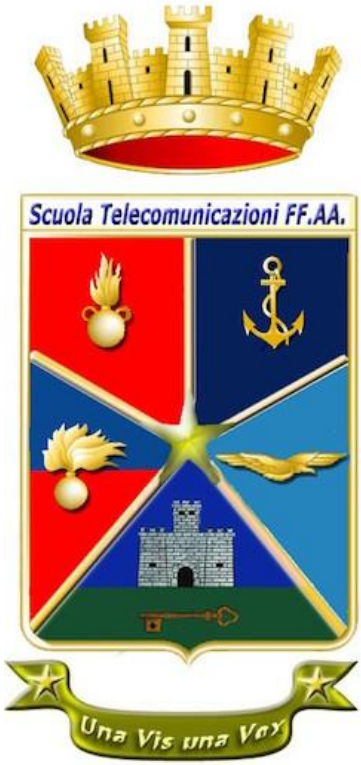
SCUOLA TELECOMUNICAZIONI FF.AA.
E
POLO FORMATIVO CYBER



Calendario dei Corsi Interforze
A.A. 2026

Edizione novembre 2025

Scuola Telecomunicazioni FF.AA.

ATTO DI APPROVAZIONE

Approvo il Calendario dei Corsi della Scuola Telecomunicazioni Forze Armate e Polo Formativo Cyber in Chiavari per l'Anno Accademico 2026.

Chiavari, 14.11.2025

IL COMANDANTE

C.V. Stefano COSSU

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

1	
2	
3	
4	
5	
6	
7	
8	

ELENCO DI DISTRIBUZIONE

SEGRETARIATO GENERALE DELLA DIFESA - I REPARTO
DIREZIONE GENERALE PER IL PERSONALE CIVILE
AGENZIA INDUSTRIE DIFESA

STATO MAGGIORE DELLA DIFESA
- UFFICIO GENERALE DEL CAPO DI SMD
- I REPARTO PERSONALE
- II REPARTO INFORMAZIONI E SICUREZZA
- III REPARTO DIREZIONE STRATEGICA E COOPERAZIONE MILITARE
- REPARTO PIANIFICAZIONE GENERALE
- VI REPARTO INFORMATICA, CYBER E TELECOMUNICAZIONI

COMANDO OPERATIVO DI VERTICE INTERFORZE
COMANDO INTERFORZE PER LE OPERAZIONI DELLE FORZE SPECIALI
COMANDO PER LE OPERAZIONI IN RETE
CENTRO ALTI STUDI PER LA DIFESA E SCUOLA SUPERIORE UNIVERSITARIA A ORDINAMENTO SPECIALE DELLA DIFESA
COMANDO DELLE OPERAZIONI SPAZIALI

STATO MAGGIORE DELL'ESERCITO - DIPARTIMENTO IMPIEGO DEL PERSONALE

COMANDO SCUOLE DELLA MARINA MILITARE
DIREZIONE PER L'IMPIEGO DEL PERSONALE MILITARE DELLA MARINA
STATO MAGGIORE DELLA MARINA - REPARTO C4S

STATO MAGGIORE DELL'AERONAUTICA - REPARTO GENERALE SICUREZZA
COMANDO LOGISTICO DELL'AERONAUTICA - 3^ DIVISIONE

COMANDO GENERALE DELL'ARMA DEI CARABINIERI
- UFFICIO ADDESTRAMENTO E REGOLAMENTI
- UFFICIO SICUREZZA
- UFFICIO SVILUPPO TECNOLOGICO

COMANDO GENERALE DELLE CAPITANERIE DI PORTO

BRIGATA DI SUPPORTO AL NRDC-ITA
ITALIAN NATIONAL SUPPORT ELEMENT – ALLIED JFC BRUNSSUM (NLD)
QUARTIER GENERALE ITALIANO - ALLIED JFC NAPLES
NATO SECURITY FORCE ASSISTANCE COE (SFA COE)
NATO MODELLING AND SIMULATION COE (M&S COE)

ISTITUZIONI/ALTRI ENTI/COMANDI/AMMINISTRAZIONI DELLO STATO

PRESIDENZA DELLA REPUBBLICA - SEGRETARIATO GENERALE

PRESIDENZA DEL CONSIGLIO DEI MINISTRI - UFFICIO DEL SEGRETARIO GENERALE

MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE

DIPARTIMENTO DI PUBBLICA SICUREZZA
DIREZIONE CENTRALE DEI SERVIZI TECNICO LOGISTICI E DELLA GESTIONE PATRIMONIALE

COMANDO GENERALE GUARDIA DI FINANZA

DIPARTIMENTO DELL'AMMINISTRAZIONE PENITENZIARIA
DIREZIONE GENERALE DEL PERSONALE E DELLE RISORSE
UFFICIO VIII – SEZIONE TELECOMUNICAZIONI

DIPARTIMENTO DEI VIGILI DEL FUOCO SOCCORSO PUBBLICO E DIFESA CIVILE
DIREZIONE CENTRALE DELLE RISORSE LOGISTICHE E STRUMENTALI
UFFICIO MEZZI MATERIALI ED ATTREZZATURE – SEZIONE TELECOMUNICAZIONI

CORPO MILITARE ACISMOM

Sommario

1. PREMESSA

a. Il presente documento ha lo scopo di fornire la programmazione di dettaglio dei corsi che saranno erogati da questo Istituto nell'anno accademico 2026 e riporta, inoltre, le indicazioni dell'*iter* da seguire per segnalare il personale designato alla frequenza dei corsi e per l'accertamento dei requisiti richiesti. In **annesso "A"** è riportato lo sviluppo dei corsi del Calendario 2026 in formato grafico e in **annesso "B"** sono riportate le schede analitiche riepilogative di ogni singolo corso contenenti i requisiti richiesti per l'ammissione alla frequenza, le date di svolgimento e le assegnazioni dei posti destinati ad ogni Ente Programmatore.
Il presente Calendario dei Corsi 2025 è pubblicato, in formato Adobe Acrobat (pdf), nei seguenti siti istituzionali:

- www.difesa.it
- www.marina.difesa.it

Ulteriori informazioni possono essere chieste alla Direzione Corsi della Scuola ai seguenti punti di contatto:

Segreteria Nucleo Studi, Programmazione e Innovazione

– Rete civile 0185-3334509/510
– Sotrin 72-28509/510
– Rinam 8000+7228509/510 (diretto);
– Rete M.M. 72-28509/510
– E-mail stelmilit.corsi@marina.difesa.it

Segreteria Nucleo Coordinamento Didattico

– Rete civile 0185-3334457/511
– Sotrin 72-28457/511
– Rinam 8000+7228457/511 (diretto);
– Rete M.M. 72-28457/511
– E-mail stelmilit.corsi@marina.difesa.it

b. Sono di seguito elencati gli Enti della Difesa e di altre Amministrazioni dello Stato preposti all'individuazione delle esigenze di partecipazione ai corsi e responsabili dell'iscrizione e della comunicazione dei frequentatori alla Scuola[1].

1) Ministero della Difesa

– Segretariato Generale della Difesa - I Reparto;
– Direzione Generale per il Personale Civile;
– Agenzia Industrie Difesa.

[1] Per il Corso "Operatori Cyber della Difesa" la responsabilità è unicamente di SMD I Reparto.

2) <u>Difesa</u>

– Stato Maggiore della Difesa:
  - I Reparto - Personale;
  - II Reparto - Informazioni e Sicurezza;
  - III Reparto - Direzione Strategica e Cooperazione Militare;
  - Reparto Pianificazione Generale
  - VI Reparto – Informatica, Cyber e Telecomunicazioni;
– Comando Operativo di Vertice Interforze (COVI);
– Comando Interforze per le Operazioni delle Forze Speciali (COFS);
– Comando per le Operazioni in Rete (COR);
– Centro Alti Studi per la Difesa (CASD) e Scuola Superiore Universitaria a Ordinamento Speciale della Difesa;
– Comando delle Operazioni Spaziali (COS);

3) <u>Esercito</u>

– Stato Maggiore dell'Esercito - Dipartimento Impiego del Personale – Ufficio Formazione e Politica d'impiego;

4) <u>Marina Militare</u>

– Comando Scuole della Marina Militare;
– Direzione per l'impiego del Personale della Marina Militare;
– Stato Maggiore Marina - Reparto C4S;

5) <u>Aeronautica Militare</u>

– Stato Maggiore dell'Aeronautica - Reparto Generale Sicurezza (per i soli corsi dell'area INFOSEC);
– Comando Logistico - III Divisione.

6) <u>Arma dei Carabinieri</u>

– Comando Generale dell'Arma dei Carabinieri:
  - S.M. - Ufficio Addestramento e Regolamenti;
  - S.M. - Ufficio Sicurezza;
  - Ufficio Sviluppo Tecnologico.

7) <u>Capitanerie di Porto</u>

– Comando Generale delle Capitanerie di Porto.

8) <u>Comandi NATO / Organismi Internazionali</u>

– Brigata di supporto al NRDC-ITA;
– Italian National Support Element – Allied JFC Brunssum (NLD)
– Quartier Generale Italiano – Allied JFC Naples;
– NATO Security Force Assistance COE (SFA COE);
– NATO Modelling & Simulation COE (M&S COE).

c. Gli Enti assegnatari dei posti, al fine di agevolare il compito organizzativo della Scuola Telecomunicazioni ed ottimizzare le risorse economiche, sono tenuti a:

- *assicurare* la copertura totale dei posti loro assegnati prevedendo anche un'aliquota di riserva in caso di indisponibilità dei discenti inizialmente individuati per la frequenza dei corsi;
- *segnalare,* almeno 3 settimane prima dell'inizio del corso, i dati richiesti per ciascun frequentatore secondo quanto indicato al successivo para 4;
- *comunicare* tempestivamente l'indisponibilità del proprio personale designato. In caso di mancata segnalazione del discente o di un suo sostituto la Scuola provvederà a riassegnare tale posto;
- *segnalare,* per i corsi che lo richiedono, il possesso dei requisiti di sicurezza del personale frequentatore;
- *certificare* il possesso dei requisiti professionali del personale frequentatore.

2. VALUTAZIONI DEI CORSI E PROPOSTE SVOLGIMENTO DI NUOVI CORSI

Gli Enti Programmatori possono avanzare a SMD I Reparto richieste di svolgimento di nuovi corsi nel settore *Information Technologies* (IT) *e Cyber*. Successivamente, valutata la fattibilità e la sua rispondenza a nuove esigenze tecnico/operative con il personale della Direzione Corsi della Scuola, il nuovo corso sarà inserito nella prima edizione favorevole del Catalogo dei Corsi della Scuola.

3. NOTIZIE LOGISTICHE/AMMINISTRATIVE

a. Utilizzo risorse

Al fine di razionalizzare l'impiego delle risorse disponibili, corre l'obbligo di sensibilizzare gli Enti Programmatori al rigoroso rispetto della programmazione dei corsi, in stretta aderenza alle indicazioni di dettaglio inserite in questo documento, al fine di raggiungere l'obiettivo comune che è la formazione del personale dipendente.

b. Oneri di viaggio, vitto e alloggio

Gli oneri di viaggio e di diaria sono a carico degli Enti Programmatori di appartenenza del frequentatore e questo Istituto non può pertanto intervenire nel processo di liquidazione dei documenti di viaggio del personale discente.

Il personale designato alla frequenza di corsi dovrà presentarsi munito di Foglio di Viaggio che comprenda tutto il periodo di durata dell'attività, così come definito nelle schede di cui all'annesso "B".

Le fasi frontali dei corsi erogati presso questa Scuola sono svolte interamente nelle aule e nei laboratori dell'Istituto ad eccezione di alcuni periodi dedicati all'esecuzione di visite addestrative presso altri Enti della Difesa e/o Aziende civili site in località raggiungibili in giornata con i mezzi di trasporto collettivo della Scuola. Le località dove si svolgeranno le predette visite addestrative, indicate nel presente Calendario dei Corsi, dovranno essere riportate dall'Ente/Comando di appartenenza sul predetto Foglio di Viaggio del frequentatore. Eventuali interruzioni della frequenza dei corsi da parte dei discenti, per concomitanti attività esterne alla Scuola (concorsi, citazioni testi, attività di servizio, ecc.), dovranno essere

comunicate, con la massima urgenza, al Comando della Scuola (*email PEI* *stelmilit@marina.difesa.it* - *PEC* *stelmilit@postacert.difesa.it*) dal Comando del discente, indicando la natura dell'esigenza, la data di esecuzione ed il suo periodo massimo di svolgimento. L'emissione del relativo Foglio di Viaggio sarà a cura del Comando di appartenenza del discente e STELMILIT, nel caso in cui l'assenza dal corso per missione superi il tetto massimo di assenza previsto dal Catalogo dei Corsi 2026, segnalerà al discente e al suo Comando le conseguenti dimissioni d'autorità dal corso.
Le eventuali richieste di Licenza Straordinaria da parte dei discenti saranno concesse da questa Scuola solo dopo aver ricevuto il "Nulla Osta" da parte dei relativi Comandi di appartenenza.
Infine, ai frequentatori, di corsi interforze svolti in presenza, non è consentito assentarsi, per nessun motivo, nei giorni d'esame pena il mancato rilascio del diploma/attestato di fine corso e quindi la relativa impossibilità di iscrivere a matricola il corso frequentato (non saranno organizzate sessioni d'esami prima o dopo il corso).
I frequentatori militari e civili dell'A.D., potranno fruire delle strutture logistiche alloggiative (laddove possibile) e di ristorazione di STELMILIT con oneri a carico dell'Amministrazione.
La Scuola offre un servizio di mensa, dal lunedì alla domenica (compresi i giorni festivi), gestito da una ditta convenzionata.
Il personale frequentatore non appartenente all'A.D., laddove possibile, è autorizzato alla fruizione del pasto meridiano presso la mensa della Scuola a titolo oneroso, previa prenotazione e relativo pagamento. L'importo, determinato annualmente dalle SS.AA., dovrà essere versato presso la Cassa della Scuola che emetterà un'apposita quietanza.
La Scuola non fornisce ai frequentatori effetti di vestiario e materiali per l'igiene personale.
Le tipologie delle sistemazioni alloggiative per i frequentatori sono:

- Camere doppie con bagno in comune in camera;
- Camere singole con bagno in camera.

Le assegnazioni dei precitati alloggi, con particolare riferimento alle loro tipologie, sono effettuate dal Nucleo Accasermamento, Vettovagliamento e Alloggi della Scuola tenendo conto del grado del frequentatore, della durata del corso e di eventuali esigenze alloggiative straordinarie del Comando della Scuola.

4. MODALITÀ PER LA SEGNALAZIONE DEI FREQUENTATORI E REQUISITI PER L'AMMISSIONE

a. Segnalazione

(1) Le Autorità preposte dovranno segnalare il nominativo del personale designato con un anticipo di almeno 3 settimane dall'inizio del corso. La segnalazione dovrà essere formalizzata con l'invio del messaggio il cui *facsimile* è posto al para. 5 del presente Calendario. In alternativa al Message Handling sarà possibile inviare il predetto messaggio a mezzo sistema documentale o posta elettronica istituzionale ai seguenti indirizzi stelmilit@postacert.difesa.it (PEC) o stelmilit@marina.difesa.it (PEI).

(2) Particolare attenzione dovrà essere posta nella compilazione e successivo inoltro a STELMILIT, anch'essa con un anticipo di almeno 3 settimane dall'inizio del corso, della Scheda Anagrafica del discente posta al para. 6.

(3) Il ritardo nella segnalazione nei termini di cui sopra del personale designato per la frequenza di corsi, può comportare la riassegnazione del proprio posto ad un altro Comando/Ente in lista d'attesa.

(4) In caso di attivazione, per i *Master*/Corsi di Formazione Specialistica in convenzione con le Università, l'iscrizione ai corsi/*master* dovrà avvenire direttamente sulla piattaforma informatica degli atenei in convenzione.
Le istruzioni iniziali per raggiungere il sito *web* dell'Università, dove sarà pubblicato il bando con tutte le informazioni di dettaglio, saranno indicate sui messaggi di attivazione dei corsi universitari editi da questo Istituto.
Il frequentatore, una volta completato l'*iter* di iscrizione al corso con gli atenei, dovrà darne comunicazione, a mezzo *email*, al seguente indirizzo di posta elettronica: stelmilit.corsi@marina.difesa.it. Si rammenta che la Scuola non può intervenire in nessun modo nei processi di iscrizione dei frequentatori alle università che sono sotto l'esclusiva diretta responsabilità degli atenei stessi.

b. <u>Requisiti per l'ammissione ai corsi interforze</u>

(1) È fatto obbligo ai Comandi/Enti di appartenenza dei discenti di:
- accertare il possesso dei requisiti di sicurezza ai singoli corsi dei propri dipendenti (para CHARLIE del messaggio, *facsimile* al para. 5);
- certificare, il possesso dei requisiti professionali del personale frequentatore (para DELTA del messaggio, *facsimile* al para. 5);
- assicurare, la presa visione da parte del discente del documento "Vita d'Istituto" (para ECHO del messaggio, *facsimile* al para. 5);
- per i corsi in presenza assicurarsi che il frequentatore si accrediti preliminarmente alla piattaforma E-learning della Difesa (https://elearning.difesa.it).

(2) La Scuola può sottoporre i discenti a *test* di ingresso, il cui scopo è quello di verificare il loro livello di conoscenza in una determinata materia.

c. <u>Annullamento dei corsi a carattere universitario</u>

Qualora attivati, i Corsi ed i *Master* universitari saranno annullati qualora il numero dei frequentatori, segnalati e/o effettivamente presenti alla data di inizio del corso, risulti inferiore a 5 unità dandone immediata comunicazione a SMD I Reparto.

5. FORMATO DEL MESSAGGIO PER LA SEGNALAZIONE DEI NOMINATIVI

Il messaggio di segnalazione del nominativo del discente, da inviare utilizzando il SIC BAB, dovrà contenere le seguenti informazioni:

Oggetto: Segnalazione discente corso A.A. 2026

Riferimento: Catalogo dei Corsi Interforze di STELMILIT anni accademici 2026

ALFA: Nome del Corso che deve essere frequentato con indicazione del codice, sessione e data;

BRAVO: Grado, Cognome, Nome del discente, *e-mail* istituzionale/funzionale, Codice Fiscale, Ente/Comando di appartenenza;

CHARLIE: Indicare il possesso dei Requisiti di Sicurezza;

DELTA: Indicare il possesso dei Requisiti Professionali;

ECHO: Assicurare presa visione da parte dell'interessato del documento "Vita d'Istituto" raggiungibile con il link di seguito indicato:

https://www.difesa.it/smd/entimi/stelmilit/vita-d-istituto/27973.html

6. SCHEDA ANAGRAFICA DEL DISCENTE

La compilazione della Scheda Anagrafica da parte degli Enti/Comandi di appartenenza del discente riveste una grande importanza in quanto in essa sono contenuti i dati necessari per la redazione della prevista documentazione valutativa di fine corso dei discenti da parte di questo Istituto.
Tale Scheda, una volta compilata dal Comando di appartenenza del discente, dovrà essere inviata almeno 3 settimane prima dell'inizio del corso, al seguente indirizzo di posta elettronica stelmilit.corsi@marina.difesa.it o tramite il sistema documentale. La scheda è disponibile in formato elettronico sulla citata pagina "Vita d'Istituto".

SCUOLA TELECOMUNICAZIONI DELLE FF.AA.

DIREZIONE CORSI

Data di compilazione

A **Segreteria Studi**

stelmilit.corsi@marina.difesa.it
Tel. 72 28509/10 0185-3334509/10

SCHEDA ANAGRAFICA DEL FREQUENTATORE DI CORSI

Sessione e Nome del Corso

Forza Armata | Grado | Arma (solo E.I.)

Corpo | Ruolo | Posizione di Stato

Specializzazione

Nome (indicare tutti quelli in anagrafe) | Cognome

Data di nascita | Località di nascita | Prov.

Codice Fiscale | Tipo e n° doc. riconoscimento | Scadenza

Tel. Ufficio militare | Tel. Ufficio civile | Cellulare

e-mail Istituzionale (p.es. marco.rosso@marina.difesa.it oppure 3uff2sez@esercito.difesa.it)

Titolo di studio

Comando/Reparto di appartenenza

Il presente trattamento non si basa sul consenso dell'interessato, poichè necessario all'esecuzione di un contratto di cui l'interessato è parte (art. 6. co. 1 p.to b del Regolamento Generale sulla Protezione dei Dati UE/2016/679).

SCUOLA TELECOMUNICAZIONI DELLE FF.AA.
DIREZIONE CORSI

Comando/Reparto di appartenenza

Indirizzo postale (indicare Via/Piazza/... e numero civico)

CAP | **Località** | **Prov.**

Telefono Ufficio - linea militare | **Telefono Ufficio - linea civile**

PEC/PEI

Comando/Reparto dove dovrà essere inviata la documentazione di fine corso (campo da compilare, unitamente a quelli successivi, solo se diverso dall'Ente/Comando di appartenenza)

Indirizzo postale (indicare Via/Piazza/... e numero civico)

CAP | **Località** | **Prov.**

Telefono Ufficio - linea militare | **Telefono Ufficio - linea civile**

PEC/PEI

Parte da compilare a cura del Frequentatore una volta giunto a STELMILIT

Modello auto | **Targa auto** | **N° Passauto**

N° Passpersonale | **N° camera** | **Varie**

Il presente trattamento non si basa sul consenso dell'interessato, poichè necessario all'esecuzione di un contratto di cui l'interessato è parte (art. 6. co. 1 p.to b del Regolamento Generale sulla Protezione dei Dati UE/2016/679).

ANNESSO A - CALENDARIO IN FORMATO GRAFICO

SCUOLA TELECOMUNICAZIONE FF.AA. ANNO ACCADEMICO 2026

COD	CORSI	Durata (DAD+PRES.)	GENNAIO				FEBBRAIO				MARZO					APRILE				MAGGIO				GIUGNO					LUGLIO				AGOSTO				SETTEMBRE					OTTOBRE				NOVEMBRE				DICEMBRE				
	Data inizio settimana		05	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28
	TRANSPORT & NETWORKING																																																					
AE306A	MANUTENTORE FIBRE OTTICHE	1+2 asinc										1^					2^							3^														4^					5^													
R236B	FONDAMENTI IP ROUTING	1															1^																																						
R153I	FONDAMENTI DI CABLAGGIO STRUTTURATO	1																		1^							2^												3^																
R235I	PROGETTO GESTIONE RETI LOCALI ETHERNET	2							1^																					2^																	3^							
ER235I	PROPREDEUTICO RETI LOCALI ETHERNET	2+0 asinc			1^							2^												3^																										4^					
ER309B	FONDAMENTI DI TEORIA DELLE COMUNICAZIONI SATELLITARI E SISTEMA SICRAL	1+0 asinc				1^					2^												3^																																
EA001B	FREQUENCY SPECTRUM MANAGMENT	3+0 asinc						1^					2^																		3^																								

DAD

PRESENZA

SCUOLA TELECOMUNICAZIONE FF.AA. ANNO ACCADEMICO 2026

COD	CORSI	Durata (DAD+PRES.)	GENNAIO				FEBBRAIO				MARZO					APRILE				MAGGIO				GIUGNO					LUGLIO				AGOSTO				SETTEMBRE					OTTOBRE					NOVEMBRE				DICEMBRE				
	Data inizio settimana		05	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28
	SOFTWARE, APPLICATIVI E-LEARNING																																																					
T448I	INFORMATICO DI FA (MM)	3																																			1°					2°																
TE262A	S.O. SERVER IN NETWORKING	1+2 asinc/olt					1°				2°																																													
ET23B	S.O. LINUX BASE	2+0 asinc			1°			2°									3°														4°						5°																		
TE285A	SO LINUX	2+2 sincrono/olt									el		1°												el		2°																				el		3°								
ET291A	WS 2016 SERVER	4/olt																				1°																		2°																
ET295A	WS 2019 SERVER	1/olt																												1°		2°																						
ET298A	VIRTUALIZZAZIONE	1/olt																																			1°			2°															
ET299A	MICROSOFT EXCHANGE SERVER 2016/2019	1/olt																																				1°																
ET300A	SHAREPOINT 2016	1/olt																																										1°										
ET301A	PROVISIONING SQL DATABASES	1/olt																																											1°									
TE79I	APPLICAZIONI WEB	1+1 sincr/olt					1°							2°								3°																					4°									5°			
ET24B	ELEMENTI DI VIRTUALIZZAZIONE	1+0 asinc											1°				2°																																3°			4°				
ET18B	IT SPECIALIST	4+0 asinc					1°					2°																3°																										
ET17B	INFORMATICA DI BASE ICDL	5+0 asinc					1°															2°																																		

DAD

PRESENZA

SCUOLA TELECOMUNICAZIONE FF.AA. ANNO ACCADEMICO 2026

COD	CORSI	Durata (DAD+PRES.)	GENNAIO				FEBBRAIO				MARZO					APRILE				MAGGIO				GIUGNO					LUGLIO				AGOSTO				SETTEMBRE					OTTOBRE				NOVEMBRE				DICEMBRE				
	Data inizio settimana		05	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28
	INFOSEC E INFORMATION ASSURANCE																																																						
JE429A	KNMS 2100 IP	1+1 asinc																										1^			el	2^																el	3^							
J450A	IT-EKMS CUSTODE CIFRA PER UTENTI LDF DELLE FF.AA.	1																																								1^		2^													
JE427A	Op. CM 2000 IP	1+1 asinc				1^		2^		3^																																														
JE428A	Op. CM 2100 IP	1+1 asinc										1^		2^			3^		4^																													5^									
J439A	COMMON CRITERIA ITSEC	1																						1^													2^																		
J451A	UFF.li CIS	2			1^			2^				3^						4^			5^						6^										7^					8^				9^								
J447A	UFF.li COMSEC	2							1^									2^																			3^													4^					
J437A	CUST COMSEC CIFRA	2			1^									2^										3^																					4^									
EJ400B	SICUREZZA IT	2+0 asinc								1^							2^																																							

DAD

PRESENZA

SCUOLA TELECOMUNICAZIONE FF.AA. ANNO ACCADEMICO 2026

COD	CORSI	Durata (DAD+PRES.)	GENNAIO				FEBBRAIO				MARZO					APRILE				MAGGIO				GIUGNO					LUGLIO				AGOSTO				SETTEMBRE					OTTOBRE					NOVEMBRE				DICEMBRE				
	Data inizio settimana		05	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28
CYBER DEFENCE E LAW & FORENSICS																																																					
Y001A Y002A	OPERATORE CYBER DELLA DIFESA										1^ Livello BASE					1^ Livello BASE																				2° Livello SPECIALISTICO																	
YE447A	CYBER NETWORK PROTECTION	2												1^																																								
YE449I	VULNERABILITY ASSESMENT	3			1^																			2^																															
Y455A	CYBER THREAT HUNTING	2									1^																																											
Y445A	CSIRT	2																					1^							2^																								
EY18A	MALWARE ANALYSIS	3+0 sinc																				1^																																
EY456A	CHIEF INFORMATION SECURITY OFFICER	2+0 sinc																							1^																													
EY15A	DIGITAL FORENSICS	3+0 sinc																												1^																								
EY442B	FONDAMENTI di CD	1+0 sinc				1^		2^		3^										4^				5^																															

DAD

PRESENZA

SCUOLA TELECOMUNICAZIONE FF.AA. ANNO ACCADEMICO 2026

COD	CORSI	Durata (DAD+PRES.)	GENNAIO				FEBBRAIO				MARZO					APRILE				MAGGIO				GIUGNO					LUGLIO				AGOSTO				SETTEMBRE					OTTOBRE				NOVEMBRE				DICEMBRE				
	Data inizio settimana		05	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28
DATA SCIENCE E INTELLIGENZA ARTIFICIALE																																																						
X0004A	BIG DATA ANALYSIS	3+0 asinc																									1^																													
EX002B	FONDAMENTI di IA	1+0 asinc																																									1^					2^								

DAD

PRESENZA

ANNESSO B – SCHEDE CORSI

AREA TRANSPORT & NETWORKING

1. MANUTENTORE FIBRE OTTICHE - COD. AE306A

OBIETTIVI DEL CORSO
Fornire al personale frequentatore le principali nozioni inerenti agli impianti di trasmissione in fibra ottica, con riferimento ai materiali ed agli apparati utilizzabili, alle problematiche di realizzazione, d'installazione e di esercizio, anche attraverso attività di laboratorio.

DURATA: 1 settimana in modalità *e-learning* asincrono (15 ore in piattaforma) e 2 settimane in presenza. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 02 al 06 marzo in DAD e dal 09 al 20 marzo in presenza;

2ª – dal 07 al 10 aprile in DAD e dal 13 marzo al 24 aprile in presenza;

3ª – dal 18 al 22 maggio in DAD e dal 25 maggio al 05 giugno in presenza;

4ª – dal 14 al 18 settembre in DAD e dal 21 settembre al 02 ottobre in presenza;

5ª – dal 12 al 16 ottobre in DAD e dal 19 al 30 ottobre in presenza.

PARTECIPANTI (max 10)

COMANDI/ENTI	**Sessioni**				
	1ª	***2ª***	***3ª***	***4ª***	***5ª***
ESERCITO	3	3	2	3	3
MARINA MILITARE	2	2	2	2	1
AERONAUTICA	2	3	3	3	2
PERSOCIV					1
CONGEDATI	2	2	2	2	2
STELMILIT	1		1		
TOTALE	**10**	**10**	**10**	**10**	**9**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: possedere una buona conoscenza di sistemi di telecomunicazioni e sistemi di multiplazione TDM-FDM;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN ESAME FINALE.

2. PROPEDEUTICO RETI LOCALI ETHERNET - COD. ER235I

OBIETTIVI DEL CORSO

Il corso costituisce la prima fase di un percorso formativo più ampio, finalizzato alla capacità di progettare e gestire, in qualità di amministratore, reti LAN Ethernet. In particolare, il corso ha lo scopo di fornire una conoscenza di base delle Reti Locali Ethernet,a partire dalle tipologie dei mezzi trasmissivi utilizzati, con connessi fenomeni elettrici ed ottici, caratterizzanti le moderne tecnologie oggi impiegate nelle Reti IP. La trattazione del modello di riferimento ISO/OSI e di basilari concetti di protocollo fornisceal frequentatore nozioni fondamentali per comprendere il funzionamento e le interazioni tra i diversi livelli OSI, per arrivare ai concetti di indirizzo fisico e indirizzo logico e loro valenza inun ambiente di Virtual LAN. In ultimo verranno trattate le classi di reti ed il relativo indirizzamento IPv4.Sarà utilizzato software per la Simulazione reti Ethernet. Gli argomenti teorici sono propedeutici alla frequenza del corso progetto e gestione reti LAN Ethernet.

DURATA: 2 settimane in modalità *e-learning* sincrono. Le lezioni sincrone si svolgeranno in videoconferenza con modalità che saranno comunicate sulla piattaforma *e-learning* a cura del docente. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª - dal 19 al 30 gennaio in DAD;

2ª - dal 09 al 20 marzo in DAD;

3ª - dal 01 al 12 giugno in DAD;

4ª – dal 30 novembre al 11 dicembre in DAD.

PARTECIPANTI (max 12)

COMANDI/ENTI	**Sessioni**			
	1ª	***2ª***	***3ª***	***4ª***
ESERCITO	4		2	3
MARINA MILITARE	2	2	1	2
CAPITANERIE di PORTO	1	1		
AERONAUTICA	3	3	3	3
CARABINIERI			1	
SMD II		1	2	1
SGD		1		
COS		1	1	
COFS			1	
ITAQUARTIGEN				1
PERSOCIV	2	2		2
MAECI		1	1	
TOTALE	**12**	**12**	**12**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: N.N.;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

REQUISITI TECNICI

La banda necessaria minima per il corretto svolgimento delle attività è di 2 Mbps circa.

Si rammenta che la partecipazione alle attività sincrone (Contenuti in Piattaforma, Videoconferenze/Virtual Classroom), definite e comunicate dagli Istruttori, sono da considerarsi didatticamente ed amministrativamente parte integrante del corso stesso ed obbligatorie ai fini dell'accesso all'esame finale.
Inoltre, i discenti dovranno essere dotati di postazioni/client con hardware in grado di soddisfare le esigenze di connettività necessarie alla partecipazione alle VTC.

É PREVISTO UN TEST INTERMEDIO NON SBARRANTE E UN ESAME FINALE

3. PROGETTO E GESTIONE DI RETI LOCALI ETHERNET - COD. R235I

OBIETTIVI DEL CORSO

Introdurre il frequentatore alla fase di progettazione, di realizzazione e di manutenzione del cablaggio strutturato di una rete locale (LAN Ethernet) secondo gli Standard internazionali EIA/TIA e ISO/IEC, valutandone le prestazioni attraverso l'analisi di specifici parametri, attraverso apposita strumentazione professionale. Si prevede inoltre per gli apparati di rete la prima configurazione attraverso differenti metodi e successiva gestione, in riferimento ai più utilizzati protocolli nelle LAN, come lo *Spanning Tree*, l'Aggregazione dei Link e le Virtual Lan. In ultimo è contemplata l'analisi dei pacchetti catturati nella rete generati da protocolli di più alto livello della Architettura TCP/IP, con alcuni cenni al Routing IPv4.

DURATA: 2 settimane in presenza, percentuale di laboratorio 50%.

PERIODO SESSIONI:

1ª – dal 16 al 27 febbraio in presenza;

2ª – dal 13 al 24 luglio in presenza (sessione dedicata all'Accademia EI);

3ª – dal 09 al 20 novembre in presenza.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni		
	1ª	***2ª***	***3ª***
ESERCITO	4		5
EI – ACCADEMIA MILITARE		14	
MARINA MILITARE	2		1
CAPITANERIE di PORTO			
AERONAUTICA	2		3
SMD II	1		1
COVI			1
ITAQUARTIGEN	1		
PERSOCIV	1		1
MAECI	1		
TOTALE	**12**	**14**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva obbligatoria: Corso propedeutico reti locali Ethernet - COD. ER235I;
   b. Conoscenze basiche richieste: cablaggio strutturato rame; reti LAN switching Ethernet 802.3; indirizzamento/subnetting FLSM reti IP.;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN TEST D'INGRESSO E UN ESAME FINALE

4. FONDAMENTI DI CABLAGGIO STRUTTURATO - COD. R153I

OBIETTIVI DEL CORSO
Il corso, prevalentemente pratico e di laboratorio, mira ad introdurre il frequentatore alla fase di progettazione, realizzazione e manutenzione di un cablaggio strutturato di una rete locale (LAN) secondo gli standard attualmente in vigore.

DURATA: 1 settimana in presenza di cui 60% laboratorio.

PERIODO SESSIONI:
1ª – dal 04 al 08 maggio in presenza;
2ª – dal 22 al 26 giugno in presenza;
3ª – dal 28 settembre al 02 ottobre in presenza.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni		
	1ª	***2ª***	***3ª***
ESERCITO	3	3	2
MARINA MILITARE	1		
CAPITANERIE di PORTO	1		
AERONAUTICA	2	2	1
CARABINIERI	1	7	7
S.G.D.	1		
COVI	1		
COS	1		
PERSOCIV			1
MAECI	1		
CONGEDATI			1
TOTALE	**12**	**12**	**12**

REQUISITI PER L'AMMISSIONE:
1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: N.N.;
   c. Studio preventivo sinossi / testi propedeutici: N.N.;
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN ESAME FINALE.

5. FREQUENCY E SPECTRUM MANAGEMENT - COD. EA001B

OBIETTIVI DEL CORSO

Fornire le conoscenze fondamentali agli operatori di *Frequency e Spectrum Management* (FM/SM) del Comparto Difesa e Sicurezza impiegati sia in articolazioni centrali che periferiche. Il corso prevede l'acquisizione del necessario *know-how* in termini di fondamenti dottrinali e concettuali, riferimenti normativi primari nazionali e internazionali, procedure operative e standard di gestione, controllo di configurazione spettrale.
Il corso non prevede formazione teorica e/o pratica sugli applicativi di settore impiegati in operazioni, attualmente previsti nell'offerta didattica NATO.

DURATA: 3 settimane (2 settimane per la Scuola di Applicazione EI) in modalità *e-learning* asincrono (45 ore in piattaforma). Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 09 febbraio al 27 febbraio in DAD;

2ª – dal 16 marzo al 03 aprile in DAD;

3ª – dal 20 al 31 luglio in DAD (sessione dedicata alla Scuola di Applicazione dell'EI).

PARTECIPANTI (max 25) -

COMANDI/ENTI	Sessioni		
	1ª	***2ª***	***3ª***
ESERCITO	12	11	
EI- SCUOLA APPLICAZIONE			14
MARINA MILITARE	2	3	
AERONAUTICA	2	3	
CARABINIERI		1	
COS	2	2	
ITAQUARTIGEN	1		
PERSOCIV	2	1	
MAECI	1		
TOTALE	**22**	**21**	**14**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: N.N.;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa e della Guardia di Finanza, Polizia di Stato, Vigili del Fuoco, Polizia Penitenziaria e Presidenza del Consiglio dei Ministri, provenienti dall'area telecomunicazioni, impiegati o designati a ricoprire incarichi di *Frequency o Spectrum Management*.

È PREVISTO UN ESAME FINALE

6. FONDAMENTI DI TEORIA DELLE COMUNICAZIONI SATELLITARI E SISTEMA SICRAL - COD. ER309B

OBIETTIVI DEL CORSO

Fornire al personale frequentatore le nozioni fondamentali relative ai sistemi di comunicazione satellitare (meccanica orbitale, applicazioni e servizi di telecomunicazioni, tecniche trasmissive) con particolare riferimento al sistema SICRAL.

DURATA: 1 settimana in modalità *e-learning* asincrono (20 ore - non sono previste attività di laboratorio). Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 26 al 30 gennaio in DAD;

2ª – dal 02 al 06 marzo in DAD;

3ª – dal 25 al 29 maggio in DAD (sessione dedicata all' Accademia EI).

PARTECIPANTI (max 26)

COMANDI/ENTI	Sessioni		
	1ª	***2ª***	***3ª***
ESERCITO	8	8	
EI - ACCADEMIA MILITARE			14
MARINA MILITARE	2	3	
AERONAUTICA	7	8	
CARABINIERI	1	2	
SMD II	3	2	
PERSOCIV	4	1	
MAECI	1	1	
TOTALE	**26**	**25**	**14**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: Sufficienti conoscenze di sistemi di telecomunicazioni, tecniche di accesso a canali condivisi, modulazioni numeriche;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** Non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN ESAME FINALE

7. FONDAMENTI DI IP ROUTING- COD. R236B

OBIETTIVI DEL CORSO

Fornire al personale frequentatore le conoscenze base sui protocolli di *routing IP* per la gestione e la realizzazione di moderne reti IP di tipo LAN, concetti generali di una rete *WAN*, teoria sui protocolli di *routing* statico e dinamico, *routing* di tipo adattivo distribuito *Distance-Vector/Link-State*, architettura di *INTERNET* e gestione base di un router generico

.

DURATA: 1 settimana in presenza

PERIODO SESSIONI:

1ª – dal 13 al 17 aprile in DAD;

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni
	1ª
ESERCITO	3
MARINA MILITARE	1
AERONAUTICA	2
SMD II	1
COVI	1
CASD	1
COR	1
PERSOCIV	1
STELMILIT	1
TOTALE	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: Corso Progetto e Gestione di Reti Locali Cod. R235I o in alternativa essere in possesso delle conoscenze richieste al punto b;
   b. Conoscenze basiche richieste: Buona conoscenza dei protocolli *TCP/IP*, indirizzamento/*subnetting* IP e tecnologie di *LAN Ethernet;*
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** Non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN ESAME FINALE

AREA SOFTWARE, APPLICATIVI E-LEARNING

8. SISTEMI OPERATIVI SERVER IN NETWORKING - COD. TE262A

OBIETTIVI DEL CORSO

Portare il frequentatore a conoscenza delle principali tecniche per:

- far comunicare i diversi sistemi operativi utilizzando protocolli comuni;
- effettuare la configurazione e l'accesso alle reti LAN/WAN indipendentemente dall'ambiente.

DURATA: 1 settimana in modalità e-learning asincrono (15 ore) e 2 settimane in presenza. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI

1ª – dal 26 al 30 gennaio in DAD e dal 02 al 13 febbraio in presenza;

2ª – dal 02 al 06 marzo in DAD e dal 09 al 20 marzo in presenza.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni	
	1ª	**2ª**
ESERCITO	6	6
MARINA MILITARE	2	2
AERONAUTICA	1	1
CARABINIERI		1
MAECI	3	2
TOTALE	**12**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva:
      - Corso Windows Server per Amministratori;
      - corso Progettazione e gestione reti locali Cod.T235J;
      - Corso S.O. LINUX - COD. T285A.

   b. Conoscenze basiche richieste:

      In alternativa alla frequenza preventiva il frequentatore dovrà possedere un'ottima conoscenza degli ambienti server Microsoft/Linux e buona conoscenza dei protocolli di rete TCP/IP.

   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

REQUISITI TECNICI NECESSARI PER IL CORRETTO SVOLGIMENTO DELLA FORMAZIONE A DISTANZA

- Prima settimana: fase DAD asincrona (SCORM e contenuti in piattaforma).
  La banda necessaria, per il corretto svolgimento delle attività in *web streaming*, è di 2 Mbps circa.
- Seconda e terza settimana
  In presenza.

Requisiti Tecnici per l'accesso alla VPN dei laboratori remoti nel caso in cui venga attivata la modalità online training:

- Banda necessaria per il corretto svolgimento delle attività: 5 Mbps circa.
- Sui Client che utilizzeranno i discenti sarà necessario:
- assicurare la connettività di rete sulle porte logiche 443/TCP e 443/UDP necessarie per la connessione ai Lab remoti attestati sui gateway VPN STELMILIT;
- avere diritti/privilegi per poter installare il software Cisco Anyconnect VPN ed i relativi certificati digitali associati all'utente;
- avere diritti/privilegi per poter installare un client RDP (remote desktop) per il controllo dei PC collocati nell'aula fisica;
- utilizzare doppio monitor per le attività didattiche/laboratoriali

Tutto il software necessario al discente per il collegamento in VPN sarà scaricato automaticamente al primo accesso alla VPN e su indicazioni/istruzioni dei Docenti del corso.
Si rammenta che la partecipazione alle attività asincrone/sincrone (Contenuti in Piattaforma, Videoconferenze/Virtual Classroom), definite e comunicate dagli Istruttori, sono da considerarsi didatticamente ed amministrativamente parte integrante del corso stesso ed obbligatorie ai fini dell'accesso all'esame finale.
Inoltre, i discenti dovranno essere dotati di postazioni/client con hardware in grado di soddisfare le esigenze di connettività necessarie alla partecipazione alle VTC e svolgere i laboratori proposti.

È PREVISTO UN ESAME FINALE.

9. SISTEMA OPERATIVO WINDOWS 2016 SERVER - COD. ET291A

OBIETTIVI DEL CORSO

Fornire al frequentatore le nozioni sulle principali caratteristiche e funzionalità del prodotto mettendolo in condizione di saper installare, configurare, personalizzare ed amministrare, in sicurezza, l'ambiente Windows Server 2016 evidenziando le principali innovazioni rispetto alle versioni precedenti fornendo le necessarie competenze per operare su tale S.O. Il Corso si prefigge, inoltre, l'obiettivo di fornire le conoscenze necessarie per permettere ai discenti di gestire gli scenari di impiego di Windows Server 2016, i requisiti, il calcolo e la gestione della memoria in una infrastruttura IT, le competenze di rete necessarie per il *deploy* del sistema e come distribuire e configurare i servizi di dominio *Active Directory* (AD DS) in un ambiente distribuito, implementare i criteri di gruppo, eseguire il *backup* e il ripristino e come monitorare e risolvere eventuali problemi relativi a *Active Directory* con Windows Server 2016. Ulteriormente, il Corso ha l'obiettivo di insegnare ai frequentatori su come migliorare la sicurezza dell'infrastruttura IT amministrata, utilizzando l'*auditing* e le funzionalità di analisi delle minacce avanzate in Windows Server 2016 per identificare i problemi di sicurezza e come mitigare le minacce *malware*, protezione della piattaforma di virtualizzazione e utilizzo opzioni di distribuzione come i Nano server.

DURATA: 4 settimane di cui 40% di laboratorio. Il corso sarà svolto a distanza in modalità "*on-line training*". Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI

1ª – dal 18 maggio al 12 giugno in DAD;

2ª – dal 21 settembre al 16 ottobre in DAD.

PARTECIPANTI (max 12)

COMANDI/ENTI	sessioni	
	1ª	***2ª***
ESERCITO	7	7
MARINA MILITARE	1	2
AERONAUTICA	2	2
CARABINIERI		1
SMD II	1	
PERSOCIV	1	
TOTALE	**12**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: Corso Progettazione e gestione reti locali Cod. RE235I;
   b. Conoscenze basiche richieste:
      - ottima conoscenza ed esperienza di amministrazione di un sistema operativo Windows Server;
      - ottima conoscenza ed esperienza di gestione Reti e *Networking* e dei protocolli di rete TCP/IP;
      - conoscenza ed esperienza con AD DS e nozioni di Sicurezza Informatica.
      - capacità di leggere documentazione tecnica in lingua inglese;

c. Studio preventivo sinossi / testi propedeutici: N.N.

2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN ESAME FINALE.

10.SISTEMA OPERATIVO WINDOWS 2019 SERVER - COD. ET295A

OBIETTIVI DEL CORSO

Fornire al frequentatore le nozioni sulle principali caratteristiche e funzionalità del prodotto, mettendolo in condizione di saper installare, configurare, personalizzare ed amministrare in sicurezza l'ambiente Windows Server 2019, evidenziando le principali innovazioni rispetto alle versioni precedenti e fornendo le necessarie competenze per operare su tale S.O. Il Corso si prefigge inoltre l'obiettivo di fornire le conoscenze necessarie per permettere ai discenti di gestire gli scenari di impiego di Windows Server 2019. Questo corso consente agli amministratori di server delle precedenti versioni ad aggiornare le loro conoscenze e competenze relative a Windows Server 2019.

DURATA: 1 settimana di cui 50% di laboratorio. Il corso sarà svolto a distanza in modalità "*on-line training*". Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 13 al 17 luglio in DAD;

2ª – dal 27 al 31 luglio in DAD.

PARTECIPANTI (max 12)

COMANDI/ENTI	**Sessione**	
	1ª	***2ª***
ESERCITO	5	5
MARINA MILITARE	1	2
AERONAUTICA	2	2
SMD II		1
COVI		1
COR	1	
COFS	1	
NSFA COE	1	
ITAQUARTGEN		1
PERSOCIV	1	
TOTALE	**12**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: Corso Sistema Operativo Windows 2012 o 2016 Server.
   b. Conoscenze basiche richieste:
      - ottima conoscenza ed esperienza di amministrazione di un sistema operativo Windows Server;
      - ottima conoscenza ed esperienza di gestione Reti e *Networking* e dei protocolli di rete TCP/IP;
      - conoscenza ed esperienza con AD DS e nozioni di Sicurezza Informatica.
      - capacità di leggere documentazione tecnica in lingua inglese.
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN ESAME FINALE.

11.S.O. LINUX - COD. TE285A

OBIETTIVI DEL CORSO
Fornire una conoscenza avanzata del sistema operativo Linux e delle sue distribuzioni più utilizzate in ambito Difesa, preminentemente la distribuzione Red Hat.
Inoltre, si prefigge l'obiettivo di fornire ai discenti il *know how* necessario per il raggiungimento di una produttività elevata tramite l'uso dei principali strumenti di amministrazione di sistema. Vengono affrontate le principali operazioni di configurazione e gestione degli utenti e dei servizi fondamentali.

DURATA: 2 settimane in modalità *e-learning* sincrono (40 ore in piattaforma) con eventuali interventi via *web streaming*[2] e 2 settimane in presenza. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 02 al 13 marzo in DAD e dal 16 al 27 marzo in presenza;

2ª – dal 15 al 26 giugno in DAD e dal 29 giugno al 10 luglio in presenza;

2ª – dal 09 al 20 novembre in DAD e dal 23 novembre al 04 dicembre in presenza.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni		
	1ª	***2ª***	***3ª***
ESERCITO	5	6	8
MARINA MILITARE	2	1	1
AERONAUTICA	2	2	2
CARABINIERI		1	1
SMD II		1	
COFS			1
PERSOCIV		1	1
STELMILIT	1		
TOTALE	**10**	**12**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: CORSO E-LEARNING SU S.O. LINUX BASE – COD. **ET23B**;
   b. Conoscenze basiche richieste: In alternativa alla frequenza preventiva il discente dovrà possedere una buona conoscenza di informatica, di almeno un sistema operativo (possibilmente UNIX– LINUX – SOLARIS–BSD) e della suite di protocolli TCP/IP.
   c. Studio preventivo sinossi / testi propedeutici consigliati:
      - RHCSA/RHCE Red Hat Linux Certification Study Guide (EX200 & EX300);
      - Amministrare Gnu/Linux - Quarta Edizione (ISBN-10: 1326160842).
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

[2] Le indicazioni inerenti alle eventuali attività sincrone saranno comunicate dagli Istruttori del corso (Rif. Annesso del presente Catalogo).

REQUISITI TECNICI NECESSARI PER IL CORRETTO SVOLGIMENTO DELLA FORMAZIONE A DISTANZA

- Prima e seconda settimana (fase DAD asincrona SCORM e contenuti in piattaforma)
  Eventuale DAD sincrona via WEBEX, con orari comunicati in piattaforma dagli Istruttori. La banda necessaria per il corretto svolgimento delle attività è di 2 Mbps circa.
- Terza e quarta settimana
  In presenza.

Requisiti Tecnici per l'accesso alla VPN dei laboratori remoti nel caso di attivazione della modalità online training:

- Banda necessaria per il corretto svolgimento delle attività: 5 Mbps circa.
- Sui Client che utilizzeranno i discenti sarà necessario:
- assicurare la connettività di rete sulle porte logiche 443/TCP e 443/UDP necessarie per la connessione ai Lab remoti attestati sui gateway VPN STELMILIT;
- avere diritti/privilegi per poter installare il software Cisco Anyconnect VPN ed i relativi certificati digitali associati all'utente;
- avere diritti/privilegi per poter installare un client RDP (remote desktop) per il controllo dei PC collocati nell'aula fisica;
- utilizzare doppio monitor per le attività didattiche/laboratoriali

Tutto il software necessario al discente per il collegamento in VPN sarà scaricato automaticamente al primo accesso alla VPN e su indicazioni/istruzioni dei Docenti del corso.

Si rammenta che la partecipazione alle attività asincrone/sincrone (Contenuti in Piattaforma, Videoconferenze/Virtual Classroom), definite e comunicate dagli Istruttori, sono da considerarsi didatticamente ed amministrativamente parte integrante del corso stesso ed obbligatorie ai fini dell'accesso all'esame finale.
Inoltre, i discenti dovranno essere dotati di postazioni/client con hardware in grado di soddisfare le esigenze di connettività necessarie alla partecipazione alle VTC e svolgere i laboratori proposti.

È PREVISTO TEST INGRESSO (a termine fase e-learning) E UN ESAME FINALE (a termine fase in presenza)

12. VIRTUALIZZAZIONE - COD. ET298A

OBIETTIVI DEL CORSO

Introdurre il frequentatore alle tecnologie di virtualizzazione per l'implementazione e la gestione di una infrastruttura vSphere (VMware – vSphere Framework Ver. 8), descrivendo le caratteristiche e le funzionalità dei prodotti e mettendolo in condizione di saper installare, configurare ed utilizzare i diversi ambienti anche ai fini della formazione del personale destinato ad amministrare e gestire i Sistemi Virtuali della Difesa.

DURATA: 1 settimana in modalità "*on-line training*".

PERIODO SESSIONI:

1ª – dal 07 al 11 settembre in DAD;

2ª – dal 28 settembre al 02 ottobre in DAD.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessione	
	1ª	***2ª***
ESERCITO	4	4
MARINA MILITARE	2	2
AERONAUTICA	2	3
CARABINIERI	1	
SMD II		1
COVI	1	
COR	1	1
ITAQUARTGEN		1
MAECI	1	
TOTALE	**12**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: Windows Server per Amministratori; progettazione e gestione reti locali;
   b. Conoscenze basiche richieste:

      In alternativa alla frequenza preventiva il discente dovrà possedere un'ottima conoscenza dell'ambiente server Microsoft, buona conoscenza dei protocolli di rete TCP/IP e SO Linux;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto;
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

Le posizioni disponibili dovranno essere prioritariamente riservate al personale destinato ad amministrare e gestire i servizi di collaborazione FMN.

È PREVISTO ESAME FINALE.

13. AMMINISTRAZIONE DI MICROSOFT EXCHANGE SERVER 2016/2019- COD. ET299A

OBIETTIVI DEL CORSO

Trasmettere agli allievi le conoscenze necessarie per progettare, installare e supportare correttamente un'infrastruttura di messaggistica e collaborazione evoluta, basata su *Active Directory* e *Exchange Server* 2016/2019. Inoltre si prefigge l'obiettivo di fornire ai discenti le nozioni utili a: configurare e gestire i destinatari della posta e le cartelle pubbliche, configurare e gestire il trasporto e la sicurezza dei messaggi, distribuire i servizi di accesso client, Backup e ripristino di emergenza. Il corso tratta anche altri aspetti importanti come la sicurezza perimetrale, la configurazione e la registrazione di audit, l'esecuzione di vari compiti per automatizzare le procedure di gestione di Exchange utilizzando CMDLET.

DURATA: 1 settimana in modalità "*on-line training*".

PERIODO SESSIONI:

1ª – dal 14 al 18 settembre in DAD.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessione
	1ª
ESERCITO	3
MARINA MILITARE	2
AERONAUTICA	2
SMD II	1
COVI	1
COR	1
COFS	1
PERSOCIV	1
TOTALE	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. frequenza preventiva: Windows *Server* per Amministratori;
   b. conoscenze basiche richieste:

      In alternativa alla frequenza preventiva il discente dovrà possedere i seguenti prerequisiti:
      - esperienza nella amministrazione di infrastrutture basate su Windows Server 2012;
      - esperienza nella amministrazione dei servizi Active Directory, nella risoluzione dei nomi e nella gestione del DNS;
      - familiarità con i concetti di networking e con i protocolli TCP/IP;
      - familiarità con i concetti di sicurezza quali autenticazione e autorizzazione;
      - familiarità con il protocollo SMTP (Simple Mail Transfer Protocol);
      - esperienza di lavoro con le tecnologie PKI (Public Key Infrastructure), compreso AD CS (Active Directory Certificate Services).

   c. studio preventivo sinossi / testi propedeutici: N.N.;
2. **Di segretezza:** NOS non richiesto;
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

Le posizioni disponibili dovranno essere prioritariamente riservate al personale destinato ad amministrare e gestire i servizi di collaborazione FMN.

È PREVISTO ESAME FINALE

14. PIANIFICAZIONE E AMMINISTRAZIONE DI SHAREPOINT 2016 - COD. ET300A

OBIETTIVI DEL CORSO

Fornire le conoscenze e le competenze per pianificare e gestire un ambiente Microsoft SharePoint 2016. Il corso si prefigge, inoltre, l'obiettivo di insegnare come installare, distribuire, amministrare e risolvere i problemi dell'ambiente di SharePoint fornendo linee guida, best practices e le informazioni che consentono di ottimizzare la distribuzione di SharePoint.

DURATA: 1 settimana in modalità "*on-line training*".

PERIODO SESSIONI:

1ª – dal 26 al 30 ottobre in DAD.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessione
	1ª
ESERCITO	3
MARINA MILITARE	2
AERONAUTICA	4
COR	2
PERSOCIV	1
TOTALE	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. frequenza preventiva: Windows Server per Amministratori;
   b. conoscenze basiche richieste: In alternativa alla frequenza preventiva il discente dovrà possedere i seguenti prerequisiti:
      - esperienza nell'amministrazione di IIS.
      - esperienza nella configurazione di dominio Active Directory per l'utilizzo in autenticazione, autorizzazione, e come utenti.
      - esperienza nella gestione un'applicazione in remoto tramite Windows PowerShell 4.0.
      - esperienza nella gestione database e ruoli server in SQL Server.
      - esperienza con applicazioni a SQL Server.
      - esperienza nell'utilizzo di Microsoft Hyper-V macchine virtuali
   c. studio preventivo sinossi / testi propedeutici: N.N.;
2. **Di segretezza:** NOS non richiesto;
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

Le posizioni disponibili dovranno essere prioritariamente riservate al personale destinato ad amministrare e gestire i servizi di collaborazione FMN.

È PREVISTO ESAME FINALE

15. PROVISIONING SQL DATABASES - COD. ET301A

OBIETTIVI DEL CORSO
Trasmettere agli allievi le conoscenze e le competenze per rendere disponibile un database Sql Server in modalità on-premise. Il corso si prefigge, inoltre, l'obiettivo di fornire ai discenti le conoscenze necessarie ad installare, configurare, amministrare e attuare la manutenzione di un'infrastruttura di database basata su SQL Server 2016.

DURATA: 1 settimana in modalità *"on-line training".*

PERIODO SESSIONI:
1ª – dal 02 al 06 novembre in DAD.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni
	1ª
ESERCITO	4
MARINA MILITARE	3
AERONAUTICA	2
CARABINIERI	2
PERSOCIV	1
TOTALE	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: Windows Server per Amministratori; introduzione ai Databases SQL;

      In alternativa alla frequenza preventiva il discente dovrà possedere i seguenti prerequisiti:

      - buona conoscenza dell'ambiente operativo Microsoft Windows e delle sue funzionalità core; - esperienza di lavoro con Transact-SQL;

      - esperienza di lavoro con i database relazionali;

      - è preferibile possedere una esperienza di base nel disegno di database.

   b. Conoscenze basiche richieste: conoscenze generali sull'utilizzo di sistemi operativi Windows;

   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO ESAME FINALE.

16. APPLICAZIONI WEB (HTML/CSS) - COD. TE79I

OBIETTIVI DEL CORSO

Il corso si pone come obiettivo la conoscenza e la gestione del linguaggio di marcatura HTML5 e dei fogli di stile CSS utili ai fini della realizzazione e progettazione di pagine *web*. Partendo dalle nozioni di base, verranno descritte tutte le regole e metodologie essenziali per realizzare un piccolo sito *web*, rispettando gli *standard* del W3C.

DURATA: 1 settimana in modalità *e-learning* asincrono (15 ore in piattaforma) con eventuali interventi in web streaming e 1 settimana in presenza; percentuale laboratorio: 50%. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 26 al 30 gennaio in DAD e dal 02 al 06 febbraio in presenza;

2ª – dal 23 al 27 marzo in DAD e dal 30 marzo al 03 aprile in presenza;

3ª – dal 18 al 22 maggio in DAD e dal 25 al 29 maggio in presenza;

4ª – dal 28 settembre al 02 ottobre in DAD e dal 05 al 09 ottobre in presenza;

5ª– dal 07 al 11 dicembre in DAD e dal 14 al 18 dicembre in presenza.

PARTECIPANTI (max 10)

COMANDI/ENTI	Sessioni				
	1ª	***2ª***	***3ª***	***4ª***	***5ª***
ESERCITO	2	3	5	3	4
MARINA MILITARE	1	1			
CAPITANERIE di PORTO			1		
AERONAUTICA	2	1	1	1	1
CARABINIERI				1	1
COVI		1			
SFA COE	1				
PERSOCIV	1	1	1	1	1
CONGEDATI	2	2	2	3	3
STELMILIT	1			1	
TOTALE	**10**	**9**	**10**	**10**	**10**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: Conoscenze generali sull'utilizzo di sistemi operativi Windows;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

REQUISITI TECNICI NECESSARI PER IL CORRETTO SVOLGIMENTO DELLA FORMAZIONE A DISTANZA.

- Prima settimana:

Fase DAD asincrona contenuti in piattaforma + lezioni Fase DAD sincrona via WEBEX, con orari comunicati in piattaforma dagli Istruttori per testare le connessioni (vds. specifiche punti successivi).

- Seconda settimana:
  Fase DAD sincrona (OnLine Training - Virtual Classroom) via WEBEX;

Requisiti Tecnici per i laboratori remoti nel caso in cui venga attivata la modalità online training:

La banda necessaria per il corretto svolgimento delle attività è di 2 Mbps circa;
Sui client utilizzati dai discenti sarà necessario:

- installare software (Editor di testo) che sarà comunicato dall'Istruttore
- utilizzare un secondo monitor quale supporto alle attività laboratoriali della seconda settimana.

Si rammenta che la partecipazione alle attività asincrone/sincrone (Videoconferenze/Virtual Classroom), definite e comunicate dagli Istruttori, sono da considerarsi didatticamente ed amministrativamente parte integrante del corso stesso ed obbligatorie ai fini dell'accesso all'esame finale.
Inoltre, i discenti dovranno essere dotati di postazioni/client con hardware in grado di soddisfare le esigenze di connettività necessarie alla partecipazione alle VTC.

È PREVISTO UN TEST D'INGRESSO (a termine fase *e-learning*) E UN ESAME FINALE (a termine fase in presenza).

17.INFORMATICO DI F.A. (ABILITAZIONE "INF" MM) - COD. T448I

OBIETTIVI DEL CORSO
Formare il personale designato dalla Forza Armata, per il conseguimento dell'abilitazione "INF" (Referente Informatico) fornendo la preparazione/competenza tecnico-professionale necessaria alla gestione dei servizi e dei sistemi informatici MM nell'ambito locale del Comando/Ente di appartenenza.

DURATA: 3 settimane in presenza.

PERIODO SESSIONI:

1ª – dal 14 settembre al 02 ottobre in presenza;

2ª – dal 12 al 30 ottobre in presenza.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni	
	1ª	***2ª***
MARINA MILITARE	6	8
CAPITANERIE di PORTO		1
TOTALE	**6**	**9**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:** I requisiti professionali saranno definiti dalla Marina Militare.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Personale in SPE, selezionato dalla Marina Militare a seguito della pubblicazione di specifico bando. Il personale designato potrà essere impiegato quale Referente Informatico dei Comandi/Enti della MM.

SONO PREVISTE DELLE PROVE VALUTATIVE INTERMEDIE E AL TERMINE DEL CORSO.

18. E-LEARNING DI INFORMATICA DI BASE ICDL - COD. ET17B

OBIETTIVI DEL CORSO

Il corso di informatica di base ICDL in modalità *e-learning* (*Web Based Training*) fornisce le conoscenze basiche per l'uso del computer.

Scopo del corso è quello di introdurre il frequentatore all'uso del computer, portandolo a conoscenza delle principali caratteristiche e funzionalità della suite libera per ufficio *Libre Office*, all'uso di internet ed ella posta elettronica e alla comprensione dei principali aspetti relativi alla sicurezza informatica e degli strumenti di collaborazione *on-line*.

Il corso è basato sugli argomenti previsti ICDL Full Standard dell'AICA.

DURATA: *WEB Based Training* su 5 settimane calendariali pari a circa 100 ore in modalità *e-learning* asincrono (20 ore a settimana). Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 26 gennaio al 27 febbraio in DAD;

2ª – dal 18 maggio al 19 giugno in DAD.

PARTECIPANTI (max 50)

COMANDI/ENTI	**Sessione**	
	1	***2ª***
ESERCITO	11	12
MARINA MILITARE	8	8
AERONAUTICA	3	3
CARABINIERI	1	
CAPITANERIE di PORTO	1	1
SMD II	1	1
CASD	1	
COS	1	
PERSOCIV	14	13
CONGEDATI	7	8
TOTALE	**48**	**46**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: Utilizzo basico del computer e conoscenze minime di "navigazione" internet.
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

MODALITÀ DI SVOLGIMENTO

All'atto dell'iscrizione sarà inviata al candidato una *password* per l'accesso iniziale ai contenuti della piattaforma *e-learning* della Scuola.

Il percorso formativo sarà erogato esclusivamente in modalità *e-learning* tramite la piattaforma della Scuola Telecomunicazioni FF.AA. di Chiavari (STELMILIT).

Gli iscritti attraverso le proprie credenziali potranno collegarsi ed accedere alla piattaforma di studio *on-line,* partecipando/seguendo le lezioni in modalità asincrona o, quando stabilito dalla Scuola, attraverso *forum* e *chat*.

Tale corso prepara anche all'acquisizione di un Certificato ICDL Full Standard, European Computer Driving Licence, riconosciuto internazionalmente.

Si ricorda che L'ICDL è rilasciato da strutture esterne riconosciute. Maggiori informazioni potranno essere reperite sul sito https://www.icdl.it/icdl-full-standard.

Ciascun modulo è corredato di *quiz* di autovalutazione che preparano alla prova d'esame conclusiva.

È PREVISTO UN ESAME FINALE.

19.E-LEARNING IT SPECIALIST - COD. ET18B

OBIETTIVI DEL CORSO
Formare il personale designato a svolgere mansioni afferenti il Ruolo di Referente Informatico (con riferimento allo standard EUCIP IT *ADMINISTRATOR*), fornendogli competenze ed abilità a livello basico, necessarie per la gestione di piccole infrastrutture informatiche negli ambiti: Hardware, Sistemi Operativi (Windows® e Linux), Reti e Sicurezza Informatica. In particolare, il corso è orientato su quattro moduli didattici previsti dal percorso formativo IT Administrator dell'AICA: Hardware del PC; Sistemi Operativi; Reti; Sicurezza Informatica.

DURATA: *WEB Based Training* su 4 settimane calendariali (un modulo per settimana) pari a 60 ore in modalità *e-learning* asincrono. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:
1ª – dal 26 gennaio al 20 febbraio in DAD;
2ª – dal 09 marzo al 03 aprile in DAD;
3ª – dal 29 giugno al 24 luglio in DAD;

PARTECIPANTI (max 75)

COMANDI/ENTI	Sessioni		
	1ª	***2ª***	***3ª***
ESERCITO	9	9	10
MARINA MILITARE	3	3	3
AERONAUTICA	4	4	4
CARABINIERI	41	41	40
CAPITANERIE di PORTO	2	2	3
DIFEGABINETTO	1		
SMD II	1		
SGD		1	
CASD	1		
ITAQUARTIGEN			1
PERSOCIV	5	5	5
MAECI	1	1	
CONGEDATI	6	8	6
TOTALE	**74**	**74**	**73**

REQUISITI PER L'AMMISSIONE:
1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: N.N.;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

MODALITÀ DI SVOLGIMENTO: le attività a distanza sono disciplinate nell'Annesso.

All'atto dell'iscrizione verrà inviata al candidato una *password* per l'accesso iniziale ai contenuti della piattaforma *e-learning* della Scuola. Il percorso formativo sarà erogato esclusivamente in modalità *e-learning* tramite la piattaforma della Scuola Telecomunicazioni FF.AA. di Chiavari (STELMILIT).

Gli iscritti attraverso le proprie credenziali potranno collegarsi e accedere alla piattaforma di studio *on-line*, partecipando/seguendo le lezioni in modalità asincrona o, quando stabilito dalla Scuola, attraverso *forum* e *chat*. Orientativamente, ognuno dei quattro moduli richiede una settimana di studio (prevedendo un impegno settimanale di circa 15 ore di collegamento, compresi esercizi e attività di studio).

Ciascun modulo è corredato di *quiz* di autovalutazione che preparano alla prova d'esame conclusiva.

È PREVISTO UN ESAME FINALE.

20.E-LEARNING SU S.O. LINUX BASE – COD. ET23B

OBIETTIVI DEL CORSO
Fornire le informazioni basiche del Sistema Operativo Linux e delle distribuzioni più usate.

DURATA: 2 settimane in modalità *e-learning* asincrono (40 ore in piattaforma) con eventuali interventi via *web streaming*[3]. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:
1ª – dal 19 al 30 gennaio in DAD;
2ª – dal 09 al 20 febbraio in DAD;
3ª – dal 13 al 24 aprile in DAD;
4ª – dal 20 al 31 luglio in DAD;
5ª – dal 07 al 18 settembre in DAD;

PARTECIPANTI (max 30)

COMANDI/ENTI	Sessioni				
	1ª	***2ª***	***3ª***	***4ª***	***5ª***
ESERCITO	6	5	5	6	4
MARINA MILITARE	3	3	4	4	3
CAPITANERIE di PORTO	1	1		1	
AERONAUTICA	4	3	3	4	4
CARABINIERI	2	2	1	2	2
DIFEGABINETTO		1			
SMD II			3		2
SGD		1	1		1
COR		2	2		1
COS	2			2	1
COFS				1	1
PERSOCIV	5	4	3	3	2
MAECI			1		
CONGEDATI	4	4	4	4	4
STELMILIT	1				
TOTALE	**28**	**26**	**27**	**27**	**25**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste:
      - Buona conoscenza e affinità con i computer (*hardware* e *software*) ed Internet;
      - conoscenza dei protocolli TCP/IP;
      - conoscenza di altri sistemi operativi.

[3] Le indicazioni inerenti alle eventuali attività sincrone saranno comunicate dagli Istruttori del corso (Rif. Annesso del presente Catalogo).

c. Studio preventivo sinossi / testi propedeutici: N.N.

2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

REQUISITI TECNICI NECESSARI PER IL CORRETTO SVOLGIMENTO DELLA FORMAZIONE A DISTANZA.

Fase DAD asincrona con contenuti in piattaforma + eventuali lezioni in *DAD sincrona* via WEBEX, con orari comunicati in piattaforma dagli Istruttori.

La banda necessaria per il corretto svolgimento delle attività è di 2 Mbps circa.

Si rammenta che la partecipazione alle attività asincrone/sincrone (Contenuti in Piattaforma, Videoconferenze/Virtual Classroom), definite e comunicate dagli Istruttori, sono da considerarsi didatticamente ed amministrativamente parte integrante del corso stesso ed obbligatorie ai fini dell'accesso all'esame finale.

Inoltre, i discenti dovranno essere dotati di postazioni/client con hardware in grado di soddisfare le esigenze di connettività necessarie alla partecipazione alle VTC.

È PREVISTO UN ESAME FINALE

21. ELEMENTI DI VIRTUALIZZAZIONE - COD. ET24B

OBIETTIVI DEL CORSO
Fornire ai frequentatori le conoscenze generali sulle Tecnologie di Virtualizzazione descrivendone le caratteristiche, le funzionalità e i principali vantaggi del suo utilizzo.

DURATA: 1 settimana in modalità *e-learning* asincrono con eventuali interventi via *web streaming*[4]. (15 ore in piattaforma). Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:
1ª – dal 23 al 27 marzo in DAD;
2ª – dal 13 al 17 aprile in DAD;
3ª – dal 16 al 20 novembre in DAD;
4ª – dal 30 novembre al 04 dicembre in DAD.

PARTECIPANTI (max 25)

COMANDI/ENTI	Sessioni			
	1ª	***2ª***	***3ª***	***4ª***
ESERCITO	6	7	7	6
MARINA MILITARE	1	2	2	2
CAPITANERIE di PORTO	1			
AERONAUTICA	3	3	3	3
CARABINIERI	2	2	3	3
SMD I			1	1
SMD II	2	1	1	1
S.G.D.	1			
COVI				1
COR		1	1	1
COS	1	1	1	1
COFS	1	1		1
ITAQUARTGEN	1			
PERSOCIV	2	4	3	4
MAECI	1	1	1	
TOTALE	**23**	**23**	**23**	**24**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: buona conoscenza informatica;
   c. Studio preventivo sinossi / testi propedeutici: N.N..
2. **Di segretezza:** NOS non richiesto;
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO ESAME FINALE

[4] Le indicazioni inerenti alle eventuali attività sincrone saranno comunicate dagli Istruttori del corso (Rif. Annesso del presente Catalogo).

AREA INFOSEC E INFORMATION ASSURANCE

22.OPERATORE CIFRANTI CM 2000 IP - COD. JE427A

OBIETTIVI DEL CORSO

Fornire ai frequentatori le appropriate conoscenze tecniche necessarie agli Operatori Cifra per effettuare l'installazione e la programmazione degli apparati cifranti di tipo "CM 2000 IP" che impiegano la tecnologia Internet Protocol (IP).

DURATA: 2 settimane di cui 1 settimana in modalità *e-learning* asincrono (15 ore) e 1 settimana in presenza. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 19 al 23 gennaio in DAD e dal 26 al 30 gennaio in presenza;

2ª – dal 02 al 06 febbraio in DAD e dal 09 al 13 febbraio in presenza;

3ª – dal 16 al 20 febbraio in DAD e dal 23 al 27 febbraio in presenza.

PARTECIPANTI (max 8)

COMANDI/ENTI	Sessioni		
	1ª	***2ª***	***3ª***
ESERCITO	3	3	3
MARINA MILITARE	1		
CARABINIERI	3	5	5
MAECI	1		
TOTALE	**8**	**8**	**8**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: nozioni basiche sulle Reti Ethernet, protocollo TCP/IP;
   c. Studio preventivo sinossi / testi propedeutici: normativa COMSEC in vigore.
2. **Di segretezza:** NOS SEGRETO e NATO/SECRET.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati (solo personale in Servizio Permanente) e personale civile della Difesa impiegati/designati a ricoprire incarichi nel settore CIS/COMSEC.

È PREVISTO UN ESAME FINALE.

23.OPERATORE CIFRANTI CM 2100 IP - COD. JE428A

OBIETTIVI DEL CORSO
Fornire ai frequentatori, le appropriate conoscenze tecniche necessarie agli Operatori Cifra, per effettuare l'installazione, la programmazione degli apparati cifranti di tipo "CM 2100 IP" che utilizzano la tecnologia *Internet Protocol* (IP).

DURATA: 2 settimane di cui 1 settimana in modalità *e-learning* asincrono (15 ore) e 1 settimana in presenza. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:
1ª – dal 09 al 13 marzo in DAD e dal 16 al 20 marzo in presenza;
2ª – dal 23 al 27 marzo in DAD e dal 30 marzo al 03 aprile in presenza;
3ª – dal 13 al 17 aprile in DAD e dal 20 al 24 aprile in presenza;
4ª – dal 27 al 30 aprile in DAD e dal 04 al 08 maggio in presenza;
5ª – dal 26 al 30 ottobre in DAD e dal 02 al 06 novembre in presenza.

PARTECIPANTI (max 6)

COMANDI/ENTI	**Sessioni**				
	1ª	***2ª***	***3ª***	***4ª***	***5ª***
ESERCITO	3	3	3	4	3
MARINA MILITARE		1		1	
AERONAUTICA			3	1	3
CARABINIERI	1				
SMD II		1			
COVI	1				
COR	1				
COS		1			
TOTALE	**6**	**6**	**6**	**6**	**6**

REQUISITI PER L'AMMISSIONE:
1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: nozioni basiche sulle Reti *Ethernet*, protocollo TCP/IP;
   c. Studio preventivo sinossi / testi propedeutici: normativa COMSEC in vigore.
2. **Di segretezza:** N.O.S.: SEGRETO e NATO/SECRET, posseduto dal discente al momento della segnalazione da parte dei Comandi/Enti/Amministrazioni di appartenenza.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati (solo personale in Servizio Permanente) e personale civile della Difesa, impiegati/designati a ricoprire incarichi nel settore COMSEC.

È PREVISTO UN ESAME FINALE.

24.SW KNMS 2100IP - COD. JE429A

OBIETTIVI DEL CORSO
Fornire ai frequentatori, le conoscenze tecniche sul funzionamento del software applicativo K.N.M.S. per CM 2100 IP per amministrare da remoto una rete di cifranti IP.

DURATA: 2 settimane di cui 1 settimana in modalità *e-learning* asincrono per visione video tutorial KNMS 2100 IP (15 ore in piattaforma) e 1settimana in presenza. Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 22 al 26 giugno in DAD e dal 29 giugno al 03 luglio in presenza;

2ª – dal 20 al 24 luglio in DAD e dal 27 al 31 luglio in presenza;

3ª – dal 23 al 27 novembre in DAD e dal 30 novembre al 04 dicembre in presenza.

PARTECIPANTI (max 5)

COMANDI/ENTI	**Sessioni**		
	1ª	***2ª***	***3ª***
ESERCITO	1	2	1
MARINA MILITARE			1
AERONAUTICA	3	2	2
SMD II			
COVI			1
COR	1		
COS		1	
TOTALE	**5**	**5**	**5**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: corso Operatore per Cifranti CM 2100 IP;
   b. Conoscenze basiche richieste: nozioni basiche sulle Reti *Ethernet*, protocollo TCP/IP e IP *Routing*;
   c. Studio preventivo sinossi / testi propedeutici: normativa COMSEC in vigore.
2. **Di segretezza:** NOS SEGRETO e NATO/SECRET, posseduto dal discente al momento della segnalazione da parte dei Comandi/Enti/Amministrazioni di appartenenza.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati (solo personale in Servizio Permanente) e personale civile della Difesa, impiegati/designati quali amministratori di reti geografiche classificate nel settore COMSEC.

È PREVISTO UN ESAME FINALE

25. CUSTODE MATERIALE COMSEC/CIFRA - COD. J437A

OBIETTIVI DEL CORSO
Formare il personale destinato a ricoprire incarichi relativi alla custodia del materiale COMSEC/CIFRA. Istruzione sulle norme di sicurezza, sulle procedure manuali ed automatizzate per la contabilità, la gestione e l'impiego del materiale COMSEC/CIFRA.

DURATA: 2 settimane in presenza.

PERIODO SESSIONI:

1ª – dal 19 al 30 gennaio in presenza;

2ª – dal 23 marzo al 03 aprile in presenza;

3ª – dal 01 al 12 giugno in presenza;

4ª – dal 26 ottobre al 06 novembre in presenza.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni			
	1ª	***2ª***	***3ª***	***4ª***
ESERCITO	4	4	3	3
MARINA MILITARE	1	1	1	1
CAPITANERIE di PORTO	1			
AERONAUTICA	2	2	3	3
CARABINIERI	2	2	2	2
SMD I			2	
SMD II		2		
COVI				1
COR	1			
COS		1		
NSFA - COE				1
ITAQUARTIGEN	1		1	1
MAECI	1			
TOTALE	**12**	**12**	**12**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: N.N.;
   c. Studio preventivo sinossi / testi propedeutici: normativa COMSEC in vigore.
2. **Di segretezza:** NOS SEGRETO e NATO/SECRET, posseduto dal discente al momento della segnalazione da parte dei Comandi/Enti/Amministrazioni di appartenenza.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati (solo personale in Servizio Permanente) e personale civile della Difesa impiegati/designati a ricoprire incarichi nel settore COMSEC.

È PREVISTO UN ESAME FINALE.

26. UFFICIALI COMSEC DESIGNATI - COD. J447A

OBIETTIVI DEL CORSO
Fornire ai frequentatori le conoscenze in ambito INFOSEC, sulle norme applicative di sicurezza dei sistemi di comunicazione e informativi, sotto gli aspetti COMSEC/CRYPTO e TEMPEST.

DURATA: 2 settimane in presenza.

PERIODO SESSIONI:
1ª – dal 16 al 27 febbraio in presenza;
2ª – dal 27 aprile al 08 maggio in presenza;
3ª – dal 07 al 18 settembre in presenza;
4ª – dal 30 novembre al 11 dicembre in presenza.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni			
	1ª	***2ª***	***3ª***	***4ª***
ESERCITO	3	3	4	4
MARINA MILITARE	2	1	1	1
CAPITANERIE di PORTO	1			
AERONAUTICA	3	3	2	2
CARABINIERI	2	2	2	2
SMD II			2	
SMD VI		1		
SGD	1			
COR			1	
COS	1			
COFS		1		
ITAQUARTIGEN			1	
NSFA - COE				1
MAECI		1		
TOTALE	**12**	**12**	**12**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: N.N.;
   c. Studio preventivo sinossi / testi propedeutici: normativa COMSEC in vigore.
2. **Di segretezza:** NOS SEGRETO e NATO/SECRET, posseduto dal discente al momento della segnalazione da parte dei Comandi/Enti/Amministrazioni di appartenenza.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati (solo personale in Servizio Permanente) e personale civile della Difesa, impiegati/designati a ricoprire incarichi nel settore COMSEC.

È PREVISTO UN ESAME FINALE.
***Nota**: Durante il corso è prevista una visita didattica di una giornata, presso i Laboratori Tempest del C.I.S.A.M. di San Pietro a Grado (PI). Il personale frequentatore deve pertanto essere munito di foglio di viaggio su cui deve essere riportata anche tale località.*

27.UFFICIALI ALLA SICUREZZA CIS DESIGNATI - COD. J451A

OBIETTIVI DEL CORSO
Fornire ai frequentatori conoscenze in ambito INFOSEC sulle norme di gestione della sicurezza dei sistemi CIS, sia sotto gli aspetti della Sicurezza I.C.T. che della tutela delle informazioni classificate.

DURATA: 2 settimane in presenza.

PERIODO SESSIONI:
1ª – dal 19 al 30 gennaio in presenza;
2ª – dal 09 al 20 febbraio in presenza;
3ª – dal 16 al 27 marzo in presenza;
4ª – dal 27 aprile al 08 maggio in presenza;
5ª – dal 18 al 29 maggio in presenza (sessione per gli Ufficiali AN della M.M.);
6ª – dal 29 giugno al 10 luglio in presenza (sessione per la Scuola di Applicazione dell'EI);
7ª – dal 14 al 25 settembre in presenza;
8ª – dal 05 al 16 ottobre in presenza;
9ª – dal 02 al 13 novembre in presenza.

PARTECIPANTI (max 12)

COMANDI/ENTI	Sessioni								
	1ª	***2ª***	***3ª***	***4ª***	***5ª***	***6ª***	***7ª***	***8ª***	***9ª***
ESERCITO	3	3	3	2			3	2	2
EI - SCUOLA DI APPLICAZIONE						14			
MARINA MILITARE	2	2	3	2			4	4	4
MM – UFFICIALI AN					11				
CAPITANERIE di PORTO	1								
AERONAUTICA	2	2	2	3			2	2	3
CARABINIERI	1	1	1	1	1		2	2	2
DIFEGABINETTO		1					1		
SMD I	2								
SMD II			1	1					
SMD VI		1							
SGD	1	1	1						
COVI				1					
COS		1							
COFS								1	
NSFA-COE									1
ITAQUARTIGEN			1						
PERSOCIV				1				1	
TOTALE	**12**	**12**	**12**	**12**	**12**	**14**	**12**	**12**	**12**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza auspicabile: corso Sicurezza IT – Cod. EJ400B;

b. Conoscenze basiche richieste: elementi di base di informatica e networking, normativa INFOSEC in vigore;
c. Studio preventivo sinossi / testi propedeutici: normativa COMSEC in vigore.

2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa, impiegati e/o designati a ricoprire incarichi nella gestione della sicurezza CIS.

È PREVISTO UN ESAME FINALE.

28.INFOSEC – EVALUATION COMMON CRITERIA/ITSEC - COD. J439A

OBIETTIVI DEL CORSO

Il corso è indirizzato al personale, in servizio o destinato presso il CE.VA. Difesa, O.C.S. di SMD/F.A. ed E/D/R direttamente coinvolti, congiuntamente con le ditte, nello sviluppo di sistemi classificati, e che abbia a tal fine necessità di operare nell'ambito dello "Schema di Certificazione Nazionale per i sistemi destinati a trattare informazioni classificate".
In particolare il corso fornisce le necessarie informazioni sulle procedure previste per l'ottenimento della certificazione ed omologazione dei sistemi classificati, da svolgere in coordinamento con l'industria nazionale del comparto Difesa.

DURATA: 1 SESSIONE 1 settimana in e-learning;
2 SESSIONE 1 settimana in presenza.

PERIODO SESSIONI:

1ª – dal 08 al 12 giugno in DAD;

2ª – dal 07 al 11 settembre in presenza.

PARTECIPANTI (max 10)

COMANDI/ENTI	Sessione	
	1ª	***2ª***
ESERCITO		3
MARINA MILITARE		4
AERONAUTICA		2
CARABINIERI	1	
SMD II	2	
SMD IV		
SGD	2	
COVI	1	
COFS	1	
NSFA - COE	1	
ITAQUARTIGEN	1	
TOTALE	**9**	**9**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: è consigliato aver frequentato il corso per Ufficiali alla Sicurezza CIS designati, oppure avere già esperienza consolidata in tale settore;
   b. Conoscenze basiche richieste: informatica di base;
   c. Studio preventivo sinossi / testi propedeutici: normativa COMSEC in vigore.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali.

È PREVISTO UN ESAME FINALE.

29. IT-EKMS CUSTODE CIFRA PER UTENTI LDF DELLE FF.AA. - COD. J450A

OBIETTIVI DEL CORSO
Fornire ai frequentatori le conoscenze tecniche sul funzionamento della postazione LDF (Local Device Facility) del sistema IT-EKMS.

DURATA: 1 settimana in presenza.

PERIODO SESSIONI:
1ª – dal 05 al 09 ottobre in presenza;
2ª – dal 19 al 23 ottobre in presenza

PARTECIPANTI (max 6)

COMANDI/ENTI	Sessione	
	1ª	***2ª***
ESERCITO	2	2
MARINA MILITARE	1	
AERONAUTICA	2	4
SMD II	1	
TOTALE	**6**	**6**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: Corso Operatori Cifranti CM 2100 IP – cod. JE428A e Corso Custode materiale COMSEC/Cifra – cod. J437A;
   b. Conoscenze basiche richieste:
      - conoscenze basiche delle cifranti IP (CM109/2000IP, CM2100 IP);
      - nozioni basiche sulle Reti Ethernet, protocollo TCP/IP e IP *Routing.*
   c. Studio preventivo sinossi / testi propedeutici: normativa COMSEC in vigore.

2. **Di segretezza:** NOS SEGRETO e NATO/SECRET, posseduto dal discente al momento della segnalazione da parte dei Comandi/Enti/Amministrazioni di appartenenza.

3. **Categorie:** Ufficiali, Sottufficiali, Graduati (solo personale in servizio Personale) e personale civile della Difesa, impiegati/designati a ricoprire incarichi nel settore COMSEC.

È PREVISTO UN ESAME FINALE.

30.CORSO SICUREZZA IT[5] - COD. EJ400B

OBIETTIVI DEL CORSO
Fornire ai frequentatori conoscenze generali sulla sicurezza informatica, sui comuni metodi di cifratura e sui protocolli di crittografia. Saranno inoltre fornite conoscenze sulla gestione dei log, sui principali tipi di minacce, su principi di autenticazione e resilienza ed affrontati i principali aspetti sociali, etici e legali relativi alla sicurezza informatica.

DURATA: 2 settimane in modalità *e-learning* asincrono (30 ore in piattaforma). Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:
1ª – dal 23 febbraio al 06 marzo in DAD;
2ª – dal 13 al 24 aprile in DAD.

PARTECIPANTI (max 45)

COMANDI/ENTI	Sessione	
	1ª	***2ª***
ESERCITO	15	16
MARINA MILITARE	4	5
CARABINIERI	2	2
CAPITANERIE di PORTO	1	
DIFEGABINETTO		4
SMD I	1	1
SMD II	3	2
SMD VI	1	
SGD	1	1
COVI	1	
COR	1	1
ITAQUARTIGEN	2	
PERSOCIV	9	9
MAECI	1	
TOTALE	**42**	**41**

REQUISITI MINIMI PER L'AMMISSIONE
1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: N.N.;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto
3. **Di grado:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO ESAME FINALE

[5]Contenuti tratti dal modulo "sicurezza IT" del corso "IT Specialist cod. ET18B.

AREA CYBER DEFENCE E LAW & FORENSICS

31. CORSO BASICO - OPERATORE CYBER DELLA DIFESA – COD. Y001A

OBIETTIVI DEL CORSO
Formare il personale designato ad acquisire la qualifica di operatore cyber di 1° livello, fornendo le necessarie competenze nell'ambito delle seguenti aree tematiche:

- Difesa proattiva;
- Sistemi operativi;
- Programmazione;
- Legal.

ENTE ORGANIZZATORE: *S.M.D. – I Reparto*

ENTE DI SVOLGIMENTO: *SCUOLA TELECOMUNICAZIONI DELLE FF.AA., CIFIGE*

DURATA: 14 settimane: 12 in *e-learning* e 2 in presenza (una settimana presso STELMILIT, una settimana presso il CIFIGE)

PERIODO: dal 02 marzo al 12 giugno.

	COD	CORSI			MARZO				APRILE				MAGGIO					GIUGNO				
		Data inizio settimana			2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	18	22	29
			DAD	P																		
Basico	EY452B	Fondamenti Diritto Int. applicato op. Cibernetiche	1								el 20											
	ET23B	S.O. LINUX BASE	2														el 20	el 20				
		CCNA: Introduction to Networks (ITN)	1				el 20															
		CCNA: Switching, Routing, and Wireless Essentials (SRWE)	1					el 20														
		CCNA: Enterprise Networking, Security, and Automation (ENSA)	1						el 20													
	STELM	CISCO CCNA Exam Preparation	0	1								20										
		Security information and event management (SIEM)	1													el 20						
		Windows Server	3										el 20	el 20	el 20							
		CLA: Programming Essentials in C	2		el 20	el 20																
	CIFIGE	Acquisizione forense	0	1															cifige 20			
		TOT basico	**12**	**2**																		

PARTECIPANTI (max 20):
Il corso è riservato agli Ufficiali a nomina diretta e al personale che opera nel settore cyber selezionato dallo SMD.

È richiesta la capacità di leggere e comprendere documentazione tecnica in lingua inglese.

SONO PREVISTI ESAMI INTERMEDI E UN ESAME FINALE.

32. CORSO SPECIALISTICO - OPERATORE CYBER DELLA DIFESA – COD. Y002A

OBIETTIVI DEL CORSO
Formare il personale designato ad acquisire la qualifica di operatore cyber di 2° livello, fornendo le necessarie competenze nell'ambito delle seguenti aree tematiche:

- Difesa proattiva;
- Programmazione;
- *Cyber Intel;*
- Simulazione avversario.

ENTE ORGANIZZATORE: *S.M.D. – I Reparto*

ENTE DI SVOLGIMENTO: *SCUOLA TELECOMUNICAZIONI DELLE FF.AA., CIFIGE*

DURATA: 17 settimane: 2 in e-learning e 15 in presenza (12 settimane presso STELMILIT, 3 settimane presso il CIFIGE).

PERIODO: dal 24 agosto al 18 dicembre.

	COD	CORSI			AGOSTO				SETTEMBRE				OTTOBRE					NOVEMBRE				DICEMBRE			
		Data inizio settimana			3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21
Specialistico		PCAP: Programming Essentials in Python	2					el 16	el 16																
	YE449I	VULNERABILITY ASSESMENT		2						16	16														
	SANS STELM	SEC501: Advanced Security Essentials - Enterprise Defender		1								16													
	SANS STELM	SEC501: Laboratori e attività propedeutica alle certificazioni SANS		1									16												
	SANS STELM	SEC504: Hacker Tools, Techniques, and Incident Handling		1												16									
	STELM	Laboratori e attività propedeutica alle certificazioni SANS		1													16								
	YE447A	CYBER NETWORK PROTECTION		2										16	16										
	Y455A	CYBER THREAT HUNTING		2														16	16						
	CIFIGE	Orientamento Cyber Intel		1																		16 cifige			
	SANS CIFIGE	SEC542: Web App Penetration Testing and Ethical Hacking		1																16					
	CIFIGE	Laboratori e attività propedeutica alle certificazioni SANS		1																	16				
	CIFIGE	Penetration Testing		2																			16 cifige	16 cifige	
		TOT specialistico	**2**	**15**																					

PARTECIPANTI (max 16):
Il corso è riservato agli Ufficiali a nomina diretta e al personale che opera nel settore *cyber* selezionato dallo SMD.

REQUISITI
Aver superato il corso operatore cyber di 1° livello.
È richiesta la capacità comprendere la lingua inglese, in quanto i corsi SANS (SEC501, SEC504 e SEC542) saranno svolti interamente in lingua inglese.

SONO PREVISTI ESAMI INTERMEDI E UN ESAME FINALE.

33.CYBER NETWORK PROTECTION – COD. Y447A

OBIETTIVI DEL CORSO
Fornire al personale destinato ad operare nell'ambito della *Cyber Defense*, mediante l'utilizzo di un ambiente simulato virtuale, le nozioni, le tecniche e gli strumenti per proteggere l'infrastruttura da eventi non previsti o deliberati, interni o prodotti dall'attaccante.

DURATA: 2 settimane in presenza.

PERIODO SESSIONI:
1ª – dal 23 marzo al 03 aprile in presenza.

NOTA: è prevista una 2ª sessione dal 16 al 27 novembre, in presenza, dedicata al personale straniero individuato da SMD III Reparto. In caso di mancato completamento della classe, sarà cura dello scrivente comunicare la disponibilità agli enti programmatori entro 60 gg. prima, che potranno candidare proprio personale con adeguata conoscenza lingua inglese (SLP minimo 3/2/3/2).

PARTECIPANTI (max 16)

COMANDI/ENTI	Sessioni
	1ª
ESERCITO	6
MARINA MILITARE	3
AERONAUTICA	2
CARABINIERI	1
COFS	1
COR	1
PERSOCIV	1
MAECI	1
TOTALE	**16**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: Corso Fondamenti di *Cyber Defence* (EY442B);
   b. Conoscenze basiche richieste:

      In alternativa alla frequenza preventiva del punto precedente sono richieste comprovate esperienze nel settore.

      Nozioni di programmazione, uso dei dispositivi di rete (switch/router), nozioni di TCP/IP e del software di analisi di rete Wireshark, uso dei sistemi operativi server Microsoft Windows/Linux e del software di virtualizzazione VMware *Workstation* e VirtualBox. Capacità di leggere documentazione in lingua inglese.
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN TEST DI INGRESSO NON SBARRANTE E UN ESAME FINALE.

34. COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) - COD. Y445A

OBIETTIVI DEL CORSO

Fornire al personale destinato ad operare nell'ambito della *Cyber Defence* i modelli organizzativi sui quali poter creare un CSIRT e le procedure per implementare i servizi di gestione ed analisi delle segnalazioni di eventi rilevanti per la sicurezza dei sistemi informativi della propria *costituency* e produzione di avvisi, bollettini e notizie.

DURATA: 2 settimane in presenza. Per gli Ufficiali della Scuola di Applicazione dell'Esercito il corso è stato rimodulato in 1 settimana.

PERIODO SESSIONI:

1ª – dal 25 maggio al 05 giugno in presenza;

2ª – dal 13 luglio al 17 luglio in presenza (sessione per la Scuola di Applicazione dell'EI).

PARTECIPANTI (max 14)

COMANDI/ENTI	Sessioni	
	1ª	***2ª***
ESERCITO	6	
EI - SCUOLA DI APPLICAZIONE		14
MARINA MILITARE	2	
AERONAUTICA	2	
CARABINIERI	1	
TOTALE	**11**	**14**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste:

      Dispositivi di rete (*switch/router*), protocolli TCP/IP e software di analisi di rete (Wireshark), Sistemi Operativi Server (Microsoft Windows/Linux) e software di virtualizzazione (VMware *Workstation*/VirtualBox).

      Capacità di leggere documentazione tecnica in lingua inglese.
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN TEST D'INGRESSO NON SBARRANTE E UN ESAME FINALE.

35. CYBER THREAT HUNTING - COD. Y455A

OBIETTIVI DEL CORSO

Fornire al personale destinato ad operare nell'ambito della *Cyber Defense*, mediante l'utilizzo di un ambiente simulato virtuale, le nozioni, le tecniche e gli strumenti per muoversi in modo proattivo, in particolare sulle proprie difese, partendo dall'assunto che l'attaccante sia già all'interno del proprio perimetro.

DURATA: 2 settimane in presenza.

PERIODO SESSIONI:

1ª – dal 02 al 13 marzo in presenza;

NOTA: è prevista una 2ª sessione dal 16 al 27 novembre, in presenza, dedicata al personale straniero individuato da SMD III Reparto. In caso di mancato completamento della classe, sarà cura dello scrivente comunicare la disponibilità agli enti programmatori entro 60 gg. prima, che potranno candidare proprio personale con adeguata conoscenza lingua inglese (SLP minimo 3/2/3/2).

PARTECIPANTI (max 16)

COMANDI/ENTI	Sessioni
	1ª
ESERCITO	5
MARINA MILITARE	4
CAPITANERIE di PORTO	
AERONAUTICA	4
CARABINIERI	
COFS	
COR	2
MAECI	1
TOTALE	**16**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: Corso Fondamenti di *Cyber Defence*;
   b. Conoscenze basiche richieste:

      In alternativa alla frequenza preventiva del punto precedente sono richieste comprovate esperienze nel settore.

      Nozioni di programmazione, uso dei dispositivi di rete (switch/router), nozioni di TCP/IP e del software di analisi di rete Wireshark, uso dei sistemi operativi server Microsoft Windows/Linux e del software di virtualizzazione VMware Workstation e VirtualBox. Capacità di leggere documentazione in lingua inglese.
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Di grado:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN TEST DI INGRESSO NON SBARRANTE E UN ESAME FINALE.

36.MALWARE ANALYSIS- COD. EY18A

OBIETTIVI DEL CORSO

Il Corso ha come obiettivo quello di introdurre i discenti alle moderne tecniche di analisi del malware e di fornire le competenze e gli strumenti per procedere all'analisi sia statica sia dinamica di campioni di malware reali ed attuali.

DURATA: 3 settimane in *e-learning sincrono*

PERIODO SESSIONI:

1ª – dal 18 maggio al 05 giugno in DAD.

PARTECIPANTI (max 16)

COMANDI/ENTI	Sessioni
	1ª
ESERCITO	7
MARINA MILITARE	2
AERONAUTICA	3
CARABINIERI	1
SMD II	1
COR	1
PERSOCIV	1
TOTALE	**16**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: comprovata professionalità attinente al corso;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Di grado:** Ufficiali, Sottufficiali, Sergenti, Graduati e personale civile della Difesa.

È PREVISTO ESAME FINALE

37.DIGITAL FORENSICS - COD. EY15A

OBIETTIVI DEL CORSO
Il corso ha l'obiettivo di far acquisire ai discenti le competenze necessarie nell'ambito della Digital Forensics, su aspetti teorici, tecnici, metodologie e norme giuridiche alle quali deve attenersi chi opera nel settore.

DURATA: 3 settimane in *e-learning sincrono*

PERIODO SESSIONI:
1ª – dal 13 al 31 luglio (in DAD).

PARTECIPANTI (max 16)

COMANDI/ENTI	Sessione
	1ª
ESERCITO	4
MARINA MILITARE	2
CAPITANERIE di PORTO	1
AERONAUTICA	1
CARABINIERI	1
DIFEGABINETTO	1
SMD II	1
SGD	1
COR	1
PERSOCIV	2
MAECI	1
TOTALE	**16**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: comprovata professionalità attinente al corso;
   c. Studio preventivo sinossi / testi propedeutici: N.N..
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO ESAME FINALE

38. CORSO CHIEF INFORMATION SECURITY OFFICER (CISO) - COD. EY456A

OBIETTIVI DEL CORSO

Il corso è progettato per fornire una formazione avanzata e multidisciplinare rivolta a coloro che aspirano a ricoprire il ruolo di *Chief Information Security Officer* (CISO) o che già lo ricoprono e vogliono consolidare le proprie competenze. Si affrontano le tematiche strategiche, normative, operative e tecnologiche legate alla sicurezza delle informazioni, alla *Governance*, alla gestione del rischio e alla risposta agli incidenti. Il CISO è una figura chiave nel garantire la resilienza digitale dell'organizzazione. Si occupa di gestire e attuare la strategia di sicurezza informatica in linea con la *mission* e i rischi aziendali, definire *policy* e programmi di sicurezza, coordinando personale, tecnologie e processi, monitorare e gestire i rischi *cyber*, pianificare la continuità operativa e la risposta agli incidenti, favorire la comunicazione e la cooperazione con *stakeholder* interni ed esterni e garantire la conformità alle normative e agli standard di sicurezza.

DURATA: 2 settimane in *e-learning* sincrona.

PERIODO SESSIONI:

1ª – dal 08 al 19 giugno (in DAD).

PARTECIPANTI (max 16)

COMANDI/ENTI	Sessione
	1ª
ESERCITO	4
MARINA MILITARE	1
CAPITANERIE di PORTO	1
AERONAUTICA	3
CARABINIERI	1
SMD II	1
COR	2
COFS	1
PERSOCIV	1
MAECI	1
TOTALE	**16**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste:
      - concetti di cybersecurity;
      - familiarità con *framwork* di gestione del rischio (es. NIST, ISO 27001)
   c. Studio preventivo sinossi / testi propedeutici: N.N..
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO ESAME FINALE

39. VULNERABILITY ASSESSMENT (V.A.) – COD.Y449I

OBIETTIVI DEL CORSO

Fornire al personale destinato ad operare nell'ambito della *Cyber Defence* le conoscenze di base relative alle vulnerabilità di sicurezza dei dispositivi di rete, dei sistemi operativi e delle applicazioni e far acquisire la capacità di utilizzare i programmi per il *vulnerability scanning* e le tecniche, al fine di:

- contestualizzare l'esistenza o meno di una vulnerabilità sfruttabile nei confronti di specifici *asset*;
- identificare secondo quali priorità attuare le diverse contromisure e misure di riduzione del rischio, in base alla valutazione della configurazione di sicurezza dell'infrastruttura ICT (analisi delle vulnerabilità in essa presenti e non "*patchate*").

DURATA: 3 settimane in presenza.

PERIODO SESSIONI:

1ª – dal 19 gennaio al 06 febbraio in presenza;

2ª – dal 08 al 26 giugno in presenza.

PARTECIPANTI (max 14)

COMANDI/ENTI	Sessione	
	1ª	***2ª***
ESERCITO	6	6
MARINA MILITARE	3	2
AERONAUTICA	2	2
CARABINIERI		1
SMD II	2	3
COR	1	
TOTALE	**14**	**14**

REQUISITI PER L'AMMISSIONE:

1. **Professionali**
   a. Frequenza preventiva: N.N;
   b. Conoscenze basiche richieste:

      Dispositivi di rete (*switch/router*), protocolli TCP/IP e software di analisi di rete (Wireshark), Sistemi Operativi Server (Microsoft Windows/Linux) e *software* di virtualizzazione (VMware *Workstation/VirtualBox*). Inglese tecnico;
   c. Studio preventivo sinossi / testi propedeutici:

      RFC/STD Internet per i protocolli di rete, documentazione a corredo dei dispositivi di rete, dei sistemi operativi e del *software* di virtualizzazione.
2. **Di Segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

È PREVISTO UN TEST D'INGRESSO NON SBARRANTE E UN ESAME FINALE.

40.FONDAMENTI DI CYBER DEFENCE - COD. EY442B

OBIETTIVI DEL CORSO

Fornire ai frequentatori le conoscenze generali e dottrinali sui diversi aspetti e sviluppi della *Cyber Defence* in ambito nazionale.

DURATA: 1 settimana in modalità *e-learning* asincrono (20 ore in piattaforma). Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 26 al 30 gennaio in DAD;

2ª – dal 09 al 13 febbraio in DAD;

3ª – dal 23 al 27 febbraio in DAD;

4ª – dal 04 al 08 maggio in DAD (sessione dedicata all'Accademia EI);

5ª – dal 01 al 05 giugno in DAD (sessione per gli Ufficiali AN della M.M).

PARTECIPANTI (max 35)

COMANDI/ENTI	**Sessioni**				
	1ª	***2ª***	***3ª***	***4ª***	***5ª***
ESERCITO	6	6	6	5	5
EI- ACCADEMIA MILITARE				14	
MARINA MILITARE	3	3	4	2	2
MM- UFFICIALI AN					11
CAPITANERIE di PORTO	2	2	2	1	1
AERONAUTICA	2	4	4		1
CARABINIERI	3	2	2		1
DIFEGABINETTO	3	2	2	1	
SMD I	1		1		
SMD II		2			1
SGD	1				
COVI	1				
COR	1		1		
COFS	1				
ITAQUARTIGEN					1
PERSOCIV	5	4	3	2	2
CONGEDATI	4	4	4	4	4
TOTALE	**33**	**29**	**29**	**29**	**29**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva:
      Modulo informativo per la *Cyber Defence*;
   b. Conoscenze basiche richieste:
      Conoscenze generali sulla Sicurezza informatica;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

La partecipazione alle attività sincrone/asincrone, definite e comunicate dagli Istruttori, sono obbligatorie ai fini dell'accesso all'esame finale.

È PREVISTO ESAME FINALE

AREA DATA SCIENCE E INTELLIGENZA ARTIFICIALE

41. BIG DATA ANALYSIS – COD. X004A (ex EY20A)

OBIETTIVI DEL CORSO

L'obiettivo del corso è quello di trasferire al discente le competenze necessarie per renderlo in grado di comprendere i *Big Data* e come effettuare delle analisi su di essi al fine di fornire il corretto supporto dei processi decisionali. Agli allievi saranno inoltre fornite competenze su *Social Network Analysis, Machine Learning e Data Mining*.

DURATA: 3 settimane in *e-learning*.

PERIODO SESSIONI:

1ª – dal 22 giugno al 10 luglio in DAD

PARTECIPANTI (max 16)

COMANDI/ENTI	Sessione
	1ª
ESERCITO	3
MARINA MILITARE	1
AERONAUTICA	2
CARABINIERI	1
CAPITANERIE di PORTO	1
SMD II	1
SGD	1
COR	2
PERSOCIV	2
MAECI	2
TOTALE	**16**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: comprovata professionalità attinente al corso;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.
3. **Di grado:** Ufficiali, Sottufficiali, Sergenti, Graduati e personale civile della Difesa.

42. FONDAMENTI DI INTELLIGENZA ARTIFICIALE (IA) – COD. EX002B (ex EY453B)

OBIETTIVI DEL CORSO

Il corso ha l'obiettivo di fornire ai frequentatori le conoscenze di base relative al concetto dell'Intelligenza Artificiale. Verranno affrontati gli aspetti principali dell'Intelligenza Artificiale quali i *Big Data*, l'apprendimento automatico o *Machine Learning*, l'apprendimento approfondito o *Deep Learning*, il *Natural Language Processing* quale comprensione ed elaborazione del linguaggio naturale, il confronto tra l'Intelligenza Artificiale e la robotica ed infine, verranno presentati dei campi di applicazione dell'Intelligenza Artificiale.

DURATA: 1 settimana in modalità *e-learning* sincrono (32 ore in piattaforma). Le attività a distanza sono disciplinate nell'Annesso.

PERIODO SESSIONI:

1ª – dal 19 al 23 ottobre in DAD;

2ª – dal 16 al 20 novembre in DAD.

PARTECIPANTI (max 25)

COMANDI/ENTI	Sessione	
	1ª	***2ª***
ESERCITO	4	4
MARINA MILITARE	3	3
AERONAUTICA	1	2
CARABINIERI	2	3
CAPITANERIE di PORTO	1	1
DIFEGABINETTO	1	1
SMD I -	1	
SMD II	1	
SGD	2	2
COR	1	2
COS	1	2
COFS	1	
ITAQUARTGEN	1	
PERSOCIV	3	4
MAECI	1	
ACISMOM		1
STELMILIT	1	
TOTALE	**25**	**25**

REQUISITI PER L'AMMISSIONE:

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: N.N.;
   c. Studio preventivo sinossi / testi propedeutici: N.N.
2. **Di segretezza:** NOS non richiesto.

3. **Di grado:** Ufficiali, Sottufficiali, Sergenti, Graduati e personale civile della Difesa.

È PREVISTO UN ESAME FINALE.

ANNESSO C - EROGAZIONE DEI CORSI IN MODALITÀ “DIDATTICA A DISTANZA” (DAD)

La gestione e l'erogazione di corsi e contenuti in modalità *a distanza* avviene a cura di personale docente che, utilizzando i Learning Object e gli strumenti della piattaforma, assicura l'attività di *tutoring*, monitoraggio ed *auditing*.

1. TIPOLOGIA DI CORSI IN MODALITÀ DIDATTICA A DISTANZA (DAD)

Nel presente Catalogo sono presenti le seguenti modalità di erogazione dei corsi svolti con Didattica a Distanza (DAD):

- *e-learning* asincrono: corsi erogati totalmente in modalità asincrona, che per loro natura possono essere seguiti in orari scelti in modo discrezionale del discente;
- *e-learning* sincrono: corsi che prevedono lezioni sincrone svolte attraverso *chat*, *forum* e videoconferenze. La partecipazione a tali attività, svolte in orari definiti dal docente e comunicati in piattaforma, è obbligatoria ai fini dell'accesso all'esame finale;
- *blended:* corsi che prevedono una fase a distanza propedeutica alla fase frontale. La fase a distanza può essere sincrona o asincrona ed è finalizzata a fornire le conoscenze necessarie ad armonizzare il livello dei frequentatori per una migliore efficacia didattica della successiva fase in presenza;
- *on-line training:* corsi sincroni che per la loro natura tecnica ed esperienziale richiedono l'acceso remoto in VPN ai laboratori della Scuola.

Infine, nell'area "Autoformazione" della piattaforma *e-learning* sono disponibili dei Moduli Informativi ad accesso libero, la cui fruizione non richiede la prevista iscrizione per il personale dell'A.D.
Utilizzando il link https://elearning.difesa.it/course/index.php?categoryid=171, si potrà accedere alle istruzioni riportate nella piattaforma stessa, senza alcuna ulteriore comunicazione alla Scuola.

2. MODALITÀ DI FRUIZIONE

Il personale iscritto dovrà svolgere il corso da una postazione che gli EDR dovranno mettere a disposizione dei discenti presso la sede di servizio, con *hardware, software* e connettività adeguata, come previsto dalla pubblicazione "Linee guida in materia di formazione in modalità *e-learning*" ed. 2012 dello Stato Maggiore Difesa.
Pertanto è responsabilità degli Enti di appartenenza dei frequentatori rendere disponibili le strutture e gli strumenti necessari per una proficua frequenza dei corsi svolti a distanza.
Ogni corso presenta peculiarità in termini di quantità e complessità dei contenuti da fruire a distanza, da cui discende la durata della fase *e-learning*.

Allo scopo di contemperare le esigenze di servizio con la frequenza dei corsi, per le attività che richiedono un impegno inferiore alle 36 ore settimanali, viene indicato il numero di ore da destinare allo studio dei contenuti presenti in piattaforma.
Pertanto gli impegni professionali del personale frequentatore di corso dovranno essere rimodulati in modo che non interferiscano con le attività formative programmate.
La piattaforma è raggiungibile all'indirizzo https://elearning.difesa.it[6] sia dalle reti intranet delle FF.AA. che da Internet. Sarà pertanto possibile accedere ai contenuti anche da qualsiasi postazione personale e senza alcuna limitazione temporale.

[6] Eventuali Link/URL/Portali, differenti dalla Piattaforma ed utili allo svolgimento delle attività di laboratorio effettuate a distanza, saranno comunicati ai frequentatori dai Referenti/Docenti dei relativi corsi.

Per i corsi svolti in modalità "*on line training*" l'accesso ai laboratori remoti deve essere effettuato da rete Internet con *client* di cui si posseggono i diritti amministrativi.
Per le attività di Formazione a Distanza sincrone[7] svolte in videoconferenza, l'Istituto si avvarrà di servizi commerciali esterni all'infrastruttura tecnica della Difesa (es. Cisco Webex), raggiungibili attraverso rete INTERNET. Si rammenta che è responsabilità degli Enti di appartenenza dei frequentatori rendere disponibili gli strumenti tecnici adeguati ad accedere a tali servizi.

3. NORME DI GESTIONE

a. Si rappresenta che le fasi *e-learning* di un percorso formativo sono didatticamente ed amministrativamente parte integrante del corso stesso. Non è pertanto ammessa la frequenza di più corsi contemporaneamente, anche se vi è una apparente sostenibilità in termini di sovrapposizione delle fasi didattiche.

b. La partecipazione alle attività sincrone/asincrone, definite e comunicate dagli Istruttori, sono obbligatorie ai fini dell'accesso all'esame finale.
Saranno pertanto dimessi dal corso e quindi non ammessi all'esame finale, tutti i discenti che alla scadenza definita dal docente non risulteranno in regola con tale requisito.

c. Il completamento della fase *e-learning* di un corso in modalità *blended* è condizione necessaria per la partecipazione alla successiva fase in presenza.
Saranno pertanto dimessi dal corso e quindi non ammessi alla fase in presenza, tutti i discenti che alla scadenza definita dal docente non risulteranno in regola con tale requisito.

4. TOOLS DI GESTIONE

La metodologia *e-learning* può utilizzare una serie di strumenti tecnologici funzionali a consentire l'interattività tra docenti e frequentatori e tra i frequentatori stessi. Il ricorso all'interattività, utilizzata inizialmente per sopperire ad alcune problematiche della comunicazione non verbale, è divenuto uno dei punti di forza della metodologia, vista la possibilità di utilizzare *tools* dedicati e di facile uso. Gli strumenti che in particolare potranno essere maggiormente utilizzati in ambito didattico sono:

- Videoconferenza;
- *Forum*;
- *Chat*;
- *Wiki*;
- *Mailing List*;
- *Peer Evaluation*.

5. SEGNALAZIONI ED INIZIO CORSO E-LEARNING

I percorsi formativi che prevedono una fase *e-learning* preventiva e/o che sono erogati totalmente in *e-learning* sono indicati all'interno del presente Catalogo dei Corsi.
Per tali corsi formativi (*blended/e-learning*), gli EDR deputati alla segnalazione dei frequentatori dovranno comunicare alla Scuola i dati di ciascuno di essi, comprensivi della mail istituzionale, almeno 3 settimane prima dell'inizio della fase in questione.
Si evidenzia che le *policy* di utilizzo della Piattaforma non consentono la registrazione di utenti con e-mail che NON siano istituzionali.

[7] Le attività sincrone a distanza sono riportate nelle schede dei Corsi interessati.

6. MONITORAGGIO DELLE ATTIVITÀ

Durante il periodo previsto per lo svolgimento della fase *e-learning* di un corso *blended* o di un corso *e-learning*, sarà responsabilità del frequentatore gestire i periodi di fruizione delle lezioni, ad eccezione dei periodi obbligatori eventualmente individuati dalla Scuola per attività interattive predeterminate.

Sarà responsabilità del *tutor* di processo/docente controllare e verificare l'andamento ed il raggiungimento dei risultati delle classi e dei singoli, utilizzando gli strumenti di reportistica resi disponibili dal sistema.

Qualora si evidenziassero delle problematiche nella fruizione dei contenuti, il *tutor*/docente interagirà direttamente con il frequentatore per individuare soluzioni adeguate.

Nel caso risulti compromesso il raggiungimento degli obiettivi formativi del corso (mancato completamento della fase a *e-learning* nel periodo definito e/o inadeguato avanzamento nelle attività didattiche proposte/previste), il *tutor* di processo/docente informerà la propria "*line*" al fine di decretare l'esclusione del discente dal corso, precludendone la partecipazione alla successiva fase in presenza e/o esame finale.

La Segreteria Corsi provvederà a comunicare le dimissioni dal corso al Comando di appartenenza e al discente stesso.

7. ESAME DI FINE CORSO E RICONOSCIMENTO DELLE ATTIVITÀ SVOLTE

Per i corsi erogati totalmente a distanza, in aderenza con quanto previsto al para 4 della pubblicazione "Linee guida in materia di formazione in modalità *e-learning"* ed. 2012 dello Stato Maggiore Difesa, al fine di consentire l'annotazione a matricola del corso frequentato, l'Ente/Comando di appartenenza del frequentatore dovrà, con apposito atto, nominare una "Commissione di controllo locale" con esclusiva funzione di sorveglianza, volta a garantire il corretto svolgimento del *test* di fine corso.

La Commissione di controllo dovrà essere composta da tre unità come di seguito specificato:

- Presidente (dovrà essere di grado superiore al valutato);
- Membro;
- Membro e Segretario.

Tale commissione avrà il compito di controllare che le prove si svolgano secondo le seguenti norme di correttezza:

- l'esame si dovrà svolgere in un locale nel quale non dovrà essere consentito l'accesso a personale estraneo, per tutta la durata della prova;
- il locale dovrà essere dotato di un computer per ogni discente, con accesso alla piattaforma;
- durante l'esame il frequentatore potrà accedere esclusivamente alla piattaforma e-learning e potrà utilizzare esclusivamente eventuali propri appunti. Dovrà pertanto essere preclusa la possibilità di consultare siti internet.

Per i corsi erogati in modalità *e-learning* (sia sincroni che asincroni), la Scuola Telecomunicazioni FF.AA. rilascia l'attestato di frequenza con i dati utili alla compilazione della documentazione caratteristica (mod. D o mod. B) e alla trascrizione matricolare.

La valorizzazione dei risultati conseguiti e la produzione del relativo modello è rimessa alla discrezionalità del compilatore, in quanto il corso è fruito senza alcun distacco dall'usuale luogo di lavoro e con continuità lavorativa alle dipendenze dello stesso.

Procedura per sostenere l'esame finale a distanza[8]:

- Il discente, per accedere all'esame finale di un corso, deve aver completato tutti i moduli didattici e superato eventuali accertamenti intermedi;
- Il Comando di appartenenza del discente dovrà nominare la suddetta Commissione di controllo locale con formale atto di nomina;
- Al termine dell'esame la Commissione di controllo dovrà inviare via mail alla Segreteria Corsi della Scuola (stelmilit.corsi@marina.difesa.it), copia del verbale d'esame redatto secondo il modello in appendice 1, debitamente compilato e firmato.
- Lo stesso verbale d'esame dovrà essere inoltre caricato dal discente sulla piattaforma stessa che, a seguito della sua acquisizione, rilascerà copia dell'attestato di partecipazione con indicazione dell'esito finale e del punteggio conseguito.

[8] Si rammenta che l'esame finale a distanza è differibile esclusivamente per gravi e comprovati motivi (es. malattia), opportunamente vagliati dal Comando di appartenenza del discente. Il Comando dovrà comunicare via mail, in data antecedente l'esame, tale esigenza alla Segreteria corsi della Scuola (stelmilit.corsi@marina.difesa.it), la quale valuterà la possibilità di differimento coordinandosi con le Sezioni didattiche per la pianificazione della prova in data confacente alle parti (Istruttori/Discenti).

Appendice 1

VERBALE D'ESAME DEI CORSI SVOLTI A DISTANZA

Corso:	
Data esame:	
Ora inizio:	
Ora fine:	

ELENCO CANDIDATI		
n.	Grado, Cognome, Nome	Numero CMD / tessera di riconoscimento
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Si attesta che il personale sopra elencato ha sostenuto la prova d'esame in modo autonomo, senza consultare materiale non autorizzato, secondo le indicazioni definite nel catalogo dei corsi di STELMILIT.

LA COMMISSIONE DI CONTROLLO

Grado, Cognome, Nome	Numero CMD	FIRMA