SCUOLA TELECOMUNICAZIONI FF.AA.
E
POLO FORMATIVO CYBER

Catalogo dei Corsi Interforze
Anno Accademico 2027

Edizione giugno 2026

Scuola Telecomunicazioni FF.AA.
e
Polo Formativo Cyber

ATTO DI APPROVAZIONE

Approvo il Catalogo dei Corsi Interforze della Scuola Telecomunicazioni delle Forze Armate e Polo formativo Cyber in Chiavari per l'Anno Accademico 2027.

Chiavari, 19/06/2026

IL COMANDANTE
C.V. Stefano COSSU

Firmato Digitalmente da/Signed by:
STEFANO COSSU

In Data/On Date:
venerdì 19 giugno 2026 14:00:38

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
- COMANDO INTERFORZE CYBER INTEL – R.I.S.
- 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 DELLE OPERAZIONI SPAZIALI
CENTRO ALTI STUDI PER LA DIFESA

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 ACISOM

Sommario

1. PREMESSA

La missione primaria della Scuola Telecomunicazioni delle FF.AA. è la formazione specialistica, la qualificazione e l'aggiornamento del personale militare e civile dell'Amministrazione della Difesa (AD) nel settore dell'*Information Technology (IT)* e della Sicurezza delle Informazioni (INFOSEC).

Le continue e rapide evoluzioni tecnologiche del mondo delle tecnologie IT e INFOSEC coinvolgono in pieno tutte la realtà della Difesa e, pertanto, è necessario un continuo e rapido adeguamento dell'offerta formativa proposta da questo Istituto al fine di rendere disponibile una formazione sempre aggiornata e pienamente rispondente alle necessità delle Forze Armate.

La proposta formativa presentata in questo catalogo tiene conto di tali evoluzioni ed è sviluppata sotto la supervisione dello Stato Maggiore della Difesa, elemento sovraordinato e competente a fornire gli indirizzi nel settore della formazione interforze nel campo dell'IT e dell'INFOSEC. Tali indirizzi vengono forniti in occasione del *Workshop* sulla formazione interforze in ambito IT, ICT e CYBER che si tiene annualmente nel primo trimestre.

A questo documento farà seguito il Calendario dei Corsi 2027 che sarà elaborato sulla base delle richieste di partecipazione, che perverranno da parte delle singole F.A. e delle altre Amministrazioni dello Stato indicate nell'elenco di distribuzione di questo documento.

2. SCOPO

Il presente Catalogo dei Corsi ha lo scopo di illustrare l'offerta formativa della Scuola Telecomunicazioni FF.AA. per l'Anno Accademico 2027, capacità destinata prioritariamente al personale dell'AD ma fruibile, a titolo oneroso, anche dal personale della Pubblica Amministrazione fatte salve le previste autorizzazioni di competenza da richiedere al I Reparto dello Stato Maggiore della Difesa. Inoltre, non appena saranno perfezionate le convenzioni tra l'AD e Difesa Servizi S.p.A., saranno, altresì, possibili le iscrizioni di personale di altre articolazioni dello Stato e di aziende civili previa la sottoscrizione di appositi contratti di fornitura di corsi da parte della Scuola per il tramite di Difesa Servizi S.p.A..

3. STRUTTURA E CONTENUTI

Il documento è indirizzato a:

- Enti Programmatori della Difesa, indicati al successivo para. 6., in qualità di elementi di organizzazione deputati a segnalare alla Scuola le esigenze formative del proprio personale dipendente;
- Al Ministero degli Affari Esteri e della Cooperazione Internazionale, in considerazione del Protocollo di intesa stipulato con il Ministero della Difesa nel dicembre 2023;
- Organismi governativi, indicati al successivo para. 6., che intendano usufruire dell'offerta formativa della Scuola (esclusivamente a titolo oneroso e a seguito della stipula della Convenzione tra Difesa Servizi e lo Stato Maggiore della Difesa).

In particolare, il Catalogo dei Corsi:

- elenca i Corsi che la Scuola è in grado di erogare;
- fornisce informazioni utili ad individuare i Corsi atti a soddisfare le specifiche esigenze di formazione del personale (obiettivi del corso, durata, programma del corso, requisiti minimi per l'ammissione, ecc.);
- fornisce indicazioni utili agli Enti Programmatori per l'attivazione delle procedure di segnalazione e partecipazione ai Corsi (Annesso I);
- fornisce notizie circa le modalità logistiche/amministrative per la partecipazione ai Corsi e rende disponibili informazioni di carattere generale sulle attività nell'Istituto (Annesso II);
- fornisce le modalità di erogazione dei corsi in modalità a distanza (Annesso III).

La parte descrittiva dei Corsi è suddivisa nei seguenti cinque settori:
- Livello Avanzato;
- Livello Intermedio;
- Livello Base;
- Portfolio Stranieri.

Inoltre, il Catalogo Corsi prevede dei percorsi formativi per personale straniero di competenza di SMD III Reparto. Nell'ambito dei corsi offerti in tale contesto (Portfolio Stranieri), qualora alcune posizioni non risultassero utilmente ricoperte, gli Enti Programmatori potranno avanzare le candidature del proprio personale, che potrà avere accesso ai corsi in lingua inglese con un livello minimo di conoscenza della lingua pari a L 3, R 3, S 2, W 2. Sarà cura di STELMILIT fornire dettagli circa la disponibilità di posizioni per tali corsi con adeguato preavviso.

I corsi sono inoltre raggruppati secondo le seguenti aree tematiche:

- *Transport & Networking*;
- *Software*, Applicativi e *e-Learning*;
- *Infosec* e *Information Assurance*;
- *Cyber Defence*, Law & *Forensics*;
- *Data Science* e Intelligenza Artificiale;
- Corsi di interesse del COS e del CIGC SICRAL.

Laddove, nel corso dell'anno, i corsi debbano subire modifiche nella definizione dei contenuti didattici o su aspetti di carattere organizzativo (modalità di iscrizione, siti di riferimento, requisiti di ammissione, ecc.), ne sarà data opportuna comunicazione agli Enti Programmatori e pubblicate le relative varianti.

Al fine di consentire la realizzazione del Calendario dei Corsi 2027, gli Enti Programmatori (elencati ai successivi paragrafi 6. e 7.) dovranno inoltrare le esigenze formative **entro il 30 settembre 2026 (si terrà conto della data del protocollo della segnalazione).** Nelle segnalazioni dovrà essere indicato unicamente il nome/codice del corso ed il numero delle posizioni desiderate (non saranno prese in considerazione segnalazioni che includano i nominativi dei discenti).

Il citato Calendario fornirà indicazioni sul programma temporale dei Corsi e sulle relative sessioni che saranno attivate nel 2027 e, inoltre, conterrà l'informazione relativa al numero di posti assegnati a ciascun Ente Programmatore.

Gli Enti Programmatori che intendano proporre ulteriori "percorsi formativi" potranno rappresentare l'esigenza durante il *Workshop* sulla formazione interforze. Valutata la fattibilità e la sostenibilità, la Scuola provvederà all'inserimento in catalogo del percorso formativo in questione.

Il presente Catalogo è pubblicato, in formato "pdf", nei seguenti siti istituzionali:

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

Ulteriori richieste di informazioni possono essere inoltrate dagli Enti Programmatori/Comandi di appartenenza dei discenti al seguente punto di contatto della Direzione Corsi della Scuola:
e-mail: stelmilit.corsi@marina.difesa.it, 0185 3334509/10 o 7228509/10 (linea MM).

4. NOVITÀ APPORTATE AL CATALOGO

La presente edizione del Catalogo è stata aggiornata con l'inserimento dei seguenti nuovi corsi:

CORSI DI LIVELLO AVANZATO

- Corso "Red Hat Openstack Administation" – Cod. ET305A;
- Corso "IA e Tecniche di *Prompting* Avanzato" – Cod.EX003A;

CORSI DI LIVELLO INTERMEDIO

- Corso "Cloud Computing & Virtualization Specialist"- Cod. T500I.

CORSI DI LIVELLO BASE.

Inoltre, è stato eliminato dal Catalogo il seguente corso:

CORSI DI LIVELLO AVANZATO

- Corso S.O. in Networking cod TE262A

5. METODOLOGIA DIDATTICA DEI CORSI

La Scuola eroga i corsi elencati nel presente catalogo in modalità "in presenza", in modalità "*blended"* (prevede una fase "a distanza" e una fase "in presenza") e in modalità "a distanza" (DAD), quest'ultima secondo le seguenti tipologie:

- *e-learning* asincrono*;*
- *e-learning* sincrono*;*
- *on-line training* (laboratori remotizzati),

i cui dettagli sono riportati nell'Annesso III del presente Catalogo (incluse le modalità per lo svolgimento della fase a distanza per i corsi *blended*).

I Moduli Informativi, qualora disponibili, accessibili sulla piattaforma e-learning della Scuola, sono concepiti con finalità esclusivamente divulgative, pertanto non richiedono alcuna procedura di iscrizione e non prevedono lo svolgimento di prove finali. La loro fruizione non dà luogo al rilascio di attestati né determina annotazioni a matricola.

Oltre alle citate tipologie di corsi, la Scuola può svolgere conferenze ossia eventi a scopo informativo sulle tematiche *Cyber* e sui relativi aspetti operativi presso gli Enti/Comandi che ne facciano richiesta. Tale fattispecie potrà essere prospettata alla Direzione Corsi della Scuola che valuterà la fattibilità concordando con i richiedenti le date di eventuale svolgimento delle conferenze. Gli oneri di missione del personale istruttore designato allo svolgimento di tali conferenze saranno a carico degli Enti/Comandi richiedenti. (POC: stelmilit.corsi@marina.difesa.it – linea M.M. 28509/10 - linea civile 0185 3334509/10).

6. ENTI PROGRAMMATORI DELLA DIFESA

Sono di seguito elencati gli Enti della Difesa preposti all'individuazione delle esigenze di partecipazione ai Corsi e responsabili dell'iscrizione e della comunicazione dei frequentatori alla Scuola:

a. Ministero della Difesa

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

b. Difesa

- Stato Maggiore della Difesa:
  - I Reparto Personale;
  - Comando Interforze Cyber Intel - RIS
  - 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 delle Operazioni Spaziali (COS);
- Centro Alti Studi per la Difesa (CASD).

c. Esercito

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

d. <u>Marina Militare</u>
- Comando Scuole della Marina Militare;
- Direzione per l'impiego del Personale della Marina Militare;
- Stato Maggiore Marina Reparto C4S.

e. <u>Aeronautica Militare</u>
- Stato Maggiore dell'Aeronautica - Reparto Generale Sicurezza (per i soli corsi dell'area INFOSEC);
- Comando Logistico - III Divisione.

f. <u>Arma dei Carabinieri</u>
- Comando Generale dell'Arma dei Carabinieri:
  - S.M. - Ufficio Addestramento e Regolamenti;
  - S.M. - Ufficio Sicurezza;
  - Ufficio Sviluppo Tecnologico.

g. <u>Capitanerie di Porto</u>
Comando Generale delle Capitanerie di Porto.

h. <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).

7. <u>ALTRI COMANDI/ENTI/AMMINISTRAZIONI</u>

- Presidenza della Repubblica - Segretariato Generale;
- Presidenza del Consiglio dei Ministri - Ufficio del Segretario Generale;
- Ministero degli Affari Esteri e della Cooperazione Internazionale (MAECI);
- Polizia di Stato;
- Comando Generale Guardia di Finanza;
- Polizia Penitenziaria;
- Dipartimento dei Vigili del Fuoco, Soccorso Pubblico e Difesa Civile.
- Corpo Militare ACISMOM.

8. <u>VARIE</u>

Le informazioni di carattere logistico-amministrativo e le modalità di segnalazione dei frequentatori sono inserite rispettivamente negli Annessi I e II.

<u>Agli Enti che risulteranno assegnatari di posti nel Calendario dei Corsi 2027</u> è richiesto di:

- comunicare i dati di ciascun frequentatore con **almeno 3 settimane di anticipo** rispetto all'inizio del corso mediante la Scheda "A" e inviare la Scheda Anagrafica del frequentatore, entrambe poste in Annesso I. Si chiede di prestare particolare attenzione alla compilazione della scheda anagrafica perché i dati saranno utilizzati anche per la stesura della prevista documentazione caratteristica. In particolare si chiede di prestare particolare attenzione alla corretta abbreviazione del grado, ruolo, Arma e specialità come riportato nei documenti caratteristici, luogo e data di nascita, corretta indicazione del Reparto/Ente di appartenenza.
- comunicare con il massimo anticipo l'eventuale indisponibilità del personale designato, in modo da consentire, in caso non vengano individuati dei sostituti, la riassegnazione dei posti in base alla lista di attesa (a cura della Scuola);
- segnalare, per i Corsi che lo richiedono, il possesso dei requisiti di sicurezza del personale frequentatore;
- segnalare, per i Corsi in modalità a distanza, i dati di ciascun frequentatore (comprensivi della mail istituzionale, del Codice Fiscale e del numero della tessera CMD) almeno 3 settimane prima dell'inizio del corso in questione.

CAPITOLO 1 – CORSI DI LIVELLO AVANZATO

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.

AREA
Transport & Networking

PROGRAMMA/ARGOMENTI TRATTATI
- Struttura costruttiva, propagazione della luce nelle fibre ottiche, apertura numerica, angolo limite;
- modi di propagazione, tipi di fibre, dispersione modale;
- riduzione della dispersione: fibre *Graded* Index e monomodali;
- dispersione cromatica, attenuazione e larghezza di banda, finestre ottiche, cavi in fibra ottica, protezioni primarie e secondarie, protezione *tight* e *loose*;
- accoppiamenti: perdite di interconnessione tra le fibre ottiche (intrinseche ed estrinseche), giunzioni a fusione e giunzioni meccaniche, connettori, tecnologica delle fibre ottiche;
- sorgenti ottiche: LED, diodo laser, accoppiamento sorgente-fibra;
- rivelatori ottici: fotodiodo APD e PIN, fotodiodo a valanga, accoppiamento fibra-rivelatore, amplificazione del segnale rivelato;
- trasmissione dati connettorizzazione a resinare, crimpare, prelappati e preresinati tipo ST, SC, LC;
- misura di attenuazione totale con il metodo d'inserzione nelle tre finestre operative con sorgente LED e LASER;
- principi di funzionamento dell'OTDR, determinazione delle perdite nelle giunzioni con l'OTDR, localizzazione dei guasti e misura della potenza retrodiffusa;
- giunzioni a fusione e meccaniche;
- preparazione di un armadio di rete e multiplazione di segnali digitali. Tecnica WDM.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 10.

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 III.

È PREVISTO UN ESAME FINALE.

AREA SOFTWARE, APPLICATIVI E *E-LEARNING*

2. RED HAT OPENSTACK ADMINISTRATION - COD. ET305A

OBIETTIVI DEL CORSO

Nell'attuale scenario IT, caratterizzato da un'evoluzione continua verso architetture cloud private e ibride e dalla necessità di garantire disponibilità, scalabilità e sicurezza dei servizi, la capacità di gestire piattaforme di cloud computing complesse rappresenta una competenza strategica per il personale tecnico. Il presente percorso formativo fornisce ai partecipanti una preparazione completa sull'utilizzo e sulla gestione di ***Red Hat OpenStack Platform***, la soluzione enterprise di riferimento per la realizzazione di cloud privati scalabili e sicuri.
Attraverso un approccio teorico-pratico, il corso guida i discenti nell'analisi dell'architettura *OpenStack*, nella gestione delle risorse di dominio (reti, storage, istanze, progetti) e nelle attività operative quotidiane tipiche degli ambienti enterprise. La seconda parte del percorso approfondisce le operazioni "*Day-2*", includendo gestione del control plane, sicurezza infrastrutturale, monitoraggio, automazione e *troubleshooting* avanzato, con particolare attenzione ai contesti in cui affidabilità e continuità del servizio sono requisiti essenziali.
Il corso prevede esercitazioni guidate su ambiente virtuale per consolidare le competenze acquisite e consentire ai partecipanti di operare in autonomia nella gestione di un'infrastruttura *OpenStack* in produzione.

AREA

Software/Applicativi/*E-learning*

PROGRAMMA/ARGOMENTI TRATTATI

Modulo I – (Rif. CL110)

- Architettura *OpenStack* e componenti principali
- Gestione utenti, progetti, ruoli e quote
- *Networking: subnet, router, floating IP*
- *Storage* a blocchi e a oggetti
- Deployment di istanze e stack
- *Cloud-init* e personalizzazione delle immagini
- *RHOSP Director*: installazione e gestione PoC

Modulo II – (Rif. CL210)

- Architettura *undercloud/overcloud*
- *Control plane*: servizi principali e gestione
- Sicurezza infrastrutturale e gestione privilegi
- Gestione immagini, versioni e metadati
- *Storage e Ceph backend*
- Nodi di elaborazione e scalabilità
- Monitoraggio operativo e metriche
- Automazione applicativa
- *Troubleshooting* avanzato

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva: N.N.;

b. Conoscenze basiche richieste: in ambito sistemi Linux familiarità con comandi, gestione dei processi, permessi, servizi e configurazioni essenziali. capacità di leggere e comprendere semplici *script* o automatismi, utili per l'interazione con CLI e strumenti di gestione, concetti relativi a *subnet*, *routing*, indirizzamento IP, *firewalling* e servizi di rete, comprensione dei principi di *hypervisor*, macchine virtuali, storage e reti virtuali. **Conoscenza preliminare di *Docker*** (consigliata), utile per comprendere i modelli di deployment, la gestione delle immagini e i concetti di containerizzazione che ricorrono anche nelle architetture *OpenStack* moderne
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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
2 settimane in modalità *on-line training* sincrona.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

3. 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.

AREA

Software/Applicativi/E-Learning.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- Rif. Corso MOC20740 - Installation, Storage, and Compute with Windows;
- Rif. Corso MOC20741 - Networking with Windows Server 2016;
- Rif. Corso MOC20742 - Identity with Windows Server 2016;
- Rif. Corso MOC20744 - Securing Windows Server 2016.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva:
      Corso Progettazione e gestione reti locali Cod. RE235J;
      Corso Windows Server per Amministratori.

      In alternativa alla frequenza preventiva il frequentatore dovrà possedere:
      - 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;

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

2. **Di segretezza:**
   NOS non richiesto.

3. **Categorie:**
   Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
4 settimane di cui 40% di laboratorio, in modalità "*on-line training*".

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

4. 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.

AREA
Software/Applicativi/E-Learning.

PROGRAMMA/ARGOMENTI TRATTATI
Il corso si articolerà sul seguente programma:
- Rif. Corso MOC WS 011: Administration.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva: Corso Sistema Operativo Windows 2012 o 2016 Server.
   b. Conoscenze basiche richieste:

      In alternativa alla frequenza preventiva il frequentatore dovrà possedere:
      - 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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
1 settimana di cui 50% di laboratorio, in modalità "*on-line training*".

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

5. 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.

AREA
Software/Applicativi/E-Learning

PROGRAMMA / ARGOMENTI TRATTATI
Argomenti trattati nella fase e-learning[1]
- introduzione a RedHat/CentOS;
- installazione;
- procedure di autenticazione;
- struttura del file System XFS;
- comandi Linux;
- editor di testo Vim e Gedit;
- autorizzazioni, permessi speciali e proprietà dei file;
- comandi filtro;
- processi Linux;
- processi in foreground e background;
- archiviazione e compressione;
- backup incrementali con Tar
- RPM (Package Manager);
- installazione del software con Yum;
- installazione del software con DNF.

Argomenti trattati nella fase in presenza
Concetti di Amministrazione di Sistema
- procedura di inizializzazione del sistema;
- il *boot* (*grub2*);
- sicurezza del grub;
- il processo *Systemd*;
- i target di sistema;
- il processo INIT (storia);
- la shell bash;
- utilizzo di altre *shell* (sh, csh e zsh);
- gestione degli utenti/gruppi;
- gestione degli Access Control List;
- gestione del disco (fdisk/parted);
- configurazione di più dischi in RAID;
- controlli amministrativi (comandi su e sudo)
- automazione del sistema.

[1]Argomenti trattati in maniera più esaustiva e differenziata rispetto al CORSO E-LEARNING SU S.O. LINUX BASE: COD. ET23B

Concetti di Amministrazione di Rete
- Introduzione al networking con Linux;
- configurazioni di rete;
- bonding;
- routing;
- gestione dei servizi di rete con *systemctl* (attivazione a richiesta e al *boot*)
- emulazione di terminale SSH;
- trasferimento di file con SFTP E SCP;
- configurazione dei servizi server (DNS, DHCP, Web service Apache);
- condivisione in rete (NFS, SAMBA);
- aspetti di sicurezza;
- protocolli Wrapper;
- console web di RHEL.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva: CORSO E-LEARNING SU S.O. LINUX BASE – COD. ET23B;
      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.
   b. 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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

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

È PREVISTO TEST INGRESSO (a termine fase e-learning)

È PREVISTO ESAME FINALE (a termine fase in presenza)

[2] Le indicazioni inerenti alle eventuali attività sincrone saranno comunicate dagli Istruttori del corso (Rif. Annesso III del presente Catalogo); tali attività andranno obbligatoriamente seguite e l'eventuale assenza verrà conteggiata ai fini dei requisiti per poter accedere alla fase in presenza e/o sostenere l'esame.

6. 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.

AREA
Software/Applicativi/E-Learning

PROGRAMMA/ARGOMENTI TRATTATI
Il corso si articolerà sul seguente programma:
- Rif. Corso EX052IT: Vmware Vsphere: Install, Configure, Manage (V8)®

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. frequenza preventiva: Windows Server per Amministratori; progettazione e gestione reti locali RE235I;
      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;
   b. studio preventivo sinossi / testi propedeutici: N.N.;

2. **Di segretezza:**
   NOS non richiesto;

3. **Categorie:**
   Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

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

È PREVISTO ESAME FINALE.

7. 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.

AREA
Software/Applicativi/E-Learning

PROGRAMMA/ARGOMENTI TRATTATI
Il corso si articolerà sul seguente programma:
- Rif. Corso MOC20345-1: *Administering* Microsoft *Exchange Server* 2016-2019®

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. frequenza preventiva: Windows *Server* per Amministratori;
      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).
   b. studio preventivo sinossi / testi propedeutici: N.N.;

2. **Di segretezza:**
   NOS non richiesto;

3. **Categorie:**
   Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di **12**.

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

È PREVISTO ESAME FINALE

8. 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.

AREA
Software/Applicativi/E-Learning

PROGRAMMA/ARGOMENTI TRATTATI
Il corso si articolerà sul seguente programma:
- Rif. Corso MOC20339.1: Planning and Administering SharePoint 2016®

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI
1. **Professionali:**
   a. frequenza preventiva: Windows Server per Amministratori;
      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
   b. studio preventivo sinossi / testi propedeutici: N.N.;

2. **Di segretezza:** NOS non richiesto;

3. **Categorie:**
   Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di **12**.

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

È PREVISTO ESAME FINALE

9. 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.

AREA
Software/Applicativi/E-Learning

PROGRAMMA/ARGOMENTI TRATTATI
Il corso si articolerà sul seguente programma:
- Rif. Corso MOC20765: *Provisioning* Sql Databases ®

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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. studio preventivo sinossi / testi propedeutici: N.N.;

2. **Di segretezza:** NOS non richiesto;

3. **Categorie:** Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di **12**.

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

È PREVISTO ESAME FINALE

10.LINGUAGGIO PYTHON - COD. T30A

OBIETTIVI DEL CORSO
II Corso ha l'obiettivo di fornire le conoscenze tecniche specifiche per formare figure professionali in grado di utilizzare il linguaggio Python partendo da concetti introduttivi (sintassi, semantica, tipi di dati) fino ad arrivare a tematiche più avanzate (principali vulnerabilità alle quali i programmi Python possono essere soggetti e le contromisure da adottare per mitigarle).

AREA
Software/Applicativi/E-Learning

PROGRAMMA/ARGOMENTI TRATTATI
- Introduction to Python
- Control flow - conditional blocks and loops
- Data collection – Tuples, dictionaries, lists and strings
- Functions and Excpetions
- Modules and packages
- Exceptions
- Strings
- Object-oriented Programming

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
2 settimane (la modalità "in presenza" o in "*e-learning* sincrono" verrà definita nel calendario dei corsi).

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

AREA INFOSEC E *INFORMATION ASSURANCE*

11. 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).

AREA
INFOSEC e *Information Assurance*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 8.

DURATA DEL CORSO:
2 settimane: 1 settimana in modalità *e-learning* asincrono (15 ore) e 1 settimana in presenza.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

12. 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.

AREA
INFOSEC e *Information Assurance*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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, Sottufficiali, Graduati (solo personale in Servizio Permanente) e personale civile della Difesa impiegati/designati a ricoprire incarichi nel settore COMSEC.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
2 settimane in presenza.

È PREVISTO UN ESAME FINALE.

13.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.

AREA
INFOSEC e *Information Assurance*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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, Sottufficiali, Graduati e Personale Civile della Difesa, impiegati/designati a ricoprire incarichi nella gestione della sicurezza CIS.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO:
1 settimana in presenza.
In base alla disponibilità del personale istruttore il corso potrebbe essere rimodulato in *e-learning* sincrono; in tal caso tale evenienza verrà comunicata nel Calendario Corsi o con comunicazione ad hoc.

È PREVISTO UN ESAME FINALE.

14. 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.

AREA
INFOSEC e *Information Assurance*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
2 settimane in presenza.

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.

15. 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 ICT che della tutela delle informazioni classificate.

AREA
INFOSEC e *Information Assurance*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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/designati a ricoprire incarichi nella gestione della sicurezza CIS.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
2 settimane in presenza.

È PREVISTO UN ESAME FINALE.

16.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).

AREA
INFOSEC e *Information Assurance*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 6.

DURATA DEL CORSO:
2 settimane: 1 settimana in modalità *e-learning* asincrono (15 ore) e 1 settimana in presenza.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

17.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.

AREA
INFOSEC e *Information Assurance*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 5.

DURATA DEL CORSO:
2 settimane: 1 settimana in modalità *e-learning* asincrono per visione video tutorial KNMS 2100 IP (15 ore in piattaforma) e 1 settimana in presenza.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE

18. IT-EKMS CUSTODE CIFRA PER UTENTI LDF DELLE F.A. – COD. J450A

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

AREA
INFOSEC e *Information Assurance*

REQUISITI MINIMI PER L'AMMISSIONE

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

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 6.

DURATA DEL CORSO:
1 settimana in presenza.

È PREVISTO UN ESAME FINALE.

AREA *CYBER DEFENCE*, *LAW* & *FORENSICS*

19.CORSO BASICO - OPERATORE CYBER DELLA DIFESA - COD. Y001A

OBIETTIVI DEL CORSO
Formare il personale designato ad operare in ambito cyber, fornendo le necessarie competenze nell'ambito delle seguenti aree tematiche:
- Difesa proattiva;
- Sistemi operativi;
- Programmazione;
- Legal.

AREA
Cyber Defence, Law & Forensics

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

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

PROGRAMMA/ARGOMENTI TRATTATI (rife. Syllabus approvato da SMD)
Il corso si articolerà nei seguenti moduli:

- Fondamenti di Diritto Internazionale applicato alle Operazioni cibernetiche;
- S.O. Linux base*;*
- CCNA Introduction to Networks (ITN);
- CCNA Switching, Routing and Wireless Essential (SRWE);
- CCNA Enterprise Networking, Security and Automation (ENSA);
- Modulo CISCO Exam Preparation;
- Security Information and Event Management (SIEM);
- Windows Server (2016 e 2019);
- CLA: Programming Essentials in C;
- Acquisizione Forense (**svolto presso CIFIGE**).

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   I requisiti professionali saranno definiti dallo Stato Maggiore della Difesa.

2. **Categorie:**
   Ufficiali, Sottufficiali, Graduati (solo personale in Servizio Permanente) della Difesa, impiegati/designati a ricoprire incarichi nel settore CYBER.

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

NUMERO FREQUENTATORI AMMESSI: 16 frequentatori per garantire uno standard minimo di qualità. Il numero potrà variare fino a 20 in base alle indicazioni dello SMD.

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

SONO PREVISTE PROVE VALUTATIVE PER TUTTI I MODULI DEL CORSO.

20. 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.

AREA
Cyber Defence, Law & Forensics

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

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

PROGRAMMA/ARGOMENTI TRATTATI (rife. Syllabus approvato da SMD)

Il corso si articolerà nei seguenti moduli:
- Linguaggio Python;
- Advanced Security Essentials;
- Vulnerability Assessment;
- Cyber Incident Handling e Disaster Response;
- Cyber Network Protection;
- Cyber Threat Hunting;
- Orientamento Cyber Intel (**svolto presso CIFIGE**);
- Penetration Testing (**svolto presso CIFIGE**)

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   Aver superato il corso basico per operatore cyber.
   È richiesta la capacità comprendere la lingua inglese, in quanto alcuni moduli saranno svolti interamente in lingua inglese.
2. **Categorie:**
   Ufficiali, Sottufficiali, Graduati (solo personale in Servizio Permanente) della Difesa, impiegati/designati a ricoprire incarichi nel settore CYBER.

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

NUMERO FREQUENTATORI AMMESSI: massimo 16 frequentatori.
DURATA DEL CORSO:
17 settimane: 2 in *e-learning* e 15 in presenza (12 settimane presso STELMILIT, 3 settimane presso il CIFIGE).

SONO PREVISTE PROVE VALUTATIVE PER TUTTI I MODULI DEL CORSO.

21. 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.

AREA
Cyber Defence, Law & Forensics

PROGRAMMA
Saranno fornite competenze teoriche e pratiche sui seguenti argomenti:
- reati informatici e investigazioni digitali;
- acquisizione di dati digitali su memorie di massa e dispositivi mobili;
- gestione di dati digitali;
- conservazione e protezione di dati digitali;
- ricerca della fonte di prova digitale;
- metodologie per l'analisi del traffico in rete;
- *standard* e *best practices* internazionali.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
3 settimane in *e-learning* sincrono;

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

22.MALWARE ANALYSIS – COD. Y18A

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.

AREA
Cyber Defence, Law & Forensics

PROGRAMMA
Saranno fornite competenze teoriche e pratiche sui seguenti argomenti:
- Fondamenti di Assembly Intel x86 mirati all'analisi dei *malware*;
- *Unpacking* manuale di campioni di *malware*;
- Fondamenti di analisi di *malware* a livello di codice.
- Caratteristiche dei malware a livello API Windows (DLL *injection*, *function hooking*, *keylogging*, comunicazione HTTP/HTTPS, ecc.)
- esame di proprietà statiche di documenti/eseguibili Windows sospetti;
- analisi comportamentale di documenti/eseguibili Windows malevoli;
- analisi statica e dinamica del codice di eseguibili Windows malevoli;
- Come riconoscere i malware *packed* ed individuarne l'*Original Entry Point* (OEP);
- *unpacking* automatizzato di *malware*;
- superare le difese contro l'analisi.

Potranno essere svolte attività esperienziali utilizzando le funzionalità del *Cyber Range*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
3 settimane in *e-learning* sincrono

È PREVISTO UN ESAME FINALE.

23.GESTIONE DELLA SICUREZZA DEI DATA CENTER - COD. EY19A

OBIETTIVI DEL CORSO
Il Corso ha l'obiettivo di fornire competenze fondamentali su regole, procedimenti e norme per la gestione di un Centro di Elaborazione Dati in relazione agli aspetti relativi alla privacy ed alla tutela e protezione dei dati. Si farà particolare riferimento allo standard ISO/IEC 27001 e TIA-942.

AREA
Cyber Defence, Law & Forensics

PROGRAMMA
Saranno fornite competenze teoriche e pratiche sui seguenti argomenti:
- l'ambito e gli obiettivi della ISO/IEC 27001;
- i requisiti di base di un ISMS nella ISO/IEC 27001,
- le relazioni con le *best practices* e con altri *International Standard*: ISO 9001 e ISO/IEC 20000;
- valutazione gestione del rischio;
- gestione degli accessi fisici e logici;
- gestione delle modifiche (*Change Management*);
- gestione degli *Asset*;
- gestione degli incidenti;
- gli obiettivi degli audit interni e gli audit di certificazione esterni, la loro gestione e la terminologia associata;
- *Privacy by Default* e *by Design*;
- *Disaster Recovery* e *Business Continuity*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
3 settimane in *e-learning* sincrono;

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

24.CORSO NETWORK FORENSICS – COD. Y21A

OBIETTIVI DEL CORSO
Far apprendere al personale del Comparto Difesa destinato ad operare nell'ambito della *Cyber Defence*, le nozioni utili ad acquisire e conservare, nel rispetto delle leggi vigenti e secondo le *best practices* in materia, le evidenze di azioni offensive o di intelligence avversarie, o in generale di un evento non previsto, ricostruito all'interno di laboratorio.

AREA
Cyber Defence, Law & Forensics

RUOLI E POSIZIONI RICOPRIBILI
Il Corso si propone di formare figure professionali nell'area tecnologica della *Digital Forensics*, che saranno in grado di assumere posizioni di esperto al monitoraggio ed all'analisi del traffico di reti informatiche ai fini della raccolta di informazioni, prove legali o rilevamento di intrusioni.

PROGRAMMA
Saranno fornite competenze teoriche e pratiche sui seguenti argomenti:
- gestione ed organizzazione di un sistema contro gli incidenti informatici;
- identificazione di incidente informatico, catena di custodia, individuazione dei soggetti attivi ed ostili;
- copia forense dello stato del sistema, congelamento dello stato del sistema;
- tecniche di rilevazione dati;
- *standard* e *best practices* internazionali.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
3 settimane in presenza;

È PREVISTO UN ESAME FINALE.

25.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'infostruttura da eventi non previsti o deliberati, interni o prodotti dall'attaccante.

AREA
Cyber Defence, Law & Forensics.

PROGRAMMA/ARGOMENTI TRATTATI
Il corso si articolerà sul seguente programma:
- La minaccia;
- Gli indicatori di attacco/compromissione ed il loro ciclo di vita;
- Creare una libreria per le tattiche, tecniche e procedure riconducibili alla minaccia;
- Nozioni di base ed uso di MITRE ATT&CK;
- Sviluppare la Cyber Kill *Chain* con ATT&CK *Navigator*;
- Attività di laboratorio;

Potranno essere svolte attività esperienziali utilizzando le funzionalità del Cyber Range.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO:
2 settimane in presenza.

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

26. 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 *constituency* e produzione di avvisi, bollettini e notizie.

AREA
Cyber Defence, Law & Forensics.

PROGRAMMA/ARGOMENTI TRATTATI
- Introduzione;
- Panoramica ed implementazione dei principali modelli organizzativi;
- Gestione delle segnalazioni di eventi rilevanti per la sicurezza dei sistemi informativi della propria *constituency*;
- Produzione di avvisi, bollettini e notizie;
- Attività di laboratorio.

Potranno essere svolte attività esperienziali utilizzando le funzionalità del *Cyber Range*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO: 2 settimane in presenza.

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

27.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.

AREA
Cyber Defence, Law & Forensics.

PROGRAMMA / ARGOMENTI TRATTATI
- Concetti di base di *Cyber Threat Intelligence*;
- Processo operativo;
- Attività di laboratorio.

Potranno essere svolte attività esperienziali utilizzando le funzionalità del *Cyber Range*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO: 2 settimane in presenza.

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

28. 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.

AREA

Cyber Defence, Law & Forensics.

PROGRAMMA / ARGOMENTI TRATTATI

Il programma didattico comprenderà i seguenti argomenti:

- *Governance* e strategia della cybersecurity in Italia:
  - *Architettura Nazionale di Cybersicurezza;*
  - *Agenzia per la Cybersicurezza Nazionale (ACN) Attività di laboratorio;*
  - *Sistema Nazionale di Cybersicurezza;*
  - *Framework Nazionale per la Cybersecurity;*
  - *CSIRT Italia;*
  - *Incident Response;*
  - *Crisis Management.*
- Gestione delle minacce:
  - *Threat Intelligence nazionale;*
  - *Analisi del rischio cyber;*
  - *Capacità di risposta.*
- Standard tecnici e normativi:
  - *Misure minime di sicurezza;*
  - *Codice dell'Amministrazione Digitale (CAD);*
  - *Linee Guida AGID e ACN;*
  - *Best practice nazionali.*
- Security Risk Management, Controls, Audit Management:
  - *Identificazione e valutazione dei rischi di sicurezza informatica;*
  - *Metodologie di risk assessment;*
  - *Identity and Access Management (IAM);*
  - *Cloud e modelli di servizio;*
  - *Le nuove architetture;*
  - *La crittografia;*
  - *La rete TOR;*
  - *APT e malware avanzati;*
  - *Botnet e attacchi DDoS;*
  - *Audit e monitoraggio continuo;*
- Security Program Management & Operations:

  - *Progettazione e implementazione di un programma di sicurezza;*
  - *Gestione delle risorse, personale e processi;*
  - *Incident response e gestione delle crisi;*
  - *Business Continuity e Disaster Recovery.*
- Cyber Threat Intelligence:
  - *Raccolta e analisi delle informazioni sulle minacce;*
  - *Tecniche di analisi e correlazione;*
  - *Condivisione con gli stakeholder;*
  - *Integrazione della threat intelligence nella strategia.*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

4. Professionali:

a. Frequenza preventiva: N.N.;

b. Conoscenze basiche richieste:

- Concetti di cybersecurity;
- Familiarità con i framework di gestione del rischio (es. NIST, ISO 27001)

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

5. Di segretezza:

NOS non richiesto.

6. Di grado:

Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO: 2 settimane in modalità e-learning sincrona.

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

AREA *DATA SCIENCE* E INTELLIGENZA ARTIFICIALE

29.DATA PROTECTION – COD. EX005A (ex EY16A)

OBIETTIVI DEL CORSO
Il Corso ha l'obbiettivo di fornire competenze sull'analisi dei profili di responsabilità, delle modalità ispettive, delle sanzioni, del ruolo essenziale del *Data Protection Officer (DPO)* nell'adeguamento e nelle verifiche, con attenzione anche al quadro sanzionatorio negli altri Paesi europei e alla "modularità" dei profili di responsabilità. Il corso fornisce competenze fondamentali su gestione e protezione dei dati e dei sistemi, sviluppando conoscenza e consapevolezza relativamente a *privacy* e trattamento dei dati.

AREA
Cyber Defence, Law & Forensics

PROGRAMMA
Saranno fornite competenze teoriche e pratiche sui seguenti argomenti:
- il Regolamento 679/2016 e il D. Lgs. 101/2018;
- la figura del DPO;
- intelligenza artificiale, profilazione e tutela dei dati personali;
- nuove minacce alla sicurezza dei dati e dei sistemi e possibili contromisure;
- l'approccio *risk-based* del Regolamento e la politica di *governance* dei dati;
- le responsabilità civile e penale connesse al trattamento di dati personali;
- gestione del dato per tutta la durata della sua vita (metodologie e sistemi dedicati);
- valutazioni e profili di rischio;
- *privacy by design* e *by default*;
- gestione dei *data breach*;
- sicurezza nel *cloud*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
3 settimane in *e-learning* sincrono;

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

30.BIG DATA ANALYSIS – COD. X004A (ex Y20A)

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*.

AREA
Cyber Defence, Law & Forensics

PROGRAMMA
Saranno fornite competenze teoriche e pratiche sui seguenti argomenti:
- *Big Data*;
- *Big Data Analysis*;
- le 4 tipologie di *Data Analysis*: Descrittiva, Predittiva, Prescrittiva e Automatizzata;
- cenni di Matematica e Statistica per la *Big Data Analysis*;
- algoritmi, Strutture dati e Gestione delle basi di dati con introduzione ai database relazionali e non relazionali;
- Intelligenza Artificiale e *Machine Learning*;
- *Machine Learning* e famiglie di algoritmi (elaborazione di algoritmi in grado di evidenziare entità e classificare contenuti eterogenei, ricorrendo anche a tecniche di *Neuro-Linguistic Programming*);
- Data Mining con sviluppo ed utilizzo di metodologie specifiche (regressione, *clustering*, associazioni);
- identificazione di modelli finalizzati all'interpretazione dei dati anche con capacità predittiva;
- *Social Media Analysis* (mediante lo sviluppo e l'elaborazione di specifici indicatori e metriche finalizzati alla descrizione dei principali *Social Network* e all'analisi di reti e contenuti);
- *Marketing Analytics*;
- *Google Cloud Platform* per i *Big Data* e *Google Analytics* e Dispositivi di IoT;
- strumenti di visualizzazione dei dati: *Google Data Studio*;
- esercitazioni pratiche mediante la discussione di casi reali (Laboratorio).

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
3 settimane in *e-learning* sincrono

È PREVISTO UN ESAME FINALE.

31.CORSO IA E TECNICHE DI PROMPTING AVANZATO – COD. EX003A

OBIETTIVI DEL CORSO
Il Corso ha l'obiettivo di fornire ai frequentatori competenze avanzate nell'utilizzo dell'Intelligenza Artificiale Generativa attraverso tecniche professionali di prompt engineering e context engineering. Il percorso formativo si propone di formare operatori esperti nella progettazione, ottimizzazione e implementazione di prompt strutturati per Large Language Models (LLM), con particolare focus su applicazioni in ambito Difesa.

AREA
Data Science e Intelligenza Artificiale.

PROGRAMMA/ARGOMENTI TRATTATI
Il corso si articolerà sul seguente programma:
- *fondamenti di prompt engineering*
- *tecniche avanzate di prompting*
- *context engineering e automazione;*
- *prompting per applicazioni multimodali*
- *etica e sicurezza*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

a. Frequenza preventiva: Corso "Fondamenti di Intelligenza Artificiale (IA)" - COD. Y453B o avere una formazione pregressa che garantisca le medesime conoscenze;
b. Conoscenze basiche richieste: Familiarità con concetti base di Intelligenza Artificiale (Machine Learning, Deep Learning, NLP), utilizzo professionale di strumenti informatici, capacità di lettura documentazione tecnica in lingua inglese
c. Studio preventivo sinossi / testi propedeutici: revisione degli argomenti del corso "Fondamenti di Intelligenza Artificiale cod.EY442B.

2. Di segretezza:
NOS non richiesto.

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

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO: 1 settimana in modalità *e-learning* sincrono (32 ore in piattaforma).

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

AREA CORSI DI INTERESSE DEL COS E DEL CIGC SICRAL

Capitolo 1

CORSI DI INTERESSE DEL COS E CIGC SICRAL

La SCUOLA TELECOMUNICAZIONI FF.AA. annovera nel proprio Catalogo i corsi previsti dalla direttiva “La formazione, l’addestramento e l’impiego del personale destinato al Comando delle Operazioni Spaziali e al dipendente Centro di Gestione e Controllo SICRAL”, COS-FORM-001-INCC Edizione 2023.

Tali corsi vengono erogati presso il CIGC SICRAL di Vigna di Valle (Bracciano – ROMA) e il relativo attestato di superamento corso viene rilasciato da STELMILIT secondo le previste modalità.

L’elenco dei corsi, completo e aggiornato, è contenuto all’interno della citata direttiva.

CAPITOLO 2 - CORSI DI LIVELLO INTERMEDIO

AREA *TRANSPORT & NETWORKING*

32.PROPEDEUTICO RETI LOCALI ETHERNET - COD. ER235I

OBIETTIVI DEL CORSO

Il corso costituisce la prima fase di un percorso formativo più ampio, finalizzato alla capacità diprogettare e gestire, in qualità di amministratore, reti LAN Ethernet 802.3.
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.
Verrà trattato il modello ISO/OSI come Architettura di Rete di riferimento e i relativi livelli, definendo le tipologie di protocolli che intervengono nell'ambito di sistemi real-time e sistemi caratterizzati da integrità informativa.
In particolare poi il corso si concentra sulle caratteristiche e funzionalità degli Switch, tipiche esclusive del Livello 2 partendo dalle Trame MAC Ethernet e IEEE 802.3, per poi definire in modo dettagliato protocolli come lo STP, LAG e Virtual LAN.
In ultimo verrà trattato l'indirizzo logico e le relative classi delle reti IP, l'indirizzamento IPv4 ed il Subnetting FLSM.
Gli argomenti teorici sono propedeutici alla frequenza del corso Progetto e Gestione Reti LAN Ethernet (COD. R235I)

AREA

Transport & Networking

PROGRAMMA/ARGOMENTI TRATTATI

- Reti di Computer: concetti generali;
- Modello di riferimento ISO/OSI;
- Mezzi trasmissivi Rame / Fibra Ottica;
- Apparati di rete - HUB- Schede di rete Ethernet;
- Indirizzi MAC;
- Power Over Ethernet (PoE);
- SWITCH: Spanning Tree Protocol, LAG e LAN Virtuali;
- L'Indirizzamento IPv4;
- Subnetting FLSM.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA

2 settimane in modalità *e-learning* asincrono (40 ore in piattaforma) con eventuali interventi via *web streaming*[3].

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso III.

É PREVISTO UN TEST INTERMEDIO NON SBARRANTE

É PREVISTO UN ESAME FINALE

[3] Le indicazioni inerenti alle eventuali attività sincrone saranno comunicate dagli Istruttori del corso (Rif. Annesso III del presente Catalogo). tali attività andranno obbligatoriamente seguite e l'eventuale assenza verrà conteggiata ai fini dei requisiti per poter sostenere l'esame.

33.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 cablata (LAN Ethernet 802.3), secondo lo Standard Internazionale ISO/IEC ed anche EIA/TIA, certificandone le prestazioni attraverso la misura ed il calcolo di specifici parametri standard eseguiti con apposita strumentazione professionale.
Sono previste esercitazioni pratiche riguardo la prima configurazione di Switch di differenti Vendors, attraverso i vari metodi di accesso, quindi gestione e configurazione dei principali Protocolli di Livello 2, come lo Spanning Tree e l'Aggregazione dei Link. Creazione e gestione di Virtual LAN utente e Vlan di Management.
Implementazione e gestione del PoE attraverso il controllo remotizzato dello Switch.
Analisi del pacchetto IPv4 e Subnet Mask. Creazione di sottoreti attraverso il Subnetting FLSM e VLSM messi a confronto.
In ultimo con l'ausilio di Wireshark si procederà alla cattura e analisi di pacchetti di livello Rete e livelli più alti dell'Architettura di rete TCP/IP.
Infine cenni sul Routing Statico con l'ausilio di Packet Tracer

AREA

Transport & Networking

PROGRAMMA/ARGOMENTI TRATTATI

- Reti LAN Ethernet concetti;
- Cablaggio Rame: certificazione rete LAN rame;
- Bridge e Switch: prima configurazione;
- Configurazione Protocolli di liv. 2: PoE, STP, LAG
- Configurazione di VLAN (802.1q) su Switch di differenti Vendors
- Stack TCP/IP: architettura e Protocolli
- Analisi del Datagramma IPv4, indirizzamento IPv4, Subnetting VLSM
- Funzioni e analisi dei principali Protocolli TCP/IP: ARP, ICMP, TCP, UDP, DHCP, DNS
- Switch multilivello: concetti di Routing Statico
- Laboratorio supportato da Packet Tracer
- Evoluzione della tecnologia Ethernet

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva obbligatoria: Corso propedeutico reti locali Ethernet - COD. ER235I.
      In alternativa alla frequenza preventiva il discente dovrà possedere una buona conoscenza degli argomenti trattati nel corso propedeutico.
   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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA
- 2 settimane in presenza
- Percentuale laboratorio: 50 %.

È PREVISTO UN TEST D'INGRESSO E UN ESAME FINALE

34.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 del solo Cablaggio Strutturato di una rete locale cablata (LAN 802.3) secondo gli standard attualmente in vigore ISO/IEC e ANSI EIA/TIA, analizzando differenti attuali soluzioni di connettività proposte dai Vendors sul mercato.
In ultimo attraverso l'utilizzo di apposita strumentazione professionale verranno generati i documenti relativi alla Certificazione di un Cablaggio Orizzontale con relativa analisi dei contenuti.
Cenni sui capitolati tecnici

AREA
Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI
Il corso si articolerà sul seguente programma:
- LAN concetti;
- Tecnologia Ethernet;
- Mezzi trasmissivi rame UTP;
- Mezzi trasmissivi Fibra Ottica;
- Media Converter e Transceiver;
- Power over Ethernet (PoE);

Laboratorio: connettorizzazione e certificazione di un Cablaggio Orizzontale

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
1 settimana in presenza.
Percentuale laboratorio: 60 %.

È PREVISTO UN ESAME FINALE.

AREA *SOFTWARE*, APPLICATIVI E *E-LEARNING*

35.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.

AREA
Software/Applicativi/*E-learning.*

PROGRAMMA/ARGOMENTI TRATTATI
Gli argomenti oggetto di insegnamento sono i seguenti:
- introduzione a HTML 5;
- HTML 5 struttura e contenuti;
- nuovi Tag semantici;
- altri Tag (immagini, video e audio);
- introduzione al CSS;
- regole, proprietà e valori;
- gestione contenuti;
- schemi di posizionamento;
- *layout* a larghezza fissa e progettazione per schermi di dimensioni differenti;
- progettazione e realizzazione di un sito *web* (HTML-CSS);
- realizzazione di un sito *web* e pubblicazione (*Server* Apache).

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

2. **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..

3. **Di segretezza:**
   NOS non richiesto.

4. **Categorie:**
   Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 10.

DURATA DEL CORSO:
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%.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

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

36.CLOUD COMPUTING & VIRTUALIZATION SPECIALIST- COD. T500I

OBIETTIVI DEL CORSO

Il presente percorso formativo fornisce una preparazione completa sui fondamenti del *Cloud Computing*, basata sulle definizioni e sugli standard del *NIST*. I discenti impareranno a distinguere e valutare i principali modelli di servizio, tra cui *IaaS, PaaS e SaaS* , nonché i modelli di deployment come *Public, Private e Hybrid Cloud*. Attraverso un approccio focalizzato sull'implementazione, il corso mira a formare il personale nella creazione di architetture cloud e ambienti di virtualizzazione avvalendosi di macchine virtuali e container. I partecipanti acquisiranno le competenze necessarie per progettare una baseline di sicurezza solida integrando IAM, cifratura e *logging*. Inoltre, il programma è orientato a definire la *governance*, la gestione del rischio e la stesura di SLA, permettendo la progettazione di regole efficaci per la continuità operativa. Al termine del percorso, i frequentatori saranno in grado di automatizzare operativamente gli ambienti cloud.

AREA Software/Applicativi/ E-learning

PROGRAMMA/ARGOMENTI TRATTATI

- **Fondamenti e modelli di servizio:** Evoluzione dei *Data Center*, definizioni *NIST*, caratteristiche e modelli di servizio e *deployment*.
- **Normative, compliance e *Cloud Governance*:** Standard ISO/IEC (22123, 19086, 19941), *CSA Cloud Controls Matrix, GDPR, NIS2, Shared Responsibility Model* e mappatura dei ruoli.
- **Architetture *cloud* e virtualizzazione:** *Hypervisor* (tipo 1 e 2), *Proxmox VE, Cluster, High Availability e creazione di Virtual Machine*.
- ***Networking, Storage e Container:*** *VLAN, SDN, NAS, SAN, Ceph* e containerizzazione mediante *Docker (Registry, Image, Volume, Network*).
- **Sicurezza e IAM:** *CIA Triad, Zero Trust, IAM, RBAC, MFA*, standard ISO 27017/27018 e *hardening* delle *VM*.
- ***DevOps, DevSecOps e IaC (Infrastructure as Code):*** Principi CI/CD, *Git, Terraform e Ansible per il configuration management e provisioning*.
- **Migrazioni Applicativi e *Cloud Adoption*:** *Cloud Adoption Framework, Landing Zone, e strategie di migrazione (Rehost, Replatform, ecc.).*
- ***Kubernetes* e Orchestrazione:** Architettura K8s, Control *Plane*, *Pod, Deployment, Service* e installazione K3s per il deploy di applicazioni web.
- ***Monitoring, Logging* e Resilienza:** *Observability*, gestione delle metriche (*Wazuh, Grafana), Business Continuity, Disaster Recovery (RTO e PRO*) e simulazione di guasti.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: in ambito sistemi Linux con familiarità su comandi, permessi e processi. Capacità di comprensione di concetti relativi *a subnet, routing*, principi di *hypervisor*, macchine virtuali e storage. È consigliata una conoscenza preliminare di *Docker*.

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.

NUMERO FREQUENTATORI AMMESSI: Fino ad un massimo di 10.
DURATA DEL CORSO: 2 settimane in presenza.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

37.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.

AREA
Software/Applicativi/*E-learning*

PROGRAMMA/ARGOMENTI TRATTATI
Il corso si articolerà sul seguente programma:
- modello OSI e Architettura TCP/IP;
- livello 2 OSI: Standard *Ethernet V.2 e IEE802.3;*
- *apparati di rete: HUB SWITCH;*
- indirizzamento IP v.4;
- sistemi operativi di rete;
  - introduzione all'infrastruttura di *Active Directory*[4];
  - introduzione alle tipologie di autenticazione Windows[4];
- i Sistemi Operativi *Open Source*;
- gestione della rete e cenni di interoperabilità.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

3. **Professionali:**
   I requisiti professionali saranno definiti dalla Marina Militare.

4. **Di segretezza:**
   NOS non richiesto.

5. **Di grado:**
   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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
3 settimane in presenza.

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

[4] Attività svolte qualora vi siano istruttori in grado di erogarle. In alternativa saranno svolti argomenti sul networking in ambito Windows Server

38.CORSO DOCKER & KUBERNETES - COD. ET302I

OBIETTIVI DEL CORSO

Nell'attuale scenario IT, caratterizzato da una crescente adozione del cloud e dalla necessità di sviluppare, distribuire e scalare applicazioni in modo efficiente e dinamico, le tecnologie di containerizzazione e orchestrazione rappresentano competenze cruciali. Questo corso è progettato per fornire ai partecipanti una solida preparazione sull'utilizzo di *Docker e Kubernetes*, i due strumenti leader nel campo della containerizzazione e dell'orchestrazione di container. Attraverso un approccio teorico-pratico, i partecipanti apprenderanno come creare container con *Docker*, gestire immagini e orchestrare applicazioni distribuite tramite *Kubernetes*. Il corso include esercitazioni guidate per consolidare le competenze acquisite.

AREA

Software/Applicativi/*E-learning*

PROGRAMMA/ARGOMENTI TRATTATI

- Introduzione a *Docker*;
- Installazione di *Docker*;
- Comandi di base;
- *Docker Hub*;
- *Dockerfile*;
- Creazione di un'immagine personalizzata;
- Ottimizzazione delle immagini;
- Reti *Docker*;
- Comunicazione tra container;
- Volumi *Docker*;
- Docker Compose;
- Sicurezza in *Docker*;
- Monitoraggio e *Logging;*
- CI/CD con *Docker*;
- Introduzione e *overview* di *Kubernetes*;
- Architettura di *Kubernetes*;
- Principi fondamentali di *Kubernetes*;
- Creazione di un Cluster *Kubernetes*;
- *Deploy* di un'Applicazione;
- *Pods* e *Nodes*;
- Esporre Applicazioni;
- Scalabilità delle Applicazioni;
- Gestione delle Risorse,
- Implementazione di un'Applicazione Completa;
- Monitoraggio e *Troubleshooting*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

4. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: conoscenza dei sistemi Linux, fondamenti di

programmazione, nozioni base di *networking*, familiarità con i concetti di virtualizzazione. Consigliata la conoscenza preliminare e/o concetti di *Docker*;

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

5. Di segretezza:
NOS non richiesto.

6. Di grado:
Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:
1 settimane in modalità *on-line training* sincrona.
In base alla disponibilità del personale istruttore il corso **potrebbe essere rimodulato in presenza**; in tal caso tale evenienza verrà comunicata nel Calendario Corsi o con comunicazione ad hoc.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

39.SICUREZZA DELLE APPLICAZIONI WEB - COD. ET303I

OBIETTIVI DEL CORSO
Il corso si prefigge di fornire ai i partecipanti le necessarie conoscenze per poter comprendere e distinguere le vulnerabilità del codice e le criticità logiche connesse allo sviluppo delle Applicazioni *Web*. Inoltre, il corso fornisce ai partecipanti gli apprendimenti necessari alla comprensione delle problematiche legate alla realizzazione di Applicazioni *Web* sicure e gli strumenti per riconoscere le vulnerabilità comunemente sfruttate da un agente di minaccia per ottenere un accesso illecito alle risorse e ai sistemi che erogano le Applicazioni *Web*.

AREA
Software/Applicativi/*E-learning*

PROGRAMMA/ARGOMENTI TRATTATI
Il programma didattico comprenderà i seguenti argomenti:
- Minacce e Attacchi alle Applicazioni *Web*;
- Principi della *Security*;
- *Same Origin Policy*;
- Sicurezza e *Cookie*;
- *Session Riding*;
- *Cross Site Scripting*;
- Altri tipi di *Code Injection*;
- Attacchi diversi;
- *Login*;
- Sicurezza delle API.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: Conoscenza base di html, di uno fra i principali linguaggi di programmazione *web* (ASP.NET, PHP, Java, ...) e di uno fra i principali *web* server (Microsoft IIS, Apache, JBoss, ...).
   Conoscenza base sul design, l'analisi, lo sviluppo e le altre fasi di vita di una Applicazione *Web*.
   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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO:
1 settimane in modalità *on-line training* sincrona.

In base alla disponibilità del personale istruttore il corso **potrebbe essere rimodulato in presenza**; in tal caso tale evenienza verrà comunicata nel Calendario Corsi o con comunicazione ad hoc.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III

È PREVISTO UN ESAME FINALE

40.INTRODUZIONE ALLO SVILUPPO WEB CON PHP - COD. ET304I

OBIETTIVI DEL CORSO
Questo corso introduce i concetti fondamentali dello sviluppo web e fornisce competenze pratiche nella programmazione *PHP, HTML, CSS e JavaScript*, essenziali per la creazione di applicazioni web. Il corso esplora anche le buone pratiche di programmazione e fornisce una panoramica dei framework *Bootstrap e Laravel*.

AREA
Software/Applicativi/*E-Learning*

PROGRAMMA / ARGOMENTI TRATTATI
- introduzione allo sviluppo web in ambiente *wamp*;
- i blocchi di costruzione di *php*: concetti e sintassi di base;
- come sviluppare in *php*: *server*, ambiente, strumenti di sviluppo;
- leggere l'input utente: *query string* e *post*;
- gestire la sessione;
- comunicare con il database;
- sicurezza e vettori di attacco standard;
- programmazione a oggetti;
- design pattern: *mvc*;
- *html* e *css* per sviluppatori di applicativi *web*;
- *js*: introduzione pratica;
- *framework*: cenni su *bootstrap* e *laravel*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: fondamenti di programmazione e conoscenza di networking ed infrastrutture;
   c. Studio preventivo sinossi / testi propedeutici: N.N.;

2. **Di segretezza:**
   NOS non richiesto;

3. **Categorie:**
   Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA
1 settimana in modalità "*on-line training*" sincrona.
In base alla disponibilità del personale istruttore il corso **potrebbe essere rimodulato in presenza**; in tal caso tale evenienza verrà comunicata nel Calendario Corsi o con comunicazione ad hoc.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO ESAME FINALE

AREA *CYBER DEFENCE*, *LAW* & *FORENSICS*

41.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*").

AREA
Cyber Defence, Law & Forensics.

PROGRAMMA/ARGOMENTI TRATTATI
- Esigenza, MMS e FNSC;
- *Bug, vulnerability e exploit;*
- *Vulnerability Disclosure;*
- Window *of vulnerability*;
- CVE e *public repository*;
- CVSS;
- Implementazione di un laboratorio per il *testing*;
- I programmi per il *vulnerability scanning*;
- Confronto dei risultati ottenuti;
- *Assessmen*t.

Saranno svolte attività esperienziali utilizzando le funzionalità del Cyber Range.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO: 3 settimane in presenza;

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

42. DIGITAL TRASFORMATION & EMERGING TECHNOLOGIES – COD. EY457I

OBIETTIVI DEL CORSO

Il corso offre una visione completa del fenomeno della trasformazione digitale, analizzando tecnologie emergenti, modelli organizzativi e strumenti operativi che stanno rivoluzionando imprese e pubbliche amministrazioni. Particolare attenzione è dedicata all'integrazione di dati, intelligenza artificiale, ecosistemi digitali e sicurezza, con un approccio tecnico-strategico orientato alla gestione dell'innovazione.

- Comprendere le principali dinamiche e tendenze della trasformazione digitale.
- Analizzare le tecnologie emergenti, il loro funzionamento e le applicazioni concrete.
- Acquisire competenze pratiche su strumenti e architetture digitali.
- Sviluppare consapevolezza critica su aspetti etici e di sicurezza.
- Rafforzare le capacità relazionali e manageriali in contesti tecnologicamente evoluti.

AREA

Cyber Defence, Law & Forensics.

PROGRAMMA/ARGOMENTI TRATTATI

Il programma didattico comprenderà i seguenti argomenti:

- Digitalization trends:
  - *design thinking;*
  - *framework di innovazione;*
  - *agile development and open innovation.*
- Blockchain e Tecnologie Distributed Ledger:
  - *smart contracts;*
  - *applicazioni decentralizzate (DApp);*
- Piattaforme ed ecosistemi digitali:
  - *modelli di business platform-based;*
  - *ecosistemi digitali.*
- Change Management e Leadership:
  - *leadership digital;*
  - *cambiamento organizzativo;*
  - *sviluppo delle competenze e formazione;*
  - *trasformazione culturale;*
  - *il ruolo dei dati nella trasformazione digitale.*
- Analisi dei Dati e Intelligenza Artificiale:
  - *architettura dei big data;*
  - *applicazioni del machine learning;*
  - *strategie di implementazione dell'IA;*
  - *analisi predittiva.*
- Realtà virtuale (AR/VR/MR):
  - *extended reality (xr);*
  - *virtual reality (vr);*
  - *mixed reality (mr);*
  - *digital twin;*
  - *tecnologie immersive e metaverso.*
- Quantum Cryptography and Quantum Computing:

  - *principi base;*
  - *potenziali applicazioni;*
  - *impatto sulla crittografia e sicurezza.*
- Internet of Things (IoT):
  - *architettura e piattaforme iot;*
  - *applicazioni iot industriali*
  - *soluzioni smart;*
  - *ecosistemi connessi.*
- Digital transformation e il suo impatto sulle organizzazioni.
  - *Cambiamenti nei modelli operativi e decisionali.*
- L'etica e l'innovazione tecnologica.
  - *AI ethics: bias, accountability, explainability.*
  - *Responsabilità nell'uso delle tecnologie immersive e invasive.*
  - *Implicazioni legali e regolatorie.*
- Risk Management e security:
  - *framework di cybersecurity (NIST CSF, ISO/IEC 27001, CIS Controls)*
  - *valutazione del rischio;*
  - *compliance e regolamentazioni (GDPR, DORA, NIS2);*
  - *considerazioni sulla privacy.*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO: 1 settimana in modalità e-learning sincrona.

È PREVISTO UN ESAME FINALE.

43. CYBERSECURITY GOVERNACE, RISK E COMPLIANCE – COD. EY458I

OBIETTIVI DEL CORSO

Il corso offre una formazione tecnica e strategica per comprendere e affrontare in modo strutturato le principali sfide in ambito di sicurezza informatica, gestione dei rischi e *compliance* normativa. Attraverso l'analisi dei *framework* di riferimento, delle minacce emergenti e dei requisiti regolamentari, i partecipanti acquisiranno le competenze per definire, implementare e gestire un sistema di *governance* della sicurezza efficace e resiliente.

- Fornire una comprensione approfondita delle principali minacce alla sicurezza informatica e del contesto evolutivo.
- Introdurre i concetti fondamentali di *governance* applicati alla *cybersecurity*.
- Esplorare normative e leggi nazionali ed europee in ambito sicurezza e privacy.
- Introdurre gli standard internazionali e i *framework* di riferimento.
- Fornire metodologie operative per identificare, analizzare, valutare e trattare i rischi informatici.

AREA

Cyber Defence, Law & Forensics.

PROGRAMMA/ARGOMENTI TRATTATI

Il programma didattico comprenderà i seguenti argomenti:

- Cybersecurity *Governance*
  - *introduzione alla cybersecurity e alle minacce attuali;*
  - *principi base della governance in cybersecurity;*
  - *ruoli e responsabilità nella gestione della sicurezza;*
  - *framework di governance organizzativa;*
  - *politiche e procedure di sicurezza;*
  - *definire una strategia per la cybersecurity governance;*
  - *misurare la resilienza;*
  - *cybersecurity: nuovi attori e nuovi ambiti.*
- *Compliance* e Regolamentazioni:
  - *GDPR e privacy dei dati;*
  - *normative ue e nazionali;*
  - *agenzia per la cybersicurezza nazionale (ACN);*
  - *ENISA ruoli attuali ed evoluzione futura;*
  - *procedure di audit e certificazione;*
  - *business continuity e disaster recovery;*
  - *implementazione e sanzioni.*
- Risk Management:
  - *introduzione al rischio;*
  - *standard internazionali di gestione del rischio;*
  - *risk management complete;*
  - *strategie di mitigazione del rischio.*
- Sicurezza Operativa:
  - *service and application mapping;*
  - *monitoraggio e detection degli incidenti, siem, soc, csirt;*
  - *procedure operative standard.*
- Gestione della Sicurezza delle Informazioni extended reality (XR);

  - *classificazione delle informazioni;*
  - *data protection;*
  - *sistemi di gestione documentale;*
  - *controllo degli accessi.*
- La gestione dei rischi cyber del prossimo futuro principi base;
  - *società smart e sicurezza;*
  - *intelligenza artificiale e sicurezza;*
  - *autonomia e sicurezza;*
  - *stato delle minacce;*
  - *nuove architetture sicure;*
  - *sicurezza nell'ambiente cloud.*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

4. Professionali

d. Frequenza preventiva: N.N;
e. Conoscenze basiche richieste: N.N.
f. Studio preventivo sinossi / testi propedeutici: N.N.

5. Di Segretezza: NOS non richiesto.

6. Categorie: Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO: 1 settimana in modalità e-learning sincrona

È PREVISTO UN ESAME FINALE.

CAPITOLO 3 - CORSI DI LIVELLO BASE

AREA TRANSPORT & NETWORKING

44.CISCO NETWORKING, SWITCHING AND ROUTING – COD. ER001B

OBIETTIVI DEL CORSO
Fornire al personale frequentatore una conoscenza completa e strutturata delle tecnologie di *networking*, includendo fondamenti di IP *routing* e *switching*, servizi e automazioni di rete. Inoltre, verranno forniti elementi di *network security* al fine di identificare e mitigare possibili attacchi.

AREA
Transport & Networking.

PROGRAMMA / ARGOMENTI TRATTATI
Il corso è costituito dai seguenti moduli CISCO:
- CCNA 1 - Introduction to Networks (ITN);
- CCNA 2 - Switching, Routing and Wireless Essentials (SRWE);
- CCNA 3 - Enterprise Networking, Security and Automation (ENSA).

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: reti LAN, *switching Ethernet* 802.3; indirizzamento/*subnetting* di reti IP;
   c. Studio preventivo sinossi / testi propedeutici: N.N..

2. **Di segretezza:** Non richiesto.

3. **Categorie:**
   Ufficiali, Sottufficiali, Graduati e civili della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 16.

DURATA DEL CORSO: 3 settimane in modalità *e-learning* sincrono con teoria e pratica su laboratori ufficiali CISCO e software *Packet Tracer*.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE

45.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.

AREA
Transport & Networking

PROGRAMMA/ARGOMENTI TRATTATI
- elementi di Radiopropagazione;
- fondamenti di *Frequency* e *Spectrum Management;*
- la gestione dello spettro nazionale ed internazionale;
- le interferenze e i criteri di protezione;
- la validazione e il controllo di configurazione spettrale;
- il *Battle Space Spectrum Management;*
- lo spettro come spazio di manovra.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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 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*.

NUMERO FREQUENTATORI AMMESSI: fino a un massimo di 20.

DURATA DEL CORSO: 3 settimane in modalità *e-learning* asincrono (45 ore in piattaforma);

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE

46. 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.

AREA
Transport & Networking.

PROGRAMMA / ARGOMENTI TRATTATI
- meccanica orbitale;
- generalità sulle comunicazioni satellitari;
- elementi di modulazioni numeriche in ambito SATCOM;
- tipologie di accesso multiplo e sistemi a banda condivisa;
- concetti di efficienza spettrale ed utilizzo di potenza di potenza a satellite;
- fenomeni di interferenza nelle comunicazioni satellitari;
- calcolo di Link Budget e pianificazione missioni;
- piattaforme satellitari SICRAL;
- payload satelliti SICRAL e ATHENA-FIDUS;
- segmento di Terra SICRAL e gestione operativa dei terminali;
- il centro controllo TLC di Vigna di Valle e sviluppi futuri.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 20.

DURATA DEL CORSO: 1 settimana in modalità *e-learning* asincrono (20 ore - non sono previste attività di laboratorio).

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE

47.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

AREA
Transport & Networking.

PROGRAMMA / ARGOMENTI TRATTATI
- Brevi Richiami sullo *Stack TCP /IP;*
- Brevi richiami sui protocolli *ARP, ICMP, TFTP, TELNET, SSH e DNS;*
- *Internet Protocol v4*: concetti generali, descrizione e analisi dei campi di un pacchetto *IP*;
- Indirizzamento *IPv4*: tecniche di *Subnetting e VLSM;*
- Esercizi di Progettazione del piano di indirizzamento *IP*;
- Commutazione di pacchetto nelle *WAN*: concetti generali;
- Architettura di *INTERNET, Autonomous System (AS) e NAP (Neutral Access Point);*
- Protocolli di *routing* dinamico *IGP* ed *EGP*: Classificazione generale e tipologie;
- Protocolli di protocolli *Distance-Vector e Link-State*: funzionalità di base e differenze;
- Router *IPv4*: architettura logica e funzionalità generali;
- Router Cisco: Caratteristiche fisiche, Sistema operativo *IOS* e *File System*, interfacce di gestione e di rete;
- Accesso tramite *Putty* via console seriale RS232;
- Configurazione iniziale attraverso CLI;
- Comandi *IOS* di base e livelli di privilegio amministrativo di un router Cisco;
- Configurazione di base delle Interfacce di management e di rete;
- Line *VTY*: Accesso via *Telnet*;
- Routing statico nelle reti IP e concetto di default gateway;
- Tabelle di *routing*: logica di *routing*, tipi di destinazioni, modifiche e aggiunte di rotte IP;
- Brevi cenni sui simulatori di reti *GNS3 e Packet Tracer.*

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.
DURATA DEL CORSO: 1 settimana in modalità in presenza
È PREVISTO UN ESAME FINALE

AREA *SOFTWARE*, APPLICATIVI E *E-LEARNING*

48. 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.

AREA

Software/Applicativi/*E-learning*

PROGRAMMA/ARGOMENTI TRATTATI[5]

- Computer Essentials: generalità sui personal computer;
- Online Essentials: fondamenti di attività *on-line*;
- Word Processing: elaboratori di testi;
- Spreadsheets: fogli di calcolo;
- IT-Security: sicurezza IT;
- Presentation: strumenti di presentazione;
- Online Collaboration: collaborazione *on-line*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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.

NUMERO FREQUENTATORI AMMESSI: massimo 20 frequentatori.

DURATA DEL CORSO:

WEB Based Training su 5 settimane calendariali pari a circa 100 ore in modalità *e-learning* asincrono (20 ore a settimana).

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

49.E-LEARNING IT SPECIALIST - COD. ET18B

OBIETTIVI DEL CORSO
Formare il personale designato a svolgere mansioni afferenti al 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.

AREA
Software/Applicativi/*E-Learning*

PROGRAMMA/ARGOMENTI TRATTATI

Modulo Hardware
- Schede madri;
- BIOS;
- Microprocessori;
- Memoria;
- Bus
- Risorse di sistema;
- Interfacce;
- Memoria di massa;
- Stampanti;
- Alimentazione;
- Installazione HW;
- Diagnosi e risoluzione dei problemi.

Modulo Configurazione dei sistemi operativi (Linux - Microsoft)
- Fondamenti dei sistemi operativi;
- Organizzazione di un Sistema Operativo
- Uso, configurazione e aggiornamento di un sistema operato
- Installazione HW e SW;
- Comunicazioni esterne;
- Prestazioni ed eventi;
- Gestione di Account Utenti e Account Gruppi;
- Risorse condivise e permessi account;
- Gestione delle stampanti di rete;
- Sicurezza e protezione;
- Programmi di utilità;
- Condivisione dei servizi internet;
- Diagnosi e risoluzione dei problemi.
- Database.

Modulo Reti
- Introduzione alle Reti;
- Il modello di riferimento OSI;
- Livello Fisico;
- Livello Collegamento Dati;
- Livello Rete;

- Livello Trasporto;
- Livello Sessione;
- Livello Presentazione;
- Applicazioni;
- Configurazione a basso livello;
- Uso e configurazione dei servizi di rete;
- Diagnosi e risoluzione dei problemi;
- Aspetti legali;
- Problemi fondamentali di sicurezza;

Modulo Sicurezza IT
- Gestione della Sicurezza;
- Crittografia;
- Autenticazione e controllo di accesso;
- Disponibilità;
- Codice maligno;
- Infrastruttura a chiave pubblica;
- Sicurezza di Rete;
- Aspetti sociali, etici e legali della sicurezza informatica.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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

NUMERO FREQUENTATORI AMMESSI: massimo 20 frequentatori.

DURATA DEL CORSO:
*WEB Based Tra*ining su 4 settimane calendariali (un modulo per settimana) pari a 60 ore in modalità *e-learning* asincrono.

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

Orientativamente per ognuno dei quattro moduli può essere sufficiente una settimana di studio (prevedendo circa un impegno settimanale di 15 ore di collegamento a settimana, 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.

50.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.

AREA
Software/Applicativi/*E-Learning*

PROGRAMMA/ARGOMENTI TRATTATI
- introduzione a Linux;
- introduzione alle distribuzioni di Linux;
- installazione di Linux: dalla teoria alla pratica;
- i *desktop manager* Linux;
- ambiente grafico (Gnome KDE);
- procedura di autenticazione;
- struttura del *file system*;
- primi passi fra testo e finestre
- *hard link* e *soft link*;
- editor di testo (VIM, Gedit);
- autorizzazioni con Linux;
- permessi speciali;
- proprietà dei *file*;
- comandi filtro (find, grep, wc, ecc.);
- i processi di Linux;
- processi in *backgroun*d e *foreground*;
- compressione e archiviazione;
- backup incrementale con il tar;
- RPM (*red hat package manager*);
- installazione del software con YUM e DNF;
- concetti sul networking con Linux.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

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

2. **Di segretezza:**
   NOS non richiesto.

3. **Categorie:**
   Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 20.

DURATA DEL CORSO:
2 settimane in modalità *e-learning* asincrono (40 ore in piattaforma) con eventuali interventi

via *web streaming*[6].

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE

[6] Le indicazioni inerenti alle eventuali attività sincrone saranno comunicate dagli Istruttori del corso (Rif. Annesso III del presente Catalogo). tali attività andranno obbligatoriamente seguite e l'eventuale assenza verrà conteggiata ai fini dei requisiti per poter sostenere l'esame

51.ELEMENTI DI VIRTUALIZZAZIONE - COD. ET24B

OBIETTIVI DEL CORSO
Fornire ai frequentatori le conoscenze generali sulle Tecnologie di Virtualizzazione [7] descrivendone le caratteristiche, le funzionalità e i principali vantaggi del suo utilizzo.

AREA
Software/Applicativi/*E-Learning*

PROGRAMMA / ARGOMENTI TRATTATI
- introduzione alla Virtualizzazione;
- tipologie di Virtualizzazione;
- tipologie di *Hypervisor*;
- confronto tra *Hypervisor*;
- principali caratteristiche delle macchine virtuali;
- virtualizzazione e *Cloud Computing*;
- tipologie di *Cloud*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI
1. **Professionali:**
   a. Frequenza preventiva: N.N.;
   b. Conoscenze basiche richieste: buona conoscenza informatica HW/SW;
   c. Studio preventivo sinossi / testi propedeutici: N.N.;

2. **Di segretezza:**
   NOS non richiesto;

3. **Categorie:**
   Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 20.

DURATA
1 settimana in modalità *e-learning* asincrono con eventuali interventi via *web streaming*[8] (15 ore in piattaforma).

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO ESAME FINALE

[7] Gli argomenti trattati faranno maggiormente riferimento a VMware in quanto maggiormente utilizzato in ambito Difesa.
[8] Le indicazioni inerenti alle eventuali attività sincrone saranno comunicate dagli istruttori del corso (Rif. Annesso III del presente Catalogo.

AREA INFOSEC E *INFORMATION ASSURANCE*

52.CORSO SICUREZZA IT[9] - 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.

AREA
INFOSEC e *Information Assurance*

PROGRAMMA / ARGOMENTI TRATTATI
- principi generali della Sicurezza IT;
- gestione del rischio;
- disponibilità delle risorse;
- crittografia e ambiti di impiego;
- infrastruttura a chiave pubblica;
- autenticazione e controllo di accesso;
- codice maligno;
- sicurezza delle reti;
- aspetti sociali, etici e legali della sicurezza informatica;
- sarà, inoltre, effettuato a discrezione dell'istruttore, uno o più webinar le cui modalità saranno comunicate dall'istruttore stesso sulla chat di piattaforma.

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 20.

DURATA DEL CORSO: 2 settimane in modalità *e-learning* asincrono (30 ore in piattaforma)

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO ESAME FINALE

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

AREA *CYBER DEFENCE*, LAW & FORENSICS

53.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.

AREA
Cyber Defence, Law & Forensics

PROGRAMMA/ARGOMENTI TRATTATI
- che cos'è lo spazio cibernetico?
- cosa si intende per Cyber Defence;
- la minaccia cibernetica;
- principi di prevenzione e risposta agli incidenti;
- l'architettura strategica nazionale per la sicurezza e la difesa cibernetica.

Saranno inoltre svolti, a discrezione dell'istruttore, uno o più *webinar* le cui modalità verranno comunicate sulla *chat* di piattaforma.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   a. Frequenza preventiva:
      N.N.;
   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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 20.

DURATA DEL CORSO: 1 settimana in modalità e-learning asincrono con eventuali interventi via web streaming[10] (20 ore in piattaforma).

MODALITÀ DI SVOLGIMENTO
Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO ESAME FINALE

[10] Le indicazioni inerenti alle eventuali attività sincrone saranno comunicate dagli istruttori del corso (Rif. Annesso III del presente Catalogo); tali attività andranno obbligatoriamente seguite e l'eventuale assenza verrà conteggiata ai fini dei requisiti per poter sostenere l'esame.

54. FONDAMENTI DI DIRITTO INTERNAZIONALE APPLICATO ALLE OPERAZIONI CIBERNETICHE - COD. EY452B

OBIETTIVI DEL CORSO
Fornire al personale militare e civile della Difesa le conoscenze fondamentali in tema di diritto internazionale applicabile alle operazioni cibernetiche, anche attraverso lo studio e l'analisi dei principali casi storici.

AREA
Cyber Defence, Law & Forensics

PROGRAMMA / ARGOMENTI TRATTATI
- Origine, evoluzione e soggetti dell'ordinamento internazionale;
- Le fonti del diritto internazionale;
- Cenni sulle norme inerenti la tutela dei diritti umani;
- Le operazioni cibernetiche ed analisi dei principali casi storici;
- Applicabilità delle norme di diritto internazionale alle operazioni cibernetiche.

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: N/N.

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

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 20.

DURATA
1 settimana (da lunedì a venerdì, 32 ore) in modalità e-learning sincrono, con modalità di apprendimento individuali e di gruppo.

MODALITÀ DI SVOLGIMENTO
Le attività in *e-learning* sono disciplinate nell'Annesso III al presente Catalogo
La partecipazione alle attività sincrone/asincrone, definite e comunicate dagli Istruttori, sono obbligatorie ai fini dell'accesso all'esame finale.

È PREVISTO UN ESAME FINALE.

AREA *DATA SCIENCE* E INTELLIGENZA ARTIFICIALE

55. 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.

AREA

Data Science e Intelligenza Artificiale

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- fondamenti di Intelligenza Artificiale;
- il combustibile dell'AI: *Big Data*;
- *Machine Learning*;
- *Deep Learning*: la rivoluzione dell'IA;
- IA e linguaggio NLP;
- IA e *Robots*;
- implementazioni dell'IA.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. **Professionali:**
   d. Frequenza preventiva: N.N.;
   e. Conoscenze basiche richieste: N.N.;
   f. 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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 25.

DURATA DEL CORSO: 1 settimana in modalità *e-learning* sincrono (32 ore in piattaforma).

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso III.

È PREVISTO UN ESAME FINALE.

ANNESSI

ANNESSO I - INFORMAZIONI PER GLI ENTI PROGRAMMATORI

ANNESSO I

NOTIZIE LOGISTICHE/AMMINISTRATIVE

1. ONERI DI VIAGGIO

Gli oneri di viaggio e la diaria sono a carico della F.A. di appartenenza del frequentatore e la Scuola, pertanto, non interviene nel processo di liquidazione dei documenti di viaggio del personale frequentatore.

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 del Calendario Corsi in vigore. Eventuali interruzioni delle lezioni legate a periodi di pausa per festività (es.: pausa natalizia, estiva, ecc.), saranno gestite attraverso l'interruzione della missione del discente e il successivo rientro presso il proprio Comando di appartenenza.

Le fasi frontali dei corsi erogati presso la Scuola sono svolte nelle aule della Direzione Corsi ad eccezione di alcune visite addestrative presso altri Enti della Difesa e/o Aziende del settore site in località raggiungibili in giornata con i mezzi di trasporto collettivo della Scuola. Le località dove si svolgeranno le predette visite addestrative dovranno essere riportate sul Foglio di Viaggio del frequentatore e saranno indicate preventivamente nel Calendario dei Corsi.

2. VITTO E ALLOGGIO

I frequentatori militari e civili dell'A.D. devono essere inviati presso questo Istituto in missione in regime di "Aggregazione completa", ossia con l'obbligo di fruire delle strutture logistiche alloggiative e di ristorazione di STELMILIT con oneri a carico dell'Amministrazione. Eventuale indisponibilità alloggiativa verrà comunicata anticipatamente dalla Scuola.

La Scuola offre un servizio di mensa, dal lunedì alla domenica e giorni festivi compresi, gestito da una ditta convenzionata. Gli orari della mensa sono di seguito indicati:

<table>
<tr><th></th><th>1^ Colazione</th><th>Pranzo</th><th>Cena</th></tr>
<tr><td>Lunedì – giovedì</td><td rowspan="2">07.20 – 07.50</td><td>12.55 – 14.00</td><td rowspan="4">19.00 – 20.00</td></tr>
<tr><td>Venerdì</td><td>12.30 – 13.00</td></tr>
<tr><td>Sabato</td><td rowspan="2">08.00 – 08.20</td><td rowspan="2">12.00 – 13.00</td></tr>
<tr><td>Domenica</td></tr>
</table>

Il personale frequentatore non appartenente all'A.D. è autorizzato alla fruizione della mensa di STELMILIT a titolo oneroso, previa prenotazione e relativo pagamento dell'importo, determinato annualmente dalle SS.AA., direttamente alla Ditta fornitrice del servizio di vettovagliamento.

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 citati alloggi, con particolare riferimento alle loro tipologie, sono effettuate dalla Sezione Alloggi della Scuola tenendo conto del grado del frequentatore, della durata del corso e di eventuali esigenze alloggiative straordinarie definite dal Comando della Scuola.

3. MODALITÀ DI SEGNALAZIONE DEI FREQUENTATORI PER L'AMMISSIONE AI CORSI DEL CALENDARIO DELLA SCUOLA TELECOMUNICAZIONI FF.AA.

a. Segnalazione

(1) Gli Enti Programmatori devono segnalare il nominativo del personale designato alla frequenza dei Corsi del calendario con un anticipo di almeno ***3 settimane*** dall'inizio del corso in cui si intende iscrivere il personale dipendente. La segnalazione deve essere formalizzata con l'invio di un messaggio telegrafico/lettera i cui elementi sono riportati sulla Scheda A dell'Annesso I e con l'invio della Scheda Anagrafica del Frequentatore (Scheda B Annesso I). Il ritardo nella segnalazione del personale designato per la frequenza dei Corsi oltre i termini precedentemente indicati, può comportare la riassegnazione da parte della Scuola di quelle posizioni ad un altro Comando/Ente in lista d'attesa.

(2) Gli Enti Programmatori di FA dovranno tempestivamente comunicare a questa Scuola l'eventuale indisponibilità del personale designato ed il nominativo di un suo sostituto.

b. Requisiti per l'ammissione ai corsi

È fatto obbligo ai Comandi/Enti di accertare il possesso dei requisiti (professionali e di sicurezza indicati nella scheda del corso riportata sul Catalogo dei Corsi) dei propri dipendenti per l'ammissione ai singoli Corsi fornendo assicurazione mediante la compilazione dei paragrafi CHARLIE, DELTA e ECHO del messaggio di segnalazione di cui alla Scheda "A" al presente Annesso.
Per alcuni Corsi è previsto un test iniziale che ha unicamente lo scopo di verificare del grado di conoscenza nella specifica materia.

c. Annullamento dei corsi

La Direzione Corsi si riserva la facoltà di non attivare/differire l'erogazione di eventuali corsi sulla base della situazione contingente ed in particolare per i seguenti motivi:

- mancato raggiungimento del numero minimo necessario all'attivazione di un corso (5 discenti);
- esigenze organizzative e/o logistico/amministrative della Scuola (indisponibilità dell'istruttore, aspetti di carattere logistico, mancanza fondi, etc.).

4. ADEMPIMENTI DEGLI ENTI PROGRAMMATORI

Il Comando di appartenenza del frequentatore dovrà compilare ed inviare a stelmilit.corsi@marina.difesa.it la **Scheda Anagrafica** (vedi Scheda "B" allegata al presente Annesso) scaricabile dalla pagina web dell'Istituto:
https://e-learning.difesa.it/mod/page/view.php?id=11296.
Sulla stessa pagina sono inoltre pubblicate:

- le notizie sulla vita d'Istituto dei frequentatori più aggiornate;
- eventuali varianti alle predette procedure.

ANNESSO I

Scheda A

FORMATO DEL MESSAGGIO PER LA SEGNALAZIONE DEI NOMINATIVI

Il messaggio di segnalazione del nominativo del frequentatore che dovrà essere trasmesso per Competenza alla Scuola, deve contenere le seguenti informazioni:

Oggetto: Segnalazione nominativo corso "nome corso"
Riferimento: Catalogo dei Corsi Interforze di STELMILIT AA XXXX

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

BRAVO: Grado, Cognome, Nome, Ente/Reparto di appartenenza, Codice Fiscale e numero CMD;

CHARLIE: Requisiti di sicurezza;
Il Comando/Ente che invia la segnalazione deve assicurare il possesso dei (noti) requisiti di sicurezza da parte dell'interessato (vedasi descrizione del corso);

DELTA: Requisiti professionali:
Il Comando/Ente che invia la segnalazione deve certificare il possesso dei requisiti per l'ammissione dell'interessato (vedasi descrizione del corso);

ECHO: Assicurare che il designato frequentatore abbia preso visione del documento "Vita di istituto" disponibile al seguente indirizzo:
https://www.difesa.it/smd/entimi/stelmilit/vita-d-istituto/27973.html

Scheda B

Scheda Anagrafica del frequentatore

(da compilare a cura del Comando di
appartenenza del frequentatore)

ANNESSO I

Data di compilazione

A Scuola Telecomunicazioni FF.AA.
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

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° Pass auto**

N° Pass personale | **N° camera** | **Varie**

ANNESSO II - INFORMAZIONI PER I FREQUENTATORI

ANNESSO II

Le presenti informazioni sono rivolte ai Frequentatori dei Corsi presso la Scuola Telecomunicazioni delle F.A. in Chiavari allo scopo di fornire preventivamente notizie di carattere generale utili per la preparazione, il viaggio, l'arrivo e la permanenza alla Scuola.

1. UBICAZIONE

La Scuola Telecomunicazioni, Caserma "GIORDANO LEONE ", è ubicata in Via Parma, n. 34 Chiavari, a circa 2 Km dal centro della città sulla Statale 225 per Parma/Piacenza.
Per eventuali informazioni telefonare alla Segreteria Corsi durante le ore d'ufficio (0185-3334509/10) o, fuori dall'orario di servizio, al personale di guardia della Scuola (0185-3334443).

2. TRASPORTI

Collegamenti disponibili per raggiungere la Scuola:

a. In autovettura

Si consiglia percorrere l'Autostrada A12 ed uscire al casello di Lavagna. È consentito l'accesso nel comprensorio della Scuola alle autovetture dei frequentatori ad eccezione del periodo 01.00 - 05.00 di ogni giorno quando è garantito il solo accesso pedonale.

b. In treno

La stazione ferroviaria di Chiavari è ubicata al centro della città ed è collegata con la Scuola da un servizio di autobus cittadino (www.atpesercizio.it).

c. In aereo

Lo scalo civile più vicino è l'aeroporto "CRISTOFORO COLOMBO" di Genova a 50 Km circa da Chiavari. Lo scalo è collegato con *bus navetta* fino alle principali stazioni ferroviarie di Genova e *Trenitalia* fino a Chiavari.

3. PRESENTAZIONE

Le informazioni per i frequentatori più aggiornate sono scaricabili dal link:
https://www.difesa.it/smd/entimi/stelmilit/vita-d-istituto/27973.html

Sulla stessa pagina saranno comunicate tutte le future significative varianti.

4. PARCHEGGIO

I frequentatori che giungono alla Scuola con automezzo privato possono usufruire delle aree di parcheggio ubicate nel comprensorio della Scuola previa compilazione dell'apposito modulo consegnato all'arrivo.

5. MENSE - SALE CONVEGNO

Alla Scuola sono funzionanti:
- una Mensa Unica disponibile per 1^ colazione, pranzo e cena;
- una Sala Convegno.

6. ORARIO DI SERVIZIO

La Scuola adotta il seguente orario di servizio su cinque giornate lavorative settimanali:

- dal lunedì al giovedì 08.00 – 16.30;
- venerdì 08.00 – 12.00.

L'orario delle lezioni è suddiviso in sette periodi giornalieri dal lunedì al giovedì e in quattro periodi giornalieri il venerdì.

7. UNIFORMI ED ABBIGLIAMENTO

a. Frequentatori militari.
Durante la permanenza nell'Istituto e l'attività d'aula deve essere indossata l'uniforme stagionale di servizio/combattimento/operativa.

Il personale frequentatore **dovrà avere al seguito** l'uniforme Ordinaria da utilizzare in occasione di eventuali cerimonie organizzate dalla Scuola (es. in occasione delle ricorrenze di F.A.). Nei periodi prossimi al cambio uniforme stagionale, il personale frequentatore dovrà avere al seguito le due versioni delle predette uniformi.
Al di fuori dell'orario di servizio, per la frequenza della Mensa e nonché delle altre aree ricreative, è consentito l'uso dell'abito civile, purché consono all'ambiente. Non è consentito l'uso di calzoncini e sandali.

b. Frequentatori civili.
Durante le ore lavorative e per la frequenza di Mensa, Sala Convegno e sale ricreative, dovrà essere indossato un abbigliamento decoroso. In ogni caso sono **assolutamente vietati** l'uso di calzoncini e di sandali all'interno del comprensorio della Scuola.

8. LICENZE E PERMESSI

Durante la frequenza dei Corsi **non vengono concesse licenze e permessi**, se non per gravi o comprovati motivi.
I giorni di licenza e/o le ore di permesso eventualmente concessi saranno oggetto di annotazione e successiva segnalazione all'Ente/Comando di appartenenza per le discendenti azioni di competenza.
Le eventuali richieste di Licenze Straordinarie da parte dei discenti, fatta eccezione quella per GMF, saranno concesse da questa Scuola solo dopo aver ricevuto il "Nulla Osta" da parte dei relativi Comandi di appartenenza.
Eventuali interruzioni della frequenza dei corsi per concomitanti attività esterne alla Scuola dei discenti (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. STELMILIT, nel caso in cui l'assenza dal corso per missione superi il tetto massimo di assenza previsto dal Catalogo dei Corsi (25% delle ore di lezione), segnalerà al discente e al suo Comando le possibili conseguenti dimissioni d'autorità dal corso.

9. DIMISSIONE DAI CORSI

Il frequentatore è dimesso dal corso nei seguenti casi:

a. Dimissioni d'autorità:

- quando non sia in possesso dei requisiti richiesti per lo specifico corso, ovvero che impediscano lo svolgimento anche in parte di alcune attività teoriche e/o pratiche;

- per motivi disciplinari;
- per assenze (per servizio, motivi privati e sanitari) superiori al 25% delle ore di lezione previste per i Corsi Interforze;
- per impreviste esigenze di servizio, rappresentate dall'Ente/Comando di appartenenza;
- per altre tipologie per le quali si provvederà ad una specifica valutazione al momento.

b. <u>Dimissioni volontarie</u>:
il frequentatore dovrà comunicare l'intenzione di dimettersi dal corso che frequenta mediante un'istanza scritta in cui rappresenti le motivazioni di tale scelta.

10. <u>ASSISTENZA SANITARIA</u>

L'Infermeria della Scuola provvede, in caso di necessità, a fornire solo l'assistenza di primo soccorso durante l'orario di servizio. Per l'ulteriore assistenza sanitaria, i frequentatori in possesso del tesserino sanitario personale, potranno usufruire dei servizi offerti dalla locale A.S.L. 4 chiavarese, dall'ospedale civile di Lavagna ubicato a circa 2 Km dalla Scuola e dal servizio 118 per le EMERGENZE.
In caso di assenza per motivi di salute il frequentatore dovrà immediatamente informare la Scuola direttamente o tramite il Capo Corso.

11. <u>SPORT E TEMPO LIBERO</u>

Le strutture della Scuola disponibili per l'attività ginnico-sportiva e del tempo libero includono:
- una palestra attrezzata;
- una sala svago\TV (Piano terra - Palazzina N).

Per la frequenza della palestra il frequentatore dovrà presentare un "certificato medico" rilasciato dal proprio DSS attestante l'idoneità alla *<u>pratica sportiva non agonistica</u>* oppure il certificato di idoneità al SMI.

ANNESSO III - EROGAZIONE DEI CORSI IN DIDATTICA A DISTANZA (DAD)

ANNESSO III

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 o connessione verso laboratori esterni se erogati da ditte esterne per conto della 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[11] sia dalle reti intranet delle F.A. che da Internet. Sarà pertanto possibile accedere ai contenuti anche da qualsiasi postazione personale e senza alcuna limitazione temporale.
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[12] 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

[11] 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.
[12] Le attività sincrone a distanza sono riportate nelle schede dei Corsi interessati.

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 E 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.

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 ed 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.

Procedura per sostenere l'esame finale a distanza[13]:
- 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 allegato, 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

[13] 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).

indicazione dell’esito finale e del punteggio conseguito. indicazione dell’esito finale e del punteggio conseguito.

ANNESSO III

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