornaliera da effettuarsi entro le ore 09:00, muniti di codice fiscale:

- a titolo gratuito se appartenenti all'Amministrazione Difesa, fermo restando l'espletamento della procedura di aggregazione prevista per la fruizione del pasto.
- a pagamento tutti gli altri frequentatori. Il pagamento di Euro 8,32 (Euro 10,72 per le giornate solenni) dovrà essere effettuato tramite bonifico a:

  IBAN: IT35J0103076341000000800837

  Istituto bancario: Banca Monte dei Paschi di Siena s.p.a.

  Intestatario: Althea s.r.l.

  C.F.: 041011480657

  Causale: "Nome Cognome Pranzo presso il CASD nel/i giorno/i _____".

Gli oneri indiretti connessi alla frequenza del Corso (es: viaggio, alloggio, etc.), sono a carico degli interessati se a titolo privato o carico dell'Amministrazione di appartenenza secondo la normativa vigente. Il CASD non dispone di soluzioni alloggiative e/o convenzioni con strutture alberghiere, inoltre, la carenza di adeguati spazi all'interno del comprensorio non consente il rilascio di permessi per il parcheggio di auto o moto da parte dei frequentatori.

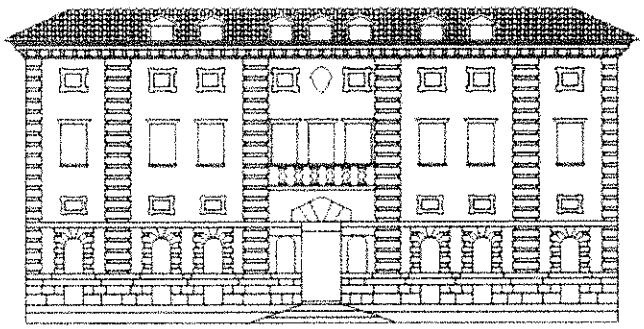
14. NORME DI COMPORTAMENTO, PRESCRIZIONI E OBBLIGHI

I frequentatori sono tenuti a osservare le norme generali di buon senso e le norme di sicurezza sui luoghi di lavoro, nonché le procedure organizzative interne. Resta impregiudicata la facoltà della Direzione del Corso di segnalare eventuali situazioni di incompatibilità/comportamenti dei discenti e prendere le opportune misure a salvaguardia dell'Istituzione. Segnatamente, si richiama l'attenzione sui seguenti punti:

- astensione da comportamenti lesivi dell'immagine e del decoro dell'Istituzione, anche al di fuori della struttura;
- rispetto degli ambienti e cura dei beni di proprietà del CASD/SSUOS e/o di terzi;
- rispetto dell'orario delle lezioni e delle attività calendarizzate;
- rispetto del divieto di fumo, consentito solo negli spazi appositamente contraddistinti con segnaletica dedicata.

Il *dress code* è l'uniforme di servizio per i frequentatori militari e abbigliamento *business casual* per i frequentatori civili, salvo quanto diversamente comunicato per eventuali attività specifiche.

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 16 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 15 di 31



Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 17 di 35

Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 16 di 31

Corso Cyber Senior Leader
Microstruttura didattica

28 lezioni da 50 minuti in 4 giornate da 7 lezioni ciascuna + 25 ore di studio individuale e esercitazioni a casa
La struttura rispecchia l'indicazione «4 giornate da 7 ore da 50 minuti»: 4 × 7 = 28 lezioni da 50'.

1. Struttura del corso e suddivisione delle ore

Ripartizione delle 28 lezioni sui 9 macro-argomenti del syllabus (MA1–MA9):

- MA1 – Governance e strategia della cybersecurity in Italia: 4 lezioni (Giornata 1)
- MA2 – Cenni sulla sicurezza informatica in un'organizzazione: 3 lezioni (Giornata 1)
- MA3 – Overview sulle iniziative NATO/UE/estere: 3 lezioni (Giornata 2)
- MA4 – Gestione del rischio, business continuity e disaster recovery: 4 lezioni, inclusa esercitazione (Giornata 2)
- MA5 – Overview sulle operazioni nel cyberspazio: 4 lezioni (Giornata 3)
- MA6 – Overview sulla Cyber Intelligence: 3 lezioni (Giornata 3)
- MA7 – Overview sulle attività di Cyber Influence: 2 lezioni (Giornata 4)
- MA8 – Capacità industriali nazionali nel settore cyber: 2 lezioni (Giornata 4)
- MA9 – Collaborazione con le università nel settore cyber: 1 lezione (Giornata 4)
- Esercitazione finale integrativa (tabletop decisionale multidominio): 2 lezioni (Giornata 4)

Giornata 1 (7 lezioni): MA1 + MA2 • Giornata 2 (7 lezioni): MA3 + MA5• Giornata 3 (7 lezioni): MA6 + MA7+MA8 • Giornata 4 (7 lezioni): MA4 + tabletop finale.
Riuso dei «materiali esistenti»: i moduli Approccio strategico di Cybersecurity & Privacy, E-leadership e modelli di governance, Governance del change management, Architettura nazionale di cybersicurezza, Architettura europea (EU policy e normative) e Quadro della sicurezza nazionale sono riutilizzati — opportunamente compressi — nelle lezioni indicate con la sigla [ME]. I materiali su operazioni, intelligence, influence, industria e università sono di nuova produzione.

2. Obiettivi e skill (legenda per la mappatura)

Obiettivo generale (dal syllabus)

OG – Sviluppare una leadership strategica capace di comprendere, indirizzare e governare le dinamiche operative, tecnologiche, organizzative e decisionali del dominio cibernetico, rafforzando prevenzione, analisi, decisione e risposta alle minacce digitali in un quadro interforze, interagenzia e multidominio.

Obiettivi di skill (dal syllabus)

- S1 - Comprendere le policy cyber;
- S2 - Coordinare lo sviluppo e l'impiego della capacità cyber in coerenza con ruoli, compiti e responsabilità della Difesa, a livello nazionale e internazionale;
- S3 - Interpretare rischi e opportunità del dominio cibernetico;

Obiettivi formativi (dal syllabus)

- F1 - Interpretare gli scenari cyber e le implicazioni strategiche, operative e organizzative;
- F2 - Analizzare processi decisionali in contesti caratterizzati da incertezza, rapidità evolutiva e interdipendenze tecnologiche;
- F3 - Prioritizzare risorse e capacità per la protezione degli asset critici e la resilienza del sistema Paese;
- F4 - Coordinare attori diversi in architetture interforze, inter agenzia e internazionali;

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 18 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 17 di 31

- F5 - Comprendere il dominio cyber nel multidominio valorizzando le sinergie con spazio, elettromagnetico, informativo e domini convenzionali;
- F6 - Conoscere la cultura della sicurezza e la visione strategica all'interno delle organizzazioni;

Obiettivi aggiuntivi proposti (attinenti ai microargomenti)

- A1 - Conoscere l'architettura normativa nazionale ed europea (ACN, Perimetro, L.90/2024, NIS2, GDPR, DORA, CER, CRA, AI Act);
- A2 - Applicare i principi di e-leadership e change management alla trasformazione cyber delle organizzazioni;
- A3 - Comprendere logiche, vincoli giuridici ed effetti delle operazioni cyber offensive e difensive (compresi diritto internazionale e regole di ingaggio);
- A4 - Analizzare prodotti di cyber intelligence e integrarli nei processi decisionali di vertice;
- A5 - Riconoscere operazioni di influenza, disinformazione e minacce ibride nella dimensione cognitiva;
- A6 - Descrivere il ruolo dell'autonomia tecnologica, supply chain e base industriale nazionale come fattori strategici;
- A7 - Spiegare il valore dei partenariati ricerca-industria-Difesa per lo sviluppo capacitivo e del capitale umano;
- A8 - Applicare procedure per la gestione di crisi cyber a livello di vertice (comunicazione, escalation, continuità operativa).

Al termine del percorso, il discente sarà inoltre in grado di:

- B1 - Comprendere il linguaggio comune tra livello tecnico e livello decisionale, utilizzando correttamente modelli di riferimento quali kill chain e MITRE ATT&CK per dialogare con gli esperti, porre le domande giuste e tradurre le informazioni tecniche in opzioni decisionali;
- B2 – Controllare/presiedere un'esercitazione decisionale (tabletop), gestendo l'incertezza informativa, l'iniezione di eventi, la prioritizzazione sotto pressione temporale e il debriefing strutturato come strumento di apprendimento organizzativo;
- B3 - Analizzare un prodotto di intelligence, riconoscendo il linguaggio estimativo, i livelli di confidenza e i limiti dell'attribuzione, e produrre un decision brief sintetico (formato BLUF) per il vertice politico-militare;
- B4 - Applicare gli obblighi normativi nel processo decisionale in tempo di crisi, distinguendo notifiche obbligatorie (NIS2, GDPR, Perimetro/ACN), responsabilità del vertice e implicazioni giuridiche delle scelte, inclusa la decisione sul pagamento di un riscatto;
- B5 - Interpretare gli impatti delle tecnologie emergenti (intelligenza artificiale, agenti autonomi, tecnologie quantistiche) sulla velocità e sulla qualità delle decisioni;
- B6 - Riconoscere la dimensione cognitiva del conflitto, distinguendo disinformazione, misinformazione e malinformazione e analizzando gli effetti sulle campagne di influenza;
- B7 - Comprendere la dipendenza tecnologica e la sicurezza della supply chain come fattori di rischio strategico, utilizzando gli strumenti disponibili (Golden Power, CVCN, certificazioni, procurement) per orientare scelte di autonomia e resilienza del sistema-Paese;
- B8 - Comprendere l'importanza del capitale umano cyber, attivando partenariati con università e industria, valorizzando percorsi di reclutamento e ritenzione dei talenti e alimentando una cultura della sicurezza duratura nella propria organizzazione.

3. Microstruttura per giornate e lezioni (28 × 50')

Giornata 1 – Governance, strategia e sicurezza dell'organizzazione (7 lezioni)

U1 – MA1: Comprendere il quadro strategico nazionale e l'architettura normativa di cybersicurezza [ME: Architettura nazionale]

- Strategia Nazionale di Cybersicurezza e ruolo dei vertici
- Legge istitutiva ACN; Perimetro di Sicurezza Nazionale Cibernetica

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 19 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 18 di 31

- Legge 90/2024; NIS1/NIS2 e recepimenti italiani (ultime determine); GDPR in sintesi per decisori

Mappatura obiettivi/skill: OG, S1, F1, F3, A1

Esempi/casi di studio: Caso: applicazione degli obblighi NIS2 a un operatore essenziale; discussione sulle notifiche ad ACN.

U2 – MA1: Coordinare gli attori: ruoli, compiti e responsabilità della Difesa nel dominio cyber

- Governance interministeriale: ACN, DIS/AISE/AISI, Difesa (COR/CIOC), NCS
- Quadro della sicurezza nazionale e implicazioni nei processi decisionali politico, civile e militare [ME]
- Catene di comando, deconflitto e coordinamento interagenzia

Mappatura obiettivi/skill: OG, S2, F4, A1

Esempi/casi di studio: Caso: gestione nazionale di un attacco a infrastruttura critica energetica – chi decide cosa.

U3 – MA1: Definire policy e strategia cyber [ME: Approccio strategico C&P]

- Approccio proattivo basato sul rischio; visione, valori e principi
- Security & privacy by design/by default; shift-left; obiettivi di cybersecurity
- Adozione di framework allineati agli obiettivi (NIST CSF, ISO 27001, FNCS) e KPI di monitoraggio

Mappatura obiettivi/skill: S1, S3, F6, A1

Esempi/casi di studio: Esercizio: bozza di policy statement per la propria organizzazione con 5 KPI strategici.

U4 – MA1: Monitorare la strategia e prioritizzare gli interventi di miglioramento continuo [ME]

- Modello operativo integrato di cybersecurity governance
- Profilo corrente vs profilo obiettivo, prioritizzazione degli interventi
- KPI/KRI di governance, reporting al vertice, miglioramento continuo

Mappatura obiettivi/skill: S1, F2, F3

Esempi/casi di studio: Caso di studio [ME]: esempi e casi studio di strategie di governance; lettura di un cyber risk report per il board.

U5 – MA2: Interpretare la sicurezza informatica in un'organizzazione: fondamenti, minacce e rischi per il vertice

- Concetti essenziali: CIA, superficie d'attacco, difesa in profondità, zero trust (livello executive)
- Minacce principali: ransomware, phishing/BEC, supply chain, insider
- Ruoli e responsabilità della cybersicurezza in azienda [ME: change management]

Mappatura obiettivi/skill: F1, F6, S3

Esempi/casi di studio: Casi: Colonial Pipeline e attacco Regione Lazio letti dal punto di vista del vertice.

U6 – MA2: Applicare l'e-leadership alla cybersecurity [ME: e-leadership]

- Definizione di e-leadership e applicazione alla cybersecurity
- Competenze di e-leadership e loro sviluppo
- Valutazione del contesto cyber dell'organizzazione e principali sfide attuative

Mappatura obiettivi/skill: F2, F6, A2

Esempi/casi di studio: Esercizio: self-assessment delle competenze di e-leadership dei partecipanti.

U7 – MA2: Applicare il change management per costruire la cultura della sicurezza [ME: change management]

- Sfide, rimedi e modelli di change management; dal change management al change engagement
- Leader autorevole vs autoritario; continuous change
- Costruire la cultura della sicurezza: awareness, incentivi, misurazione

Mappatura obiettivi/skill: F6, A2, S3

Esempi/casi di studio: Casi reali [ME] di programmi di change verso la cybersicurezza; statistiche italiane.

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 20 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 19 di 31

Giornata 2 – Dimensione internazionale e gestione del rischio (7 lezioni)

U8 – MA3: Conoscere policy e normative dell'Unione Europea e i meccanismi di cooperazione [ME: architettura europea] –

- DORA, direttiva CER, Cybersecurity Act, Cyber Resilience Act, Cyber Solidarity Act
- DSA, DMA, AI Act e Digital Omnibus: intro per decisori
- ENISA, certificazioni e cooperazione europea (CSIRT network, EU-CyCLONe)

Mappatura obiettivi/skill: F4, A1, S2

Esempi/casi di studio: Caso: risposta europea coordinata a una campagna ransomware transnazionale.

U9 – MA3: Comprendere il ruolo della NATO nel dominio cyber e i vincoli del diritto internazionale–

- Il cyberspazio come dominio operativo NATO; Cyber Defence Pledge; SCEPVA
- Struttura: NCIA, CCDCOE, Cyberspace Operations Centre; art. 5 e soglia di attacco armato
- Tallinn Manual e diritto internazionale applicato al cyber (cenni)

Mappatura obiettivi/skill: S2, F4, F5, A3

Esempi/casi di studio: Caso: dibattito sull'applicabilità dell'art. 5 dopo NotPetya e WannaCry.

U10 – MA3: Analizzare e confrontare gli approcci esteri–

- USA: persistent engagement e defend forward; UK e National Cyber Force
- Modelli di Francia, Germania, Israele; approcci di Russia e Cina
- Lezioni per l'Italia: posture, deterrenza, partnership

Mappatura obiettivi/skill: F1, F4, S2

Esempi/casi di studio: Analisi comparata: strategie cyber nazionali pubblicate (US, UK, FR) a confronto.

U11 – MA4: Interpretare e prioritizzare il rischio cyber a livello di vertice

- Concetti di risk management: identificazione, analisi, trattamento; risk appetite e tolerance
- Metodologie e standard: ISO 31000/27005, NIST RMF (livello executive)
- Quantificazione del rischio e trasferimento (cyber insurance)

Mappatura obiettivi/skill: S3, F2, F3

Esempi/casi di studio: Esercizio: costruzione di una matrice di rischio per uno scenario di comando.

U12 – MA4: Prioritizzare servizi e capacità critiche: business continuity e disaster recovery

- BIA, RTO/RPO, strategie di continuità; ISO 22301
- Piani di DR e resilienza delle infrastrutture; dipendenze e single point of failure
- Test, esercitazioni e manutenzione dei piani

Mappatura obiettivi/skill: F3, S3, A8

Esempi/casi di studio: Caso: Maersk/NotPetya – ricostruire un'azienda globale da un domain controller superstite.

U13 – MA4: Applicare procedure di crisis management cyber per senior leader

- Escalation, ruoli del vertice, comunicazione di crisi interna ed esterna
- Coordinamento con autorità (ACN, AGID, autorità giudiziaria) e obblighi di notifica
- Decision making sotto pressione: pagare o non pagare un riscatto?

Mappatura obiettivi/skill: F2, F4, A8, S3

Esempi/casi di studio: Caso introduttivo: ransomware con esfiltrazione dati – impostazione del comitato di crisi.

U14 – MA4: Esercitazione tabletop – gestire rischio, continuità e crisi sotto pressione

- Scenario guidato: attacco ransomware a un ente del Perimetro con impatti su servizi essenziali
- Lavoro in gruppi: valutazione del rischio, attivazione BC/DR, decisioni del vertice, comunicazione e notifiche
- Debriefing: confronto tra le scelte dei gruppi e le best practice; lezioni apprese

Mappatura obiettivi/skill: S3, F2, F3, A8

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 21 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 20 di 31

Esempi/casi di studio: Tabletop completa (50') che integra le lezioni U11–U13; griglia di valutazione fornita ai gruppi.

Giornata 3 – Operazioni nel cyberspazio e cyber intelligence (7 lezioni)

U15 – MA5: Interpretare il cyberspazio come dominio operativo

- Caratteristiche del dominio: anonimato, dual use, velocità, attribuzione incerta
- Tipologie di operazioni: difensive (DCO), offensive (OCO), ISR cyber
- Attori della minaccia: APT statuali, proxy, criminalità organizzata, hacktivismo

Mappatura obiettivi/skill: F1, F5, A3

Esempi/casi di studio: Casi: Stuxnet e le operazioni cyber in Ucraina (Viasat, wiper) come archetipi.

U16 – MA5: Comprendere pianificazione, condotta e vincoli giuridici delle operazioni cyber

Ciclo di targeting ed effetti cyber; integrazione nel processo di pianificazione operativa

- Kill chain e MITRE ATT&CK come linguaggio comune tra tecnici e decisori
- Regole di ingaggio, vincoli giuridici (DIU) e autorizzazioni politiche

Mappatura obiettivi/skill: S2, F5, A3

Esempi/casi di studio: Esercizio: valutare opzioni di risposta (diplomatica, cyber, cinetica) a un attacco simulato.

U17 – MA5: Comprendere il cyber nel multidominio e valorizzarne le sinergie

- Sinergie con spazio, spettro elettromagnetico, dominio informativo e domini convenzionali
- Multi-Domain Operations: comando e controllo, effetti convergenti
- Protezione delle capacità proprie: mission assurance e cyber resilience operativa

Mappatura obiettivi/skill: F5, S2, F1

Esempi/casi di studio: Caso: attacco a Viasat KA-SAT (2022) come esempio di effetto cyber-spazio su operazioni militari.

U18 – MA5: Interpretare l'impatto di AI e tecnologie emergenti sulle operazioni cyber e sulle decisioni –

Attacchi potenziati dall'AI: phishing generativo, deepfake, malware adattivo, agenti autonomi offensivi

- Difesa AI-driven: detection, automazione della risposta, human-in-the-loop e responsabilità del decisore
- Implicazioni per dottrina, addestramento e velocità decisionale del vertice

Mappatura obiettivi/skill: F1, F2, A3

Esempi/casi di studio: Casi: frode deepfake da 25 M$ (Hong Kong 2024); uso documentato di LLM da parte di threat actor; dibattito su autonomia e controllo umano.

U19 – MA6: Comprendere i fondamenti della cyber intelligence

- Definizioni: CTI strategica, operativa, tattica; il ciclo dell'intelligence
- Fonti: OSINT, SIGINT, HUMINT, dark web; information sharing (ISAC, CERT)
- Il ruolo dell'intelligence nazionale (DIS, AISE, AISI) nel dominio cyber

Mappatura obiettivi/skill: F1, A4, S3

Esempi/casi di studio: Esempio: come un bollettino CSIRT Italia/ACN informa le decisioni del vertice.

U20 – MA6: Dall'intelligence alla decisione: analizzare prodotti di intelligence e produrre decision brief

- Threat landscape e profilazione degli attori (naming, capacità, intenti)
- Attribuzione: metodi, limiti, attribuzione pubblica e sue implicazioni politiche
- Linguaggio estimativo, confidence level e briefing ai decisori

Mappatura obiettivi/skill: F2, A4, F1

Esempi/casi di studio: Caso: attribuzione di SolarWinds e Olympic Destroyer (false flag) – cosa può decidere un vertice.

U21 – MA6: Integrare early warning e intelligence a supporto della resilienza nazionale

- Indicatori strategici e early warning; monitoraggio delle infrastrutture critiche

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 22 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 21 di 31

- Condivisione interagenzia e internazionale dell'intelligence cyber
- Esercitazione guidata: lettura critica di un report CTI e brief di 5 minuti al comandante

Mappatura obiettivi/skill: F3, F4, A4

Esempi/casi di studio: Esercizio pratico su report CTI reale (sanitizzato).

Giornata 4 – Influence, industria, università e sintesi (7 lezioni)

U22 – MA7: Riconoscere le operazioni di cyber influence nella dimensione cognitiva

Information operations, disinformazione, misinformazione, malinformazione

- Tecniche: bot, troll farm, amplificazione algoritmica, deepfake e AI generativa
- Minacce ibride e interferenze elettorali; quadro NATO/UE (StratCom, EEAS)

Mappatura obiettivi/skill: F1, F5, A5

Esempi/casi di studio: Casi: interferenze elettorali documentate (USA 2016, UE) e campagne pro-russe in Europa.

U23 – MA7: Contrastare le operazioni di influenza con la comunicazione strategica

Resilienza cognitiva: media literacy, prebunking/debunking, fact-checking

- Ruoli di istituzioni, piattaforme (DSA) e Difesa; limiti giuridici ed etici
- Comunicazione strategica come capacità del leader

Mappatura obiettivi/skill: F6, A5, S1

Esempi/casi di studio: Esercizio: progettare la risposta comunicativa a una campagna di disinformazione contro le Forze Armate.

U24 – MA8: Descrivere la base industriale nazionale cyber come fattore di autonomia strategica

- Panorama dell'industria italiana: grandi player, PMI, startup; il ruolo del procurement Difesa
- Autonomia strategica e tecnologica: crittografia, cloud nazionale (PSN), 5G, Golden Power
- Supply chain security e valutazione dei fornitori (CVCN, certificazioni)

Mappatura obiettivi/skill: F3, A6, S2

Esempi/casi di studio: Caso: esercizio del Golden Power su tecnologie critiche; screening di un fornitore ICT.

U25 – MA8: Valutare innovazione, PNRR e sviluppo capacitivo

- Programmi nazionali ed europei: PNRR, EDF, Horizon Europe, Digital Europe
- Dual use e trasferimento tecnologico civile-militare
- AI, quantum e tecnologie emergenti: implicazioni per la capacità cyber futura

Mappatura obiettivi/skill: S2, A6, F3

Esempi/casi di studio: Esempi: progetti EDF a partecipazione italiana; roadmap quantum-safe.

U26 – MA9: Attivare la collaborazione con le università e valorizzare il capitale umano

- Ecosistema ricerca: centri di competenza, CINI/Cybersecurity National Lab, dottorati e lauree cyber
- Strumenti: convenzioni, laboratori congiunti, CyberChallenge.IT, riserva cyber
- Talent pipeline per la Difesa: reclutamento, ritenzione, formazione continua

Mappatura obiettivi/skill: F6, A7, S2

Esempi/casi di studio: Casi: CyberChallenge.IT e accordi Difesa-atenei come modelli di partenariato.

U27 – Esercitazione finale integrativa (parte 1): tabletop decisionale multidominio – valutare la situazione e prioritizzare le opzioni

- Scenario: campagna coordinata (attacco a infrastruttura critica + disinformazione + pressione sulla supply chain)
- Iniezione degli eventi e lavoro in gruppi: valutazione della situazione, opzioni disponibili
- Prime decisioni dei gruppi: priorità, escalation, coordinamento interagenzia

Mappatura obiettivi/skill: OG, F1–F5, S1–S3, A8

Esempi/casi di studio: Tabletop che integra tutti i macro-argomenti del corso; ruoli assegnati (vertice politico, militare, ACN, comunicazione).

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 23 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 22 di 31

U28 – Esercitazione finale integrativa (parte 2): decidere, comunicare e condurre il debriefing

- Seconda iniezione: evoluzione dello scenario (attribuzione incerta, pressione mediatica); decisioni finali e comunicazione strategica
- Presentazione delle decisioni dei gruppi e confronto
- Debriefing strutturato, lezioni apprese, sintesi finale del corso e verifica del raggiungimento degli obiettivi

Mappatura obiettivi/skill: OG, F1–F6, S1–S3, A5, A8

Esempi/casi di studio: Griglia di valutazione formativa dei gruppi; chiusura con mappatura esplicita sugli obiettivi del syllabus.

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 24 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 23 di 31

4. Studio individuale ed esercitazioni a casa (25 ore)

Il carico di 25 ore è distribuito in approfondimenti pre/post giornata ed esercitazioni individuali o di gruppo, con output verificabili.

HW1 – Prima della Giornata 1 (3h)

Lettura guidata: Strategia Nazionale di Cybersicurezza 2022–2026 (sintesi) e schede su ACN, Perimetro, L.90/2024. Output: mappa mentale dell'architettura nazionale.

Obiettivi mappati: A1, F1

HW2 – Dopo la Giornata 1 (4h)

Esercitazione: redigere una policy cyber di 2 pagine per la propria organizzazione con obiettivi, framework di riferimento e 5 KPI; autovalutazione e-leadership con piano di sviluppo personale. [Riuso ME: materiali approccio strategico e e-leadership come dispense]

Obiettivi mappati: S1, A2, F6

HW3 – Prima della Giornata 2 (2h)

Lettura: sintesi di NIS2, DORA e CRA (schede fornite); strategia cyber di un Paese estero a scelta (US/UK/FR). Output: 10 righe di confronto con l'Italia.

Obiettivi mappati: A1, F4

HW4 – Dopo la Giornata 2 (4h)

Esercitazione: Business Impact Analysis semplificata su 3 servizi critici della propria organizzazione (RTO/RPO, dipendenze, strategia di continuità) + piano di comunicazione di crisi di 1 pagina.

Obiettivi mappati: S3, F3, A8

HW5 – Prima della Giornata 3 (2h)

Lettura: caso Stuxnet e dossier sulle operazioni cyber in Ucraina (dispense); glossario kill chain / MITRE ATT&CK per decisori.

Obiettivi mappati: F1, A3

HW6 – Dopo la Giornata 3 (4h)

Esercitazione: analisi di un report CTI sanitizzato e produzione di un decision brief di 1 pagina (BLUF, valutazione, opzioni, raccomandazione) per il vertice.

Obiettivi mappati: A4, F2

HW7 – Dopo la Giornata 4 (4h)

Elaborato finale individuale: «Piano d'azione del leader» (4–5 pagine) che integri governance, rischio, operazioni, intelligence, influence e partenariati per la propria realtà organizzativa, con mappatura esplicita sugli obiettivi F1–F6 e S1–S3.

Obiettivi mappati: OG, tutti

HW8 – Trasversale (2h)

Visione di 2 briefing/lezioni registrate (es. panel su minacce ibride e su autonomia tecnologica) con domande di verifica.

Obiettivi mappati: A5, A6

Totale studio a casa: 3+4+2+4+2+4+4+2 = 25 ore.

5. Note finali

- Tutti i 9 macro-argomenti del syllabus sono coperti; i moduli dei «materiali esistenti» (12h complessive) sono riutilizzati in forma compressa nelle lezioni marcate [ME] (U1, U2, U3, U4, U5, U6, U7, U8) e come dispense per lo studio individuale (HW2).
- Ogni lezione riporta la mappatura sull'obiettivo generale (OG), sugli obiettivi di skill (S1–S3), sugli obiettivi formativi (F1–F6) e sugli obiettivi aggiuntivi proposti (A1–A8).
- La valutazione consigliata combina: partecipazione ai tabletop (U14 e U27–U28), decision brief (HW6) ed elaborato finale (HW7).

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 25 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 24 di 31

Allegato B

CALENDARIO SETTIMANALE CORSO SENIOR LEADER CYBER 30NOV-04DIC 2026

Periodi / Giorno	08:30-09:20	09:30-10:20	10:40-11:30	11:40-12:30		13:30-14:20	14:30-15:20	15:40-16:30
Lunedì 30.11.26	Saluti istituzionali e MA1: Il quadro strategico nazionale e l'architettura di cybersicurezza [ME: Architettura nazionale]	MA1: Ruoli, compiti e responsabilità della Difesa nel dominio cyberateria	MA1: Definire policy e strategia cyber [ME: Approccio strategico C&P]	MA1: Monitoraggio della strategia e miglioramento continuo [ME]		MA2: La sicurezza informatica in un'organizzazione: fondamenti per il vertice	MA2: E-leadership per la cybersecurity [ME: e-leadership]	MA2: Change management verso la cybersicurezza [ME: change management]
	A.I. Gino MAZZEI /A.Valentini	A.Valentini	A.Valentini	A.Valentini		A.Valentini	A.Valentini	A.Valentini
Martedì 01.12.26	MA3: L'Unione Europea: policy e normative [ME: architettura europea]	MA3: La NATO e il dominio cyber	MA3: Approcci esteri a confronto	MA5: Il cyberspazio come dominio operativo	**PRANZO**	MA5: Pianificazione e condotta delle operazioni cyber	MA5: Cyber nel multidominio	MA5: AI e tecnologie emergenti nelle operazioni cyber
	A.Politi	A.Politi	A.Politi	G.Placanica/M.Lapi		G.Placanica/M.Lapi	G.Placanica/M.Lapi	G.Placanica/M.Lapi
Merceledì 02.12.26	MA6: Fondamenti di cyber intelligence	MA6: Dall'intelligence alla decisione	MA6: Early warning e intelligence a supporto della resilienza nazionale	MA7: Cyber influence e dimensione cognitiva		MA7: Contrasto alle operazioni di influenza	MA8: La base industriale nazionale cyber	MA8: Innovazione, PNRR e sviluppo capacitivo
	M.Lapi	M.Lapi	M.Lapi	P.Tarsitano		P.Tarsitano	P.Tarsitano	P.Tarsitano
Giovedì 03.12.26	MA4: Gestione del rischio cyber a livello di vertice	MA4: Business continuity e disaster recovery	MA4: Crisis management cyber per senior leader	MA4: Esercitazione tabletop – rischio, continuità e crisi		MA9: Collaborazione con le università e capitale umano	Esercitazione finale integrativa (parte 1): tabletop decisionale multidominio	Esercitazione finale integrativa (parte 2): decisioni, comunicazione e debriefing
	A.Valentini	A.Valentini	A.Valentini	A.Valentini		A.Valentini	A.Valentini	A.Valentini
Venerdì 04.12.26	Studio individuale	Test a risposta multipla 16 domande	Test a risposta multipla 16 domande	Consegna attestati				

Alessia Valentini Direttore scientifico

Alessandro Politi NATO Defense College Foundation Director - lecturer per M3

Mirko Lapi CEO Proteggimi Srl | Docente universitario | Co-founder & Presidente OSINTITALIA APS - lacturer per M6

Giuseppe Placanica - Cyber & R&D Director @ Silicondev | Head of Bachelor in Cybersecurity @ University of Malta | Scientific Coordinator & Lecturer @ ITS ICT Academy La Sapienza | Ethical Hacking & Cyber Assessment - lecturer per M5

Paolo Tarsitano - Ingegnere informatico, Cyber Security & Data Protection Advisor, formatore, socio Clusit, DPO - lecturer per M7 e M8

Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 25 di 31

Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 26 di 31

Allegato C

PIANO IMPIEGO DEL TEMPO
SENIOR LEADER CYBER 30.11-04.12 A.A. 26-27

Fase	Attività didattica	Sigla	Pre-corso	Lezioni/ verifiche	Attività applicative	Attività didattiche integrative	Studio indiv.	Periodi complessivi	CFU	SSD
In-Processing	Salluti istituzionali	-	0	0	0	1	0	1		-
Out-Processing	Preparazione + Test + Consegna attestati	-	0	0	0	3	1	4		-
Modulo didattico	MA1 – Governance e strategia della cybersecurity in Italia	MA1	0	3	0	0	2	5		INFO-01/A
	MA2 – Cenni sulla sicurezza informatica in un'organizzazione	MA2	0	3	0	0	2	5		INFO-01/A
	MA3 – Overview sulle iniziative NATO/UE/estere	MA3	0	3	0	0	2	5		INFO-01/A
	MA4 – Gestione del rischio, business continuity e disaster recovery	MA4	0	4	0	0	3	7		INFO-01/A
	MA5 – Overview sulle operazioni nel cyberspazio	MA5	0	4	0	0	3	7		INFO-01/A
	MA6 – Overview sulla Cyber Intelligence	MA6	0	3	0	0	2	5		INFO-01/A
	MA7 – Overview sulle attività di Cyber Influence	MA7	0	2	0	0	2	4		INFO-01/A
	MA8 – Capacità industriali nazionali nel settore cyber	MA8	0	2	0	0	1	3		INFO-01/A
	MA9 – Collaborazione con le università nel settore cyber	MA9	0	1	0	0	1	2		INFO-01/A
	Tabletop Ex	Ex	0	0	2	0	0	2		INFO-01/A
	Totale (1 settimana)		**0**	**25**	**2**	**4**	**19**	**50**	**2**	

Allegato D

PIANO DELLE AMMISSIONI PER IL CORSO DI ALTA FORMAZIONE "SENIOR LEADER CYBER"

N	ENTI COMPETENTI A EFFETTUARE LE SEGNALAZIONI NEI LIMITI DEI POSTI INDICATI	Nr. FRQ.	Nr. RIS.	ANNOTAZIONI
1	PRESIDENZA CONSIGLIO DEI MINISTRI	1	1	Incluso Uffici di diretta collaborazione, Dipartimenti e Uffici.
2	AGENZIA PER LA CYBERSICUREZZA NAZIONALE	4	2	
3	AGENZIA SPAZIALE ITALIANA	1	1	
4	MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE	1	1	
5	MINISTERO DEGLI AFFARI EUROPEI, SUD, POLITICHE DI COESIONE E PNRR	1	1	
6	MINISTERO DEGLI AFFARI REGIONALI E AUTONOMIE	1	1	
7	MINISTERO DELL'AGRICOLTURA, SOVRANITÀ ALIMENTARE E FORESTE	1	1	
8	MINISTERO DELL'AMBIENTE E SICUREZZA ENERGETICA	1	1	
9	MINISTERO DELLA CULTURA	1	1	
10	MINISTERO DELLA DIFESA	2	2	Gabinetto del Ministro e Uffici di Diretta Collaborazione, Uffici Centrali, Onorcaduti
11	MINISTERO DELL'ECONOMIA E DELLE FINANZE	1	1	
12	MINISTERO DELLA GIUSTIZIA	1	1	
13	MINISTERO DELLE IMPRESE E MADE IN ITALY	1	1	
14	MINISTERO DELE INFRASTRUTTURE E DEI TRASPORTI	1	1	Provvede anche per FS, ENAC e ANAS.
15	MINISTERO DELL'INTERNO	2	1	
16	MINISTERO DELL'ISTRUZIONE E MERITO	1	1	
17	MINISTERO DEL LAVORO E DELLE POLITICHE SOCIALI	1	1	
18	MINISTERO DELLA PROTEZIONE CIVILE E POLITICHE DEL MARE	1	1	
19	MINISTERO DELLA PUBBLICA AMMINISTRAZIONE	1	1	
20	MINISTERO DELLA SALUTE	1	1	
21	MINISTERO DELLO SVILUPPO ECONOMICO	1	1	
22	MINISTERO DEL TURISMO	1	1	
23	MINISTERO DELL'UNIVERSITÀ E DELLA RICERCA	1	1	
24	STATO MAGGIORE DELLA DIFESA	2	2	Provvede per l'Organizzazione Centrale e Intermedia dell'area tecnico-operativa ad eccezione degli EdO ivi riportati
25	COMANDO OPERATIVO DI VERTICE INTERFORZE	1	1	

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 28 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 27 di 31

N	ENTI COMPETENTI A EFFETTUARE LE SEGNALAZIONI NEI LIMITI DEI POSTI INDICATI	Nr. FRQ.	Nr. RIS.	ANNOTAZIONI
26	COMANDO PER LE OPERAZIONI IN RETE	2	1	
27	COMANDO INTERFORZE PER LE OPERAZIONI DELLE F.S.	1	1	
28	COMANDO PER LE OPERAZIONI SPAZIALI	1	1	
29	CENTRO ALTI STUDI DIFESA	1	1	
30	SCUOLA TLC DELLE F.A.	1	1	
31	SCUOLA INTERFORZE PER LA DIFESA NBC	1	1	
32	SCUOLA DI AEROCOOPERAZIONE	1	1	
33	SEGRETERIATO GENERALE DELLA DIFESA	2	1	
34	DIREZIONE NAZIONALE DEGLI ARMAMENTI	2	1	
35	ESERCITO ITALIANO - DIREZIONE PER IMPIEGO PERSONALE ESERCITO (DIPE)	2	1	Provvedono per il personale in servizio presso le proprie articolazioni.
36	MARINA MILITARE - DIREZIONE PER L'IMPIEGO DEL PERSONALE MILITARE DELLA MARINA (MARIPERS)	2	1	
37	AERONAUTICA MILITARE - DIREZIONE PER IMPIEGO PERSONALE MILITARE AERONAUTICA (DIPMA)	2	1	
38	ARMA DEI CARABINIERI	2	1	
39	GUARDIA DI FINANZA	2	1	
40	COMANDO GENERALE DEL CORPO DELLE CAPITANERIE DI PORTO	1	1	
41	CORPO MILITARE DELLA CROCE ROSSA ITALIANA	1	1	
42	VOLONTARI DI CROCE ROSSA ITALIANA	1	1	
43	UNIVERSITÀ	2	1	
44	INDUSTRIE / IMPRESE (tramite AIAD)	4	2	
	TOTALI	**62**	**48**	

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 29 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 28 di 31

Allegato E

FASCICOLO
PER LA SEGNALAZIONE DEL CANDIDATO AL

CORSO DI ALTA FORMAZIONE

"SENIOR LEADER CYBER"

Il fascicolo per la segnalazione del candidato si compone dei seguenti documenti, da compilare e sottoscrivere seguendo le indicazioni contenute:

- scheda di pre-iscrizione del candidato;
- dichiarazione sostitutiva della certificazione del titolo di studio.

Il fascicolo per la segnalazione del candidato deve essere inviato ai seguenti indirizzi *e-mail*:

A:
Centro Alti Studi Difesa/Scuola Superiore Universitaria
Direzione Alta Formazione e Ricerca
Segreteria Studenti
e-mail certificata difealtistudi@postacert.difesa.it
e-mail segreteriastudenti@unicasd.it

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 30 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 29 di 31

segue **Allegato E**

foto digitale formato tessera	**A Centro Alti Studi Difesa/Scuola Superiore Universitaria** **Direzione Alta Formazione e Ricerca** **Segreteria Studenti** difesaltistudi@postacert.difesa.it; segreteriastudenti@unicasd.it SCHEDA DI PRE-ISCRIZIONE DEL CANDIDATO AL CAF **SENIOR LEADER CYBER** Organizzazione di appartenenza / Privato

Grado / Titolo ..... C.F. .....

Cognome ..... Nome .....

nato/a il ..... a ..... cittadinanza .....

Doc. di riconoscimento (tipo) ..... Nr .....

rilasciato da ..... il ..... scadenza il .....

Indirizzo .....

C.A.P. ..... Città ..... Prov./Stato estero ..... Telefono .....

e-mail .....

(all'*e-mail* indicata verranno inviate le comunicazioni della Direzione del Corso, nonché il *link* per accedere alla piattaforma del CASD. Considerato che non verranno trattati argomenti classificati, si suggerisce di indicare una *e-mail* personale, in quanto le *e-mail* istituzionali hanno un elevato grado di protezione e talune volte identificano come "spam" le comunicazioni inviate dalla Direzione del Corso a tutti i frequentatori)

Telefono cellulare (per eventuale reperibilità durante il corso) .....

Ente di appartenenza .....

Incarico/Posizione .....

Tipo di laurea: Triennale ☐ Magistrale ☐ Vecchio Ord. ☐

facoltà .....

Allega i seguenti documenti compilati e firmati:

- "Dichiarazione sostitutiva della certificazione del titolo di studio".

Il candidato dichiara di aver preso visione e accettare quanto contenuto nei Lineamenti didattici del Corso.

Luogo e Data

In Fede

L'Ente di appartenenza dovrà consentire al frequentatore la partecipazione a tutte le attività didattiche previste nei Lineamenti, che possono essere organizzate in differenti modalità (in presenza, a distanza, *e-learning*, ricerca e studio, conferenze, *workshop*, *webinar*, etc.).

Luogo e Data

VISTO
IL COMANDANTE/IL DIRIGENTE
RESPONSABILE

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 31 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 30 di 31

segue **Allegato E**

DICHIARAZIONE SOSTITUTIVA DELLA CERTIFICAZIONE DEL TITOLO DI STUDIO
(Art. 46 - lettera l, m, n - D.P.R. 28 dicembre 2000, n. 445)

Il/la

sottoscritto/a_____

nato/a a (_____) il _____

residente a (_____) in Via_____ n°_____

consapevole che chiunque rilascia dichiarazioni mendaci è punito ai sensi del codice penale e delle leggi speciali in materia, ai sensi e per gli effetti dell'art. 46 D.P.R. n. 445/2000,

DICHIARA

DI AVER:

Conseguito il/la [1] _____

in _____

in data _____/_____/_____ presso_____

con il seguente punteggio_____

Esente da imposta di bollo ai sensi dell'art. 37 D.P.R. 28 dicembre 2000, n. 455

_____ li, _____

_____

Firma del dichiarante (per esteso e leggibile) *

Si allega copia di un documento d'identità valido

*La firma non va autenticata, né deve necessariamente avvenire alla presenza dell'impiegato dell'Ente che ha richiesto il certificato.

[1] Laurea (L, 1° ciclo), Laurea Magistrale (LM, 2° ciclo), laurea vecchio ordinamento.

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 32 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Lineamenti_didattici_SENIOR_LEADER_CYBER.pdf pag. 31 di 31

Allegato "A"

ELENCO INDIRIZZI

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
Ufficio del Consigliere Militare
Palazzo Chigi - Piazza Colonna
00187 ROMA

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
Dipartimento della funzione pubblica
Palazzo Vidoni, Corso Vittorio Emanuele II, 116
00186 Roma

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
Dipartimento della Protezione Civile
Via Ulpiano, 11
00193 ROMA

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
Corso d'Italia, 41
00198 ROMA

AGENZIA SPAZIALE NAZIONALE
Via del Politecnico
00133 ROMA

MINISTERO DEGLI AFFARI ESTERI
E DELLA COOPERAZIONE INTERNAZIONALE
Gabinetto del Ministro
Piazzale della Farnesina, 1
00194 ROMA

MINISTERO DEGLI AFFARI ESTERI
E DELLA COOPERAZIONE INTERNAZIONALE
Direzione Generale per gli Affari Politici e di Sicurezza
Piazzale della Farnesina, 1
00194 ROMA

MINISTERO DEGLI AFFARI ESTERI
E DELLA COOPERAZIONE INTERNAZIONALE
Direzione Generale per la Cooperazione allo Sviluppo
Piazzale della Farnesina, 1
00194 ROMA

MINISTERO DEGLI AFFARI EUROPEI, SUD, POLITICHE DI COESIONE E PNRR
Largo Chigi, 19
00186 ROMA

MINISTERO DEGLI AFFARI REGIONALI E AUTONOMIE
Via della Stamperia, 8
00187 Roma

MINISTERO DELL'AGRICOLTURA, SOVRANITÀ ALIMENTARE E FORESTE
Via XX Settembre, 20
00187 Roma

MINISTERO DELL'AMBIENTE E SICUREZZA ENERGETICA
Segreteria del Ministro
Via Cristoforo Colombo, 44
00147 ROMA

MINISTERO DELLA CULTURA
Via del Collegio Romano, 27
00186 ROMA

MINISTERO DELLA DIFESA
Gabinetto del Ministro
Via XX Settembre, 8
00187 ROMA

MINISTERO DELLA DIFESA
Segretariato Generale della Difesa / DNA
Via di Centocelle, 301
00175 ROMA

MINISTERO DELL'ECONOMIA E DELLE FINANZE
Gabinetto del Ministro
Via XX Settembre 97
00187 ROMA

MINISTERO DELLA GIUSTIZIA
Via Arenula, 70
00186 ROMA

MINISTERO DELLE IMPRESE E DEL MADE IN ITALY
Via Veneto, 33
00187 ROMA

MINISTERO DELLE INFRASTRUTTURE E DEI TRASPORTI
Organo Centrale di Sicurezza
Viale del Policlinico, 2
00161 ROMA

MINISTERO DELL'INTERNO
Dipartimento di Pubblica sicurezza
Piazza del Viminale, 1
00184 ROMA

MINISTERO DELL'INTERNO
Dipartimento dei VVFF, del Soccorso Pubblico e della Difesa Civile - Direzione Centrale della Difesa Civile
Via Cavour, 5
00184 ROMA

MINISTERO DELL'INTERNO
Dipartimento per le Politiche del Personale l'Amministrazione Civile e per le Risorse Strumentali e Finanziarie
Piazza del Viminale, 1
00184 ROMA

MINISTERO DELL'ISTRUZIONE DEL MERITO
Viale Trastevere, 76/A
00153 ROMA

MINISTERO DEL LAVORO E DELLE POLITICHE SOCIALI
Via Vittorio VENETO, 56
00187 ROMA

MINISTERO DELLA PROTEZIONE CIVILE E POLITICHE DEL MARE
Largo Chigi, 19
00187 ROMA

MINISTERO DELLA PUBBLICA AMMINISTRAZIONE
Corso Vittorio EMANUELE II, 116
00186 ROMA

MINISTERO DELLA SALUTE
Direzione Generale della Prevenzione Sanitaria
Viale Giorgio Ribotta, 5
00144 ROMA

MINISTERO DEL TURISMO
Via di Villa Ada, 55
00199 ROMA

MINISTERO DELL'UNIVERSITÀ E DELLA RICERCA
Largo Antonio RUBERTI, 1
00153 ROMA

STATO MAGGIORE DELLA DIFESA
I Reparto Personale - Ufficio Formazione-
Via XX Settembre, 11
00187 ROMA

COMANDO PER LE OPERAZIONI IN RETE
Via Stresa, 31/B
00135 ROMA

COMANDO PER LE OPERAZIONI SPAZIALI
Via XX Settembre, 123/A
00187 ROMA

STATO MAGGIORE DELL'ESERCITO
Dipartimento Impiego del Personale dell'Esercito
Via XX Settembre, 123
00187 ROMA

DIREZIONE PER L'IMPIEGO DEL PERSONALE MILITARE DELLA MARINA
Piazzale della Marina, 4 - 00196 ROMA

DIREZIONE IMPIEGO PERSONALE MILITARE AERONAUTICA
Viale dell'Università, 4 - 00185 ROMA

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 33 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Elenco_indirizzi(1).pdf pag. 1 di 2
Digitally signed by GIUSEPPE URBANO
Date: 2026.10.08 11:11:23 CEST

COMANDO GENERALE DELL'ARMA DEI CARABINIERI
Viale Romania, 45
00197 ROMA

COMANDO OPERATIVO DI VERTICE INTERFORZE
Via di Centocelle, 301
00175 ROMA

COMANDO INTERFORZE PER LE OPERAZIONI DELLE FORZE SPECIALI
Via di Centocelle 301
00175 – ROMA

COMANDO GENERALE DELLA GUARDIA DI FINANZA
Viale XXI aprile, 51 - 00162 ROMA

FEDERAZIONE AZIENDE ITALIANE PER L'AEROSPAZIO LA DIFESA E LA SICUREZZA (A.I.A.D.)
Via Nazionale, 54
00184 - ROMA

Per estensione di copia interna:

CENTRO ALTI STUDI PER LA DIFESA
- Reparto di Presidenza SEDE
- Quartier Generale SEDE
- IASD SEDE
- ISSMI SEDE
- IRAD SEDE
- CEFLI SEDE

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 34 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_Elenco_indirizzi(1).pdf pag. 2 di 2

M_D A349694 REG2026 0007273 08-10-2026

Centro Alti Studi Difesa

Scuola Superiore Universitaria

Direzione Alta Formazione e Ricerca

Indirizzo postale: Piazza della Rovere, n. 83 – 00165 ROMA
Posta elettronica: difealtistudi@casd.difesa.it
Posta elettronica certificata: difealtistudi@postacert.difesa.it
PdC: Col. Giuseppe URBANO Tel. 06.4691.3031
e-mail: diafr.uppd.capo@casd.difesa.it

All.: 2 (due)

OGGETTO: Corso di Alta Formazione "*Senior Leader Cyber*" - Anno Accademico 2026-2027.

A (ELENCO INDIRIZZI - **ALLEGATO "A"**)
^^^^^^^^

1. Il Centro Alti Studi Difesa/Scuola Superiore Universitaria a Ordinamento Speciale (CASD/SSUOS), nella sua duplice veste di istituzione di alta formazione militare e universitaria, ha l'obiettivo di formare una dirigenza militare e civile altamente qualifica, in un contesto intergovernativo, interagenzia e internazionale, consapevole dei rapidi cambiamenti, capace di sviluppare un pensiero critico e predisposta all'innovazione. Questa doppia anima, che coniuga il *mindset* militare tipicamente strategico e pragmatico con l'approccio scientifico e critico del mondo accademico, garantisce al CASD/SSUOS la potenzialità di agire quale propulsore della formazione di livello strategico, della ricerca e della consulenza a favore della Difesa e del Paese.
2. Per quanto attiene al dominio cibernetico, questo Centro – responsabile del "Polo Formativo *Cyber* della Difesa" – per l'A.A. 2026-27 ha programmato l'erogazione in presenza del Corso di Alta Formazione (CAF) "***Senior Leader Cyber***" (**30 novembre – 4 dicembre 2026**) (Lineamenti didattici in **Allegato B**), con l'obiettivo di sviluppare figure a livello dirigenziale in grado di comprendere e governare le dimensioni operative, tecnologiche, organizzative e normative del dominio cibernetico, rafforzando, le capacità di prevenzione, analisi, decisione e risposta alle minacce *cyber* in un contesto interforze, interagenzia e internazionale.
3. Il Corso è rivolto a Ufficiali Superiori/Generali e/o Funzionari/Dirigenti civili dell'Amministrazione Difesa/Guardia di Finanza (a titolo gratuito) e Funzionari/Dirigenti delle altre Amministrazioni/Enti Pubblici e mondo accademico/industriale (a titolo oneroso), in accordo al piano delle ammissioni (All. D ai Lineamenti). Le segnalazioni, nei numeri espressi nel piano delle ammissioni, dovranno essere inoltrate all'indirizzo di porta certificata difealtistudi@postacert.difesa.it e ordinario segreteriastudenti@unicasd.it entro le ore **23:59 del 22 novembre 2026**, complete del "Fascicolo per la segnalazione del candidato" (All. E ai Lineamenti).
4. Per ogni ulteriore dettaglio e aspetti amministrativi si invita a consultare i **Lineamenti didattici** del Corso (**cit. All. B**) e a prendere contatto con la Segreteria Studenti per informazioni.

d'ordine
IL DIRETTORE
(Contrammiraglio Gaetano VIRGILIO)

Digitally signed by GIUSEPPE URBANO
Date: 2026.10.08 11:11:23 CEST

Documento non idoneo alla verifica della firma digitale.
Document not suitable for digital signature verification.

Ministero della Giustizia - Allegato_m_dg.GDAP.03-11-2026.0499168.U_BANDO_CAF_"SENIOR_LEADER_CYBER".pdf pag. 35 di 35
Ministero della Giustizia - Allegato_m_dg.GDAP.12-10-2026.0459193.E_perstampa_Lettera_Corso_Senior_Leader_Cy.pdf pag. 1 di 1