

MINISTERO DELLA DIFESA

DIREZIONE GENERALE PER IL PERSONALE CIVILE

1° Reparto – 2^ Divisione – 2^ Sezione

Indirizzo Postale: Viale dell'Università, 4 00185 ROMA

Posta elettronica: persociv@persociv.difesa.it

Posta elettronica certificata: persociv@postacert.difesa.it

Pdc: Funz. Amm. dr. Marco MARRACCINI

Tel. 06/4986.2475 (sotrin 600/2475) lunedì e mercoledì h. 8:00 – 13:00

Utenza mobile di servizio 366/625.82.96

posta elettronica: rep1div2sez2@persociv.difesa.it

OGGETTO: Catalogo dei Corsi Interforze in programma presso la Scuola di Telecomunicazioni FF.AA. di Chiavari. Anno 2022. "Bozza"

A ELENCO INDIRIZZI IN ALLEGATO

^^

Riferimento:

a) f.n. M_D SSTEMIL0002791 del 08/07/2021;

b) f.n. M_DSGDNA REG2021 0050156 del 14/07/2021.

^^

La Scuola di Telecomunicazioni di Chiavari ha trasmesso una bozza del catalogo in oggetto riguardante la programmazione dei corsi di possibile attivazione nel 2022, consultabile sul sito internet della citata Scuola (www.stelmilit.difesa.it).

Nelle more dell'approvazione della suddetta bozza e con l'avvertenza che eventuali soppressioni di corsi non daranno luogo al successivo inoltro delle richieste, si prega di voler inviare a questa Direzione Generale, in conformità a quanto disposto dal Segretariato Generale della Difesa e Direzione Nazionale degli Armamenti – 1° Reparto con il foglio in riferimento, le segnalazioni del personale civile interessato ai Corsi, Master Universitari e Corsi di Formazione Specialistica e di Perfezionamento, **entro il 27 settembre 2021**.

Le DD.GG. e gli Enti dovranno segnalare i nominativi, **comprensivi di e-mail**, in ordine di priorità per ciascun corso o master, previa verifica del possesso dei requisiti previsti per l'ammissione agli stessi.

Considerato il numero limitato dei posti e il costo sostenuto dall'Amministrazione Difesa, si raccomanda, una volta confermata la partecipazione, che il predetto personale **assicuri la frequenza alle lezioni per tutta la relativa durata**.

Informazioni dettagliate concernenti i suddetti corsi possono essere reperite sul citato sito internet della Scuola, ed in particolare nelle **"notizie logistico amministrative"**.

Gli eventuali oneri di missione sono a carico degli Enti di servizio.

IL DIRETTORE GENERALE
Dr.ssa Gabriella MONTEMAGNO

ELENCO INDIRIZZI ALLEGATO ALLA CIRCOLARE N. DEL

PER SUCCESSIVA RIPRODUZIONE E DISTRIBUZIONE A CURA DEGLI ENTI INTERESSATI

DIFESA GABINETTO ROMA

STAMADIFESA ROMA

STATESERCITO ROMA

MARISTAT ROMA

STATAEREO SEDE

COMANDO GENERALE ARMA DEI CARABINIERI ROMA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE
DEGLI ARMAMENTI ROMA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE
DEGLI ARMAMENTI – DIREZIONE INFORMATICA, TELEMATICA E
TECNOLOGIE AVANZATE (TELEDIFE) SEDE

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE
DEGLI ARMAMENTI – DIREZIONE DEGLI ARMAMENTI TERRESTRI
(TERRARM) ROMA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE
DEGLI ARMAMENTI – DIREZIONE DEGLI ARMAMENTI NAVALI
(NAVARM) ROMA

SEGRETARIATO GENERALE DELLA DIFESA E DIREZIONE NAZIONALE
DEGLI ARMAMENTI - DIREZIONE DEGLI ARMAMENTI AERONAUTICI
(ARMAEREO) SEDE

CONSIGLIO MAGISTRATURA MILITARE ROMA

BILANDIFE ROMA

ISPEDIFE ROMA

PREVIMIL ROMA

PERSOMIL ROMA

GENIODIFE ROMA

COMMISERVIZI ROMA

DIFEFORM ROMA

ONORCADUTI ROMA

DIFEAMMISPEC ROMA

ALL' U.D.G. INTERNO

ALL' URP

STATO MAGGIORE DELLA DIFESA

I REPARTO – Ufficio Formazione



*Catalogo dei Corsi Interforze
della
Scuola Telecomunicazioni delle FF.AA.
Anno 2022*

Edizione 2021



STATO MAGGIORE DELLA DIFESA

ATTO DI APPROVAZIONE

Approvo il Catalogo dei Corsi Interforze della Scuola Telecomunicazioni delle Forze Armate in Chiavari per l'Anno Accademico 2022.

Roma, _____

IL SOTTOCAPO DI STATO MAGGIORE

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

UFFICIO GENERALE DEL CAPO DI SMD
SMD I REPARTO PERSONALE
SMD II REPARTO INFORMAZIONI E SICUREZZA
SMD III REPARTO POLITICA MILITARE E PIANIFICAZIONE
SMD VI REPARTO SISTEMI C4I E TRASFORMAZIONE
COMANDO OPERATIVO DI VERTICE INTERFORZE
COMANDO PER LE OPERAZIONI IN RETE
COMANDO PER LE OPERAZIONI SPAZIALI
COMANDO INTERFORZE PER LE OPERAZIONI DELLE FORZE SPECIALI

CENTRO INTELLIGENCE INTERFORZE
CENTRO ALTI STUDI PER LA DIFESA
CENTRO DI GESTIONE E CONTROLLO DEL SICRAL
CENTRO INTERFORZE STUDI PER LE APPLICAZIONI MILITARI

SME - DIPARTIMENTO IMPIEGO DEL PERSONALE
COMANDO LOGISTICO ESERCITO
COMANDO PER LA FORMAZIONE, SPECIALIZZAZIONE E DOTTRINA
DELL'ESERCITO
COMANDO DELLE FORZE OPERATIVE TERRESTRI DI SUPPORTO

COMANDO DELLE SCUOLE DELLA MARINA MILITARE
DIREZIONE PER L'IMPIEGO PER IL PERSONALE MILITARE DELLA MARINA

SMM - REPARTO C4 E SICUREZZA

COMANDO GENERALE DELLE CAPITANERIE DI PORTO

COMANDO SQUADRA AEREA
COMANDO LOGISTICO 3[^] DIVISIONE
STATO MAGGIORE AERONAUTICA - REPARTO GENERALE SICUREZZA

COMANDO GENERALE DELL'ARMA DEI CARABINIERI - UFFICIO
ADDESTRAMENTO
COMANDO GENERALE DELL'ARMA DEI CARABINIERI - UFFICIO RETI
COMANDO GENERALE DELL'ARMA DEI CARABINIERI - UFFICIO SISTEMI
INFORMATIVI

BRIGATA DI SUPPORTO AL NRDC-ITA
QUARTIER GENERALE ITALIANO LAGOPATRIA
CIMIC GROUP SOUTH

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 - UFFICIO TECNICO ED ANALISI DI MERCATO

COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI

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

COMANDO GENERALE GUARDIA DI FINANZA

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

Sommario

ATTO DI APPROVAZIONE.....	III
REGISTRAZIONE DELLE AGGIUNTE E VARIANTI.....	IV
ELENCO DI DISTRIBUZIONE	V
1.PREMESSA	XII
CAPITOLO 1 - ALTA FORMAZIONE UNIVERSITARIA.....	1
AREA TRANSPORT & NETWORKING.....	3
1. MASTER DI II LIVELLO IN TELECOMUNICAZIONI - COD. MR06P.....	5
2. MASTER DI II LIVELLO IN RETI E COMUNICAZIONI SATELLITARI - COD. MS09P	7
3. CORSO DI PERFEZIONAMENTO IN TELECOMUNICAZIONI - COD. CA02P	9
4. CORSO DI SPECIALIZZAZIONE IN RETI E COMUNICAZIONI SATELLITARI - COD. FS04P	10
5. CORSO DI SPECIALIZZAZIONE SULLA QUALITÀ DEL SERVIZIO (QoS) SU RETI ETEROGENEE - COD. FR06P	11
6. CORSO DI SPECIALIZZAZIONE SULLE RETI M.A.NET. (Mobile Ad-hoc Network) - COD. FR149P.....	13
7. CORSO SUI SISTEMI DI RADIOCOMUNICAZIONE AVANZATI - COD. FR150A	14
8. CORSO DI SPECIALIZZAZIONE SUI SISTEMI SOFTWARE DEFINED RADIO (S.D.R.) - COD. FA313P	15
AREA SOFTWARE, APPLICATIVI E E-LEARNING	17
9. MASTER DI II LIVELLO PER PROGETTISTI DI SISTEMI INFORMATICI - COD. MT04P	19
10. MASTER DI II LIVELLO IN MODELLING & SIMULATION - COD. MT10P	20
11. CORSO DI SPECIALIZZAZIONE SUI SISTEMI DI SIMULAZIONE E MODELLIZZAZIONE - COD. FT03P	21
AREA CYBER DEFENCE, FORENSICS & LAW	23
12. MASTER DI I LIVELLO IN “CYBER DEFENCE E DIGITAL FORENSICS” – COD. MY22P	25
ALTRE AREE FORMATIVE	27
13. MASTER DI II LIVELLO IN DIFESA ELETTRONICA - COD. MZ01P.....	29
14. MASTER DI II LIVELLO IN FOTONICA ED OPTOELETTRONICA - COD. MZ02P.....	31
15. MASTER DI II LIVELLO IN INGEGNERIA DEI SISTEMI ELETTRONICI COMPLESSI - COD. MZ03P	32
16. MASTER DI II LIVELLO IN SYSTEM ENGINEERING E PROJECT MANAGEMENT - COD. MZ05P	33
17. MASTER DI II LIVELLO IN MUNIZIONAMENTO AVANZATO (“GUN LAUNCHED GUIDED MUNITIONS”) - COD. MZ12P.....	35
18. MASTER DI II LIVELLO IN SISTEMI COMPLESSI AVANZATI - COD. MZ13P	36

CAPITOLO 2 - LIVELLO AVANZATO	37
AREA TRANSPORT & NETWORKING.....	39
19. CORSO AVANZATO SULLA QUALITÀ DEL SERVIZIO (QoS) SU RETI ETEROGENEE - COD. FR06A	41
20. CORSO AVANZATO DI SISTEMISTA DI 2° LIVELLO IN RETI TELEMATICHE - COD. FR66A	43
21. CORSO AVANZATO DI TECNICHE VOICE OVER IP - COD. A126A.....	45
22. CORSO AVANZATO DI MANUTENTORE FIBRE OTTICHE - COD. AE306A.....	46
23. CORSO AVANZATO PER TECNICI TELEMATICI ARMA CC (2° CICLO) - COD. A311A.....	48
24. CORSO AVANZATO INSTALLATORE E MANUTENTORE MULTIPLEX FLESSIBILE MT301F - COD. A115A.....	50
25. CORSO AVANZATO DI OPERATORE MULTIPLEX FLESSIBILE MT301F - COD. A116A.....	52
26. CORSO SUL BORDER GATEWAY PROTOCOL (BGP) - COD. A117A	54
27. CORSO SU INTERNET PROTOCOL VERSIONE 6 -IPv6 - COD. A118A	56
28. CORSO AVANZATO IP ROUTING - COD. RE229A	58
29. CORSO AVANZATO FIREWALL & VPN - COD. R282A	60
AREA CONTROLLO SATELLITI.....	63
30. CORSO OPERATORE SALA CONTROLLO SATELLITE - COD. TE285A.....	65
31. CORSO CAPO TURNO SALA CONTROLLO SATELLITE - COD. S002A	67
32. CORSO SPECIALISTA CONTROLLO D'ASSETTO E DATABASE SATELLITE - COD. S003A	69
33. CORSO SPECIALISTA PIATTAFORMA SATELLITE - COD. S004A	71
34. CORSO SPECIALISTA COMUNICAZIONI TERRA-BORDO SATELLITE - COD. S005A	72
35. CORSO SUPERVISORE SALA CONTROLLO SATELLITE E STAZIONI TT&C - COD. S006A	73
36. CORSO INGEGNERE SATELLITE - COD. S007A	75
37. CORSO SPECIALISTA CENTRO DI CONTROLLO SATELLITE GEO - COD. S008A	77
38. CORSO CONTROLLORE STAZIONE TT&C GEO - COD. S009A	79
39. CORSO SPECIALISTA STAZIONI TT&C GEO - COD. S010A.....	80
40. CORSO CONTROLLORE DINAMICA DEL VOLO GEO - COD. S011A	81
41. CORSO SPECIALISTA DINAMICA DEL VOLO GEO - COD. S012A.....	82
CONTROLLO SATELLITI IN ORBITA BASSA	83
42. CORSO CONTROLLORE CENTRO DI CONTROLLO SATELLITE OPTSAT-3000 - COD. S013A.....	85
43. CORSO CONTROLLORE SATELLITE OPTSAT-3000 - COD. S014A	86
44. CORSO SPECIALISTA CENTRO DI CONTROLLO SATELLITE OPTSAT-3000 - COD. S015A	87
45. CORSO SPECIALISTA CONTROLLO ASSETTO ED ORBITA SATELLITE OPTSAT-3000 - COD. S016A.....	89
46. CORSO SPECIALISTA PIATTAFORMA SATELLITE OPTSAT-3000 - COD. S017A	91
47. CORSO SPECIALISTA PAYLOAD SATELLITE OPTSAT-3000 - COD. S018A.....	93
48. CORSO CONTROLLORE STAZIONE TT&C OPTSAT-3000 - COD. S019A.....	95

49. CORSO SPECIALISTA STAZIONI TT&C OPTSAT-3000 - COD. S020A	96
50. CORSO CONTROLLORE DINAMICA DEL VOLO OPTSAT-3000 - COD. S021A.....	97
51. CORSO SPECIALISTA DINAMICA DEL VOLO OPTSAT-3000 - COD. S022A	98
52. CORSO SUPERVISORE CENTRI DI CONTROLLO E STAZIONI TT&C OPTSAT- 3000 - COD. S023A	100
53. CORSO INGEGNERE SATELLITE OPTSAT-3000 - COD. S024A	101
AREA SOFTWARE, APPLICATIVI E E-LEARNING	103
54. CORSO AVANZATO DI PROGETTAZIONE E GESTIONE DATABASE - COD. FT68A	105
55. CORSO AVANZATO DI PROGETTAZIONE E GESTIONE DATABASE ORACLE - COD. FT69A.....	106
56. CORSO AVANZATO SU S.O. LINUX - COD. TE285A	107
57. CORSO AVANZATO SU SISTEMI OPERATIVI SERVER IN NETWORKING - COD. TE262A.....	109
58. CORSO AMMINISTRATORI SISTEMA DI COMANDO E CONTROLLO JOINT – C2I ADV - COD. T293A.....	111
59. CORSO ADVANCED MySQL FOR HIGH AVAILABILITY AND PERFORMANCE – COD. TE297A	113
60. CORSO SISTEMA OPERATIVO WINDOWS 2016 SERVER - COD. T291A	115
61. CORSO SISTEMA OPERATIVO WINDOWS 2019 SERVER - COD. T295A	117
62. CORSO AVANZATO PER AMMINISTRATORI S.O. UNIX/LINUX - COD. FT67A	118
63. CORSO AVANZATO PER AMMINISTRATORE ORACLE - COD. FT70A	119
64. CORSO AVANZATO LINGUAGGIO PHP - COD. FT80A.....	120
65. CORSO AVANZATO LINGUAGGIO JAVASCRIPT - COD. FT82A	121
66. CORSO AVANZATO PROGRAMMAZIONE OBJECT ORIENTED E LINGUAGGIO JAVA - COD. FT73A	122
67. CORSO AVANZATO DI PROGRAMMAZIONE IN LINGUAGGIO C/C++ - COD. FT74A	123
68. CORSO AVANZATO SUL LINGUAGGIO XML - COD. FT277A	124
69. CORSO AVANZATO BASE DATI PER IL SUPPORTO ALLE DECISIONI (DATA WAREHOUSE) - COD. FT71A	125
70. CORSO ANALISTI DI SISTEMI - COD. FT78A	126
71. CORSO PROGRAMMAZIONE DI BASE FASE 1 - COD. FT76A	127
72. CORSO PROGRAMMAZIONE DI BASE FASE 2 LINGUAGGIO C - COD. FT77..	128
73. CORSO DI FORMAZIONE AVANZATA IN TECNOLOGIE DI SVILUPPO SOFTWARE E WEB ASP.NET - COD. FT81A	129
74. CORSO M&S EDUCATIONAL PACKAGE ADVANCED: MS-EPA - COD. FT02A	130
75. CORSO DI MODELLING & SIMULATION EDUCATIONAL PACKAGE FUNDAMENTALS: MS EPF - COD. FT01A	132
76. CORSO PER OPERATORE CIFRANTI CM 2000 IP - COD. JE427A	135
77. CORSO CUSTODE MATERIALE COMSEC/CIFRA - COD. J437A	136
78. CORSO INFOSEC – EVALUATION COMMON CRITERIA/ITSEC - COD. J439A	137
79. CORSO PER AMMINISTRATORE CIFRANTI IP CON SISTEMA KNMS - COD. J433A	138
80. CORSO PER UFFICIALI COMSEC DESIGNATI - COD. J447A	139
81. CORSO PER UFFICIALI ALLA SICUREZZA CIS DESIGNATI - COD. J451A ...	140

82. CORSO PER OPERATORE CIFRANTI CM_2100_IP - COD. JE428A	141
83. CORSO PER AMMINISTRATORE CIFRANTI IP CON SISTEMA KNMS 2100 IP - COD. JE429A	142
84. CORSO IT-EKMS CUSTODE CIFRA PER UTENTI LDF DELLE FF.AA. – COD. J450A	143
AREA CYBER DEFENCE, FORENSICS & LAW.....	145
85. CORSO IN DIGITAL FORENSICS – COD. FY15P	147
86. CORSO SU DATA PROTECTION E DATA GOVERNANCE – COD. FY16P	148
87. CORSO PROPEDEUTICO SU MALWARE ANALYSIS – COD. FY17P	149
88. CORSO SU MALWARE ANALYSIS – COD. FY18P	150
89. CORSO SULLA GESTIONE DELLA SICUREZZA DEI DATA CENTRE – COD. FY19P.....	151
90. CORSO SULLA BIG DATA ANALYSIS – COD. FY20P	152
91. CORSO NETWORK FORENSICS – COD. FY21P	153
92. CORSO CYBER NETWORK ANALYSIS – COD. Y446A	154
93. CORSO CYBER NETWORK PROTECTION – COD. YE447A	155
94. CORSO AVANZATO VULNERABILITY ASSESSMENT (V.A.) – COD. YE449A	156
95. CORSO ENDPOINT HARDENING - COD. Y452A	157
96. CORSO COMPUTER EMERGENCY/INCIDENT RESPONSE TEAM - COD. EY445A	158
97. CORSO SU DoS e DDoS - ATTACK & MITIGATION - COD. Y454A	159
98. CORSO CYBER THREAT HUNTING - COD. Y455A	161
99. CORSO RESPONSABILE DELLA CONTINUITA' OPERATIVA - COD. Y456A	162
CAPITOLO 3 - CORSI LIVELLO INTERMEDIO.....	163
AREA TRANSPORT & NETWORKING.....	165
100.CORSO SULLE RETI DI TRASPORTO PER UFFICIALI PROVENIENTI DA ISTITUTI DI FORMAZIONE - COD. R142I	167
101.CORSO PROPEDEUTICO RETI LOCALI ETHERNET - COD. ER235I	169
102.CORSO PROGETTO E GESTIONE DI RETI LOCALI ETHERNET - COD. R235I	171
103.CORSO GESTORE RETI PER UFFICIALI DELLE ARMI NAVALI - COD. R236I	172
104.CORSO FONDAMENTI DI CABLAGGIO STRUTTURATO - COD. R153I.....	173
AREA SOFTWARE, APPLICATIVI E E-LEARNING	175
105.CORSO APPLICAZIONI WEB (HTML/CSS) - COD. TE79I.....	177
106.CORSO E-LEARNING MOODLE - RUOLI STUDENTE DOCENTE - COD. ET22I	179
107.CORSO PIATTAFORMA E-LEARNING MOODLE - RUOLI DOCENTE - AMMINISTRATORE - COD. TE295I.....	181
108.CORSO MYSQL - LINGUAGGIO SQL E GESTIONE DATABASE OPEN SOURCE - COD. TE291I.....	183
109.CORSO INFORMATICO DI F.A. (ABILITAZIONE INF) - COD. T448I.....	185
110.CORSO “USER AND COP MANAGER” DEL SISTEMA DI COMANDO E CONTROLLO JOINT – C2I ADV - COD. T293I	186
AREA CYBER DEFENCE, FORENSICS & LAW.....	187

111.CORSO VULNERABILITY ASSESSMENT (V.A.) – COD. YE449I.....	189
CAPITOLO 4 - CORSI DI LIVELLO BASE	191
AREA TRANSPORT - NETWORKING.....	193
112.CORSO TECNICI TELEMATICI ARMA C.C. (1° CICLO) - COD. A311B	195
113.CORSO DI FREQUENCY E SPECTRUM MANAGEMENT – COD. EA001B	196
114.CORSO SU FONDAMENTI DI TEORIA DELLE COMUNICAZIONI SATELLITARI E SISTEMA SICRAL – COD. ER309B	197
AREA SOFTWARE, APPLICATIVI E E-LEARNING	199
115.CORSO E-LEARNING DI INFORMATICA DI BASE ECDL - COD. ET17B	201
116.CORSO E-LEARNING IT SPECIALIST - COD. ET18B.....	203
117.CORSO E-LEARNING SU S.O. LINUX BASE – COD. ET23B	205
118.CORSO ELEMENTI DI VIRTUALIZZAZIONE - COD. ET24B	207
AREA INFOSEC E INFORMATION ASSURANCE	209
119.CORSO SICUREZZA IT: COD. EJ400B	211
AREA CYBER DEFENCE, FORENSICS & LAW.....	213
120.CORSO FONDAMENTI DI INTELLIGENZA ARTIFICIALE (IA) – COD. Y453B	215
121.CORSO FONDAMENTI DI CYBER DEFENCE - COD. EY442B	216
122.CORSO FONDAMENTI DI DIGITAL FORENSICS - COD. EY446B.....	217
123.CORSO FONDAMENTI DI INFORMATICA GIURIDICA PER IL PERSONALE DELLA DIFESA - COD. EY450B	218
124.CORSO SU TRATTAMENTO DEI DATI PERSONALI PER IL PERSONALE DELLA DIFESA - COD. EY451B	219
125.MODULO INFORMATIVO SULLA CYBER DEFENCE – COD. EY430B	220
126.MODULO INFORMATIVO SULL’INFORMATICA GIURIDICA - COD. EY431B	221
ANNESI.....	223
ANNESSO I - INFORMAZIONI PER GLI ENTI PROGRAMMATORI.....	225
ANNESSO II - INFORMAZIONI PER I FREQUENTATORI	233
ANNESSO III - INFORMAZIONI MASTER E CORSI UNIVERSITARI.....	241
ANNESSO IV - EROGAZIONE DEI CORSI IN DIDATTICA A DISTANZA (DAD).....	251

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 (A.D.) nel settore dell'*Information Technology (IT)* e della *Sicurezza delle Informazioni (INFOSEC)*.

Le continue e rapide evoluzioni tecnologiche che interessano tali sfidanti settori coinvolgono in pieno tutte la realtà della Difesa e, pertanto, è necessario un continuo e rapido adeguamento dell'offerta formativa proposta dalla Scuola per potere rendere disponibile una formazione sempre aggiornata e pienamente rispondente alle necessità delle F.A..

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.

Nel periodo della pandemia da COVID-19, per garantire la continuità formativa in favore del personale delle FF.AA., l'Istituto ha modificato la modalità di erogazione di un largo numero di corsi in presenza trasformandoli in corsi erogati a distanza (Didattica a Distanza – DAD). In particolare, numerosi corsi sono stati trasformati in corsi a distanza sincroni (mediante l'uso di applicazioni per erogare lezioni in *live streaming*) e a distanza asincroni (mediante contenuti didattici disponibili sulla piattaforma *e-learning* della Difesa).

A questo documento sono collegati e faranno seguito il Calendario dei Corsi 2022 e quello dell'Alta Formazione Universitaria per l'Anno Accademico 2022 che saranno elaborati sulla base delle richieste di partecipazione, che perverranno da parte delle singole FF.AA. e delle altre Amministrazioni dello Stato elencate nell'elenco di distribuzione di questo documento.

In esito all'applicazione delle linee guida sanitarie anti-COVID 19 dettate dalle SS.AA., questo Istituto ha introdotto degli adempimenti che dovranno essere assolti dai discenti entro il giovedì antecedente l'inizio del corso pena l'esclusione d'autorità dal corso stesso. Tali adempimenti sono elencati al para 13 dell'Annesso II e scaricabili col link:

https://www.difesa.it/SMD_/EntiMI/STELMILIT/Pagine/vita_istituto.aspx.

2. SCOPO

Il presente Catalogo dei Corsi ha lo scopo di illustrare l'offerta formativa della Scuola Telecomunicazioni delle FF.AA. per l'anno 2022, capacità destinata prioritariamente al personale dell'A.D. ma fruibile anche dal personale della Pubblica Amministrazione fatte salve le previste autorizzazioni di competenza da inoltrare al I Reparto dello Stato Maggiore della Difesa. Sono, altresì, possibili le iscrizioni di personale di altre articolazioni dello Stato e di aziende civili previa la sottoscrizione di accordi, ovvero, attraverso 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. 5., in qualità di elementi di organizzazione deputati a riportare alla Scuola le necessità di partecipazione ai Corsi del personale dipendente;
- Organismi governativi, indicati al successivo para. 6., che intendano usufruire dell'offerta formativa della Scuola.

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 notizie circa le caratteristiche ed i requisiti dei frequentatori dei corsi/master universitari ed altre notizie utili sui precitati corsi/master (Annesso III);
- fornisce le modalità di erogazione dei corsi in modalità a distanza (Annesso IV).

Inoltre, la parte descrittiva dei Corsi è suddivisa nei seguenti quattro settori:

- Alta Formazione Universitaria;
- Livello Avanzato;
- Livello Intermedio;
- Livello Base.

In ognuno dei già menzionati settori sono raccolti gli elementi descrittivi salienti dei singoli Corsi suddivisi per le seguenti aree tematiche di appartenenza:

- *Transport & Networking*;
- *Controllo Satelliti*;
- *Software, Applicativi e e-Learning*;
- *INFOSEC e Information Assurance*;
- *Cyber Defence, Forensics & Law*;
- Altre aree formative.

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.

Per consentire la realizzazione del Calendario dei Corsi 2022 le prenotazioni di frequenza ai Corsi, dovranno pervenire a questo Istituto, da parte degli Enti Programmatori elencati ai paragrafi 5. e 6. del presente documento, entro il **31 ottobre 2021**.

Il predetto Calendario fornirà indicazioni sul programma temporale dei Corsi e sulle relative sessioni che saranno attivate nel 2022 e, inoltre, conterrà l'indicazione relativa al numero di posti assegnati a ciascun Ente Programmatore.

L'attivazione dei Master e dei Corsi Universitari, facenti parte dell'Alta formazione Universitaria, oltre a prevedere un iter procedurale differente rispetto ai Corsi Interforze, è legata alle esigenze mirate degli Enti Programmatori ed alle specifiche valutazioni/disposizioni dello Stato Maggiore della Difesa.

Gli Enti Programmatori che intendano proporre ulteriori “percorsi formativi” potranno rappresentare l’esigenza alla Scuola la quale, fatte le proprie valutazioni di fattibilità, provvederà a proporre l’inserimento a Catalogo allo Stato Maggiore Difesa I e VI Reparto. A valle dell’autorizzazione di SMD si provvederà all’inserimento in calendario della attività formativa in questione.

Il presente Catalogo è pubblicato, in formato Acrobat (pdf), nei seguenti siti istituzionali:

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

Ulteriori richieste di informazioni possono essere inoltrate al seguente punto di contatto della Direzione Corsi della Scuola:

e-mail: stelmilit.corsi@marina.difesa.it, 0185 3334510 (linea civile); 7228510 (linea MM).

4. METODOLOGIA DIDATTICA DEI CORSI

La Scuola eroga i corsi elencati nel presente catalogo in modalità sia “in presenza” sia “a distanza (DAD)”, quest’ultima secondo le seguenti tipologie:

- *e-learning* asincrono;
 - *e-learning* sincrono;
 - *blended*;
 - *on-line training* (laboratori remotizzati),
- i cui dettagli sono riportati nell’Annesso IV del presente Catalogo.

Per i corsi erogati in modalità a distanza è consentita la loro annotazione su libretto matricolare secondo le modalità descritte in Annesso IV.

I corsi in modalità informativa, introdotti nel 2020, prevedono l’erogazione di appositi Moduli Informativi, di livello basico, sempre accessibili nella piattaforma *e-learning* della Scuola e che non necessitano di iscrizione. Infine, tali Moduli non prevedono esami finali, rilascio di attestati e relativa annotazione a matricola.

Oltre alla precedente tipologia di corsi la Scuola potrà svolgere Conferenze Cyber ossia conferenze informative su tematiche di natura Cyber e relativi aspetti legali presso gli Enti/Comandi che ne facciano richiesta. La fattibilità di tali eventi sarà confermata di volta in volta dalla Direzione Corsi della Scuola che concorderà 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. 28519 - linea civile 0185 3334519).

5. 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 Difesa:
 - . I Reparto Personale;
 - . II Reparto Informazioni e Sicurezza;
 - . III Reparto Politica Militare e Pianificazione;
 - . VI Reparto Sistemi C4I e Trasformazione;
- Comando Operativo di Vertice Interforze;
- Comando per le Operazioni in Rete;
- Comando per le Operazioni Spaziali;
- Comando Interforze per le Operazioni delle Forze Speciali.

c. Esercito

- Stato Maggiore Esercito;
 - Dipartimento Impiego del Personale – Ufficio Formazione e Politica d'impiego;
- Comando per la formazione, specializzazione e dottrina dell'Esercito.

d. Marina Militare

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

e. Capitanerie di Porto

- Comando Generale delle Capitanerie di Porto.

f. Aeronautica Militare

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

g. Arma Carabinieri

- Comando Generale dell'Arma dei Carabinieri:
 - . Ufficio Reti;
 - . Ufficio Sistemi Informativi;
 - . Ufficio Addestramento.

h. Comandi NATO

- Quartier Generale Italiano Lago Patria;
- NATO Rapid Deployable Corps Italy;
- CIMIC Group South.

6. ALTRI COMANDI/ENTI/AMMINISTRAZIONI

- Presidenza della Repubblica - Segretariato Generale;
- Presidenza del Consiglio dei Ministri - Ufficio del Segretario Generale;
- Ministero degli Affari Esteri e della Cooperazione Internazionale;
- Comando Generale Guardia di Finanza;
- Polizia di Stato;
- Polizia Penitenziaria.

7. NOVITÀ APPORTATE AL CATALOGO

La presente edizione del Catalogo si differenzia dalla precedente per alcune modifiche apportate. In particolare, sono stati inseriti i seguenti nuovi corsi:

- CORSO SU CYBER THREAT HUNTING – COD. Y455A;
- CORSO SU TRATTAMENTO DEI DATI PERSONALI PER IL PERSONALE DELLA DIFESA – COD. EY451B;
- CORSO RESPONSABILE CONTINUITÀ OPERATIVA – COD. Y456A;
- CORSO SU SISTEMA OPERATIVO WINDOWS 2019 SERVER – COD. T295A.

8. VARIE

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

Agli Enti che risulteranno assegnatari di posti nel Calendario dei Corsi 2022 è richiesto di:

- comunicare i dati di ciascun frequentatore con almeno 3 settimane di anticipo rispetto all'inizio del corso mediante la Scheda A in Annesso I;
- comunicare al discente designato di attenersi scrupolosamente alle norme ed alle procedure anti-COVID19 adottate dalla Scuola su indicazione delle SS.AA.;
- comunicare con il massimo anticipo l'eventuale indisponibilità del personale designato, in modo da consentire la riassegnazione dei posti in base alla lista di attesa;
- 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 - ALTA FORMAZIONE
UNIVERSITARIA**

AREA TRANSPORT & NETWORKING

1. MASTER DI II LIVELLO IN TELECOMUNICAZIONI - COD. MR06P

OBIETTIVI DEL CORSO

Presentare strumenti e metodi di base per la progettazione, realizzazione e gestione dei sistemi per le Telecomunicazioni di ultima generazione.

Preparare le professionalità per la gestione ed il monitoraggio dei sistemi di telecomunicazioni nella realtà industriale e militare.

Fornire strumenti per l'analisi e la valutazione dei processi operativi, decisionali ed informativi nel campo delle telecomunicazioni, anche in relazione a sistemi e a tecnologie innovative con particolare attenzione alle tecnologie Internet e al ruolo degli *smartphone* nelle reti mobili.

AREA

Transport & Networking

RUOLI E POSIZIONI RICOPRIBILI

Il Master si propone di formare figure professionali nell'area tecnologica ed organizzativa delle telecomunicazioni in grado di assumere posizioni di:

- Capo progetto;
- Supervisore di Progetti;
- Esperto di progettazione e sviluppo;
- Esperto per l'integrazione di sistemi complessi.

Le figure professionali, conseguendo un'approfondita preparazione sulle tecniche e tecnologie avanzate nel campo della progettazione, impianto, gestione e sperimentazione di sistemi di Telecomunicazione (fissi e mobili), caratterizzati da alta capacità di sopravvivenza anche in condizioni di funzionamento severe e/o in ambiente ostile, sono tipicamente impiegate nei processi industriali ed in particolare nell'intero ciclo di vita del sistema di erogazione del servizio di Telecomunicazioni.

PROGRAMMA

I corsi di insegnamento sono:

- antenne e loro evoluzione;
- comunicazioni a banda larga;
- compressione di immagini e sequenze video e nuovi protocolli;
- elaborazione numerica dei segnali;
- ponti Radio;
- impianti RF;
- tecnologie internet;
- reti mobili;
- comunicazioni e reti satellitari;
- sicurezza informatica delle reti telematiche;
- vulnerabilità e difesa elettronica;
- misure e collaudi elettronici sui sistemi di telecomunicazioni;
- bioelettromagnetismo;
- gestione e controllo nelle reti di telecomunicazioni;
- fibre ottiche;
- reti geografiche: trasporto a banda larga su fibra ottica (tecnologia *Dense Wavelength Division Multiplexing* – DWDM).

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione;
- stage.

2. MASTER DI II LIVELLO IN RETI E COMUNICAZIONI SATELLITARI - COD. MS09P

OBIETTIVI DEL CORSO

Fornire conoscenze su strumenti e metodi di base per la progettazione, realizzazione e gestione dei sistemi comunicazioni e reti basati su trasmissione satellitare.

Fornire strumenti per l'analisi e la valutazione dei processi operativi, decisionali ed informativi nel campo delle comunicazioni e reti satellitari, anche in relazione a sistemi di nuova generazione.

Formare una professionalità completa per la gestione ed il monitoraggio dei sistemi di comunicazioni e reti satellitari nella realtà industriale e militare.

AREA

Transport & Networking

RUOLI E POSIZIONI RICOPRIBILI

Il Master si propone di formare figure professionali nell'area tecnologica ed organizzativa delle comunicazioni satellitari in grado di assumere posizioni di:

- Capo progetto di Progetti ad alta tecnologia per le comunicazioni e reti;
- Supervisore di Progetti ad alta tecnologia per le comunicazioni e reti;
- Dirigente per la qualità di Progetti ad alta tecnologia per le comunicazioni e reti;
- Esperto di progettazione e sviluppo ad alta tecnologia per le comunicazioni e reti;
- Esperto per l'integrazione di sistemi complessi ad alta tecnologia per le comunicazioni e reti;
- Esperto per la pianificazione e valutazione di sistemi complessi ad alta tecnologia per le comunicazioni e reti.

Le figure professionali sopra elencate, conseguendo un'approfondita preparazione sulle tecnologie avanzate e sulle metodologie per la progettazione, l'impianto, la gestione e la sperimentazione di sistemi satellitari (fissi e mobili) caratterizzati da alta capacità di sopravvivenza ed operatività anche in ambiente ostile, sono complessivamente orientate all'assunzione di responsabilità nei processi industriali ed in particolare nell'intero ciclo di vita del sistema di erogazione del servizio in una rete satellitare.

PROGRAMMA

Gli argomenti trattati sono i seguenti:

- antenne e propagazione elettromagnetica per sistemi di comunicazione via satellite;
- elaborazione numerica di segnali e immagini per le comunicazioni satellitari;
- reti di telecomunicazioni satellitari e spaziali¹;
- sistemi di trasmissione satellitare;
- elettronica dei sistemi satellitari;
- telerilevamento e monitoraggio via satellite;
- sistemi di localizzazione e navigazione satellitare;
- architetture eterogenee e integrazione satellitare-radio-terrestre;
- applicazioni e servizi via satellite in ambito militare;
- terminali fissi e mobili;
- gestione della sicurezza in ambito satellitare¹;

¹Tecnologie degli *hub* di trasmissione dati in TDMA - es. DVB/S2-RCS, *iDirect*, ecc...) e la relativa sicurezza.

- gestione di programmi satellitari di telecomunicazioni;
- controllo di piattaforme satellitari in orbita geostazionaria;
- gestione della sicurezza in ambito satellitare;
- i sistemi e le reti di comunicazioni satellitari nelle applicazioni militari.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione;
- stage.

3. CORSO DI PERFEZIONAMENTO IN TELECOMUNICAZIONI - COD. CA02P

OBIETTIVI DEL CORSO

Fornire conoscenze teoriche e pratiche sugli apparati, i sistemi e le reti di telecomunicazioni allo scopo di formare figure professionali in grado di comprendere a fondo il funzionamento di un sistema di telecomunicazioni per garantire una corretta pianificazione e gestione.

AREA

Transport & Networking

RUOLI E POSIZIONI RICOPRIBILI

In particolare, dette figure professionali opereranno nell'area organizzativa delle telecomunicazioni e saranno pertanto in grado di assumere posizioni di:

- esperto per la pianificazione valutazione di sistemi avanzati ad alta tecnologia;
- esperto per l'integrazione di sistemi avanzati ad alta tecnologia.

I sistemi di telecomunicazione (fissi e mobili) che vengono trattati, sono caratterizzati da alta capacità di sopravvivenza, anche in condizioni di funzionamento severe e/o in ambiente ostile.

PROGRAMMA

I corsi di insegnamento sono:

Richiami di matematica applicata all'ingegneria dei sistemi TLC;

- fondamenti di microonde e antenne e loro evoluzione;
- basi di comunicazioni a banda larga;
- elementi di codifica di immagini e di sequenze video;
- elementi di elaborazione numerica dei segnali e nuovi protocolli;
- introduzione ai ponti radio;
- introduzione ai sistemi e impianti radio;
- introduzione alle reti di telecomunicazioni;
- fondamenti di comunicazioni mobili;
- introduzione alle comunicazioni via satellite;
- elementi di sicurezza delle telecomunicazioni;
- tecniche fondamentali di difesa elettronica;
- misure e collaudi elettronici sui sistemi TLC;
- elementi di compatibilità elettromagnetica e Bio-elettromagnetismo;
- fibre ottiche;
- reti geografiche: trasporto a banda larga su fibra ottica (tecnica *Dense Wavelength Division Multiplexing* – DWDM nella realizzazione delle reti geografiche).

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

4. CORSO DI SPECIALIZZAZIONE IN RETI E COMUNICAZIONI SATELLITARI - COD. FS04P

OBIETTIVI DEL CORSO

Il Corso ha l'obiettivo di fornire conoscenze di base relative alle reti, alle comunicazioni e ai servizi via satellite e di fornire strumenti per la comprensione e la progettazione di soluzioni orientate alle comunicazioni e alle reti satellitari.

AREA

Transport & Networking

RUOLI E POSIZIONI RICOPRIBILI

I frequentatori, conseguendo un'approfondita preparazione sulle tecniche e tecnologie avanzate nel campo della progettazione, impianto, gestione e sperimentazione di sistemi di comunicazione satellitari, caratterizzati da alta capacità di sopravvivenza anche in condizioni di funzionamento severe e/o in ambiente ostile, sono orientati all'assunzione di responsabilità nell'intero ciclo di vita del sistema di erogazione del servizio di comunicazioni.

PROGRAMMA

Gli argomenti trattati sono i seguenti:

- introduzione alla propagazione elettromagnetica per sistemi di comunicazione via satellite;
- elementi di elaborazione numerica di segnali e immagini;
- reti di telecomunicazioni satellitari e spaziali;
- introduzione ai sistemi di trasmissione satellitare;
- elementi di elettronica dei sistemi satellitari;
- introduzione ai sistemi di localizzazione e navigazione satellitare;
- servizi via satellite in ambito militare;
- elementi di terminali fissi e mobili;
- introduzione alla sicurezza in ambito satellitare;
- progettazione di piattaforme di telecomunicazioni satellitari orbitanti;
- elementi di sistemi e reti di comunicazioni satellitari nelle applicazioni militari;
- tecnologie relative agli *hub* di trasmissione dati in TDMA (es. DVB/S2-RCS, iDirect, ecc.) e la relativa sicurezza.

PERIODICITÀ E DURATA DEL CORSO

Il corso si svolge una volta all'anno ed ha una durata di 5 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

5. CORSO DI SPECIALIZZAZIONE SULLA QUALITÀ DEL SERVIZIO (QoS) SU RETI ETEROGENEE - COD. FR06P

OBIETTIVI DEL CORSO

Introdurre concetti fondamentali per la gestione delle qualità del servizio in reti eterogenee quali il "mapping" verticale ed orizzontale, le architetture di QoS, il *signalling*, il concetto di *gateway* a garanzia del servizio.

Proporre alcuni argomenti avanzati come l'allocazione di risorse in reti a qualità garantita e le reti DTN (*Delay Tolerant Networks*) e presentare in dettaglio la soluzione SDN (*Software Defined Networking*) come soluzione orientata alla gestione della qualità del servizio di una rete eterogenea.

Per la frequenza del corso è richiesta la preventiva frequenza del corso "QoS livello avanzato" o comprovata conoscenza degli argomenti in esso trattati.

AREA

Transport & Networking

PROGRAMMA

Gli argomenti trattati sono i seguenti:

Gestione della QoS in reti eterogenee:

- richiami elementi del Corso Base;
- QoS *Internetworking* su reti eterogenee;
- *vertical QoS mapping*;
- *horizontal QoS mapping*;
- realizzazione dell'interfaccia opportuna;
- architetture QoS;
- stato dell'arte;
- *IP centric QoS Architecture*;
- *MPLS centric QoS Architecture*;
- *IPv6 centric QoS Architecture*;
- segnalazione su architetture QoS;
- RSVP;
- RSVP TE;
- NSIS.

QoS Gateway per comunicazioni radio e satellitari:

- ruolo del *gateway*;
- soluzioni industriali;
- soluzioni *cross-layer*;
- allocazione di banda in reti radio e satellitari.

Architettura DTN (*Delay Tolerant Networks*):

- funzionalità, caratteristiche, aspetti progettuali;
- esempi operativi: comunicazioni interplanetarie, comunicazioni sottomarine, reti pervasive ed opportunistiche;
- necessità di memorizzare l'informazione in modo permanente nei nodi intermedi.
- aspetti di ricerca e di evoluzione futura del SDN (*Software Defined Networking*);
- introduzione e scopo;
- architettura;
- *OpenFlow*;

- *Flow Table*;
- realizzazioni pratiche ed esempi operativi.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno ed ha una durata di 1 settimana.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

6. CORSO DI SPECIALIZZAZIONE SULLE RETI M.A.NET. (*Mobile Ad-hoc Network*) - COD. FR149P

OBIETTIVI DEL CORSO

Fornire ai frequentatori le principali conoscenze sulle soluzioni tecnologiche che garantiscono la comunicazione e l'interazione di un insieme di nodi di comunicazione mobile (sensori, decisor, piattaforme e sistemi d'arma), che interagiscono e comunicano tra di loro in una rete ad elevata capacità, senza disporre di un'infrastruttura fissa, né di collegamenti già pianificati.

Descrivere i protocolli d'instradamento Multi-Hop, che consentono a tutti gli utenti di una rete radio di costituirsi come nodi di una rete mobile auto-configurante (*self-configuring*), in grado di operare in modalità *relay*, adattandosi dinamicamente alle variazioni di topologia dovute al movimento relativo dei nodi ed al fraporsi di ostacoli (*self-healing*).

AREA

Transport & Networking

PROGRAMMA

Gli argomenti trattati sono i seguenti:

- reti *wireless ad hoc*;
- protocolli di accesso multiplo;
- *routing multi-hop*;
- reti veicolari (VANET);
- reti opportunistiche (cenni);
- reti MANET come base sistemi di *Data Fusion*;
- algoritmi di stima e *detection* distribuita;
- simulazione seriale e parallela su calcolatore di sistemi Manet.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno ed ha una durata di 1 settimana.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

7. CORSO SUI SISTEMI DI RADIOCOMUNICAZIONE AVANZATI - COD. FR150A

OBIETTIVI DEL CORSO

Il Corso ha l'obiettivo di fornire conoscenze avanzate nel campo dei sistemi di radiocomunicazione (es.: antenne di nuova generazione, nuovi protocolli, ecc.) e nuove tecnologie di comunicazione (es. 4G, 5G, ecc).

AREA

Transport & Networking

PROGRAMMA

Gli argomenti di insegnamento saranno sia a carattere teorico che applicativo. L'articolazione del Corso sarà la seguente:

- classificazione e caratteristiche dei sistemi *wireless*;
- modelli di canali wireless;
- modulazione digitale per sistemi wireless;
- trasmissione su canali *wireless*;
- tecniche di accesso multiplo;
- reti e sistemi
- sistemi cellulari;
- 5G.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e si articolerà, nell'arco di due settimane, in 60 ore di lezioni (teoriche e/o pratiche) più 3 ore per l'esame finale.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

8. CORSO DI SPECIALIZZAZIONE SUI SISTEMI SOFTWARE DEFINED RADIO (S.D.R.) - COD. FA313P

OBIETTIVI DEL CORSO

Fornire ai frequentatori le principali conoscenze sulle soluzioni tecnologiche che consentano, con un hardware funzionalmente unico, orientato alla ricetrasmisione radio, di configurare le principali caratteristiche della trasmissione: banda RF, formato di modulazione, codifica di canale. Lo scopo è stabilire collegamenti radio dinamici e flessibili, mediante opportuna configurazione di differenti moduli software.

AREA

Transport & Networking

PROGRAMMA

Gli argomenti trattati sono i seguenti:

- vantaggi ed utilità della SDR rispetto ai sistemi radio tradizionali;
- architetture SDR;
- sezione RF e conversione D/A;
- algoritmi di filtraggio, di decimazione e di interpolazione;
- processing in banda base, modulazione-demodulazione;
- sintesi di forme d'onda a larga banda: OFDM;
- dalla *Software Radio alla Cognitive Radio*: architetture;
- *spectrum sensing*;
- esempi applicativi e sviluppi futuri;
- cenni al *Radio Description Language*.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno ed ha una durata di 1 settimana.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

AREA SOFTWARE, APPLICATIVI E E-LEARNING

9. MASTER DI II LIVELLO PER PROGETTISTI DI SISTEMI INFORMATICI - COD. MT04P

OBIETTIVI DEL CORSO

Il Master di II livello in “progettisti di sistemi informatici” presenterà strumenti e metodi in grado di fornire ai frequentatori un’approfondita preparazione tecnico-scientifica ed applicativa per la progettazione, realizzazione e gestione di sistemi informativi gestionali ed operativi con approfondimenti riguardanti le tecnologie hardware e software dei sistemi, comprese l’ingegneria e la qualità del software, le architetture orientate ai servizi (SOA), i sistemi SDR, l’elaborazione delle immagini e la grafica computerizzata, la sicurezza delle informazioni e la crittografia, la valutazione e l’acquisizione di sistemi informatici, la protezione elettromagnetica degli stessi.

AREA

Software, Applicativi e *e-Learning*

RUOLI E POSIZIONI RICOPRIBILI

Il Master si propone di formare figure professionali in grado di assumere posizioni di:

- capo progetto, supervisore di progetti di sistemi informatici;
- esperto di progettazione e sviluppo di sistemi informatici;
- esperto per l’integrazione dei sistemi informatici.

PROGRAMMA

I corsi di insegnamento frontale sono sia a carattere tematico che a carattere disciplinare e sono:

- progettazione orientata agli oggetti e basi dati;
- sistemi operativi proprietari e *open source*;
- ingegneria del *software*;
- sicurezza informatica e sicurezza dei processi di autenticazione e autorizzazione;
- requisiti di *secure by design*;
- reti di telecomunicazioni;
- elaborazione digitale dei segnali;
- architetture classiche ed orientate ai servizi (SOA) per sistemi informatici;
- sistemi informativi, sistemi *real time*;
- elaborazione di immagini e grafica computerizzata;
- sistemi SDR;
- valutazione e acquisizione;
- sicurezza delle informazioni in rete e crittografia²;
- la minaccia e la protezione elettromagnetica, ricerca e sviluppo nei sistemi informatici.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d’iscrizione e *stage*.

² Sicurezza dei processi di autenticazione e autorizzazione e requisiti di *Secure by Design*.

10.MASTER DI II LIVELLO IN *MODELLING & SIMULATION* - COD. MT10P

OBIETTIVI DEL CORSO

Fornire conoscenze avanzate ed approfondite di strumenti e metodi per la progettazione, realizzazione e gestione di sistemi di simulazione.

Fornire approfondite capacità professionali orientate alla gestione ed al monitoraggio di un sistema di simulazione avanzato ed alla valutazione del suo impatto nella realtà operativa.

Fornire strumenti per l'analisi e la valutazione di soluzioni operative, supporti decisionali e sistemi net-centrici.

Conseguire un'approfondita preparazione sulle tecnologie avanzate per progettazione, gestione e sperimentazione di sistemi di simulazione.

AREA

Software, Applicativi e e-Learning

RUOLI E POSIZIONI RICOPRIBILI

Il Master si propone di formare figure professionali in grado di assumere posizioni di responsabilità e supervisione in relazione a progetti ad alta tecnologia nel settore specifico. Tali figure conseguiranno un'approfondita preparazione sulle tecnologie avanzate per progettazione, gestione e sperimentazione di sistemi di simulazione.

PROGRAMMA

Gli argomenti da trattare sono i seguenti:

- metodologie avanzate per la simulazione;
- introduzione al *Modelling & Simulation*;
- sistemi stocastici e deterministici;
- simulazione continua;
- simulazione discreta;
- simulazione *live*;
- simulazione *virtual*;
- simulazione *constructive*;
- *design of experiments and variance*;
- *verification, validation & accreditation*;
- simulazione distribuita e parallela;
- *high level architecture*;
- simulazione per il *training*;
- supporto decisionale e simulazione;
- simulazione per l'analisi.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione;
- stage.

11.CORSO DI SPECIALIZZAZIONE SUI SISTEMI DI SIMULAZIONE E MODELLIZZAZIONE - COD. FT03P

OBIETTIVI DEL CORSO

Fornire conoscenze relative a simulazione e strumenti operativi per effettuare simulazioni in specifici ambienti.

Il corso dovrà inoltre consentire di integrare le conoscenze di base dei frequentatori, in particolare dei Sistemi di Modellizzazione e Simulazione utilizzati in ambito Difesa.

AREA

Software, Applicativi e e-Learning

RUOLI E POSIZIONI RICOPRIBILI

Il corso è rivolto al personale preposto a svolgere incarichi di utilizzo e conduzione di sistemi di Simulazione e Modellizzazione.

PROGRAMMA

Gli argomenti trattati sono i seguenti:

- introduzione alla simulazione;
- la modellizzazione di sistemi ad eventi discreti;
- la simulazione ad eventi discreti: basi teoriche ed operative;
- elementi di visualizzazione tridimensionale;
- strumenti di simulazione ad eventi discreti;
- esempi operativi: il simulatore NS3;
- la simulazione di reti di computer: approcci tradizionali ed avanzati;
- l'ambiente di simulazione *network simulator 3 (ns3)*: installazione e passi iniziali;
- la struttura interna di NS3;
- gli eventi discreti in NS3;
- creazione in NS3 degli elementi base per l'inoltro di pacchetti di dati;
- *router* e *host* in NS3;
- gestione di *link* e *buffer* in NS3;
- il livello di trasporto in NS3;
- cenni di programmazione avanzata di NS3: *debugging*, sviluppo di nuovi moduli;
- simulazione e sperimentazione basata sull'uso di apparecchiature localizzate presso il laboratorio didattico come, ad esempio reti radio militari tattiche, reti di accesso a larga banda wireless e VoIP;
- interfacciamento tra reti tattiche e reti governative e, eventualmente, di altra strumentazione che la Scuola TLC FF.AA. ritenga di interesse per la formazione;
- la simulazione in ambiente militare.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 5 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

AREA CYBER DEFENCE, FORENSICS & LAW

12.MASTER DI I LIVELLO IN “CYBER DEFENCE E DIGITAL FORENSICS” – COD. MY22P

OBIETTIVI DEL CORSO

Il Master ha l’obiettivo di fornire le basi teoriche e pratiche relative ai sistemi operativi, a Internet e ai servizi basati su internet e presenta le metodologie e gli strumenti per condurre attività di difesa Cyber e di analisi ed investigazione di Digital Forensics nel rispetto del Codice di Procedura Penale e degli standard internazionali comunemente adottati

AREA

Cyber Defence, Forensics & Law

RUOLI E POSIZIONI RICOPRIBILI

Il Master si propone di formare figure professionali nell’area tecnologica della *cyber* e della *Digital Forensics*, che saranno in grado di assumere posizioni di:

- esperto di analisi e recupero dati da supporti di memoria dei principali pc, server e dispositivi mobili;
- esperto di sicurezza dei sistemi in rete;
- esperto di *penetration testing* e *vulnerability assessment*;
- analista di *Security Operations Center* (SOC);
- analista di sistemi compromessi;
- consulente tecnico di ufficio (CTU) e di parte (CTP).

PROGRAMMA

- sistemi operativi;
- internet;
- tecnologie software per il *web*;
- crittografia e controlli crittografici;
- *network security*;
- *computer security*;
- *web security*;
- *cyber security* dei sistemi di controllo industriale;
- sistemi di *logging*, monitoraggio e analisi degli eventi;
- *vulnerability assessment* e *penetration testing*;
- reati informatici e aspetti giuridici della *digital forensics* e della *privacy*;
- *privacy by design & by default*;
- procedure della *cyber defence* e della *digital forensics* e conformità ai principali standard e procedure;
- quadro normativo nazionale;
- *computer forensics* per sistemi Windows, Unix/Linux, Mac OS;
- *mobile forensics*;
- *cyber exercise*.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno ed ha una durata di 11 settimane (300 ore).

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

ALTRE AREE FORMATIVE

13.MASTER DI II LIVELLO IN DIFESA ELETTRONICA - COD. MZ01P

OBIETTIVI DEL CORSO

Il Master ha l'obiettivo di fornire una preparazione nel campo della difesa elettronica, con una prospettiva rivolta in particolare agli aspetti analitici e di sistema, allo scopo di:

- consentire la comprensione e la stesura dei requisiti operativi di un sistema di difesa elettronica, nonché la valutazione della congruenza di essi rispetto alla finalità del sistema;
- consentire la valutazione, sia teorica che sperimentale, dell'efficacia di un sistema di difesa elettronica rispetto alle sue finalità.

A tal fine verranno impartite le conoscenze per la comprensione:

- della teoria e delle tecniche su cui si basano i componenti specifici di un sistema di difesa elettronica;
- delle caratteristiche salienti delle piattaforme su cui i sistemi di difesa elettronica sono integrati (piattaforme terrestri, navali, avioniche e spaziali);
- delle moderne tecnologie dell'ingegneria dei sistemi complessi con particolare riferimento alle necessità della difesa elettronica;
- degli aspetti progettuali dei sistemi di difesa elettronica e della valutazione sperimentale delle loro prestazioni.

AREA

Altre Aree Formative

RUOLI E POSIZIONI RICOPRIBILI

Il Master è indirizzato a formare personale in grado di operare su tutto il ciclo di vita di un sistema di Difesa Elettronica (D.E.) sia dal punto di vista della preparazione dei requisiti, che da quello della specificazione, valutazione ed utilizzo di tali sistemi.

I discenti conseguiranno una solida base per assumere le seguenti responsabilità nel campo della Difesa Elettronica:

- definizione e valutazione dei requisiti di D.E.;
- definizione e valutazione del progetto di un sistema di D.E. nell'ambito dei sistemi complessi.

Riceveranno altresì le basi per comprendere le problematiche connesse a:

- gestione di progetto/programma nell'ambito dei progetti/programmi complessi;
- definizione e valutazione di procedure ottimali di impiego di apparati e sistemi complessi.

PROGRAMMA

Il programma è articolato nei seguenti moduli didattici:

- teoria dei segnali;
- elaborazione digitale dei segnali;
- propagazione e antenne;
- teoria e tecniche dei sistemi radar;
- teoria e tecniche dei sistemi di comunicazione a radiofrequenza;
- teoria e tecniche dei sistemi elettro-ottici;
- sistemi d'arma;
- tecniche dei sensori passivi;
- tecniche delle contromisure;
- sistemi di sensori passivi;
- sistemi di contromisure;
- sistemi integrati di difesa elettronica;

- utilizzo in sicurezza dell'energia elettromagnetica;
- tecniche di controllo di programma e progetto.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione;
- *stage*.

14.MASTER DI II LIVELLO IN FOTONICA ED OPTOELETTRONICA - COD. MZ02P

OBIETTIVI DEL CORSO

Fornire un'approfondita preparazione sui fenomeni fisici e le tecnologie associate alla generazione, modulazione, trasmissione e rivelazione dei fotoni nell'ambito dei sistemi di comunicazione, di misura e di elaborazione dei segnali; ed altresì di formare figure professionali per il progetto, la realizzazione, la gestione e la valutazione di sistemi basati sulla luce ed i processi ad essa connessi, dall'ottica all'optoelettronica, alla sensoristica, all'ottica non lineare.

AREA

Altre Aree Formative

RUOLI E POSIZIONI RICOPRIBILI

Il Master si pone l'obiettivo di preparare professionisti in grado di assumere ruoli di:

- Capo progetto, supervisore, di progetti di sistemi fotonici e optoelettronici;
- Esperto di progettazione e sviluppo di sistemi optoelettronici;
- Esperto di progettazione e sviluppo di sistemi ottici;
- Esperto per la pianificazione e la valutazione di sistemi ottici e optoelettronici.

Le figure professionali sopra individuate si formeranno attraverso un'approfondita preparazione tecnico-scientifica ed applicativa per il progetto, la realizzazione e la gestione di dispositivi e sistemi fotonici, con approfondimenti riguardanti sia materiali nanostrutturati, che le tecnologie dei dispositivi e dei sistemi, la generazione, la trasmissione, l'elaborazione e la rivelazione di segnali ottici per comunicazioni ottiche, sensoristica e misure. Tali figure saranno dedicate all'assunzione di responsabilità nei processi tecnici connessi all'intero ciclo di tali sistemi.

PROGRAMMA

Il corso sarà suddiviso in due fasi nel corso delle quali sono effettuate lezioni sui seguenti argomenti:

- tecniche matematiche;
- ottica generale;
- caratterizzazione dei materiali e fisica delle nano strutture;
- elaborazione di immagini digitali;
- comunicazioni ottiche, materiali e dispositivi per l'optoelettronica;
- fisica e applicazione dei laser;
- ottica integrata e fibre ottiche;
- sensori elettro-ottici, progettazione di strumenti ottici;
- sistemi elettro-ottici, propagazione e sondaggio atmosferico;
- sicurezza dei laser per TLC;
- stage e tesi finale.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione;
- *stage*.

15. MASTER DI II LIVELLO IN INGEGNERIA DEI SISTEMI ELETTRONICI COMPLESSI - COD. MZ03P

OBIETTIVI DEL CORSO

Il Master presenterà strumenti e metodi di base per la progettazione, realizzazione e gestione dei sistemi elettronici avanzati; preparerà professionalità per la gestione ed il monitoraggio dell'impatto dei sistemi elettronici complessi nella realtà industriale; fornirà strumenti per l'analisi e la valutazione sulle principali modifiche nei sistemi elettronici di nuova generazione, indotte dall'applicazione delle varie tecnologie innovative.

AREA

Altre Aree Formative

RUOLI E POSIZIONI RICOPRIBILI

Il Master è indirizzato a formare figure professionali in grado di progettare, gestire, integrare e valutare i sistemi elettronici complessi. In particolare, il Master si propone di formare figure professionali in grado di assumere posizioni di:

- Capo progetto, supervisore di progetti di sistemi elettronici complessi;
- Esperto di progettazione e sviluppo di sistemi elettronici complessi;
- Esperto per l'integrazione dei sistemi elettronici complessi;
- Esperto per la pianificazione e valutazione di sistemi elettronici complessi.

PROGRAMMA

Sono effettuate lezioni sui seguenti argomenti:

- apparati radar e tecnica degli impianti radar;
- artiglieria e munizionamento;
- carichi paganti;
- componenti per gli apparati radar;
- controlli automatici;
- elaboratori elettronici;
- optoelettronica – principi ed apparati;
- simulazione;
- tecniche di difesa elettronica;
- teoria dei sistemi missilistici e impianti missilistici;
- teoria del telerilevamento;
- utilizzo in sicurezza dell'energia elettromagnetica.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione;
- *stage*.

16.MASTER DI II LIVELLO IN SYSTEM ENGINEERING E PROJECT MANAGEMENT - COD. MZ05P

OBIETTIVI DEL CORSO

Fornire una preparazione nel campo della ingegneria dei sistemi e della ingegneria del supporto logistico con una prospettiva rivolta in particolare al committente piuttosto che al costruttore allo scopo di trasferire:

- conoscenze e competenze tecniche esaustive per quanto concerne la gestione tecnico/operativa/logistica di sistemi d'arma e del relativo supporto logistico;
- conoscenze e competenze tecniche realizzative propedeutiche per quanto concerne la gestione economica e finanziaria necessaria per la figura professionale del responsabile del programma di acquisizione di un sistema d'arma (Program Manager o Project Manager).

AREA

Altre Aree Formative

RUOLI E POSIZIONI RICOPRIBILI

Il master è destinato a personale tecnico della A.D. destinato a svolgere incarichi di coordinamento e gestione dei Sistemi d'Arma e delle associate infrastrutture logistiche relativamente ad aspetti specifici della acquisizione e della utilizzazione quali:

- acquisizione del sistema primario, in particolare per le attività di:
 - . definizione dei requisiti contrattuali;
 - . valutazione delle offerte;
 - . controllo del progetto e collaudo delle prestazioni contrattuali.
- acquisizione del sistema di supporto logistico e dei relativi elementi: (pubblicazioni, parti di ricambio, dati tecnici, apparecchiature di prova, addestramento e ausili didattici), in particolare per le attività di:
 - . definizione dei requisiti contrattuali;
 - . valutazione delle offerte;
 - . controllo del progetto e collaudo delle prestazioni contrattuali.
- conduzione tecnica e manutentiva di sistemi d'arma e delle associate infrastrutture logistiche acquisiti dalla AD e gestiti dalla Forza Armata;
- gestione del supporto logistico e dei relativi elementi (manutenzione correttiva e preventiva, parti di ricambio, manuali e pubblicazioni tecniche, corsi di istruzione, laboratori di manutenzione, sistemi informativi logistici, ecc.) acquisiti dalla AD e gestiti dalla forza armata.

PROGRAMMA

Gli argomenti da trattare sono i seguenti:

- assicurazione del prodotto;
- contrattualistica;
- procurement;
- economia e organizzazione della produzione;
- identificazione e codificazione materiali di approvvigionamento;
- introduzione ai sistemi e al *System Engineering*;
- metodi di allocazione delle risorse e ricerca operativa;
- metodi di supporto alle decisioni;
- metodi per la schedulazione e minimizzazione dei costi;
- modellizzazione e simulazione;

- probabilità e statistica;
- progetto del supporto logistico integrato;
- *project management*;
- *system engineering*;
- sistemi informativi;
- gestione dell'innovazione;
- *supply chain management*.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione;
- *stage*.

17.MASTER DI II LIVELLO IN MUNIZIONAMENTO AVANZATO ("GUN LAUNCHED GUIDED MUNITIONS") - COD. MZ12P

OBIETTIVI DEL CORSO

Il Master ha l'obiettivo di fornire una preparazione nel campo del munizionamento di artiglieria guidato che rappresenta il limite della tecnologia attuale e della ricerca. Saranno trattati gli aspetti analitici e di sistema che consentano di:

- comprendere gli aspetti salienti, i punti di forza, le criticità tecniche, operative e logistiche delle munizioni considerate;
- valutare le prestazioni delle munizioni e, più in generale, dei sistemi d'arma che le impiegano;
- assumere decisioni in merito ai programmi di ricerca, sviluppo, acquisizione, impiego e supporto sul munizionamento considerato.

AREA

Altre Aree Formative

RUOLI E POSIZIONI RICOPRIBILI

Il Master si propone di formare una professionalità completa nel settore del munizionamento ad alta tecnologia, fornendo ampie ed aggiornate conoscenze, inclusi gli aspetti manageriali e quelli relativi alla sicurezza.

PROGRAMMA

Il programma didattico comprenderà:

- chimica generale e organica;
- richiami di termodinamica;
- sistemi di radiocomunicazione e radar;
- fondamenti di probabilità e statistica;
- sistemi ottici e optoelettronici;
- esplosivistica;
- controlli automatici;
- artiglieria;
- munizionamento avanzato;
- sistemi missilistici, guida e controllo;
- simulazione nei sistemi d'arma;
- compatibilità elettromagnetica applicata al munizionamento;
- sicurezza del munizionamento.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione;
- *stage*.

18.MASTER DI II LIVELLO IN SISTEMI COMPLESSI AVANZATI - COD. MZ13P

OBIETTIVI DEL CORSO

Il Master ha l'obiettivo di fornire una preparazione nel campo dei sistemi elettronici complessi, ivi inclusi i sensori radar, i sensori optronici, sistemi missilistici e sistemi di artiglieria e relativo munizionamento, presentando la teoria e la tecnica loro sottesa, gli strumenti necessari alla loro progettazione, sviluppo e gestione nonché gli elementi per la compiuta valutazione, teorica e sperimentale, della loro efficacia.

AREA

Altre Aree Formative

RUOLI E POSIZIONI RICOPRIBILI

Il Master si propone di formare una professionalità completa nel settore dei sistemi elettronici complessi fornendo ampie ed aggiornate conoscenze in favore degli Ufficiali addetti ai sistemi di combattimento.

PROGRAMMA

Il programma didattico comprenderà:

- teorie e tecniche dei sistemi radar e radiocomunicazione;
- controlli automatici;
- sistemi ottici e optoelettronici;
- modellizzazione e simulazione nei sistemi d'arma;
- tecniche di difesa elettronica;
- teoria dei sistemi missilistici;
- la minaccia e la protezione elettromagnetica nel munizionamento;
- chimica generale ed organica;
- richiami di termodinamica;
- esplosivistica;
- artiglieria;
- munizionamento avanzato;
- sicurezza del munizionamento.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- periodicità e durata del master;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione;
- *stage*.

CAPITOLO 2 - LIVELLO AVANZATO

AREA TRANSPORT & NETWORKING

19.CORSO AVANZATO SULLA QUALITÀ DEL SERVIZIO (QoS) SU RETI ETEROGENEE - COD. FR06A

OBIETTIVI DEL CORSO

Fornire le conoscenze tecniche specifiche per formare figure professionali in grado gestire reti a qualità garantita, in ambito Locale e Geografico (LAN-MAN-WAN).

Gestire la qualità del servizio (QoS), elemento fondamentale nelle reti evolute di telecomunicazioni, le cui applicazioni richiedono alla rete specifici livelli di prestazione, in termini di latenza, banda, *jitter*, *packet loss* ed *error ratio*.

Fornire ai frequentatori una visione approfondita dell'argomento, illustrando le soluzioni adottate, per rendere le reti adeguate a supportare i servizi evoluti.

AREA

Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI

Richiami generali:

- concetti generali sulle reti di telecomunicazioni;
- modello di riferimento ISO/OSI, TCP/IP, protocolli;
- architettura a livelli funzionali;
- definizione delle primitive;
- dettaglio header protocolli internet (suite TCP/IP);
- dettaglio ATM, MPLS;
- reti QoS *based*;
- definizione di qualità del servizio;
- metriche di qualità del servizio;
- applicazioni;
- concetto di flusso e classe di traffico;
- misure sperimentali;
- reti eterogenee;
- concetto di sistema autonomo;
- tecnologie QoS *oriented*;
- ATM;
- MPLS;
- QoS IPv4;
- *integrated services*;
- *differentiated services*;
- QoS IPv6;
- *network control*;
- QoS *management functions*;
- *over provisioning*;
- *flow identification*;
- *resource reservation*;
- CAC;
- *traffic control*;
- *scheduling*;
- *flow Control*;

- *Qos Routing*;
- controllo di flusso del TCP;
- rischio causato dalla mancanza dei diversi algoritmi di controllo.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 1 settimana.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

20.CORSO AVANZATO DI SISTEMISTA DI 2° LIVELLO IN RETI TELEMATICHE - COD. FR66A

OBIETTIVI DEL CORSO

Formare figure professionali con capacità di:

- comprensione e stesura delle specifiche tecniche;
- progettazione e gestione efficienti di reti;
- gestione di sistemi telematici, e di reti di piccole (Reti in Area Locale - LAN) e medie dimensioni (Reti in area Metropolitana/Geografica –MAN / WAN).

AREA

Transport & Networking.

PROGRAMMA

Richiami generali:

- modello di riferimento ISO/OSI;
- commutazione di pacchetto e circuito. Motivazioni di un modello funzionale. Principali tecnologie e mezzi trasmissivi. Funzionalità del *data-link*: principali standard e prodotti. Livello 3: funzioni di commutazione e instradamento;
- architettura DoD;
- confronto con modello ISO/OSI. Il livello IP: tecniche di numerazione, uso della *netmask*, concetto di rete. *Routing* a maschera variabile (VLSN). Protocolli ICMP e TCP;
- apparati di rete;
- varie tipologie di cablaggio. HUB: funzionalità e impieghi. Bridge e *switch*: funzionalità e impiego. *Wireless Access point*. Router commerciali e *open*, basati su sistema operativo Linux.

Gestione avanzata degli apparati per LAN:

- *link aggregation*: motivazione e limiti di impegno. Standard (IEEE 802.3ad) e modalità operative;
- realizzazione di infrastrutture di rete Fault-Tolerant: motivazioni, vantaggi e svantaggi, principali algoritmi (*Spanning Tree*) e standard (IEEE 802.1D);
- Virtual LAN (VLAN): definizione, motivazioni e limiti di impiego. *Trunking* di VLAN. Principali standard: IEEE 802.1q e VTP;
- amministrazione delle LAN e VLAN: monitoraggio degli apparati e controllo degli accessi. Protocolli e strumenti per l'autenticazione (IEEE 802.1x, RADIUS). Cenni sul NAC di Cisco.

Gestione avanzata delle reti IP:

- *switch* di livello 3;
- architettura e funzionalità. Inter-VLAN *routing*;
- tecnologie emergenti per l'interfacciamento con le reti geografiche;
- Tecnologia ATM: elementi base. Sistemi xDSL: definizione e caratteristiche tecniche di base. Protocolli di livello 2 per WLAN: PPPoATM, PPPoE;
- *routing* IP;
- routing statico e dinamico. Algoritmi di *routing*: *distance vector* e *link state packet*. Concetto di *Autonomous System* (AS). Protocolli dinamici per il *routing* interno; all'AS: RIP, EIGRP e OSPF. Esempi di configurazione;
- protocolli dinamici per il *routing* fra AS: EGP e BGP (cenni).

Sicurezza nelle reti dati:

- protocolli per la realizzazione di canali “sicuri”;
- concetto di *tunneling* e principali protocolli: IPIP, GRE. Nozioni di base sulla cifratura. *tunneling* IPSEC. Virtual Private Network (VPN): definizione e caratteristiche distintive. Applicativi per VPN (*Open VPN*);
- interconnessione ad Internet di reti IP non connesse;
- richiami al CIDR (*Classless InterDomain Routing*). Motivazioni per l’uso di classi IP non connesse/non annunciate. Protocolli di NAT e PAT: esempi di configurazione su apparati Cisco e su open router basati su Linux;
- *firewall*;
- architettura e di una “rete sicura”: concetto di DMZ. Caratteristiche dei firewall, problematiche derivanti dal loro impiego. Principali prodotti commerciali (Cisco PIX) e di dominio pubblico. Esempi di configurazione;
- interfacciamento con ambienti basati su tecnologie *Microsoft*;
- utilizzo di sistemi Linux in un contesto di dominio basato su *Active Directory Microsoft*. Winbind e PAM: esempi di configurazione;
- utilizzo di server Linux come *Primary Domain Controller* (PDC) mediante l’impiego di Samba e di server LDAP.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 4 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d’iscrizione.

21. CORSO AVANZATO DI TECNICHE VOICE OVER IP - COD. A126A

OBIETTIVI DEL CORSO

Approfondire l'aspetto delle comunicazioni voce con il protocollo IP e la tecnologia esistente nel campo.

Fornire ai frequentatori le nozioni necessarie per operare e saper configurare gli apparati di Voice Over IP in ambito Amministrazione Difesa.

AREA

Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI

Gli argomenti trattati sono i seguenti:

- cenni sul protocollo IP- Reti LAN;
- il mondo Voice over IP;
- tecniche di codifica del segnale audio;
- i protocolli di segnalazione e gestione della Rete VoIP;
- analisi server VoIP e Qualità del servizio su rete IP.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: N.N.;
- b. Conoscenze basiche richieste: sufficiente conoscenza di reti e protocollo TCP/IP;
- c. Studio preventivo sinossi / testi propedeutici: N.N..

2. Di segretezza:

NOS non richiesto.

3. Categorie:

Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:

2 settimane di cui 30% laboratorio.

È PREVISTO UN ESAME FINALE.

22.CORSO AVANZATO DI 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, tecnologia 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 moltiplicazione 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 moltiplicazione 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 IV.

È PREVISTO UN ESAME FINALE.

23.CORSO AVANZATO PER TECNICI TELEMATICI ARMA CC (2° CICLO) - COD. A311A

OBIETTIVI DEL CORSO

Il corso in esame costituisce la prima fase dell'iter formativo dei militari dell'Arma dei Carabinieri, prescelti per il conseguimento della specializzazione di "Tecnico Telematico", propedeutica alla seconda, che sarà effettuata direttamente dal Comando Generale dell'Arma. L'attività addestrativa nella 1^a fase si sviluppa su due cicli della durata complessiva di 22 settimane. Il secondo ciclo è finalizzato al raggiungimento di una conoscenza avanzata in ambito Telematico. In questo periodo vengono sviluppate attività di studio in Reti di Telecomunicazione, Sicurezza delle Reti, Sistemi Trasmissivi e Sistemi Operativi per server di rete.

AREA

Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI

Gli argomenti trattati sono i seguenti:

- antenne e propagazione radio;
- modulo di telefonia analogica e digitale;
- modulo di telefonia VoIP;
- modulo *hardware*;
- modulo sicurezza informatica;
- modulo avanzato progetto e gestione reti locali *ethernet*;
- modulo fondamenti cablaggio strutturato;
- modulo IP *routing*;
- modulo *hardening*;
- modulo Unix/Linux;
- modulo S.O. Windows Server.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: avere partecipato con profitto al 1° ciclo del corso;
- 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:

15 settimane di cui 50% laboratorio.

SONO PREVISTE DELLE PROVE INTERMEDIE SCRITTE, ORALI E PRATICHE, SU OGNI SINGOLA MATERIA, CON ATTRIBUZIONE DI PUNTEGGI IN TRENTESIMI.

È PREVISTO UN ESAME FINALE.

24.CORSO AVANZATO INSTALLATORE E MANUTENTORE MULTIPLEX FLESSIBILE MT301F - COD. A115A

OBIETTIVI DEL CORSO

Fornire ai frequentatori le informazioni tecniche per l'installazione e la configurazione dell'apparato. Inserire e gestire le tipologie di utenza voce, dati, VoIP e predisporre i canali per l'esercizio di una videoconferenza in una centrale collegata in rete. Eseguire varie esercitazioni necessarie alla comprensione dell'algoritmo utilizzato per la selezione della sorgente di temporizzazione principale, sia in caso sincrono che asincrono per asservire le centrali di una rete. Preparare i connettori per i collegamenti inter-centrale, dati e fonia fino all'utenza. Compilazione completa di file di configurazione della centrale per tutti gli ambienti operativi principali. Valutare il significato dei messaggi e dei tracciamenti informativi forniti dal database della centrale a qualsiasi livello, per addestrare il personale installatore all'individuazione delle problematiche, dei difetti di natura hardware e/o software che ne degradano o ne bloccano il funzionamento.

AREA

Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI

Gli argomenti trattati sono i seguenti:

- presentazione della Rete Operativa Integrata della Difesa;
- introduzione trame EUROCOM, multiplazione TDM, rete IP;
- pannello frontale MT 301/F;
- lettura informazione ed interpretazione degli allarmi;
- *login logout* uso della password e ID di default come gestore ES;
- comandi di installazione centrale e di azzerata centrale;
- comandi di configurazione apparato MT301/F;
- casi di espansione *multibox* (2-3-4 apparati);
- sorgenti di clock e loro origine - pratica sul funzionamento e sulla scelta degli orologi;
- cenni sulle unità ISDN - Piano di numerazione tipo EUROCOM (Presidiarie);
- cenni sulla tecnologia di trasporto IP integrando utenze VOIP (sia H323 sia SIP);
- inserimento utenti digitali secondo le norme EUROCOM (utilizzo solo a quattro fili);
- inserimento degli utenti dati in standard V10, V11, V35;
- inserimento utenti VOIP;
- realizzazione dei circuiti PAP di utente e di canale analogici e digitali;
- realizzazione collegamenti *gateway*, intercentrale con MIUSIP "*Multi Interface Unit Service IP*";
- realizzazione dei connettori di tutte le interfacce verso l'esterno della centrale;
- compilazione di un file di configurazione completo con tutti i comandi di: configura apparato, configura centrale, configura moduli, configura unità, inserimento utenti nelle varie modalità e servizi, differenziando la ricerca in rete a diffusione totale o limitata;
- installazione della centrale con un file di configurazione già creato;
- integrazione delle reti a commutazione di circuito, VoIP e delle reti di trasporto IP presenti sulla centrale.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

a. Frequenza preventiva: N.N.;

b. Conoscenze basiche richieste:

È richiesta una buona conoscenza teorico pratica sulla rete dati e fonia; informatica di base, telefonia TDM, a bassa frequenza, nonché collegamenti in ponte radio TDM. Inoltre, una buona preparazione pratica sugli apparati multiplex TDM, centrali telefoniche ed apparecchi di utenza di vario tipo, faciliterà meglio l'apprendimento delle lezioni;

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 di cui 10% laboratorio.

È PREVISTO UN ESAME FINALE.

25.CORSO AVANZATO DI OPERATORE MULTIPLEX FLESSIBILE MT301F - COD. A116A

OBIETTIVI DEL CORSO

Fornire ai frequentatori le capacità di impiegare l'apparato come operatore, saper leggere un piano di numerazione di utenza, approfondire le conoscenze sulle diverse tipologie di utenza locale, compresi gli utenti VOIP associati al modulo MIUSIP, approfondire le conoscenze di collegamenti inter-centrali con interfaccia elettrico ottica e IP, sui modi di traffico, le classi di servizio, i barramenti dal livello centrale fino all'utente.

Fornire le necessarie competenze per permettere di interpretare gli allarmi sul *display* a frontale, impiego dei comandi software di visualizzazione necessari a comprendere lo stato di funzionamento dell'utente e della centrale, interpretazione necessaria delle informazioni di sintesi e di allarme fornite dall'apparato considerate utili all'operatore per gestire l'apparato in ambito locale.

AREA

Transport & Networking.

PROGRAMMA / ARGOMENTI TRATTATI

Gli argomenti da trattare sono i seguenti:

- presentazione della Rete ROID: funzione, architettura;
- utenze collegate al sistema;
- introduzione trame EUROCOM, moltiplicazione TDM, reti IP, modulatore delta, cenni sulla segnalazione, cenni sulle centrali TDM e cenni sulle centrali VOIP;
- spiegazione pannello frontale MT 301/F, impiego pratico dei deviatori Erase e Reset, assemblaggio delle parti costituenti l'apparato;
- lettura informazione ed interpretazione degli allarmi forniti dal *display* a frontale simulando alcune situazioni di linea *trunk* aperta e poi chiusa;
- display a Frontale, controllo e comando dell'apparato tramite il pannello SCU a frontale;
- *login-logout* uso della password e ID di *default* come gestore ES - Help dell'apparato, impostazione corretta del comando, tipi di comandi;
- comandi di visualizzazione apparato, centrale, modulo, unità, canale, utente - comandi di inserimento utente;
- compilazione di un file di configurazione completo con tutti i comandi di: configura apparato, configura centrale, configura moduli, configura unità, inserimento utenti e modalità per l'installazione della centrale con un file di configurazione già creato;
- pratica relativa ai comandi di visualizza entità ai vari livelli funzionali della centrale (moduli, unità, canali, utenti);
- utilizzo delle prestazioni di utente: trasferimento di chiamata, *follow me*, uso della priorità, diffusione tra utenti, utente *step-up*;
- servizi di base di una centrale: linea calda, FC, operatore di gruppo;
- pratica: configurazione e utilizzazione della centrale in una rete di tipo ROID e/o similari;
- differenze tra la diffusione limitata e totale attinente alla ricerca dell'utente, particolarmente riferita al processo telefonico (segnalazione di utente tipo analogica e digitale CPC e segnalazione di rete riferita ad una trama EUROCOM);
- integrazione delle reti a commutazione di circuito, VoIP e delle reti di trasporto IP presenti sulla centrale.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

a. Frequenza preventiva: N.N.;

b. Conoscenze basiche richieste:

È richiesta una sufficiente conoscenza teorico pratica sulla rete dati e fonia; informatica di base; telefonia TDM e a bassa frequenza e collegamenti in ponte radio TDM. Inoltre, una buona preparazione pratica sugli apparati multiplex TDM, centrali telefoniche ed apparecchi di utenza di vario tipo, faciliterà meglio l'apprendimento delle lezioni;

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 di cui 10% laboratorio.

È PREVISTO UN ESAME FINALE.

26. CORSO SUL *BORDER GATEWAY PROTOCOL* (BGP) - COD. A117A

OBIETTIVI DEL CORSO

Corso teorico-pratico sul protocollo di *routing* della rete internet BGPv4, che permette di acquisire la conoscenza delle caratteristiche del protocollo, del meccanismo di *path selection*, dei meccanismi di filtraggio e di *traffic engineering*, della ricerca di informazioni su reti e prefissi pubblici internet.

AREA

Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

Introduzione:

- *the three napkins protocol*;
- principali differenze rispetto ai più comuni IGP;
- perché è utilizzato in internet?;
- la struttura di internet e la FIRT.

Concetti fondamentali:

- *autonomous system*;
- natura degli indirizzi internet e prefissi;
- reti *single* e *multi-homed*;
- tipologie di connettività.

Attributi e sessioni BGP:

- *neighbor*;
- annunci;
- gli attributi *well known (mandatory & discretionary)*, *optional (transitive, non transitive)*;
- aspetti correlati alle community;
- il processo di *path selection*;
- iBGP ed eBGP – propagazione delle rotte e *split-horizon*.

Annunci, filtraggio e aggregazione di prefissi:

- *prefix-list*;
- *route-map*;
- BCP38;
- realizzazione al simulatore di una rete con *routing* BGP;
- utilizzo dei principali database (RIPE-DB, RADB) per la ricerca di informazioni su prefissi IPv4 e IPv6;
- *looking Glasses*;
- la difesa agli attacchi DDOS di un ISP, RPKI e Flow SPEC.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: N.N.;
- b. Conoscenze basiche richieste:
Buona conoscenza dello *stack* TCP/IP, del *subnetting*, funzionamento dei protocolli di *routing*, del sistema operativo CISCO IOS. Auspicabile pratica pregressa con simulatori di reti (es. GNS3, Packet Tracer, EVE-ng, etc.);
- 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: 1 settimana di cui 25% di laboratorio.

È PREVISTO UN ESAME FINALE.

27. CORSO SU INTERNET PROTOCOL VERSIONE 6 -IPv6 - COD. A118A

OBIETTIVI DEL CORSO

Corso teorico-pratico su Internet Protocol versione 6, che permette di acquisire la conoscenza del formato degli indirizzi e delle tecniche di abbreviazione, di come realizzare un piano di indirizzamento, delle principali differenze con IPv4, dei meccanismi di coesistenza dei due protocolli (IPv4 e IPv6). È prevista la realizzazione al simulatore di una rete *dual stack* IPv4/IPv6.

AREA

Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

Introduzione:

- limitazioni di IPv4 e motivazioni per il passaggio ad IPv6;
- principali caratteristiche di IPv6;
- *tips & tricks* sulla notazione esadecimale degli indirizzi.

IPv6:

- *header, next-headers*;
- natura degli indirizzi *link local, unique local, global, multicast e anycast*;
- principali classi *multi cast*;
- prefissi IPv6 e loro allocazione.

ICMPv6:

- *neighbor & router discovery*.

Diagnostica e Address management:

- *auto configuration*;
- modalità *stateless*;
- modalità *stateful* (DHCPv6);
- *stateless* DHCPv6 (DHCPv6-lite).

Transition Mechanism:

- *dual stack*;
- *tunnel broker*;
- meccanismi 6to4 e 6rd;
- modello 6PE;
- *dual stack-lite* (DS-lite);
- NAT64;
- redazione di un piano di indirizzamento e *best practices* di dimensionamento;
- realizzazione al simulatore di una rete IPv6.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva:
N.N.;
- b. Conoscenze basiche richieste:
Buona conoscenza dello *stack* TCP/IP, del partizionamento delle reti in IPv4, della notazione CIDR, della notazione esadecimale, dei meccanismi di ARP in IPv4.
Auspicabile pratica pregressa con simulatori di reti (es. GNS3, Packet Tracer, EVE-ng, etc.);
- 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: 1 settimana di cui 25% laboratorio.

È PREVISTO UN ESAME FINALE.

28. CORSO AVANZATO IP ROUTING - COD. RE229A

OBIETTIVI DEL CORSO

Corso teorico-pratico improntato sul progetto, realizzazione e gestione di Reti IP LAN-MAN-WAN. Verranno trattati i concetti di *Routing IP* statico/dinamico in particolar modo il Protocollo OSPF. Attraverso esperienze pratiche di laboratorio, si acquisiranno le capacità di installare, configurare e gestire ROUTER IP. Si analizzeranno tecniche di instradamento/bilanciamento del carico del traffico IP tramite criteri di Politiche di Routing (PBR). Si implementeranno algoritmi di alta disponibilità IP con HSRP/VRRP. Si apprenderanno tecniche di cattura e filtraggio dei pacchetti tramite ACL integrando metodi di mascheramento delle reti e pubblicazione di servizi con NAT/PAT. Si configureranno protocolli di *tunneling* (GRE, mGRE) e Bridging geografico. Si illustreranno tecniche di IP QoS e metodologie di ricerca guasti in IP *Internetworking*. Sarà inoltre usato il simulatore reti opensource GNS3.

AREA

Transport & Networking

PROGRAMMA/ARGOMENTI TRATTATI

- Richiami su: LAN, MAN, WAN, *switching* L2, TCP/IP, indirizzi IP/*subnetting*;
- Progettazione del piano di indirizzamento IP della WAN di laboratorio;
- Router IP: architettura e funzionalità;
- Router CISCO: Sistema operativo IOS, File System, accesso via console seriale, Telnet e http/https, configurazione iniziale, fase di *boot* e procedura di *password recovery*;
- Applicativi PUTTY *terminal*, TELNET, TFTP, FTP, SFTP, SCP;
- Salvare/aggiornare via TFTP/FTP/SCP la configurazione e IOS;
- Interfacce: configurazione e collegamento in rete;
- Protocollo PPP: Collegamenti *Multilink* e aggregazione di Banda;
- Algoritmi di *hashing*: MD5, SHA; Autenticazione PAP / CHAP;
- Accesso via SSH al *router*. *Sniffer* di rete WireShark, cattura del traffico IP;
- Logica di *routing* IP. Tabelle di *routing* su *hosts* e *router*;
- *Routing* IP statico sui *router* fisici di laboratorio. Sincronizzazione su NTP *server*;
- Controllo accessi: privilegi utente e autorizzazioni: RADIUS e TACACS+;
- SYSLOG *server*: Registrazione accessi amministrativi e delle modifiche di sistema
- DHCP *server* e *relay agent* sul *router* Cisco;
- *High Availability* su reti IP: *Hot Stand-by Router Protocol* (HSRP); VRRP;
- Misure e *test* sulle reti IP: Cisco IP SLA *monitoring with object tracking*;
- Instradamento IP: protocolli di *routing* IGP ed EGP;
- Sistemi autonomi; *Routing* gerarchico; Architettura di INTERNET;
- *Routing* di tipo adattativo distribuito: Distance-Vector / Link-State;
- Protocollo di *routing* OSPF: Configurazione e implementazione di laboratorio;
- Risoluzione problemi di instradamento IP sulla rete di laboratorio;
- OSPF: Autenticazione, *Virtual links*, *Fast hello*, BFD (*bidirectional forward, Detect*)
- *Route Filtering*, *route-distribution* e *Route map*;
- Instradamento / bilanciamento del carico dei flussi IP con implementazioni dei criteri in base a Politiche di *Routing* (PBR), *Route-Map*;
- Configurazione BRIDGE/ROUTER geografici;
- VLAN layer 2 e *inter Vlan Routing*, *Trunking* Vlan dot1Q;

- Inter Vlan *Routing*, *Subinterfaces* sui *router*;
- Configurazione di *Switch* layer 3 e VLAN layer 3;
- Sicurezza su reti IP: Filtraggio del traffico IP, Access Control List (ACL);
- Mascheramento di indirizzi IP privati: NAT e PAT;
- Gestione del traffico *multicast*: protocolli di *tunneling* GRE ed mGRE;
- *Sniffing* del traffico IP su *switch* e *router* ai fini della sicurezza ICT;
- Messa in sicurezza dei *router*: *hardening* del *router* e dei protocolli di rete;
- Qualità del servizio (QoS) nelle reti IP: misure, *testing*;
- Simulazione grafico Reti Lan/Wan GNS3 su VMWARE.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva consigliata: corso progetto e gestione di reti locali cod. R235I.
In alternativa essere in possesso delle conoscenze basiche richieste al punto b.
- b. Requisiti minimi richiesti: buona conoscenza dei protocolli TCP/IP, indirizzamento/*subnetting* IP; Reti LAN *switching Ethernet*; cablaggi rame/fibra.
- c. Studio preventivo sinossi / testi propedeutici: Manuale TCP/IP.

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 e-learning asincrono, di cui 1 giorno via Webex, e 3 settimane in presenza. Per esigenze logistiche/sanitarie, la fase in presenza potrà essere svolta a distanza in modalità “*on-line training*”.

Lo svolgimento delle attività a distanza è disciplinato dall’Annesso IV.

Percentuale laboratorio: 65%

È PREVISTO UN TEST D’INGRESSO ED UN ESAME FINALE

29. CORSO AVANZATO FIREWALL & VPN - COD. R282A

OBIETTIVI DEL CORSO

Concetti sulla Sicurezza ICT e responsabilità tecnico/legali riguardo la registrazione degli accessi ed il monitoraggio degli eventi di sicurezza. Fornire le competenze tecniche sui sistemi di sicurezza perimetrale IP basate sulle tecnologie dei Firewall di tipo Stateful-Inspection e Alta disponibilità. Trattare le Reti DMZ e pubblicazione dei servizi WEB verso reti esterne o Internet. Fornire conoscenze sui protocolli di crittografia simmetrica, asimmetrica e di *hashing*. Affrontare le tecnologie di creazione di VPN basate sul protocollo IPSEC e accesso remoto *web* VPN-ClientSSL/TLS/DTLS. Introdurre il concetto di *Certification Authority* per l'emissione di certificati digitali utente ai fini dell'accesso *client* VPN tramite PC e Dispositivi Mobile. Implementare laboratori pratici di simulazioni *operative real* incentrate su sessioni individuali e di gruppo.

AREA

Transport & Networking

PROGRAMMA/ARGOMENTI TRATTATI

- Introduzione alla sicurezza ICT; panoramica sui rischi informatici; responsabilità tecnico/legali riguardo la registrazione accessi e monitoraggio degli eventi di sicurezza;
- riguardo la registrazione accessi e monitoraggio degli eventi di sicurezza;
- politiche di sicurezza delle reti: standard linee guida e obblighi legali;
- architetture dei moderni Firewall; Tecnologia *packet filtering* e *Stateful-Inspection*;
- *Best Practices* e *Hardening* dei Firewall; Cenni sui sistemi IDS / IPS;
- filtraggio dei pacchetti con ACL, Object ACL, *Content Filtering* e *Identity Firewall*;
- *Identity Firewall*: filtraggio degli accessi in base al nome utente/gruppo;
- caratteristiche del *firewall* Cisco Security Appliance (ASA);
- Procedura di *password recovery*;
- *management* del *firewall* con Cisco *Adaptive Security Device Manager* (ASDM);
- protocolli SSH, RADIUS, TACACS+;
- autenticazione, Autorizzazione, Accounting (AAA);
- *Switching*, *routing* statico e dinamico; Configurazione di interfacce logiche e VLAN L2;
- Rilevamento delle minacce e statistiche tramite *Syslog server*; protocolli *Sylog* e *NTP*; normative sulla registrazione gestione degli eventi;
- Simulazione del Traffico TCP/IP: Utilizzo di *packet-tracer* e risoluzione dei problemi
- Cattura e analisi del traffico IP sul *Firewall* ai fini della sicurezza ICT e individuazione di attacchi informatici, *malware*, intrusioni; Decodifica traffico IP con *sniffer* WIRESHARK;
- protocollo NAT / PAT: concetti, tipi e funzionalità; pubblicazione di servizi WEB.
- Attivazione Portale SSL/TLS per la pubblicazione di servizi verso Internet
- Crittografia: algoritmi simmetrici (3DES, AES) e asimmetrici (RSA), gestione delle chiavi (Diffie-Hellman), *hashing* (MD5, SHA), certificati digitali, *Certification Authority*;
- Architettura IPSEC: AH, ESP, HMAC, IKEv1, IKEv2;

- Reti VPN basate su Gateway SSL/TLS/DTLS e su Gateway IPSEC;
- Creazione di reti IPSEC VPN *Site-to-Site* e *Hub and spoke* in TUNNEL-MODE;
- *Certification Authority* (CA) sul Firewall per il supporto dell'accesso remoto *client* VPN;
- Configurazione accesso remoto in modalità WEB-VPN SSL / TLS / DTLS
- *Software Client* VPN: installazione configurazione ed uso.
- Autenticazione utenti VPN tramite certificati digitali e *Active Directory Windows Server*.
- Firewall in Alta disponibilità (HA): Configurazione e verifica di *fail overactive/standby*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva richiesta: Corso Avanzato di IP Routing cod. R229A o, in alternativa essere in possesso delle conoscenze minime richieste al punto b.
- b. Conoscenze minime richieste:
 - Modello ISO/OSI, TCP/IP, Indirizzamento IP e *subnetting*;
 - Reti *Ethernet* Switching; IP Routing LAN /WAN;
 - Conoscenza sistema operativo client Windows 7 / 10;
 - Uso di *sniffer* di rete (*Wireshark*) per la decodifica e lettura contenuto pacchetti 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: 3 settimane in presenza.

MODALITÀ DI SVOLGIMENTO

Attività d'aula teorico-pratica con percentuale di laboratorio del 65%

É PREVISTO UN TEST D'INGRESSO

É PREVISTO UN ESAME FINALE

AREA CONTROLLO SATELLITI

30.CORSO OPERATORE SALA CONTROLLO SATELLITE³ - COD. S001A

OBIETTIVI DEL CORSO

Dare ai frequentatori una visione completa degli apparati che compongono le stazioni TT&C del Centro Controllo Satellite e della Sala di Controllo Satellite, delle loro specificità e delle modalità di funzionamento. Sono inoltre mostrate alcune operazioni peculiari che si svolgono sugli apparati di Terra e sul satellite e la modalità di controllo dello stato di salute dei sottosistemi di bordo. L'obiettivo del corso è fornire ai frequentatori una base teorico/pratica che permetta loro di iniziare l'attività lavorativa sul sistema. Al termine del corso i frequentatori dovranno:

- conoscere la struttura delle catene TT&C in banda S e EHF;
- conoscere gli apparati che costituiscono le catene TT&C;
- conoscere gli apparati che costituiscono la Banda Base;
- conoscere le funzioni di telecomando, telemetria e *ranging*;
- conoscere la struttura della Sala di Controllo Satellite;
- conoscere le interfacce del CCS;
- conoscere le modalità operative e i modi di funzionamento del CCS;
- conoscere le modalità di controllo della stazione TT&C;
- conoscere le modalità di controllo del satellite;
- conoscere le operazioni che si svolgono in Sala Controllo Satellite.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso teorico per ottenere la qualifica/abilitazione di Operatore Sala Controllo Satellite si svolgerà in due sessioni:

- sessione Operatore TT&C, della durata di tre settimane;
- sessione Operatore CONTROLLO SATELLITE, della durata di due settimane.

Le materie oggetto di insegnamento sono le seguenti:

Sessione Operatore TT&C:

- descrizione del sistema TT&C;
- operazioni RF Banda EHF/S;
- cenni di Sistema TT&C;
- modem S/S;
- banda base.

Sessione Operatore CCS:

- introduzione alle operazioni CCS;
- interfacce operative del CCS;
- gestione del satellite;
- scenario operativo e modi di funzionamento del CCS;

³ Corso svolto in base alla direttiva SMD-FORM-005 sull'addestramento e l'impiego del personale destinato al controllo dei satelliti in orbita geostazionaria. Si svolgerà su richiesta specifica del CIGC di Vigna di Valle.

- utilizzo del M&C nel CCS;
- operazioni CCS;
- operazioni di dinamica del volo.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI:

Personale del CIGC SICRAL.

DURATA DEL CORSO:

La durata prevista del corso per ottenere la qualifica/abilitazione di Operatore sala controllo satellite è di 17 settimane, 5 per la parte di teorica e 12 per quella di OJT.

La parte teorica si articolerà in due sessioni: la prima di Operatore TT&C della durata di tre settimane, la sessione di Operatore CCS della durata di due settimane.

Durante l'OJT l'Operatore sala controllo satellite svolgerà con il supporto del simulatore satellite tutte le procedure e le operazioni di competenza, secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine di ciascuna delle due sessioni teoriche del corso, i frequentatori dovranno svolgere esami scritti (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

31.CORSO CAPO TURNO SALA CONTROLLO SATELLITE⁴ - COD. S002A

OBIETTIVI DEL CORSO

Fornire ai frequentatori un'approfondita conoscenza delle macchine e degli apparati della Sala Controllo Satellite, del software ad esse associato e dei diversi sottosistemi del satellite. Si fornirà un maggior dettaglio delle operazioni nominali e di contingenza da effettuare in Turno, sia sulle WS del Centro di Controllo, sia sugli apparati della stazione TT&C e si illustreranno le relative procedure. Si fornirà al frequentatore anche una panoramica delle possibili anomalie e la modalità di risoluzione. L'obiettivo del corso è fornire ai frequentatori una base teorico/pratica che permetta loro di svolgere l'attività di comando e controllo del sistema. Al termine del corso i frequentatori dovranno:

- conoscere il sistema di M&C;
- conoscere le modalità di collegamento Terra bordo;
- conoscere le procedure nominali e di contingenza delle Stazioni TT&C;
- conoscere le procedure nominali e di contingenza della Sala Controllo;
- conoscere gli applicativi della sala controllo satellite;
- conoscere la struttura e le operazioni del sottosistema SICS;
- conoscere la struttura e le operazioni del sottosistema EPS;
- conoscere la struttura e le operazioni del sottosistema TCS;
- conoscere la struttura e le operazioni del sottosistema TT&C;
- conoscere la struttura e le operazioni del sottosistema PAYLOAD.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- presentazione del Centro di Controllo;
- sistema di Monitor e Control;
- sistema di comunicazione Terra-Bordo;
- procedure stazione TT&C;
- sala controllo satellite;
- dinamica del volo;
- attività di turno;
- *database*;
- sottosistema SICS;
- sottosistema EPS;
- sottosistema TCS;
- sottosistema Payload.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti:

- essere in possesso della qualifica/abilitazione di Operatore Sala Controllo Satellite;
- avere un'esperienza di almeno 6 mesi in Turno.

⁴ Corso svolto in base alla direttiva SMD FORM 005 sull'addestramento e l'impiego del personale destinato al controllo dei satelliti in orbita geostazionaria. Si svolgerà su richiesta specifica del CIGC di Vigna di Valle.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Capoturno sala controllo satellite è di 40 settimane, 4 per la parte di teorica e 36 per quella di OJT.

Durante l'OJT il Capoturno sala controllo satellite svolgerà con il supporto del simulatore satellite tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

32.CORSO SPECIALISTA CONTROLLO D'ASSETTO E DATABASE SATELLITE⁵ - COD. S003A

OBIETTIVI DEL CORSO

Fornire ai frequentatori un'approfondita conoscenza sulle caratteristiche e le operazioni del sottosistema di controllo d'assetto, sul Data Handling (DHC), sulla struttura del database di bordo e sulla struttura e composizione dei comandi e delle telemetrie del satellite.

Si fornirà un maggior dettaglio delle operazioni nominali e di contingenza da effettuare e si illustreranno le relative procedure. Si fornirà al frequentatore anche una panoramica delle possibili anomalie e la modalità di risoluzione.

L'obiettivo del corso è fornire ai frequentatori una base teorico/pratica che permetta loro di svolgere l'attività di comando e controllo del Sottosistema di competenza. Al termine del corso i frequentatori dovranno:

- conoscere la modalità di calcolo delle manovre orbitali;
- conoscere la struttura e le funzioni del sottosistema UPS;
- conoscere la struttura hardware e le funzioni del sottosistema SICS;
- conoscere la struttura e le funzioni del sottosistema DHC;
- conoscere la struttura hardware del computer di bordo;
- conoscere le funzionalità degli equipaggiamenti per il controllo d'assetto;
- conoscere come si strutturano i telecomandi e telemetrie;
- conoscere il software di bordo con le relative funzioni e modalità di operare;
- conoscere le procedure nominali e di contingenza dei sottosistemi SICS-UPS e DHC.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- dinamica orbitale;
- sottosistema di propulsione;
- sottosistema integrato di controllo satellite;
- *data handling & control*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Operatore Sala Controllo Satellite.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Controllo d'assetto e database satellite è di 39 settimane, 3 per la parte di teorica e 36 per quella di OJT.

⁵ Corso svolto in base alla direttiva SMD FORM 005 sull'addestramento e l'impiego del personale destinato al controllo dei satelliti in orbita geostazionaria. Si svolgerà su richiesta specifica del CIGC di Vigna di Valle.

Durante l'OJT lo Specialista Controllo d'assetto e database satellite svolgerà con il supporto del simulatore satellite tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

33.CORSO SPECIALISTA PIATTAFORMA SATELLITE⁶ - COD. S004A

OBIETTIVI DEL CORSO

Fornire ai frequentatori un'approfondita conoscenza sulle caratteristiche e le operazioni dei sottosistemi di piattaforma (termico e elettrico) e sul *data handling* (DHC).

Si fornirà un maggior dettaglio delle operazioni nominali e di contingenza da effettuarsi illustreranno le relative procedure. Si fornirà al frequentatore anche una panoramica delle possibili anomalie e la modalità di risoluzione. L'obiettivo del corso è fornire ai frequentatori una base teorico/pratica che permetta loro di svolgere l'attività di comando e controllo del Sottosistema di competenza. Al termine del corso i frequentatori dovranno:

- conoscere la struttura hardware e le funzioni del sottosistema EPS;
- conoscere la struttura hardware e le funzioni del sottosistema TCS;
- conoscere la struttura e le funzioni del sottosistema DHC;
- conoscere le funzionalità degli equipaggiamenti per il controllo termico;
- conoscere le funzionalità degli equipaggiamenti per la distribuzione della potenza elettrica;
- conoscere il software di bordo con le relative funzioni e modalità di operare;
- conoscere le procedure nominali e di contingenza dei sottosistemi EPS, TCS e DHC.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- *electric & power subsystem*;
- *thermal control subsystem*;
- *data handling & control*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti:
Essere in possesso della qualifica/abilitazione di Operatore Sala Controllo satellite.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Piattaforma Satellite è di 39 settimane, 3 per la parte di teorica e 36 per quella di OJT.

Durante l'OJT lo Specialista Piattaforma Satellite svolgerà con il supporto del simulatore satellite tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

⁶ Corso svolto in base alla direttiva SMD FORM 005 sull'addestramento e l'impiego del personale destinato al controllo dei satelliti in orbita geostazionaria. Si svolgerà su richiesta specifica del CIGC di Vigna di Valle.

CORSO SPECIALISTA COMUNICAZIONI TERRA-BORDO SATELLITE⁷ - COD. S005A

OBIETTIVI DEL CORSO

Fornire ai frequentatori un'approfondita conoscenza sulle caratteristiche e le operazioni dei sottosistemi preposti a mantenere il link di comando e controllo con il satellite (TT&C) e sul carico utile. Si fornirà un maggior dettaglio delle operazioni nominali e di contingenza da effettuare e si illustreranno le relative procedure. Si fornirà al frequentatore anche una panoramica delle possibili anomalie e la modalità di risoluzione.

L'obiettivo del corso è fornire ai frequentatori una base teorico/pratica che permetta loro di svolgere l'attività di comando e controllo del Sottosistema di competenza. Al termine del corso i frequentatori dovranno:

- conoscere la struttura hardware e le funzioni del sottosistema TT&C;
- conoscere la struttura hardware e le funzioni delle stazioni TT&C;
- conoscere la struttura hardware e le funzioni del sottosistema *Payload*;
- conoscere le funzionalità degli equipaggiamenti del *Payload*;
- conoscere le funzionalità degli equipaggiamenti per il link di comando e telemetria;
- conoscere le procedure nominali e di contingenza dei sottosistemi TT&C e *Payload*.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- stazioni TT&C;
- sottosistema TT&C;
- sottosistema *Payload*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Operatore Sala Controllo Satellite.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Comunicazioni Terra-Bordo satellite è di 39 settimane, 3 per la parte di teorica e 36 per quella di OJT.

Durante l'OJT lo Specialista Piattaforma Satellite svolgerà con il supporto del simulatore satellite tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

⁷ Corso svolto in base alla direttiva SMD FORM 005 sull'addestramento e l'impiego del personale destinato al controllo dei satelliti in orbita geostazionaria. Si svolgerà su richiesta specifica del CIGC di Vigna di Valle.

CORSO SUPERVISORE SALA CONTROLLO SATELLITE E STAZIONI TT&C⁸ - COD. S006A

OBIETTIVI DEL CORSO

Dare ai frequentatori un'approfondita conoscenza sulle caratteristiche e le operazioni dei sistemi che compongono la stazione TT&C e la sala controllo satellite.

Si descriveranno tutte le operazioni nominali e di contingenza. In particolare il personale dovrà acquisire il necessario *know-how* per poter individuare i comportamenti anomali del sistema. L'obiettivo del corso è fornire ai frequentatori una base teorico/pratica che permetta loro di svolgere l'attività di comando e controllo del satellite. Al termine del corso i frequentatori dovranno:

- conoscere i protocolli e le tecniche di trasmissione e modulazione dei segnali;
- conoscere le tecniche di comunicazione analogica e digitale;
- conoscere le modalità di collegamento Terra bordo;
- conoscere le procedure nominali e di contingenza delle stazioni TT&C;
- conoscere le procedure nominali e di contingenza della Sala Controllo;
- conoscere gli applicativi della sala controllo satellite;
- conoscere la struttura hardware e le funzioni delle stazioni TT&C.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- teoria dei segnali;
- trasmissione dei segnali;
- codifica dei segnali;
- antenne;
- link budget;
- emissioni fuori banda/interferenze;
- stazioni TT&C;
- sala controllo satellite;
- modi di funzionamento del CCS.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve aver seguito e superato il corso biennale in Ingegneria Astronautica (Scuola di Ingegneria Aerospaziale) oppure aver seguito e superato master/corso di specializzazione in "Sistemi Spaziali" e/o "Gestione operativa di satelliti".

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Supervisore sala CCS e stazioni TT&C è di 9 settimane, 4 per la parte di teorica e 5 per quella di OJT.

⁸ Corso svolto in base alla direttiva SMD FORM 005 sull'addestramento e l'impiego del personale destinato al controllo dei satelliti in orbita geostazionaria. Si svolgerà su richiesta specifica del CIGC di Vigna di Valle.

Durante l'OJT il Supervisore sala CCS e stazioni TT&C svolgerà tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

34.CORSO INGEGNERE SATELLITE⁹ - COD. S007A

OBIETTIVI DEL CORSO

Dare ai frequentatori un'approfondita conoscenza sulle caratteristiche e le operazioni dei sottosistemi che compongono il satellite. Si descriveranno tutte le operazioni nominali e di contingenza. In particolare, il personale dovrà acquisire il necessario *know-how* per poter individuare i comportamenti anomali del satellite e scegliere prontamente la procedura più idonea alla messa in sicurezza del satellite. L'obiettivo del corso è fornire ai frequentatori una base teorico/pratica che permetta loro di svolgere l'attività di comando e controllo del satellite. Al termine del corso i frequentatori dovranno:

- conoscere la modalità di calcolo delle manovre orbitali;
- conoscere la struttura e le funzioni del sottosistema UPS;
- conoscere la struttura hardware e le funzioni del sottosistema SICS;
- conoscere la struttura e le funzioni del sottosistema DHC;
- conoscere la struttura hardware del computer di bordo;
- conoscere le funzionalità degli equipaggiamenti per il controllo d'assetto;
- conoscere come si strutturano i telecomandi e telemetrie;
- conoscere il software di bordo con le relative funzioni e modalità di operare;
- conoscere le procedure nominali e di contingenza dei sottosistemi SICS-UPS e DHC;
- conoscere la struttura hardware e le funzioni del sottosistema EPS;
- conoscere la struttura hardware e le funzioni del sottosistema TCS;
- conoscere le funzionalità degli equipaggiamenti per il controllo termico;
- conoscere le funzionalità degli equipaggiamenti per la distribuzione della potenza elettrica;
- conoscere la struttura hardware e le funzioni del sottosistema TT&C;
- conoscere la struttura hardware e le funzioni del sottosistema *Payload*;
- conoscere le funzionalità degli equipaggiamenti del *Payload*;
- conoscere le procedure nominali e di contingenza dei sottosistemi TT&C e *Payload*.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- dinamica orbitale;
- sottosistema di propulsione;
- sottosistema integrato di controllo satellite;
- *data handling & control*;
- *electric & power subsystem*;
- *thermal control subsystem*;
- sottosistema TT&C;
- sottosistema *payload*.

⁹ Corso svolto in base alla direttiva SMD FORM 005 sull'addestramento e l'impiego del personale destinato al controllo dei satelliti in orbita geostazionaria. Si svolgerà su richiesta specifica del CIGC di Vigna di Valle.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve aver:

- seguito e superato il corso biennale in Ingegneria Astronautica (Scuola di Ingegneria Aerospaziale) oppure aver seguito e superato master/corso di specializzazione in “Sistemi Spaziali” e/o “Gestione operativa di satelliti”;
- svolto e superato il corso Supervisore sala controllo satellite e stazioni TT&C.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Ingegnere Satellite è di 48 settimane, 6 per la parte di teorica e 42 per quella di OJT.

Durante l’OJT l’Ingegnere Satellite svolgerà tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

35. CORSO SPECIALISTA CENTRO DI CONTROLLO SATELLITE GEO - COD. S008A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire lo Specialista Centri di Controllo Satellite ad effettuare la sorveglianza ed il controllo (CCS off-line monitor & control) di tutte le attività atte al mantenimento dell'efficienza e delle prestazioni dei sistemi per il Controllo dei Satelliti geostazionari (Centri di Controllo). Lo Specialista è abilitato all'invio di comandi e alle operazioni di manutenzione di 1° e 2° livello tecnico previste dalle procedure all'uso predisposte. Inoltre, egli dovrà essere in possesso di competenze nell'ambito della "Sicurezza Sistemi EAD classificati" al fine di potere svolgere, come da direttive vigenti, incarichi legati all'Amministrazione di Reti informatiche classificate.

Il corso fornirà allo Specialista le competenze per espletare le seguenti attività:

- eseguire la verifica delle prestazioni dei Centri di Controllo (*trend analysis*);
- eseguire le operazioni nominali non ricorrenti e di *contingency* applicando le Procedure Operative di Terra ed interviene in caso di "escalation" causate da avarie significative e/o allarmi;
- eseguire le procedure previste dall'incarico di "Amministratore di Rete Classificata" secondo le direttive e regolamenti di sicurezza vigenti.

Al termine del corso i frequentatori dovranno:

- conoscere i dettagli architeturali della Sala Controllo satellite geostazionari (*Storm-View, SCOS2000*);
- conoscere il sistema di M&C e le modalità di scambio dati con il centro di controllo;
- conoscere il sistema di Dinamica del Volo e le modalità di scambio dati con il centro di controllo;
- conoscere gli aspetti legati alla gestione del database di telemetria e telecomandi;
- saper eseguire attività manutentive di 1° e 2° livello sui sistemi.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- architettura di dettaglio del Centro di Controllo;
- sala controllo satellite;
- sala apparati e *server*;
- sistema di *monitor & control*;
- sistema di dinamica del volo;
- database telemetria e telecomandi;
- gestione reti classificate e sistemi EAD.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: avere competenze nell'ambito della "Sicurezza Sistemi EAD classificati".

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Centro di Controllo Satellite GEO è di 8 settimane, 3 per la parte di teorica e 5 per quella di OJT. Durante l'OJT lo Specialista Centro di Controllo Satellite GEO svolgerà tutte le operazioni di competenza, eseguendo tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

36.CORSO CONTROLLORE STAZIONE TT&C GEO - COD. S009A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire il Controllore Stazioni TT&C ad effettuare la sorveglianza e il controllo (TT&C monitor & control) di tutte le attività atte alla salvaguardia della vita operativa dei sistemi di Terra (antenne, apparati a Radio Frequenza e Bande Basi) deputati al controllo dei satelliti geostazionari SICRAL 1, SICRAL 1B e SICRAL2 (configurazione GEO-2015). Il controllore è abilitato all'invio di comandi agli apparati della Stazione TT&C, alle operazioni di manutenzione di 1° livello tecnico previste dalle procedure all'uopo predisposte ed è direttamente responsabile del mantenimento della configurazione del sistema.

Il corso fornirà al Controllore le competenze per espletare le seguenti attività:

- eseguire la verifica dei parametri della Stazione TT&C (monitor);
- eseguire le operazioni nominali e di *contingency* applicando le Procedure Operative di Terra ed avvia la prevista procedura di “*escalation*” in caso di avarie significative (control).

Al termine del corso i frequentatori dovranno:

- conoscere la stazione TT&C, a livello BB/MODEM, RF ed Antenne;
- conoscere il sistema di M&C;
- conoscere il sistema di Network;
- conoscere le modalità di collegamento Terra bordo;
- conoscere le procedure nominali e di contingenza delle Stazioni TT&C.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- stazione TT&C: BB/MODEM, Radio Frequenza ed Antenne;
- sistema di M&C di Stazione;
- sistema NTW;
- modalità di collegamento Terra bordo;
- procedure nominali e di contingenza delle Stazioni TT&C.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Personale del CIGC SICRAL.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Controllore Stazioni TT&C GEO è di 4 settimane, 2 per la parte di teorica e 2 per quella di OJT.

Durante l'OJT il Controllore Stazioni TT&C GEO svolgerà tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

37.CORSO SPECIALISTA STAZIONI TT&C GEO - COD. S010A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire lo Specialista Stazioni TT&C ad effettuare la sorveglianza e il controllo (TT&C off-line monitor & control) di tutte le attività atte al mantenimento dell'efficienza e delle prestazioni delle stazioni TT&C deputate al controllo dei satelliti geostazionari SICRAL 1, SICRAL 1B e SICRAL2 (configurazione GEO-2015). Lo Specialista è abilitato all'invio di comandi agli apparati della Stazione TT&C e alle operazioni di manutenzione di 1° e 2° livello tecnico previste dalle procedure all'uopo predisposte.

Il corso fornirà allo Specialista le competenze per espletare le seguenti attività:

- eseguire la verifica delle prestazioni dei sottosistemi della Stazione TT&C (*trend analysis*);
- eseguire le operazioni nominali non ricorrenti e di *contingency* applicando le Procedure Operative di Terra predisposte dal Servizio ed interviene in caso di "escalation" causate da avarie significative e/o allarmi;
- eseguire campagne di misure con l'utilizzo di moduli software e strumenti di misura da laboratorio (es. Analizzatore Spettro, LabView, ecc.).

Al termine del corso i frequentatori dovranno:

- conoscere il dettaglio architettuale del sistema di M&C;
- conoscere il dettaglio architettuale del sistema Network;
- conoscere i dettagli delle modalità di collegamento Terra bordo;
- saper eseguire attività manutentive di 1° e 2° livello sui sistemi;
- saper eseguire campagne di misure con l'utilizzo di moduli software e strumenti di misura da laboratorio.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- dettagli architetture Stazione TT&C: BB/MODEM, Radio Frequenza ed Antenne;
- dettagli architetture di M&C di Stazione;
- dettagli architetture sistema NTW;
- campagne di misura.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Controllore Stazioni TT&C GEO.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Stazioni TT&C GEO è di 6 settimane, 2 per la parte di teorica e 4 per quella di OJT.

Durante l'OJT lo Specialista Stazioni TT&C GEO svolgerà tutte le operazioni di competenza, eseguendo tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

38. CORSO CONTROLLORE DINAMICA DEL VOLO GEO - COD. S011A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire il Controllore Dinamica del Volo ad effettuare la sorveglianza e il controllo (FDS monitor & control) di tutte le attività atte al mantenimento della corretta orbita dei satelliti geostazionari (SICRAL1-SICRAL1B-SICRAL2).

Il corso fornirà al Controllore le competenze per espletare le seguenti attività:

- eseguire la verifica dei parametri dei sistemi di Dinamica del Volo (monitor);
- eseguire le operazioni nominali ricorrenti e di *contingency* applicando le Procedure Operative di Dinamica del Volo ed avvia la prevista procedura di “escalation” in caso di avarie significative e/o allarmi (control).

Al termine del corso i frequentatori dovranno:

- avere nozioni fondamentali di dinamica orbitale;
- conoscere l’architettura del sistema di dinamica del volo GEO;
- conoscere le procedure nominali e di contingenza di FDS;
- saper verificare i parametri dei sistemi di dinamica del volo GEO.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- nozioni di dinamica orbitale;
- sistema FDS;
- procedure nominali e di contingenza di FDS.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Personale del CIGC SICRAL.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Controllore Dinamica del Volo GEO è di 4 settimane, 2 per la parte di teorica e 2 per quella di OJT.

Durante l’OJT il Controllore Dinamica del Volo GEO svolgerà tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

39.CORSO SPECIALISTA DINAMICA DEL VOLO GEO - COD. S012A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire lo Specialista Dinamica del Volo ad effettuare la sorveglianza e il controllo (FDS off-line monitor & control) di tutte le attività atte al mantenimento dell'efficienza e delle prestazioni dei sistemi di Dinamica del Volo per la gestione di satelliti geostazionari (SICRAL1-SICRAL1B-SICRAL2). Lo Specialista è abilitato all'utilizzo degli apparati di Dinamica del Volo alle operazioni di manutenzione di 1° e 2° livello tecnico previste dalle procedure all'uso predisposte. Inoltre egli dovrà essere in possesso di competenze nell'utilizzo di moduli software aggiuntivi ai sistemi di Dinamica del Volo, al fine di eseguire operazioni di anticollisione per i satelliti gestiti dalle Forze Armate, ovvero fornire supporto in tale campo per i satelliti gestiti da Società e/o Enti italiani, come previsto da accordi con il *Joint Space Operation Centre* del USSTRATCOM e con l'Agenzia Spaziale Italiana.

Il corso fornirà allo Specialista le competenze per espletare le seguenti attività:

- eseguire la verifica delle prestazioni dei sistemi di Dinamica del Volo (*trend analysis*);
- eseguire le operazioni nominali non ricorrenti e di *contingency* applicando le Procedure Operative di Dinamica del Volo ed interviene in caso di "escalation" causate da avarie significative e/o allarmi;
- eseguire operazioni di anticollisione con l'utilizzo di moduli software aggiuntivi (es. *Satellite Tool Kit*).

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- approfondimenti di dinamica orbitale;
- pianificazione manovre orbitali;
- dettagli architetturali sistema FDS;
- prestazioni dei sistemi di dinamica del volo;
- moduli software aggiuntivi: STK;
- operazioni anticollisione.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Controllore Dinamica del Volo GEO.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Dinamica del Volo GEO è di 6 settimane, 2 per la parte di teorica e 4 per quella di OJT.

Durante l'OJT lo Specialista Dinamica del Volo GEO svolgerà tutte le operazioni di competenza, eseguendo tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

CONTROLLO SATELLITI IN ORBITA BASSA

40.CORSO CONTROLLORE CENTRO DI CONTROLLO SATELLITE OPTSAT-3000 – COD. S013A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire il Controllore Centro Controllo Satellite ad effettuare la sorveglianza ed il controllo (CCS monitor & control) di tutte le attività atte al mantenimento dell'efficienza del sistema che consente il comando e controllo del satellite OPTSAT-3000. Il corso fornirà al Controllore le competenze per espletare le seguenti attività:

- eseguire la verifica dei parametri del Centro di Controllo Satellite (monitor);
- eseguire le operazioni nominali ricorrenti e di *contingency* applicando le Procedure Operative del Centro Controllo Satellite ed avvia la prevista procedura di “escalation” in caso di avarie significative e/o malfunzionamenti (control).

Al termine del corso i frequentatori dovranno:

- conoscere le procedure nominali e di contingenza della sala controllo;
- conoscere gli applicativi della sala controllo satellite;
- conoscere il sistema di M&C;
- conoscere il sistema di dinamica del volo;
- conoscere gli aspetti legati alla gestione del database di telemetria e telecomandi.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- presentazione del centro di controllo;
- sala controllo satellite;
- sistema di *monitor & control*;
- sistema di dinamica del volo;
- database telemetria e telecomandi.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Personale del CIGC SICRAL.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Controllore Centro di Controllo Satellite OptSat-3000 è di 4 settimane, 2 per la parte di teorica e 2 per quella di OJT.

Durante l'OJT il Controllore Centro di Controllo Satellite OptSat-3000 svolgerà tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

41.CORSO CONTROLLORE SATELLITE OPTSAT-3000 - COD. S014A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire il Controllore Satellite ad effettuare la sorveglianza e il controllo (Satellite *on-line monitor & control*) di tutte le attività atte alla salvaguardia della vita operativa dei satelliti. Il Controllore è abilitato all'invio di comandi a bordo del satellite ed è direttamente responsabile del mantenimento della configurazione del sistema.

Il corso fornirà al Controllore le competenze per espletare le seguenti attività:

- eseguire la verifica dei parametri dei sottosistemi di bordo del satellite (monitor);
- eseguire le operazioni nominali ricorrenti e le operazioni di *contingency* applicando le Procedure Operative di Volo ed avvia la prevista procedura di "*escalation*" in caso di avarie significative (control).

Al termine del corso i frequentatori dovranno:

- conoscere le modalità di collegamento terra-bordo;
- conoscere le procedure nominali e di contingenza per la gestione del satellite;
- conoscere la struttura e le operazioni del sottosistema SICS;
- conoscere la struttura e le operazioni del sottosistema EPS;
- conoscere la struttura e le operazioni del sottosistema TCS;
- conoscere la struttura e le operazioni del sottosistema TT&C;
- conoscere la struttura e le operazioni del sottosistema PAYLOAD.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- attività di turno;
- sottosistema SICS;
- sottosistema EPS;
- sottosistema TCS;
- sottosistema *Payload*;
- sistema di comunicazione terra-bordo;
- operazioni su database satellite.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Controllore Centro di Controllo Satellite OptSat-3000.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Controllore Satellite OptSat-3000 è di 8 settimane, 3 per la parte di teorica e 5 per quella di OJT.

Durante l'OJT il Controllore Satellite OptSat-3000 svolgerà tutte le operazioni di competenza, eseguendo con l'ausilio del simulatore satellite tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

42.CORSO SPECIALISTA CENTRO DI CONTROLLO SATELLITE OPTSAT-3000 - COD. S015A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire lo Specialista Centri di Controllo Satellite ad effettuare la sorveglianza ed il controllo (CCS off-line monitor & control) di tutte le attività atte al mantenimento dell'efficienza e delle prestazioni dei sistemi per il Controllo dei Satelliti in orbita bassa (Centri di Controllo). Lo Specialista è abilitato all'invio di comandi e alle operazioni di manutenzione di 1° e 2° livello tecnico previste dalle procedure all'uopo predisposte. Inoltre, egli dovrà essere in possesso di competenze nell'ambito della "Sicurezza Sistemi EAD classificati" al fine di potere svolgere, come da direttive vigenti, incarichi legati all'Amministrazione di Reti informatiche classificate.

Il corso fornirà allo Specialista le competenze per espletare le seguenti attività:

- eseguire la verifica delle prestazioni dei Centri di Controllo (*trend analysis*);
- eseguire le operazioni nominali non ricorrenti e di *contingency* applicando le Procedure Operative di Terra ed interviene in caso di "*escalation*" causate da avarie significative e/o allarmi;
- eseguire le procedure previste dall'incarico di "Amministratore di Rete Classificata" secondo le direttive e regolamenti di sicurezza vigenti.

Al termine del corso i frequentatori dovranno:

- conoscere i dettagli architeturali della Sala Controllo satellite (IAI-SCC, IAI-TCC);
- conoscere il sistema di M&C e le modalità di scambio dati con il centro di controllo;
- conoscere il sistema di Dinamica del Volo e le modalità di scambio dati con il centro di controllo;
- conoscere gli aspetti legati alla gestione del database di telemetria e telecomandi;
- saper eseguire attività manutentive di 1° e 2° livello sui sistemi.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- architettura di dettaglio del centro di controllo;
- sala controllo satellite;
- sala apparati e *server*;
- sistema di *monitor & control*;
- sistema di dinamica del volo;
- database telemetria e telecomandi;
- gestione reti classificate e sistemi EAD.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti:

- essere in possesso della qualifica/abilitazione di Controllore Satellite OptSat-3000;
- avere competenze nell'ambito della "Sicurezza Sistemi EAD classificati".

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Centro di Controllo Satellite OptSat-3000 è di 8 settimane, 3 per la parte di teorica e 5 per quella di OJT.

Durante l'OJT lo Specialista Centro di Controllo Satellite OptSat-3000 svolgerà tutte le operazioni di competenza, eseguendo tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

43.CORSO SPECIALISTA CONTROLLO ASSETTO ED ORBITA SATELLITE OPTSAT-3000 - COD. S016A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire lo Specialista Controllo Assetto Satellite ed Orbita ad effettuare la sorveglianza e il controllo (AOCS monitor & control) di tutte le attività atte al mantenimento dell'efficienza e delle prestazioni del sottosistema di Controllo di Assetto ed Orbita del satellite OPTSAT-3000 e della gestione delle aeree di memoria di bordo. Lo Specialista è abilitato all'invio di comandi a bordo del satellite ed è direttamente responsabile del mantenimento della configurazione del sottosistema di competenza.

Il corso fornirà allo Specialista le competenze per espletare le seguenti attività:

- eseguire la verifica delle prestazioni dei sottosistemi satellite di competenza (*trend analysis*);
- eseguire le operazioni nominali non ricorrenti e di *contingency* applicando le Procedure Operative di Volo ed interviene in caso di “*escalation*” causate da avarie significative e/o allarmi al sottosistema satellite di competenza.

Al termine del corso i frequentatori dovranno:

- conoscere la modalità di calcolo delle manovre orbitali;
- conoscere la struttura e le funzioni del sottosistema propulsivo;
- conoscere la struttura hardware e le funzioni del sottosistema di controllo d'assetto;
- conoscere la struttura hardware del computer di bordo;
- conoscere le funzionalità degli equipaggiamenti per il controllo d'assetto;
- conoscere come si strutturano i telecomandi e telemetrie;
- conoscere il software di bordo con le relative funzioni e modalità di operare;
- conoscere le procedure nominali e di contingenza dei sottosistemi legati al controllo d'assetto ed al computer di bordo.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- sottosistema di controllo d'assetto;
- sottosistema di propulsione;
- computer di bordo;
- software di volo;
- dinamica orbitale;
- database satellite.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Controllore Satellite OptSat-3000.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Controllo Assetto ed Orbita Satellite OptSat-3000 è di 8 settimane, 3 per la parte di teorica e 5 per quella di OJT.

Durante l'OJT lo Specialista Controllo Assetto ed Orbita Satellite OptSat-3000 svolgerà tutte le operazioni di competenza, eseguendo tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

44.CORSO SPECIALISTA PIATTAFORMA SATELLITE OPTSAT-3000 - COD. S017A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire lo Specialista Piattaforma Satellite OPTSAT-3000 ad effettuare la sorveglianza e il controllo (EPS-TCS monitor & control) di tutte le attività atte al mantenimento dell'efficienza e delle prestazioni del sottosistema di Controllo termico ed elettrico del satellite. Lo Specialista è abilitato all'invio di comandi a bordo del satellite ed è direttamente responsabile del mantenimento della configurazione del sottosistema di competenza.

Il corso fornirà allo Specialista le competenze per espletare le seguenti attività:

- eseguire la verifica delle prestazioni dei sottosistemi satellite di competenza (*trend analysis*);
- eseguire le operazioni nominali non ricorrenti e di *contingency* applicando le Procedure Operative di Volo ed interviene in caso di "escalation" causate da avarie significative e/o allarmi al sottosistema satellite di competenza.

Al termine del corso i frequentatori dovranno:

- conoscere la struttura hardware e le funzioni del sottosistema EPS;
- conoscere la struttura hardware e le funzioni del sottosistema TCS;
- conoscere la struttura e le funzioni del software di volo;
- conoscere le funzionalità degli equipaggiamenti per il controllo termico;
- conoscere le funzionalità degli equipaggiamenti per la distribuzione della potenza elettrica;
- conoscere il software di bordo con le relative funzioni e modalità di operare;
- conoscere le procedure nominali e di contingenza dei sottosistemi coinvolti.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- *electric & power subsystem*;
- *thermal control subsystem*;
- software di volo;
- *database satellite*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Controllore Satellite OptSat-3000.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Piattaforma Satellite OptSat-3000 è di 6 settimane, 2 per la parte di teorica e 4 per quella di OJT.

Durante l'OJT lo Specialista Piattaforma Satellite OptSat-300 svolgerà tutte le operazioni di competenza, eseguendo tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

45. CORSO SPECIALISTA PAYLOAD SATELLITE OPTSAT-3000 - COD. S018A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire lo Specialista *Payload* Satellite ad effettuare la sorveglianza e il controllo (PAY-TTC *monitor & control*) di tutte le attività atte al mantenimento dell'efficienza e delle prestazioni del sottosistema inerente al carico utile e del sottosistema TT&C del satellite (antenne, trasponditori TT&C, sottosistema di comunicazione nel caso di satelliti geostazionari, sensori di telerilevamento nel caso di satelliti in orbita bassa). Lo Specialista è abilitato all'invio di comandi a bordo del satellite ed è direttamente responsabile del mantenimento della configurazione del sottosistema di competenza. Inoltre egli dovrà essere in possesso di competenze nell'utilizzo di moduli software e strumenti di misura di laboratorio, al fine di eseguire campagne di test del tipo IOT (*In Orbit Test*).

Il corso fornirà allo Specialista le competenze per espletare le seguenti attività:

- eseguire la verifica delle prestazioni del sottosistema satellite di competenza (*trend analysis*);
- eseguire le operazioni nominali non ricorrenti e di *contingency* applicando le Procedure Operative di Volo ed interviene in caso di “*escalation*” causate da avarie significative e/o allarmi al sottosistema satellite di competenza;
- eseguire campagne di misure di In Orbit Test (IOT) con l'utilizzo di moduli software e strumenti di misura da laboratorio (es. Analizzatore Spettro, LabView, ecc.).

Al termine del corso i frequentatori dovranno:

- conoscere la struttura hardware e le funzioni del sottosistema *Payload*;
- conoscere le funzionalità degli equipaggiamenti del *Payload*;
- conoscere la struttura hardware e le funzioni del sottosistema TT&C;
- conoscere la struttura hardware e le funzioni delle stazioni TT&C;
- conoscere le funzionalità degli equipaggiamenti per il *link* di comando e telemetria;
- conoscere le procedure nominali e di contingenza dei sottosistemi TT&C e *Payload*.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- sottosistema TT&C;
- sottosistema *Payload*;
- software di volo;
- *database satellite*;
- attività di IOT/CAL-VAL.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Controllore Satellite OptSat-3000.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista *Payload* Satellite OptSat-3000 è di 6 settimane, 2 per la parte di teorica e 4 per quella di OJT. Durante l'OJT lo Specialista *Payload* Satellite OptSat-3000 svolgerà tutte le operazioni di competenza, eseguendo tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

46.CORSO CONTROLLORE STAZIONE TT&C OPTSAT-3000 - COD. S019A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire il Controllore Stazioni TT&C ad effettuare la sorveglianza e il controllo (TT&C monitor & control) di tutte le attività atte alla salvaguardia della vita operativa dei sistemi di Terra (antenne, apparati a Radio Frequenza e Bande Basi) deputati al controllo dei satelliti in orbita bassa. Il controllore è abilitato all'invio di comandi agli apparati della Stazione TT&C, alle operazioni di manutenzione di 1° livello tecnico previste dalle procedure all'uso predisposte ed è direttamente responsabile del mantenimento della configurazione del sistema.

Il corso fornirà al Controllore le competenze per espletare le seguenti attività:

- eseguire la verifica dei parametri della Stazione TT&C (monitor);
- eseguire le operazioni nominali e di *contingency* applicando le Procedure Operative di Terra ed avvia la prevista procedura di "*escalation*" in caso di avarie significative (control).

Al termine del corso i frequentatori dovranno:

- conoscere la stazione TT&C, a livello BB/MODEM, RF ed Antenne;
- conoscere il sistema di M&C;
- conoscere il sistema di *Network*;
- conoscere le modalità di collegamento Terra bordo;
- conoscere le procedure nominali e di contingenza delle Stazioni TT&C.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- stazione TT&C: BB/MODEM, Radio Frequenza ed Antenne;
- sistema di M&C di Stazione;
- sistema NTW;
- modalità di collegamento terra-bordo;
- procedure nominali e di contingenza delle Stazioni TT&C.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Personale del CIGC SICRAL.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Controllore Stazioni TT&C OptSat-3000 è di 4 settimane, 2 per la parte di teorica e 2 per quella di OJT.

Durante l'OJT il Controllore Stazioni TT&C OptSat-3000 svolgerà tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

47.CORSO SPECIALISTA STAZIONI TT&C OPTSAT-3000 - COD. S020A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire lo Specialista Stazioni TT&C ad effettuare la sorveglianza e il controllo (TT&C *off-line monitor & control*) di tutte le attività atte al mantenimento dell'efficienza e delle prestazioni delle stazioni TT&C deputate al controllo dei satelliti in orbita bassa. Lo Specialista è abilitato all'invio di comandi agli apparati della Stazione TT&C e alle operazioni di manutenzione di 1° e 2° livello tecnico previste dalle procedure all'uopo predisposte.

Il corso fornirà allo Specialista le competenze per espletare le seguenti attività:

- eseguire la verifica delle prestazioni dei sottosistemi della Stazione TT&C (*trend analysis*);
- eseguire le operazioni nominali non ricorrenti e di *contingency* applicando le Procedure Operative di Terra predisposte dal Servizio ed interviene in caso di "escalation" causate da avarie significative e/o allarmi;
- eseguire campagne di misure con l'utilizzo di moduli software e strumenti di misura da laboratorio (es. Analizzatore Spettro, LabView, ecc.).

Al termine del corso i frequentatori dovranno:

- conoscere il dettaglio architettuale del sistema di M&C;
- conoscere il dettaglio architettuale del sistema Network;
- conoscere i dettagli delle modalità di collegamento Terra bordo;
- saper eseguire attività manutentive di 1° e 2° livello sui sistemi;
- saper eseguire campagne di misure con l'utilizzo di moduli software e strumenti di misura da laboratorio.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- dettagli architeturali Stazione TT&C: BB/MODEM, Radio Frequenza ed Antenne;
- dettagli architeturali di M&C di Stazione;
- dettagli architeturali sistema NTW;
- campagne di misura.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Controllore Stazioni TT&C OptSat-3000.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Stazioni TT&C OptSat-3000 è di 6 settimane, 2 per la parte di teorica e 4 per quella di OJT.

Durante l'OJT lo Specialista Stazioni TT&C OptSat-3000 svolgerà tutte le operazioni di competenza, eseguendo tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

48.CORSO CONTROLLORE DINAMICA DEL VOLO OPTSAT-3000 - COD. S021A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire il Controllore Dinamica del Volo OPSTAT-3000 ad effettuare la sorveglianza e il controllo (FDS *monitor & control*) di tutte le attività atte al mantenimento della corretta orbita dei satelliti LEO.

Il corso fornirà al Controllore le competenze per espletare le seguenti attività:

- eseguire la verifica dei parametri dei sistemi di Dinamica del Volo (monitor);
- eseguire le operazioni nominali ricorrenti e di *contingency* applicando le Procedure Operative di Dinamica del Volo ed avviare la prevista procedura di “escalation” in caso di avarie significative e/o allarmi (control).

Al termine del corso i frequentatori dovranno:

- avere nozioni di fondamenti di dinamica orbitale;
- conoscere l’architettura del sistema di dinamica del volo LEO;
- conoscere le procedure nominali e di contingenza di FDS;
- saper verificare i parametri dei sistemi di dinamica del volo LEO.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- nozioni di dinamica orbitale;
- sistema FDS;
- procedure nominali e di contingenza di FDS.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Personale del CIGC SICRAL.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Controllore Dinamica del Volo OptSat-3000 è di 4 settimane, 2 per la parte di teorica e 2 per quella di OJT.

Durante l’OJT il Controllore Dinamica del Volo OptSat-3000 svolgerà tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

49.CORSO SPECIALISTA DINAMICA DEL VOLO OPTSAT-3000 - COD. S022A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire lo Specialista Dinamica del Volo OPTSAT-3000 ad effettuare la sorveglianza e il controllo (FDS off-line monitor & control) di tutte le attività atte al mantenimento dell'efficienza e delle prestazioni dei sistemi di Dinamica del Volo per la gestione di satelliti in orbita LEO. Lo Specialista è abilitato all'utilizzo degli apparati di Dinamica del Volo alle operazioni di manutenzione di 1° e 2° livello tecnico previste dalle procedure all'uopo predisposte. Inoltre, egli dovrà essere in possesso di competenze nell'utilizzo di moduli software aggiuntivi ai sistemi di Dinamica del Volo, al fine di eseguire operazioni di anticollisione per i satelliti gestiti dalle Forze Armate, ovvero fornire supporto in tale campo per i satelliti gestiti da Società e/o Enti italiani, come previsto da accordi con il *Joint Space Operation Centre* del US STRATCOM e con l'Agenzia Spaziale Italiana.

Il corso fornirà allo Specialista le competenze per espletare le seguenti attività:

- eseguire la verifica delle prestazioni dei sistemi di Dinamica del Volo (*trend analysis*);
- eseguire le operazioni nominali non ricorrenti e di *contingency* applicando le Procedure Operative di Dinamica del Volo ed interviene in caso di "escalation" causate da avarie significative e/o allarmi;
- eseguire operazioni di anticollisione con l'utilizzo di moduli software aggiuntivi (es. *Satellite Tool Kit*).

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- approfondimenti di dinamica orbitale;
- pianificazione manovre orbitali;
- dettagli architetturali sistema FDS;
- prestazioni dei sistemi di dinamica del volo;
- moduli software aggiuntivi: STK;
- operazioni anticollisione.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve avere i seguenti requisiti: essere in possesso della qualifica/abilitazione di Controllore Dinamica del Volo OptSat-3000.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Specialista Dinamica del Volo OptSat-3000 è di 6 settimane, 2 per la parte di teorica e 4 per quella di OJT.

Durante l'OJT lo Specialista Dinamica del Volo OptSat-3000 svolgerà tutte le operazioni di competenza, eseguendo tutte le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico.

50.CORSO SUPERVISORE CENTRI DI CONTROLLO E STAZIONI TT&C OPTSAT-3000 - COD. S023A

OBIETTIVI DEL CORSO

Il corso ha il compito di istruire il Supervisore Centri di Controllo Satellite e Stazioni TT&C a sovrintendere, pianificare, coordinare e controllare tutte le attività inerenti alla gestione delle operazioni (nominali e di contingenza) svolte ai Centri di Controllo dei Satelliti e delle Stazioni TT&C. Il Supervisore è abilitato all'invio di comandi agli apparati della Stazione TT&C e dei Centri di Controllo.

Il corso fornirà al Supervisore le competenze per espletare le seguenti attività:

- pianificazione, coordinamento e verifica delle attività relative delle manutenzioni preventive e correttive relative alle Stazioni TT&C e Centri di controllo satellite;
- preparazione, redazione e verifica delle procedure relative alle stazioni TT&C e ai Centri di Controllo Satellite;
- verifica delle attività di invio dei comandi e ricezione delle telemetrie.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- antenne;
- *link budget*;
- emissioni fuori banda/interferenze;
- stazioni TT&C;
- sottosistema *network*;
- sala controllo satellite;
- modi di funzionamento del centro di controllo;
- architettura di sistema.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve aver seguito e superato il corso biennale in Ingegneria Astronautica (Scuola di Ingegneria Aerospaziale) o Elettronica/Telecomunicazioni oppure aver seguito e superato master/corso di specializzazione in "Sistemi Spaziali" e/o "Gestione operativa di satelliti".

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Supervisore Centri di Controllo e Stazioni TT&C OptSat-3000 è di 5 settimane, 3 per la parte di teorica e 2 per quella di OJT.

Durante l'OJT il Supervisore svolgerà tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

51.CORSO INGEGNERE SATELLITE OPTSAT-3000 - COD. S024A

OBIETTIVI DEL CORSO

Dare ai frequentatori un'approfondita conoscenza sulle caratteristiche e le operazioni dei sottosistemi che compongono il satellite OPTSAT-3000. Si descriveranno tutte le operazioni nominali e di contingenza. In particolare, il personale dovrà acquisire il necessario *know-how* per poter individuare i comportamenti anomali del satellite e scegliere prontamente la procedura più idonea alla messa in sicurezza del satellite. L'obiettivo del corso è fornire ai frequentatori una base teorico/pratica che permetta loro di svolgere l'attività di comando e controllo del satellite. Al termine del corso i frequentatori dovranno:

- conoscere la struttura hardware e le funzioni del sottosistema di controllo d'assetto;
- conoscere le funzionalità degli equipaggiamenti per il controllo d'assetto;
- conoscere la struttura hardware del computer di bordo e del software di volo;
- conoscere come si strutturano i telecomandi e telemetrie;
- conoscere la struttura e le funzioni del sottosistema propulsivo;
- conoscere la modalità di calcolo delle manovre orbitali;
- conoscere la struttura hardware e le funzioni del sottosistema EPS;
- conoscere le funzionalità degli equipaggiamenti per la distribuzione della potenza elettrica;
- conoscere la struttura hardware e le funzioni del sottosistema TCS;
- conoscere le funzionalità degli equipaggiamenti per il controllo termico;
- conoscere la struttura hardware e le funzioni del sottosistema TT&C;
- conoscere la struttura hardware e le funzioni del sottosistema *Payload*;
- conoscere le funzionalità degli equipaggiamenti del *Payload*;
- conoscere le procedure nominali e di contingenza di tutti i sottosistemi satellite.

AREA

Controllo Satelliti.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- sottosistema di controllo d'assetto;
- sottosistema di propulsione;
- computer di bordo e codice di volo;
- *electric & power subsystem*;
- thermal control subsystem;
- sottosistema tt&c;
- sottosistema *payload*;
- dinamica del volo;
- concetto operativo di missione.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

Per poter accedere alla frequenza di tale corso il personale deve aver:

- seguito e superato il corso biennale in Ingegneria Astronautica (Scuola di Ingegneria Aerospaziale) o Elettronica/Telecomunicazioni oppure aver seguito e superato

master/corso di specializzazione in “Sistemi Spaziali” e/o “Gestione operativa di satelliti”;

- svolto e superato il corso Supervisore sala controllo satellite e stazioni TT&C.

DURATA DEL CORSO

La durata prevista del corso per ottenere la qualifica/abilitazione di Ingegnere Satellite OptSat-3000 è di 8 settimane, 4 per la parte di teorica e 4 per quella di OJT.

Durante l'OJT il Supervisore svolgerà tutte le operazioni di competenza, eseguendo le procedure nominali e di contingenza secondo quanto previsto dalle schede relative a tale figura professionale.

VERIFICHE

Al termine della sessione teorica del corso, i frequentatori dovranno svolgere un esame scritto (test a scelta multipla suggerita). Al termine della fase di OJT si svolgerà un esame pratico al simulatore satellite.

AREA SOFTWARE, APPLICATIVI E E-LEARNING

52.CORSO AVANZATO DI PROGETTAZIONE E GESTIONE DATABASE - COD. FT68A

OBIETTIVI DEL CORSO

Il Corso fornirà le conoscenze per formare figure professionali in grado di progettare e gestire Basi Dati col necessario *know-how*.

In particolare, durante il corso il frequentatore sarà addestrato a:

- progettare una Base Dati con le metodologie più utilizzate;
- usare il linguaggio di interrogazione SQL.

AREA

Software/Applicativi/E-Learning.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- generalità sui database;
- progettazione di basi di dati in sicurezza (*Secure by Design*);
- linguaggio SQL;
- *compliance* al *General Data Protection Regulation* (GDPR).

PERIODICITA E DURATA DEL CORSO

Il corso si svolge una volta all'anno ed ha una durata di 2 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

53.CORSO AVANZATO DI PROGETTAZIONE E GESTIONE DATABASE ORACLE - COD. FT69A

OBIETTIVI DEL CORSO

Il Corso formerà figure professionali in grado di progettare e gestire Basi Dati in ambiente Oracle. In particolare, durante il corso l'allievo sarà addestrato a:

- configurare gestire ed implementare una Base Dati in ORACLE;
- risolvere problematiche di sicurezza (*Secure by Design*).

AREA

Software/Applicativi/E-Learning.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- introduzione al linguaggio PL/SQL;
- Oracle.NET;
- architettura del Database Server Oracle 11g, 12c e 18c;
- amministrazione del Database Server Oracle 11g, 12c e 18c;
- procedure di *backup* e *recovery*;
- progettazione di basi di dati in sicurezza (*Secure by Design*);
- *compliance* al *General Data Protection Regulation* (GDPR).

PERIODICITÀ E DURATA DEL CORSO

Il corso si svolge una volta all'anno ed ha una durata di 3 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

54. CORSO AVANZATO SU 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-learning¹⁰

- 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

- inizializzazione del sistema;
- il *boot* (*grub2*);
- sicurezza del grub;
- il processo *Systemd*;
- i target di sistema;
- il processo INIT (storia)
- la shellbash;
- utilizzo di altre *shell* (sh e csh)
- gestione degli utenti/gruppi;
- controlli amministrativi (comandi su e sudo)
- automazione del sistema;
- networking con Linux;
- configurazioni di rete;
- routing;
- gestione dei servizi di rete con *systemctl* (attivazione a richiesta e al *boot*)
- emulazione di terminale SSH;

¹⁰Argomenti trattati in maniera più esaustiva e differenziata rispetto al CORSO E-LEARNING SU S.O. LINUX BASE: COD. ET23B

- trasferimento di file con SFTP E SCP;
- configurazione dei servizi server (DNS, DHCP, NTP);
- condivisione in rete (NFS, SAMBA);
- aspetti di sicurezza;
- protocolli Wrapper.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

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

2. Di segretezza:

NOS non richiesto.

3. Categorie:

Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:

- 2 settimane in modalità *e-learning* sincrone (40 ore in piattaforma) con eventuali interventi via *web streaming* e 2 settimane in presenza.
 - Le attività a distanza sono disciplinate nell'Annesso IV.
- Per esigenze logistiche/sanitarie, il corso potrà essere svolto a distanza in modalità “*on-line training*” per un massimo di 8 frequentatori.

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

È PREVISTO ESAME FINALE (a termine fase in presenza)

55.CORSO AVANZATO SU SISTEMI OPERATIVI SERVER IN NETWORKING - COD. TE262A

OBIETTIVI DEL CORSO

Portare il frequentatore a conoscenza delle principali tecniche per:

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

AREA

Software/Applicativi/E-Learning.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- introduzione alla suite TCP/IP (*e-learning*);
- IP Routing. Risoluzione dei nomi NetBIOS;
- assegnazione automatica indirizzi IP con APIPA e DHCP;
- DHCP e risoluzione nomi con WINS;
- il servizio *Server DNS / Networking* con Linux / *networking* di base;
- configurazione in rete di un sistema, indirizzi e maschera di rete;
- attivazione e disattivazione delle schede e del servizio di rete;
- tabella di instradamento / *routing*: instradamento diretto e indiretto;
- configurazione di un sistema come *gateway*: controllo attivazione e disattivazione del *forwarding*;
- realizzazione di due reti con indirizzi IP e dominio / Prove di raggiungibilità;
- comandi *ping traceroute* e *TCP dump* / Configurazione del *file hosts*;
- i servizi di rete: *standalone* e via *xinetd* / Attivazione/disattivazione dei servizi;
- servizio *telnet*, *rlogin*, *Klogin SSH* / Servizio *ftp SFTP* / Il servizio *DNS*;
- introduzione a *bind 8* / Configurazione di un *DNS Master*;
- configurazione di un *DNS slave* / *Forwarding* di zone / *DNS* prove di *resolving*;
- inserimento di un server *DHCP* per ogni rete. / Il file *dhcpd.conf*;
- assegnazione di indirizzi randomici / Assegnazione di indirizzi prefissati;
- database degli affitti / Condivisione in rete / Il servizio *NFS* / *Nfs* e *rpc* / Il *portmapper*;
- configurazione di *nfs* con *yast2* / il file */etc/exports* / il comando *showmount*;
- prove di montaggio e smontaggio di un *filesystem* remoto;
- la cartella */mnt* / introduzione al protocollo *smb* / il servizio *samba*;
- configurazione di *samba* con *yast2* / condivisioni aperte e con autenticazione;
- il file *smb.conf* / condivisione tra macchine miste / creazione di un utente *Samba*;
- il database *smb passwd*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

a. Frequenza preventiva:

Corso Windows Server per Amministratori; corso Progettazione e gestione reti locali Cod.T235J e corso S.O. LINUX: COD. T285A;

b. Conoscenze basiche richieste:

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

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

2. Di segretezza:

NOS non richiesto.

3. Categorie:

Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:

- 1 settimana in modalità *e-learning asincrono* (15 ore) e 2 settimane in presenza;
- percentuale laboratorio: 20%;

– Le attività a distanza sono disciplinate nell'Annesso IV.

Per esigenze logistiche/sanitarie, il corso potrà essere svolto a distanza in modalità "*on-line training*" per un massimo di 8 frequentatori.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

È PREVISTO UN ESAME FINALE.

56.CORSO AMMINISTRATORI SISTEMA DI COMANDO E CONTROLLO JOINT – C2I ADV - COD. T293A

OBIETTIVI DEL CORSO

Fornire al personale destinato ad amministrare il C2IADV (Sistema di Comando e Controllo Joint a livello strategico), le conoscenze necessarie atte ad implementare, configurare e amministrare il Sistema di Comando e Controllo C2I, integrato con i *Functional Service Area* (FAS) Nazionali e della NATO, sulla base di tecnologie *Service Oriented Architecture* (SOA). Inoltre, si prefigge l'obiettivo di garantire ai frequentatori le necessarie conoscenze inerenti il contesto di architettura informativa evoluta che costituisce il Sistema e le necessarie implementazioni da attuare al fine di garantire l'interoperabilità del C2IADV, permettendo allo stesso di ricevere informazioni da Sistemi C2 Nazionali (es.:SIACCON2), Sistemi C2 NATO (es.: MCCIS, NIRIS), interoperare con Sistemi C2 Europei, Internazionali o di Comandi di coalizioni schierati nei teatri operativi.

AREA

Software/Applicativi/E-Learning.

PROGRAMMA / ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- introduzione e panoramica del sistema;
- descrizione delle versioni C2I ADV Nazionale e NATO;
- descrizione principali funzioni Weblogic Oracle;
- descrizione principali funzioni ESRI Server (Cartografico);
- descrizione e Configurazione della struttura virtuale:
 - introduzione all'ambiente Vsphere;
 - creazione e configurazione dell'architettura virtuale;
 - networking in ambiente virtuale.
- Introduzione e Configurazione C2I NATO:
 - descrizione dell'ambiente Windows (Domini, *Active Directory*, GPO, DNS, IIS);
 - *deployment* e configurazione delle *Virtual Machines* (VMs);
 - configurazione e verifica dei controlli di sicurezza (*Policy*, *Rewrite Rule*, *Firewall*, ecc.);
 - sequenza di avvio e verifica delle funzionalità del Sistema;
 - relazioni di Trust con Domini esterni, Gestione utenze e Training;
 - training C2I NATO.
- Introduzione e Configurazione C2I Nazionale:
 - descrizione dell'ambiente Linux, training sui comandi in ambiente *bash*;
 - *deployment* e Configurazione delle *Virtual Machines* (VMs);
 - configurazione e verifica dei Controlli di sicurezza (*Rewrite Rule*, *Firewall*, ecc.);
 - sequenza di avvio e verifica delle funzionalità del Sistema;
 - configurazioni e descrizione componenti Oracle IAM;
 - gestione utenze e Training IAM;
 - training C2I Nazionale.
- configurazioni per l'interoperabilità;
- replicatori FAS e *TroubleShooting* C2IADV.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

a. Frequenza preventiva:

- Windows server amministratori;
- Progettazione e gestione reti locali-cod.T235;
- Corso avanzato su S.O. Linux: cod.- T285A;
- Corso avanzato sui servizi di virtualizzazione: cod. -T281A.

b. Conoscenze basiche richieste:

Conoscenza pratica di ambienti di rete, WINDOWS Server comprendente il protocollo TCP/IP, il servizio DNS, IISe *Active Directory*, conoscenze S.O. Linux, Sistemi di Virtualizzazione (VmWare-Vsphere5.x).

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 8.

DURATA DEL CORSO:

3 settimane in presenza.

È PREVISTO ESAME FINALE.

57.CORSO ADVANCED MySQL FOR HIGH AVAILABILITY AND PERFORMANCE – COD. TE297A

OBIETTIVI DEL CORSO

Fornire al frequentatore le conoscenze per implementare un'architettura *Data Base* (DB) a disponibilità elevata (*High Availability*) utile a garantire che il *database* sia attivo ed in esecuzione per il 99,99% del tempo, anche durante le attività di *backup*, durante eventi pianificati di manutenzione ed eventi non pianificati come in caso di errore hardware.

Il frequentatore sarà guidato nella scelta delle diverse strategie di *backup* e di *recovery*. In particolare, *backup* e *recovery* logico, *backup* e *recovery* fisico a freddo ed a caldo.

Inoltre, saranno trattate le tematiche che riguardano l'upgrade delle versioni di MySQL e la configurazione di *tool* di *benchmark* del *database*.

AREA

Software/Applicativi/E-learning.

PROGRAMMA / ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- nozioni generali sulla replica, i backup, ripasso comandi base e verifica delle conoscenze (*e-learning*);
- configurazione di MySQL;
- i Binary Log;
- concetti di *Backup and Recovery*;
- *backup* fisico a freddo e *Restore*, *Backup* fisico a caldo e *Restore*;
- pianificazione *backup* tramite *workbench commercial*;
- *backup* logico di tabelle / *Database* /Struttura dati / tutto il *database*;
- *restore* da *backup* logico;
- *restore* fino all'ultima transazione committata;
- *restore Point In Time* (recupero situazione da errore utente);
- *backup* logico con dati cifrati;
- *replica master slave & Replica master master*;
- innodb *Cluster*;
- MySQL *Router*;
- *upgrade* all'interno della stessa versione principale di MySQL con recupero dei dati;
- *upgrade* da una versione di MySQL ad un'altra e relativo passaggio dei dati;
- controllo delle connessioni con SSL;
- sysbench.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

a. Frequenza preventiva:

- CORSO MYSQL;
- LINGUAGGIO SQL E GESTIONE DATABASE OPEN SOURCE COD. TE291J;

b. Conoscenze basiche richieste:

- buone conoscenze di Informatica e Reti;
- conoscenza di S.O. lato server;
- nozioni sui database e linguaggio SQL.

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 DEL CORSO:

1 settimana in modalità *e-learning asincrono* (15 ore in piattaforma) e 1 settimana in presenza.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

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

È PREVISTO ESAME FINALE (a termine fase in presenza).

58.CORSO SISTEMA OPERATIVO WINDOWS 2016 SERVER - COD. T291A

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: progettazione e gestione reti locali Cod. RE235J;
- b. Conoscenze basiche richieste:
 - ottima conoscenza ed esperienza di amministrazione di un sistema operativo Windows Server;
 - ottima conoscenza ed esperienza di gestione Reti e *Networking* e dei protocolli di rete TCP/IP;
 - conoscenza ed esperienza con AD DS e nozioni di Sicurezza Informatica.
- 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 DEL CORSO:

4 settimane di cui 40% di laboratorio.

Per esigenze logistiche/sanitarie, il corso potrà essere svolto a distanza in modalità “*on-line training*” per un massimo di 10 frequentatori.

È PREVISTO UN ESAME INTERMEDIO.

È PREVISTO UN ESAME FINALE.

59.CORSO SISTEMA OPERATIVO WINDOWS 2019 SERVER - COD. T295A

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 server 2012/2016;
- b. Conoscenze basiche richieste:
 - ottima conoscenza ed esperienza di amministrazione di un sistema operativo Windows Server;
 - ottima conoscenza ed esperienza di gestione Reti e *Networking* e dei protocolli di rete TCP/IP;
 - conoscenza ed esperienza con AD DS e nozioni di Sicurezza Informatica.
- 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 DEL CORSO:

1 settimana di cui 50% di laboratorio.

Per esigenze logistiche/sanitarie, il corso potrà essere svolto a distanza in modalità “*on-line training*” per un massimo di 10 frequentatori.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

È PREVISTO UN ESAME FINALE.

60.CORSO AVANZATO PER AMMINISTRATORI S.O. UNIX/LINUX - COD. FT67A

OBIETTIVI DEL CORSO

Formare figure professionali in grado di configurare e gestire col necessario *know-how* sia una rete LAN, sia i sistemi ad essa connessi, sia le problematiche che una tale gestione impone su piattaforma Unix/Linux (Open Source).

In particolare, durante il corso l'allievo sarà addestrato a:

- Progettare e realizzare una rete LAN;
- Installare un Server Linux;
- Amministrare un sistema Server Linux con tutti i relativi servizi;
- Amministrare e gestire Utenti (permessi e controllo accessi);
- Amministrare e gestire problematiche di sicurezza.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- Linguaggi di programmazione per amministratori di sistema:
 - . shell;
 - . AWK e Perl.
- Amministrazione avanzata:
 - . i *file system* supportati da Linux, (ext2, ext3, xfs, jfs, etc);
 - . *backup* e *restore* in locale e via rete;
 - . *system activity reporting* analisi problematiche di errore e/o malfunzionamento;
 - . attivazione, gestione e *accounting* delle quote disco anche in funzione dei File System utilizzati.
- Gestione dei sistemi di memoria di massa:
 - . *disk array*;
 - . volumi logici (LVM);
 - . sistemi disco di rete.
- Gestione avanzata degli utenti:
 - . tecniche per l'autenticazione;
 - . LDAP;
 - . kerberos;
 - . interfacciamento con ambienti basati su tecnologie Microsoft.
- Cenni sulle tecniche di clusterizzazione e la realizzazione di sistemi a macchine virtuali:
 - . definizione e architettura di un sistema a cluster. Vantaggi e vincoli per la gestione di applicazioni critiche. Bilanciamento di carico e alta affidabilità. Prodotti disponibili;
 - . infrastruttura per la creazione di macchine virtuali. Principali prodotti commerciali e non attualmente disponibili (es. Xen, Vmware, VirtualBox).

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno ed ha una durata di 4 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

61.CORSO AVANZATO PER AMMINISTRATORE ORACLE - COD. FT70A

OBIETTIVI DEL CORSO

Il Corso “Oracle amministratore” si prefigge di integrare la preparazione di figure professionali in grado di progettare e gestire Basi Dati in ambiente Oracle. In particolare, durante il corso l’allievo approfondirà aspetti di Oracle 11g ed esaminerà l’evoluzione del prodotto realizzata con la versione Oracle 12c e 18c.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- Oracle 9i - backup and recovery (RMAN) e Data Guard;
- Oracle 9i – tuning;
- Oracle database 10g New Features;
- Cenni su Oracle Forms Developer;
- backup and recovery (RMAN) e Data Guard;
- tuning;
- Oracle Database New Features;
- cenni su Oracle Forms Developer;
- introduzione alle versioni 11g, 12c e 18c;
- funzionalità principali delle versioni 11g, 12c e 18c.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno ed ha una durata di 3 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d’iscrizione.

62.CORSO AVANZATO LINGUAGGIO PHP - COD. FT80A

OBIETTIVI DEL CORSO

Fornire strumenti tecnologici e metodologici per la definizione di pagine e siti web utilizzando il linguaggio PHP.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- introduzione al linguaggio PHP;
- le componenti di base del linguaggio;
- istruzioni, *array*, funzioni nel linguaggio PHP;
- funzioni personalizzate;
- componenti avanzate del linguaggio PHP;
- interazione con le basi di dati: MySQL ed Access;
- interazione con il linguaggio XML;
- creazione di siti dinamici con PHP;
- aspetti futuri delle nuove versioni.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 4 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

63.CORSO AVANZATO LINGUAGGIO JAVASCRIPT - COD. FT82A

OBIETTIVI DEL CORSO

Il Corso ha l'obiettivo di fornire nozioni necessarie a formare programmatori orientati ad applicazioni gestionali. Si svilupperanno lezioni teoriche ed applicazioni pratiche a livello basico del Linguaggio JAVASCRIPT.

AREA

Software e Applicativi.

PROGRAMMA

Il programma didattico comprenderà i seguenti argomenti:

- introduzione al modello client server e al protocollo TCP/IP;
- introduzione al linguaggio di markup HTML ed ai CSS per la definizione di pagine web;
- introduzione al linguaggio JavaScript;
- implementazione di script JavaScript;
- integrazione di JavaScript con HTML e CSS;
- gestione ed utilizzo dei cookie con JavaScript.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e si articolerà, nell'arco di tre settimane, in 90 ore di lezioni (teoriche e/o pratiche) più 3 ore per l'esame finale (somministrazione e correzione).

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

64.CORSO AVANZATO PROGRAMMAZIONE OBJECT ORIENTED E LINGUAGGIO JAVA - COD. FT73A

OBIETTIVI DEL CORSO

Fornire ai partecipanti gli strumenti necessari per affrontare tutte le fasi per la realizzazione di un prodotto software, dall'analisi dei requisiti alla progettazione e realizzazione usando il linguaggio Java. Comprendere i dettagli della filosofia ispiratrice di java ed acquisire la capacità di utilizzarne gli aspetti evoluti. Essere in grado di interfacciarsi ad un *Database* usando JDBC e di realizzare un'applicazione su web. Acquisire la capacità di progettare applicativi *web-based* con tecnologia Java, JSP, Servlet.

AREA

Software e Applicativi.

PROGRAMMA

a. La prima fase sarà articolata su cinque moduli:

- Modulo 1: Elementi di programmazione in Java;
- Modulo 2: Classi ed oggetti, ereditarietà;
- Modulo 3: Interfacce e classi annidate;
- Modulo 4: Interfaccia grafica ed eccezioni;
- Modulo 5: Multithreading e gestione dei flussi.

b. La seconda fase sarà articolata su tre moduli:

- Modulo 1: Java Database Connectivity;
- Modulo 2: Nozioni di UML;
- Modulo 3: Nozioni su Servlet, JavaBean e Jsp.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 5 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

65.CORSO AVANZATO DI PROGRAMMAZIONE IN LINGUAGGIO C/C++ - COD. FT74A

OBIETTIVI DEL CORSO

Formare figure professionali in grado di progettare e redigere codice correttamente funzionante in linguaggio C++.

AREA

Software e Applicativi.

PROGRAMMA

Le lezioni si articolano in teoriche, progettuali ed applicazioni pratiche. Vengono essenzialmente trattati i seguenti argomenti:

- elementi di progettazione di programmi basata sugli oggetti;
- elementi di progettazione di programmi orientata agli oggetti;
- sintassi del linguaggio di programmazione C++.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 5 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

66.CORSO AVANZATO SUL LINGUAGGIO XML - COD. FT277A

OBIETTIVI DEL CORSO

Fornire strumenti tecnologici e metodologici per la manipolazione di dati e documenti XML.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- a. Il Linguaggio XML:
 - introduzione, Storia di XML, il ruolo del W3C;
 - comprensione della sintassi e della semantica del linguaggio;
 - rappresentazione di dati e informazioni attraverso XML.
- b. Linguaggi per la manipolazione di documenti XML:
 - comprensione della sintassi e della semantica dei linguaggi XPath, XSL e XQuery: standard affermati, promossi dal consorzio W3C;
 - estrazione di dati da documenti XML, trasformazioni di documenti XML.
- c. XML e le basi di dati relazionali:
 - metodologie per l'interscambio di dati attraverso XML;
 - metodologie per memorizzare dati XML nelle basi di dati relazionali;
 - metodologie per la creazione di documenti XML a partire da dati memorizzati in basi di dati relazionali.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 2 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

67.CORSO AVANZATO BASE DATI PER IL SUPPORTO ALLE DECISIONI (DATA WAREHOUSE) - COD. FT71A

OBIETTIVI DEL CORSO

Formare professionalità nella progettazione e la realizzazione di *Data Warehouse Compliance*. In particolare, saranno fornite le conoscenze per raggiungere i seguenti obiettivi:

- saper riconoscere i principi base dei sistemi di supporto alle decisioni;
- conoscere l'architettura SW di un sistema di *Data Warehouse*;
- saper progettare un *Data Warehouse* in sicurezza (*Secure by Design*);
- compliance dei sistemi al *General Data Protection Regulation* (GDPR);
- saper realizzare un processo di *Data Warehousing* con strumenti professionali;
- saper realizzare operazioni di analisi dei dati memorizzati in un *data Warehouse*.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

Prima parte

- introduzione al *data warehousing*;
- il ciclo di vita dei sistemi di *data warehousing*;
- analisi e riconciliazione delle fonti dati;
- modellazione e progettazione concettuale;
- carico di lavoro e volume dati;
- modellazione e progettazione logica;
- progettazione dell'alimentazione;
- progettazione fisica;
- *business intelligence*: oltre il *Data Warehouse*.

Seconda parte

- strumenti Oracle per il *Dataware Housing*;
- Oracle *Warehouse Builder*;
- Oracle *Business Intelligence*.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 4 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

68.CORSO ANALISTI DI SISTEMI - COD. FT78A

OBIETTIVI DEL CORSO

Fornire le conoscenze per formare figure professionali in grado di:

- saper definire e disegnare la propria realtà aziendale in termini di processi e di dati coinvolti;
- saper individuare punti critici e lacune informative nella gestione dei processi aziendali a partire dagli obiettivi posti e coerentemente con i vincoli reali;
- conoscere le metodologie alla base di tali tipi di attività, preferendo un approccio del tipo "*Object Oriented*";
- saper realizzare l'*Analysis & Design* di un sistema software attraverso metodologie orientate agli oggetti;
- avere conoscenze per la gestione del progetto, sia in termini funzionali che economici;
- avere le conoscenze di base, sia nel campo della tecnologia informatica che di quella comunicativa, per valutare l'architettura di riferimento del nuovo progetto, come responsabilità diretta o in cooperazione con gli altri responsabili.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- sistemi informativi e metodologie di sviluppo del software (*Secure by Design*);
- il linguaggio UML;
- il modello *Object-Oriented*;
- metodologie e strumenti di analisi;
- metodologie di progettazione ad oggetti;
- tecniche di organizzazione degli archivi;
- *Quality Assurance*;
- tecniche di gestione di progetti;
- compliance dei sistemi al *General Data Protection Regulation* (GDPR);
- misurazione del software.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 8 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

69.CORSO PROGRAMMAZIONE DI BASE FASE 1 - COD. FT76A

OBIETTIVI DEL CORSO

Formare programmatori orientati ad applicazioni gestionali.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- Modulo 1:
 - . architettura dei sistemi e dei dati (*Secure by Design*);
 - . compliance dei sistemi al General Data Protection Regulation (GDPR);
 - . Hardware;
 - . software di base;
 - . software applicativo
 - . cenni sui linguaggi HTML5 e CSS.

- Modulo 2:
 - . logiche delle applicazioni.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 3 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

70.CORSO PROGRAMMAZIONE DI BASE FASE 2 LINGUAGGIO C - COD. FT77A

OBIETTIVI DEL CORSO

Formare programmatori orientati ad applicazioni gestionali in riferimento al Linguaggio di programmazione C.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- introduzione al linguaggio C;
- costanti e variabili;
- operatori;
- strutture di controllo;
- input/output da console;
- puntatori;
- input/output da file;
- arrays;
- funzioni;
- strutture dati e gestione della memoria.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 5 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

71.CORSO DI FORMAZIONE AVANZATA IN TECNOLOGIE DI SVILUPPO SOFTWARE E WEB ASP.NET - COD. FT81A

OBIETTIVI DEL CORSO

Fornire le conoscenze necessarie per la progettazione e lo sviluppo in autonomia di portali web con particolare riferimento allo sviluppo di portali *web* basati su ASP.NET. In particolare, nella parte iniziale del Corso, gli studenti comprenderanno le basi del modello *client-server* su cui si basa il web e studieranno i principali protocolli di comunicazione alla base del web ed i linguaggi di markup (HTML, XML).

La parte centrale del corso sarà focalizzata sullo studio delle tecnologie di sviluppo per il *web*. Più specificamente, verranno introdotti il linguaggio JavaScript ed il linguaggio PHP come base per lo sviluppo, rispettivamente, del lato *client* e del lato *server* del *web*. Nell'ultima parte il corso si concentrerà sul *framework* ASP.NET come alternativa alle tecnologie basate su PHP e JavaScript per lo sviluppo di portali *web*.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- introduzione al modello client server e al protocollo TCP/IP;
- protocolli del livello applicativo: HTTP, FTP, DNS;
- protocolli per la posta elettronica: POP, IMAP, SMTP;
- introduzione al linguaggio di *markup* HTML ed ai CSS per la definizione di pagine *web*;
- programmazione web lato server:
 - . introduzione al linguaggio PHP;
 - . generazione di pagine dinamiche con PHP;
- gestione delle sessioni;
- introduzione alla programmazione *web* lato *client*:
 - . basi del linguaggio JavaScript;
 - . implementazione di semplici *script* JavaScript;
 - . gestione ed utilizzo dei *cookie* con JavaScript;
- definizione di linguaggi di *markup*:
 - . introduzione allo standard XML;
 - . trasformazione di XML: il linguaggio XSLT;
- programmazione in .NET;
- introduzione al *framework* ASP.NET;
- costruzione di portali basati su HTML5 e CCS3 con ASP.NET.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 4 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

72.CORSO M&S EDUCATIONAL PACKAGE ADVANCED: MS-EPA - COD. FT02A

OBIETTIVI DEL CORSO

Fornire conoscenze avanzate delle tecniche e delle metodologie di modellistica e simulazione, di verifica, validazione e *testing*, di aspetti di interoperabilità, con particolare attenzione alle architetture di alto livello ed ai metodi di gestione progettuale applicata alla simulazione.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

Modeling & Simulation (M&S):

- *M&S Background & Knowledge Assessment;*
- *M&S Topics: M&S Definition and Paradigms, M&S Basic Concepts, M&S Input;*
- *M&S Validity, M&S Output Analysis, M&S Variance, M&S Experimental Design;*
- *M&S Case Studies: Green Log Simulator;*
- *M&S Exercises: A.P.E. - Automated Production Educator;*
- *M&S Technical and Scientific References;*
- *M&S Networking & References;*
- *M&S Foreground and Knowledge Assessment: Regular M&S Certification.*

PM for Simulation Projects:

- *PM Background & Knowledge Assessment;*
- *Topics: Project Management in M&S Projects, VV&A for M&S Projects, Critical Issues in M&S Projects, Tools and Services for M&S Projects, PM & FEDEP, Simulation Based Acquisition;*
- *Case Studies: Web Integrated Logistics Designer Projects (WILD I & II);*
- *Exercises: BABEL - BAbel Experience & Lessons;*
- *PM Technical and Scientific References;*
- *PM Networking & References;*
- *Foreground and Knowledge Assessment: Regular PM Certification;*
- *Interoperability & HLA;*
- *Interoperability & HLA Background & Knowledge Assessment;*
- *Topics: Interoperability, Distributed and Parallel Simulation, HLA Concepts and Definitions, Development of Computer Simulation Systems in HLA Framework, HLA Evolution, HLA Rules, Federation and Federate Rules, Federation management, Declaration management, Object management, Ownership management, Time management, Data distribution management, Support services, Declaration and Object Services, Ownership of responsibility for modelling, Logical time: ordering events in distributed simulation, Federation execution lifecycle, Data Distribution Management;*
- *Case Studies: PIOVRA (Polyfunctional Intelligent Operational Virtual Reality Agents) Federation;*
- *Exercises: YACHTS (Yet Another Cooperative High Level Architecture Training Software) Exercise;*
- *Interoperability & HLA Technical and Scientific References;*
- *Interoperability & HLA Networking & References;*
- *Interoperability & HLA Foreground and Knowledge Assessment: Regular HLA; Certification.*

VV&A:

- *VV&A Background & Knowledge Assessment;*
- *Topics: VV&A Concepts and Definition, VV&T Life Cycle, VV&T Principles, VV&T Techniques, VV&T Credibility Assessment, Methodologies, Mean Square pure Error (MSE), VV&A & FEDEP;*
- *Case Studies: PIOVRA (Polyfunctional Intelligent Operational Virtual Reality Agents) VV&A;*
- *Exercises: LIFTS (Learning Interactively Forefront Techniques for Simulation) Exercise;*
- *VV&A Technical and Scientific References;*
- *VV&A Networking & References;*
- *VV&A Foreground and Knowledge Assessment: Regular VV&A Certification.*

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 4 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

73.CORSO DI MODELLING & SIMULATION EDUCATIONAL PACKAGE FUNDAMENTALS: MS EPF - COD. FT01A

OBIETTIVI DEL CORSO

Il Corso di Formazione MS-EPF fornisce i fondamenti dei contesti e delle metodologie di modellistica e simulazione, di verifica, validazione e *testing*, di aspetti di interoperabilità e di gestione progettuale applicata alla simulazione.

AREA

Software e Applicativi.

PROGRAMMA

Il corso si articolerà sul seguente programma:

- *M&S Topics: Simulation Concepts, M&S Definitions, Simulation Paradigms, Continuous Simulation, Discrete Simulation, Virtual, Constructive & Live Simulation;*
- *M&S: Exercises: Bursting (Ballistic Unified Rockets Simulation Testing and Interactive Numerical Grinder) Exercise;*
- *Interoperability Topics: Parallel, Distributed and Interoperable Simulation, Reasons to Use Parallel / Distributed / Interoperable Simulation, Geographically Distributed Users/Resources, Standalone vs. Federated Simulation Systems, Principal Application Domains, Different Time Concepts, Simulation Time Concept, Simulation Taxonomy, Continuous Time Simulation, Time Stepped, Event Stepped, Historical Perspective, Basics Distributed Interactive Simulation (DIS), DIS Example, Basics High Level Architecture, HLA Example, DIS/HLA Comparison on an Example;*
- *Interoperability Case Studies: IA-CGF Intelligent Agent Computer Generated Forces;*
- *VV&A Topics: VV&A Definitions, Verification, Validation & Testing (VV&T) Introduction, Verification, Validation & Accreditation (VV&A) Introduction;*
- *VV&A Case Studies: VV&A in Military Applications: Project Management (PM) for Simulation Projects, M&S Projects as Specific Framework, M&S Project Development, M&S Projects: SOW, M&S Projects: WBS, M&S Project PLAN, Cost Drivers in M&S Projects, Team Working in M&S Projects, Communication in M&S Projects, Purchasing in M&S Projects;*
- *PM for Simulation Projects: Case Studies: LESNEX - Lean Simulation Network of Excellence Approach;*
- *PM for Simulation Projects: Exercises: CUMANA (Cooperative & Competitive Utility for Management and Advanced, Networking skill Acquisition) Exercise.*

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 1 settimana.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

AREA INFOSEC E INFORMATION ASSURANCE

74.CORSO PER 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 e personale civile della Difesa impiegati/designati a ricoprire incarichi nel settore CIS/COMSEC.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 10.

DURATA DEL CORSO:

2 settimane: 1 settimana in modalit  *e-learning* asincrono (15 ore) e 1 settimana in presenza.

MODALIT  DI SVOLGIMENTO

Le attivit  a distanza sono disciplinate nell'Annesso IV.

È PREVISTO UN ESAME FINALE.

75.CORSO 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:
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 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.

È PREVISTO UN ESAME FINALE.

76.CORSO 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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:

1 settimana.

È PREVISTO UN ESAME FINALE.

77.CORSO PER AMMINISTRATORE CIFRANTI IP CON SISTEMA KNMS - COD. J433A

OBIETTIVI DEL CORSO

Fornire ai frequentatori, le conoscenze tecniche sul funzionamento del software applicativo K.N.M.S. 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 Cifranti CM 2000 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 e personale civile della Difesa, impiegati/designati a ricoprire incarichi nel settore COMSEC.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 8.

DURATA DEL CORSO:

1 settimana.

È PREVISTO UN ESAME FINALE.

78. CORSO PER 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 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.

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.

79.CORSO PER UFFICIALI ALLA SICUREZZA CIS DESIGNATI - COD. J451A

OBIETTIVI DEL CORSO

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

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.

È PREVISTO UN ESAME FINALE.

80.CORSO PER 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 e personale civile della Difesa, impiegati/designati a ricoprire incarichi nel settore COMSEC.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 10.

DURATA DEL CORSO:

2 settimane: 1 settimana in modalit  *e-learning* asincrono (15 ore) e 1 settimana in presenza.

MODALIT  DI SVOLGIMENTO

Le attivit  a distanza sono disciplinate nell'Annesso IV.

È PREVISTO UN ESAME FINALE.

81.CORSO PER AMMINISTRATORE CIFRANTI IP CON SISTEMA KNMS 2100 IP - 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 e personale civile della Difesa, impiegati/designati a ricoprire incarichi nel settore COMSEC.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 8.

DURATA DEL CORSO:

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

MODALIT  DI SVOLGIMENTO

Le attivit  a distanza sono disciplinate nell'Annesso IV.

È PREVISTO UN ESAME FINALE

82.CORSO IT-EKMS CUSTODE CIFRA PER UTENTI LDF DELLE FF.AA. – COD. J450A

OBIETTIVI DEL CORSO

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

AREA

INFOSEC e *Information Assurance*

REQUISITI MINIMI PER L'AMMISSIONE

1. Professionali:

- a. Frequenza preventiva: N.N.;
- 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 e personale civile della Difesa, impiegati/designati a ricoprire incarichi nel settore COMSEC.

NUMERO FREQUENTATORI AMMESSI: Fino ad un massimo di 8.

DURATA DEL CORSO:

1 settimana.

È PREVISTO UN ESAME FINALE.

AREA CYBER DEFENCE, FORENSICS & LAW

83.CORSO IN DIGITAL FORENSICS – COD. FY15P

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, Forensics & Law

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 di analisi e recupero dati da supporti di memoria dei principali PC, server e dispositivi mobili;
- consulente Tecnico di Ufficio (CTU) e di Parte (CTP).

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.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 3 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

84. CORSO SU DATA PROTECTION E DATA GOVERNANCE – COD. FY16P

OBIETTIVI DEL CORSO

Il Corso ha l'obiettivo di fornire competenze sull'analisi dei profili di responsabilità, delle modalità ispettive, delle sanzioni, del ruolo essenziale del Data Protection Officer nell'adeguamento e nelle verifiche, con attenzione anche al quadro sanzionatorio negli altri Paesi europei ed alla "modularità" dei profili di responsabilità. Il corso dovrà inoltre fornire competenze fondamentali su gestione e protezione dei dati e dei sistemi, nonché sviluppare conoscenza e consapevolezza relativamente a privacy e trattamento dei dati.

AREA

Cyber Defence, Forensics & Law

RUOLI E POSIZIONI RICOPRIBILI

Il Corso si propone di formare figure professionali nell'area della Cyber che saranno in grado di assumere posizioni di Data Protection Officer.

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 alla luce del D.Lgs. 101/2018;
- 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*;
- valutazioni di progetti coinvolgenti dati e che richiedono un parere di fattibilità da parte del Garante;
- sicurezza nel *cloud*.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 4 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

85.CORSO PROPEDEUTICO SU MALWARE ANALYSIS – COD. FY17P

OBIETTIVI DEL CORSO

Il Corso ha l'obiettivo di fornire competenze necessarie alla successiva frequenza del corso sul Malware Analysis.

AREA

Cyber Defence, Forensics & Law

RUOLI E POSIZIONI RICOPRIBILI

Il Corso si propone di formare figure professionali nell'area tecnologica della cyber e della Digital Forensics, che saranno in grado di assumere posizioni di esperto in Malware Analysis ed in attività forensi.

PROGRAMMA

Saranno fornite competenze teoriche e pratiche sui seguenti argomenti:

- sviluppo di un laboratorio contenente gli strumenti necessari per procedere all'analisi dei
- malware (disassembler, process dumper, imports rebuilding, ecc.);
- 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.).

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 2 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

86.CORSO SU MALWARE ANALYSIS – COD. FY18P

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, Forensics & Law

RUOLI E POSIZIONI RICOPRIBILI

Il Corso si propone di formare figure professionali nell'area tecnologica della Cyber Defence e della Digital Forensics, che saranno in grado di assumere posizioni di esperto in Malware Analysis ed in attività forensi.

PROGRAMMA

Saranno fornite competenze teoriche e pratiche sui seguenti argomenti:

- 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.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 2 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

87.CORSO SULLA GESTIONE DELLA SICUREZZA DEI DATA CENTRE – COD. FY19P

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, Forensics & Law

RUOLI E POSIZIONI RICOPRIBILI

Il Corso si propone di formare figure professionali nell'area della Governance Cyber che saranno in grado di assumere posizioni di esperto in gestione di centri di elaborazione dati.

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 associate;
- *Privacy by Default e by Design*;
- *Disaster Recovery e Business Continuity*.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 4 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

88.CORSO SULLA BIG DATA ANALYSIS – COD. FY20P

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, Forensics & Law

RUOLI E POSIZIONI RICOPRIBILI

Il Corso si propone di formare figure professionali nell'area tecnologica della Cyber e della Digital Forensics, che saranno in grado di comprendere i Big Data e di effettuare delle analisi su di essi.

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).

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 3 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

89.CORSO NETWORK FORENSICS – COD. FY21P

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, Forensics & Law

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.

PERIODICITÀ E DURATA DEL CORSO:

Il corso si svolge una volta all'anno e ha una durata di 3 settimane.

IN ANNESSO III:

- caratteristiche e requisiti dei frequentatori;
- verifiche;
- conseguimento del titolo;
- posti disponibili;
- modalità d'iscrizione.

90.CORSO CYBER NETWORK ANALYSIS – COD. Y446A

OBIETTIVI DEL CORSO

Far acquisire al personale del Comparto Difesa destinato ad operare nell'ambito della *Cyber Defence* ai sensi di Legge e dei regolamenti di SMD, le nozioni e le tecniche utili ad analizzare quanto avviene sulla propria infrastruttura, così da rilevare, caratterizzare ed identificare eventi non previsti o deliberati, interni o prodotti dall'attaccante. Sensibilizzare il personale sulle potenziali criticità derivanti da tali attività.

Saranno impiegati progetti open source (Suricata, Bro/Zeek, ELK *stack*, Evebox, Netdata, TIG *stack*, Debian Buster ecc.).

AREA

Cyber Defence, Forensics & Law.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- competenze e figure professionali dedicate e designate;
- criticità e violazioni;
- obblighi conseguenti;
- laboratorio suricata;
- laboratorio Bro/Zeek;
- network analysis panoramica sistemi;
- sistemi collettori di tipo metrico e di sicurezza;
- laboratorio Evebox e Netdata;
- laboratorio TIG stack e ELK stack;
- cenni su Sistemi SIEM in uso nella Difesa;
- laboratorio esempio sistema integrato di monitoraggio *Network* (NOC);
- laboratorio esempio sistema integrato di monitoraggio *Network Security* (SOC).

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva:N.N.;
- b. Conoscenze basiche richieste:
Buona conoscenza sistemi operativi server (Microsoft Windows/Linux), dispositivi (switch/router/firewall) e protocolli di rete (TCP/IP), Windows Server;
- c. Studio preventivo sinossi / testi propedeutici:
Progetti open source: Suricata, Bro/Zeek, Ossec, InfluxDB, Grafana, Telegraf, Elasticsearch, Filebeat, Debian Buster.

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.

È PREVISTO ESAME FINALE.

91. CORSO CYBER NETWORK PROTECTION – COD. YE447A

OBIETTIVI DEL CORSO

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

AREA

Cyber Defence, Forensics & Law.

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;
- Uso di MITRE Caldera;
- Applicare la Cyber Kill Chain;

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: Corso Fondamenti di Cyber Defence;
- 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 10.

DURATA DEL CORSO:

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

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

E' PREVISTO UN TEST DI INGRESSO SBARRANTE, SUL PROGRAMMA SVOLTO DURANTE LA FASE E-LEARNING ED UN ESAME FINALE.

92. CORSO AVANZATO VULNERABILITY ASSESSMENT (V.A.) – COD. YE449A

OBIETTIVI DEL CORSO

Fornire al personale del Comparto Difesa che ha già frequentato il Corso *Vulnerability Assessment* - COD. YE448J le conoscenze relative alle tecniche avanzate per il rilevamento di *vulnerabilità di sicurezza* e l'eliminazione di falsi positivi/negativi.

AREA

Cyber Defence, Forensics & Law.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- il *Vulnerability Assessment* ed il *Penetration Testing* (P.T.);
- metodologie e *best practices* per il *Vulnerability Assessment*;
- *Network Discovery*;
- *Host Discovery*;
- *Port Discovery*;
- *Application Identification*;
- *Vulnerability Discovery/Identification*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali

- a. Frequenza preventiva: Corso *Vulnerability Assessment* - COD. YE448J
- b. In alternativa il personale deve possedere le seguenti conoscenze: 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. *Vulnerability disclosure, identifier e repository. Common Platform Enumeration. Common Weakness Enumeration, Security Content Automation Protocol, Open Vulnerability and Assessment Language*. Principali programmi di *vulnerability scanning*.
- c. Studio preventivo sinossi / testi propedeutici: RFC/STD Internet per i protocolli di rete TCP/IP, 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 e Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 10.

DURATA DEL CORSO: 2 settimane: 1 settimana in *e-learning* asincrono e 1 settimana in presenza;

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

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

93. CORSO ENDPOINT HARDENING - COD. Y452A

OBIETTIVI DEL CORSO

Fornire al personale destinato ad operare nell'ambito della *Cyber Defence*, i principi, le tecniche e gli strumenti per definire, applicare, mantenere e controllare le politiche di configurazione di sicurezza ovvero l'*hardening* degli *endpoint* facenti parte dell'infrastruttura.

AREA

Cyber Defence, Forensics & Law.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- introduzione e riferimenti normativi SMD e NATO.
- best practices:
 - . CIS Benchmark;
 - . DISA STIGs/NSA I.A. Guidance;
 - . Altri istituti/società/enti governativi;
 - . Vendors.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: N.N.;
- b. Conoscenze basiche richieste:
Sistemi operativi server (Microsoft Windows/Linux), dispositivi (*switch/router*), *hosted hypervisor* (VMWare/VirtualBox) e protocolli di rete (TCP/IP);
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 10.

DURATA DEL CORSO:

1 settimana.

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

94. CORSO COMPUTER EMERGENCY/INCIDENT RESPONSE TEAM - COD. EY445A

OBIETTIVI DEL CORSO

Far apprendere i modelli organizzativi sui quali poter creare un CERT/CIRT (o 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, Forensics & Law.

PROGRAMMA/ARGOMENTI TRATTATI

- Introduzione
- Panoramica ed implementazione dei modelli organizzativi proposti dal CERT/CC presso la Carnegie Mellon University e dall'European Agency for Cybersecurity (ENISA)
- Gestione delle segnalazioni di eventi rilevanti per la sicurezza dei sistemi informativi della propria constituency
- Produzione di avvisi, bollettini e notizie
- Attività di laboratorio

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 25.

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

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

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

95. CORSO SU DoS e DDoS - ATTACK & MITIGATION - COD. Y454A

OBIETTIVI DEL CORSO

Corso teorico-pratico sul Denial Of Service (DOS) e sul Distributed Denial Of Service (DDOS), attacco in grado di impattare su uno degli elementi della triade della sicurezza informatica: la disponibilità del servizio. Si intendono quindi analizzare le motivazioni dell'attaccante, richiamare talune nozioni sui sistemi ICT elencare i meccanismi sfruttati dall'attaccante; strumenti e le misure da porre in essere per garantire la *Business Continuity*.

AREA

Cyber Defence, Forensics & Law.

PROGRAMMA/ARGOMENTI TRATTATI

Introduzione:

- cos'è il DOS/DDOS?
- terminologia

L'attaccante:

- motivazione
- skill
- strumenti
- TTPs

ICT:

- stack protocollari;
- dispositivi, implementazioni software, throughput
- la superficie d'attacco
- l'Internet Of Things

Tipologie di Attacchi

- volumetrici
- SYN FLOOD
- *socket exhaustion*;
- *reflection & amplification*;
- *anycast*;
- *backscatter*;
- DNS & NTP *Reflection*;

Contromisure

- analisi del rischio e dimensionamento
- prevenzione
- mitigazione
- il ruolo delle content delivery networks
- utilizzo di strumenti per Packet Forging, analisi di PCAP.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: N.N..
- b. Conoscenze basiche richieste: Buona conoscenza del modello OSI e dello *stack* TCP/IP, dei web server e della *shell* Linux.
- 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: 1 settimana di cui 25% di laboratorio.

È PREVISTO UN ESAME FINALE.

96. CORSO 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

PROGRAMMA / ARGOMENTI TRATTATI

- Concetti di base di Cyber Threat Intelligence;
- Processo operativo;

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- Frequenza preventiva: Corso Fondamenti di Cyber Defence
- 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.
- 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: 1 settimana

E' PREVISTO UN TEST DI INGRESSO NON SBARRANTE ED UN ESAME FINALE.

97. CORSO RESPONSABILE DELLA CONTINUITA' OPERATIVA - COD. Y456A

OBIETTIVI DEL CORSO

Fornire ai partecipanti la conoscenza della metodologia di gestione del rischio, le principali tecniche di valutazione dei rischi, l'impostazione della Business Impact Analysis (BIA), l'attuazione e la valutazione della corretta implementazione e dell'efficacia di un sistema di gestione della continuità operativa (BCMS) in conformità a ISO 22301:2019.

AREA

CYBER DEFENCE

PROGRAMMA / ARGOMENTI TRATTATI

- Concetti fondamentali della gestione del rischio;
- Il processo di valutazione dei rischi, coerentemente con ISO 31000;
- Selezione delle tecniche per la valutazione dei rischi, con riferimento a ISO 31010;
- La BIA come tecnica di valutazione dei rischi connessi a eventi potenzialmente distruttivi per la continuità operativa, seguendo le linee guida ISO/TS 22317:2015;
- Concetti fondamentali della continuità operativa;
- La norma ISO 22301:2019, presentazione dei requisiti;
- La norma ISO/IEC TS 17021-6, i requisiti di competenza;
- Le fasi del processo di certificazione dei BCMS secondo ISO/IEC 17021-1:2015 e ISO 19011:2018.

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.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO: 1 settimana

E' PREVISTO UN TEST DI INGRESSO NON SBARRANTE ED UN ESAME FINALE.

CAPITOLO 3 - CORSI LIVELLO INTERMEDIO

AREA TRANSPORT & NETWORKING

98. CORSO SULLE RETI DI TRASPORTO PER UFFICIALI PROVENIENTI DA ISTITUTI DI FORMAZIONE - COD. R142I

OBIETTIVI DEL CORSO

Fornire al personale frequentatore del Corso Trasmissioni presso la Scuola di Applicazione, conoscenze di base relative alla teoria dei segnali, alle tecniche di multiplazione, alle tecniche di modulazione numerica ed alle architetture delle Reti di trasporto della Difesa (AERNI – ROID - RIFON – SICRAL).

AREA

Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- Teoria dei segnali:
- Cenno all'analisi armonica dei Segnali periodici e aperiodici;
- Segnali a tempo discreto;
- Condizione di *Nyquist* e il teorema del campionamento/ Tecniche di multiplazione:
- Multiplazione TDM (evoluzione degli standard TDM; PDH, EUROCOM SDH);
- Multiplazione CDM / Tecniche di Modulazione: ASK / FSK / PSK / QAM;
- Trasmissioni radio a banda larga, il Multipath;
- *Direct Sequence Spread Spectrum* (DS-SS);
- *Frequency Hopping* (FH) / La modulazione OFDM;
- Rete Numerica Interforze "RNI" - Architettura di rete;
- Rete dati per la supervisione di rete;
- Raccolta allarmi di sito con tecnica *Polling* e tramite *Equinox*;
- Applicativi software di supervisione;
- Unità di terminazione remota UTR / Centri di Manutenzione / Centro Server d'Area;
- Presentazione apparati utilizzati in RNI;
- La tecnica *Asynchronous Transfer Mode* "ATM";
- Tecniche di commutazione e di permutazione dei flussi numerici;
- Gestione del traffico e delle risorse di rete;
- Qualità del Servizio / Presentazione apparato ATM MPS 115;
- Ponti Radio della Rete Numerica Interforze "RNI";
- Rete Operativa Integrata della Difesa ROID
- Presentazione apparati commutazione ROID;
- Presentazione particolareggiata della commutazione di circuito MT 301 F;
- Tecniche di commutazione e di gestione delle risorse di rete impegnate e rilasciate tipiche della commutazione di circuito;
- Tipologia di utenze: fonia – dati – VDC / Tipologie di interfaccia di utenze;
- Raccolta allarmi / Applicativo software di supervisione;
- Centro Gestione e Controllo - ROID;
- Struttura delle reti in fibra ottica: reti a canale singolo, WDM;
- Stratificazione protocollare: IP over ATM over SDH over WDM;
- Semplificazione protocollare e QoS: MPLS;
- La rete RIFON: architettura, topologia ed apparati/ Elementi di comunicazioni satellitari;
- Il sistema SICRAL: segmento spaziale, segmento terrestre, *payload*;
- Terminali satellitari; Interconnessione con le altre reti della Difesa.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva:
Corso Progetto e gestione di Reti Locali cod. R235J;
- a. Conoscenze basiche richieste:
Conoscenza dei sistemi di telecomunicazioni e protocolli di comunicazione per trasmissione dati basati su standard TCP/IP;
- 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 16.

DURATA DEL CORSO:

- 2 settimane;
- non è prevista alcuna attività di laboratorio.

Per esigenze logistiche/sanitarie, il corso potrà essere svolto a distanza in modalità “*e-learning* sincrono”.

È PREVISTO UN ESAME FINALE.

99. CORSO PROPEDEUTICO RETI LOCALI ETHERNET - COD. ER235I

OBIETTIVI DEL CORSO

Il corso costituisce la prima fase di un percorso formativo più ampio, finalizzato alla capacità di progettare e gestire, in qualità di amministratore, reti LAN Ethernet.

In particolare, il corso ha lo scopo di fornire una conoscenza di base delle Reti Locali Ethernet, a partire dalle tipologie dei mezzi trasmissivi utilizzati, con connessi fenomeni elettrici ed ottici, caratterizzanti le moderne tecnologie oggi impiegate nelle Reti IP.

La trattazione del modello di riferimento ISO/OSI e di basilari concetti di protocollo forniscono al frequentatore nozioni fondamentali per comprendere il funzionamento e le interazioni tra i diversi livelli OSI, per arrivare ai concetti di indirizzo fisico e indirizzo logico e loro valenza in un ambiente di Virtual LAN.

In ultimo verranno trattate le classi di reti ed il relativo indirizzamento IPv4.

Sarà utilizzato software per la Simulazione reti Ethernet.

Gli argomenti teorici sono propedeutici alla frequenza del corso progetto e gestione reti LAN Ethernet.

AREA

Transport & Networking

PROGRAMMA/ARGOMENTI TRATTATI

- Modello di riferimento ISO/OSI;
- Mezzi trasmissivi Rame / Fibra Ottica;
- Apparat di rete - HUB- Schede di rete Ethernet;
- Indirizzi MAC;
- Power Over Ethernet (POE);
- LAN Virtuali - LAG - Switch Multilivello;
- Simulazione di reti con Software Packet Tracer;
- L'Indirizzamento IPv4.

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* sincrónico.

MODALITÀ DI SVOLGIMENTO

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

É PREVISTO UN TEST INTERMEDIO NON SBARRANTE

É PREVISTO UN ESAME FINALE

100. CORSO PROGETTO E GESTIONE DI RETI LOCALI ETHERNET - COD. R235I

OBIETTIVI DEL CORSO

Introdurre il frequentatore alla fase di progettazione, realizzazione e manutenzione di un cablaggio strutturato di una rete locale (LAN) secondo le specifiche internazionali EIA/TIA e ISO/IEC, portandolo a conoscenza dei principali elementi e protocolli per la gestione e configurazione degli apparati di una rete locale (*HUB, SWITCH, ROUTER*). Il Corso comprende le informazioni necessarie ad installare e configurare computer in rete che si basano su sistemi operativi Windows con particolare riferimento al protocollo TCP-IP usato in Internet. Il corso si basa sullo standard IEEE802.3 per le reti *ETHERNET*.

AREA

Transport & Networking

PROGRAMMA/ARGOMENTI TRATTATI

- reti LAN e protocolli;
- LAN concetti;
- livello data-link;
- tecnologia Ethernet;
- bridge e switch;
- evoluzione della tecnologia Ethernet;
- lo stack TCP/IP;
- concetti di routing IPV4;
- protocolli fondamentali nelle LAN;
- analisi del datagramma IPV4;
- analisi dei pacchetti TCP e UDP;

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva obbligatoria: corso propedeutico reti locali Ethernet COD. ER235I
- 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 presenza
- Percentuale laboratorio: 20 %

È PREVISTO UN ESAME FINALE

101. CORSO GESTORE RETI PER UFFICIALI DELLE ARMI NAVALI - COD. R236I

OBIETTIVI DEL CORSO

Introdurre i frequentatori ai concetti delle reti, della loro sicurezza, dell'architettura a strati, ed alla progettazione, cablaggio, configurazione ed utilizzo delle reti, portandoli a conoscenza dei principali elementi e dei protocolli per la loro gestione.

Il Corso costituisce un modulo dell'iter di formazione per l'abilitazione T.A.O degli Ufficiali delle Armi Navali e, in particolare, tende a fornire agli Ufficiali AN destinati a bordo delle Unità Navali, le informazioni necessarie per un *Top Management Level* delle reti informatiche.

AREA

Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- concetti generali;
- livello fisico – mezzi fisici;
- Livello Data Link – Ethernet;
- architetture di rete stratificate;
- livello rete – IP;
- livello Trasporto;
- livello Applicazione;
- protocolli di Routing;
- sistemi operativi server;
- cenni di VoIP;
- cenni di Sicurezza Informatica.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

I requisiti professionali sono definiti dalla F.A.

2. Di segretezza:

NOS non richiesto;

3. Di grado:

Ufficiali delle Armi Navali della Marina Militare.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:

3 settimane

SONO PREVISTE DELLE PROVE VALUTATIVE INTERMEDIE E FINALI.

102. CORSO FONDAMENTI DI CABLAGGIO STRUTTURATO - COD. R153I

OBIETTIVI DEL CORSO

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

AREA

Transport & Networking.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- LAN concetti;
- mezzi trasmissivi;
- schede di rete;
- *hub* e *switch*;
- tecnologia ethernet;
- *power over ethernet*;
- 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:

1 settimana di cui 80% laboratorio.

È PREVISTO UN ESAME FINALE.

AREA SOFTWARE, APPLICATIVI E E-LEARNING

103. CORSO 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

1. Professionali:

- a. Frequenza preventiva: N.N.;
- b. Conoscenze basiche richieste: conoscenze generali sull'utilizzo di sistemi operativi Windows;
- c. Studio preventivo sinossi / testi propedeutici: N.N..

2. Di segretezza:

NOS non richiesto.

3. Categorie:

Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

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%.

Per esigenze logistiche/sanitarie, il corso potrà essere svolto a distanza in modalità “*e-learning* sincrono” per un massimo di 8 frequentatori.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

È PREVISTO UN TEST D'INGRESSO (a termine fase *e-learning*).

È PREVISTO UN ESAME FINALE (a termine fase in presenza).

104. CORSO E-LEARNING MOODLE - RUOLI STUDENTE DOCENTE¹¹ - COD. ET22I

OBIETTIVI DEL CORSO

Fornire le conoscenze basiche sull'utilizzo della piattaforma MOODLE lato Studente: login dello studente, gestione dei blocchi, gestione dei dati personali, utilizzo degli strumenti di *e-learning* collaborativo (*forum*, *wiki*, *chat* messaggi). Inoltre, si forniranno le conoscenze inerenti le funzioni lato Docente: creatore del corso, e gli strumenti per utilizzare gli oggetti didattici per l'*e-learning* messi a disposizione dalla Piattaforma Moodle.

AREA

Software/Applicativi/*E-learning*

PROGRAMMA/ARGOMENTI TRATTATI

Conoscere Moodle – le attività degli studenti:

- aspetti generali, la piattaforma, documentazione;
- modificare il profilo e gestire i blocchi del corso;
- partecipare al forum ed al *blog*;
- utilizzare la lezione, il libro di Moodle e le altre attività e risorse;
- rispondere ai quiz e consegnare i compiti;

Ruolo Docente - Utilizzo degli strumenti della Piattaforma:

- conoscere Moodle: le attività del docente;
- panoramica sui ruoli nella piattaforma;
- definizione di un corso;
- introduzione alle risorse di Moodle;
- valutare gli studenti con compiti e *quiz*;

Richiami alla funzionalità studente:

- analisi dell'attività svolta *on-line*;
- ruolo e funzionalità docente;
- impostazione di un corso;
- gestione della partecipazione degli utenti;
- impostazione di diversi tipi di *forum*;
- la *chat* ed i messaggi di Moodle;
- realizzazione di una lezione di Moodle;
- realizzazione di un libro di Moodle / Gestione delle risorse;
- upload di varie tipologie di file / Creazione di cartelle / *link* / pagine;
- utilizzo di *repository* / le attività *Database* e Glossario Wiki;
- creazione di quiz, domande e compiti / Valutazione dell'attività degli studenti;
- utilizzo dettagliato dei report / Realizzazione di questionari di *feedback*;
- la gestione dei *badge* / Procedure di *backup* e ripristino di un corso.

-

¹¹ Basato prevalentemente sulla fase *e-learning* del corso "PIATTAFORMA E-LEARNING MOODLE - COD. TE22I" dei precedenti Cataloghi della Scuola.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: N.N.;
- b. Conoscenze basiche richieste:
Buona conoscenza del computer, basi dell'amministrazione di sistemi operativi server Windows/Linux;
- c. Studio preventivo sinossi / testi propedeutici: N.N..

2. Di segretezza:

NOS non richiesto.

3. Categorie:

Ufficiali, Sottufficiali, Graduati e personale civile della Difesa.

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.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

È PREVISTO UN ESAME FINALE

105. CORSO PIATTAFORMA E-LEARNING MOODLE ¹² - RUOLI DOCENTE - AMMINISTRATORE - COD. TE295I

OBIETTIVI DEL CORSO

Fornire le conoscenze sulla piattaforma MOODLE partendo con l'analisi dei requisiti hardware e software e l'installazione, la configurazione e la gestione della piattaforma stessa dal lato Amministratore. Inoltre, il corso si prefigge l'obiettivo di fornire capacità per l'utilizzo della piattaforma lato docente/creatore di corsi e contenuti, con argomenti teorici, metodologici e tecnico-operativi relativi alle tecnologie e ai linguaggi visivi, audiovisivi e multimediali. Sulle metodologie della formazione a distanza disponibili su Moodle e sulle modalità produttive dei diversi settori dell'audiovisivo e del multimediale (realizzazione di *Learning Object -LO*) su standard SCORM (attraverso strumenti di *authoring* di tipo commerciale e open source).

AREA

Software/Applicativi/*E-learning*

PROGRAMMA/ARGOMENTI TRATTATI

Ruolo Docente: Utilizzo degli strumenti della Piattaforma:

- utilizzo strumenti comunicativi piattaforma *forum/chat*;
- utilizzo degli strumenti presenti su Moodle per la creazione di Lezioni *on-line* e/o contenuti;
- modalità di caricamento di varie tipologie di *file* / creazione di cartelle / *link* / pagine;
- utilizzo di *repository* / le attività database glossario e Wiki;
- creazione di *quiz*, domande e compiti / valutazione dell'attività degli studenti;
- utilizzo dettagliato dei report / realizzazione di questionari di *feedback*;
- la gestione dei *badge* / procedure di backup e ripristino di un corso;
- ruolo amministratore:
- installazione di Moodle su server Xampp;
- cenni di installazione di Moodle su *server* Linux;
- caratteristiche del *database* di supporto alla piattaforma;
- configurazione e personalizzazione del sito / gestione degli utenti e dei gruppi;
- i ruoli degli utenti;
- gestione delle categorie e dei corsi / gestione dell'aspetto e dei temi di Moodle;
- gestione della sicurezza e delle impostazioni del *server*;
- gestione *plugin*, notifiche, registrazione e altre funzionalità avanzate (es. politiche del sito);
- procedure di backup e ripristino del sito / procedure di upgrade della versione di Moodle;
- i *learning objects*:
- creazione di *Learning Object* con *Adobe Captivate*;
- creazione di *Learning Object* con strumenti *open source*;
- caricamento in piattaforma dei LO.

¹² Basato prevalentemente sulla fase *e-learning* del corso "PIATTAFORMA E-LEARNING MOODLE - COD. TE22I" dei precedenti Cataloghi della Scuola.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: CORSO E-LEARNING MOODLE – RUOLI STUDENTE - DOCENTE: COD. ET22I e/o CORSO PIATTAFORMA E-LEARNING MOODLE - COD. TE22I
- b. Conoscenze basiche richieste: buona conoscenza del computer, basi di amministrazione di sistemi operativi server Windows/Linux.
In alternativa alla frequenza preventiva del punto precedente, è richiesta la conoscenza basica sull'utilizzo della Piattaforma Moodle lato studente/docente.
- 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 modalità *e-learning* asincrono (20 ore in piattaforma) con eventuali interventi via *web streaming* e 2 settimane in presenza.

Per esigenze logistiche/sanitarie, il corso potrà essere svolto a distanza in modalità “*on-line training*” per un massimo di 8 frequentatori.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

È PREVISTO TEST D'INGRESSO (A termine fase *e-learning*)

È PREVISTO ESAME FINALE (A termine fase in presenza)

106. CORSO MYSQL - LINGUAGGIO SQL E GESTIONE DATABASE OPEN SOURCE - COD. TE291I

OBIETTIVI DEL CORSO

Introdurre il frequentatore all'utilizzo del database MYSQL portandolo a conoscenza delle principali caratteristiche e funzionalità del prodotto con installazione e configurazione su S.O. Windows e Linux. Nella prima parte del corso viene trattato l'utilizzo del linguaggio SQL per popolare ed interrogare il database. I comandi vengono eseguiti da interfaccia a carattere ed utilizzando tools grafici.

Nella fase in *e-learning* del corso verranno analizzati i principali aspetti della teoria sui database relazionali e del linguaggio SQL. Durante il corso in aula verrà approfondito l'utilizzo del linguaggio SQL per popolare ed interrogare il database. I comandi verranno eseguiti da interfaccia a carattere e anche utilizzando *tools* grafici. Inoltre, verranno analizzate le procedure di installazione, configurazione e gestione avanzata del database.

AREA

Software/Applicativi/*E-learning*

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- database relazionali;
- introduzione ai RDBMS;
- amministrazione di MYSQL su Linux;
- il *client* MYSQL;
- tipi di tabelle;
- interrogazioni del *database*;
- ordinamenti;
- le operazioni di *join* tra tabelle;
- operazioni DML (*Data Manipulation Language*);
- operazioni DDL (*Data Definition Language*);
- le *subquery*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: N.N.;
- b. Conoscenze basiche richieste:
buone conoscenze di Informatica e Reti, conoscenza di S.O. lato server, nozioni sui *database* e linguaggi di programmazione;
- 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 in modalità *e-learning* asincrono (30 ore in piattaforma) con eventuali interventi via web streaming e 2 settimane in presenza;

Per esigenze logistiche/sanitarie, il corso potrà essere svolto a distanza in modalità “*on-line training*” per un massimo di 10 frequentatori.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell’Annesso IV.

È PREVISTO TEST D’INGRESSO (a termine fase *e-learning*).

È PREVISTO ESAME FINALE (a termine fase in presenza).

107. CORSO INFORMATICO DI F.A. (ABILITAZIONE INF) - 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 IEEE802.3*;
- *apparati di rete: HUB SWITCH*;
- indirizzamento IP v.4;
- sistemi operativi di rete;
- introduzione all'infrastruttura di *Active Directory*;
- introduzione alle tipologie di autenticazione Windows;
- i Sistemi Operativi *Open Source*;
- gestione della rete e cenni di interoperabilità.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

I requisiti professionali saranno definiti dalla Marina Militare.

2. Di segretezza:

NOS non richiesto.

3. 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.

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

108. CORSO “USER AND COP MANAGER” DEL SISTEMA DI COMANDO E CONTROLLO JOINT – C2I ADV - COD. T293I

OBIETTIVI DEL CORSO

Fornire al personale delle FF.AA le conoscenze fondamentali per operare in qualità di Utenti e COP Manager del Sistema C2I ADV (Sistema di Comando e Controllo Joint a livello strategico). Fornire le competenze necessarie per poter utilizzare le *features* che il Sistema rende disponibili.

AREA

Software/Applicativi/*E-Learning*

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- Introduzione e panoramica del Sistema;
- Descrizione delle principali funzionalità utilizzabili da un utente COP Manager:
 - creazione e gestione Utenti C2I ADV Nazionale;
 - creazione e Configurazione Connettori/Replicatori C2I NATO;
 - utilizzo del sistema di messaggistica integrato;
- Descrizione delle principali funzionalità utilizzabili da utente Operatore/COP Manager:
 - utilizzo e Gestione dei *Layer* Cartografici;
 - utilizzo e Gestione dei bookmarks;
 - utilizzo e Gestione dei filtri su origine e tipologia di dati;
 - utilizzo di: *Altimetric Pick – Search Bar – Map Center*.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva: N.N.;
- b. Conoscenze basiche richieste:
Operare, quale utente, su un sistema operativo Microsoft Windows lato client;
- 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: 3 giorni (dal mercoledì al venerdì).

È PREVISTO ESAME FINALE.

AREA CYBER DEFENCE, FORENSICS & LAW

109. CORSO *VULNERABILITY ASSESSMENT* (V.A.) – COD. YE449I

OBIETTIVI DEL CORSO

Fornire al personale del Comparto Difesa destinato ad operare nell'ambito della *Cyber Defence* (C.D.) 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*, 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, Forensics & Law.

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- definizioni;
- *vulnerability disclosure, identifier e repository*;
- *common platform enumeration*;
- *common weakness enumeration*;
- *security content automation protocol*;
- *open vulnerability and assessment language*;
- il *vulnerability assessment* all'interno delle Misure Minime di Sicurezza ICT;
- implementazione di un laboratorio per il *testing*;
- i programmi per il *vulnerability scanning*;
- confronto dei risultati ottenuti;
- *assessment*.

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 10.

DURATA DEL CORSO:

3 settimane: 1 settimana in *e-learning* asincrono e 2 settimane in presenza;

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

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

CAPITOLO 4 - CORSI DI LIVELLO BASE

AREA TRANSPORT - NETWORKING

110. CORSO TECNICI TELEMATICI ARMA C.C. (1° CICLO) - COD. A311B

OBIETTIVI DEL CORSO

Il corso in esame costituisce la prima fase dell'iter formativo del personale dell'Arma dei carabinieri prescelti per il conseguimento della specializzazione di "Tecnico Telematico" propedeutica alla seconda, che sarà effettuata direttamente dal Comando Generale dell'Arma dei Carabinieri. L'attività addestrativa nella 1^ fase si sviluppa su due cicli della durata complessiva di 22 settimane

Il primo ciclo è finalizzato al raggiungimento di una conoscenza di base, necessaria alla formazione di una adeguata competenza nell'ambito dell'elettronica e dell'elettrotecnica. In questo periodo vengono effettuate anche attività di laboratorio, con lo scopo di sviluppare adeguate capacità di misura e diagnostica nel campo della radio elettronica.

AREA

Transport – Networking

PROGRAMMA/ARGOMENTI TRATTATI

Il corso si articolerà sul seguente programma:

- modulo di radio elettronica;
- modulo di attività pratica e uso degli strumenti di laboratorio;
- modulo di elettronica digitale;
- modulo manutentore fibre ottiche.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

a. Frequenza preventiva: N.N.;

b. Conoscenze basiche richieste:

La scelta dei frequentatori è effettuata dal Comando Generale dell'Arma dei Carabinieri, mediante selezione interna;

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

2. Di segretezza:

NOS non richiesto.

3. Di grado:

Il corso è prioritariamente indirizzato a Militari dell'Arma dei Carabinieri. Personale di altre FF.AA. può essere ammesso nel limite di eventuali posti disponibili non utilizzati dai militari dell'Arma.

NUMERO FREQUENTATORI AMMESSI: fino a un massimo di 12.

DURATA DEL CORSO: 11 settimane di cui 30% laboratorio.

SONO PREVISTE PROVE INTERMEDIE SCRITTE, ORALI E PRATICHE PER TUTTA LA DURATA DEL CORSO, SU OGNI SINGOLA MATERIA, CON ATTRIBUZIONE DI PUNTEGGIO IN TRENTESIMI.

È PREVISTO UN ESAME FINALE.

111. CORSO DI *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 25.

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 IV.

È PREVISTO UN ESAME FINALE

112. CORSO SU 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 12.

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 IV.

È PREVISTO UN ESAME FINALE

AREA SOFTWARE, APPLICATIVI E E-LEARNING

113. CORSO E-LEARNING DI INFORMATICA DI BASE ECDL - COD. ET17B

OBIETTIVI DEL CORSO

Il corso di informatica di base ECDL 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*.

AREA

Software/Applicativi/*E-learning*

PROGRAMMA/ARGOMENTI TRATTATI

- generalità sui personal computer;
- fondamenti di attività *on-line*;
- elaboratori di testi;
- fogli di calcolo;
- sicurezza IT;
- strumenti di presentazione;
- 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 75 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 IV.

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

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

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

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

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

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

È PREVISTO UN ESAME FINALE.

114. CORSO E-LEARNING IT SPECIALIST - COD. ET18B

OBIETTIVI DEL CORSO

Formare il personale designato a svolgere mansioni afferenti il Ruolo di Referente Informatico (con riferimento allo standard EUCIP IT ADMINISTRATOR), fornendogli competenze ed abilità a livello basico, necessarie per la gestione di piccole infrastrutture informatiche negli ambiti: Hardware, Sistemi Operativi (Windows® e Linux), Reti e Sicurezza Informatica.

In particolare, il corso è orientato su quattro moduli didattici: HW del PC; Configurazione dei Sistemi Operativi; LAN e servizi di rete; Sicurezza ICT.

AREA

Software/Applicativi/*E-Learning*

PROGRAMMA/ARGOMENTI TRATTATI

Modulo Hardware

- introduzione;
- introduzione al personal computer;
- scheda madre;
- BIOS;
- microprocessori;
- processore;
- memoria;
- bus e risorse di sistema;
- bus di comunicazione;
- risorse di sistema;
- interfacce;
- memorie di massa;
- dispositivi di visualizzazione;
- stampanti.

Modulo Configurazione dei sistemi operativi (Linux - Microsoft)

- introduzione ai sistemi operativi;
- sistemi operativi *client*: file di configurazione;
- sistemi operativi *client*: aggiornamento software;
- *file system*;
- configurazione server;
- gestione computer, utenti e gruppi;
- gestione risorse e autorizzazioni;
- implementazione TCP/IP;
- controllo delle prestazioni del sistema;

Modulo Sicurezza IT

- principi generali della sicurezza IT;
- analisi e gestione del rischio;
- aspetti organizzativi della sicurezza IT;
- disponibilità dei dati e delle risorse;
- crittografie e ambiti d'impiego; la firma digitale;
- infrastruttura a chiave pubblica;
- autenticazione e controllo di accesso;
- codice maligno;
- sicurezza di rete;
- aspetti sociali, etici e legali.

Modulo Servizi di rete

- server e networking;
- introduzione al TCP/IP e al modello OSI;
- l'indirizzamento IP;
- pacchetti UDP e Protocollo IP;
- porte; sockets e ICMP;
- Subnetting e routing IP;
- CIDR e supernetting;
- IP Multicasting e Ipv6;
- livelli Trasporto, Sessione e Presentazione;
- Protocollo TCP;
- NAT, DHCP e MIME;
- apparati di rete;
- File Transfer Protocol;
- World Wide Web;
- posta elettronica;
- collaborazione e condivisione.

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 75 frequentatori.

DURATA DEL CORSO:

WEB Based Training 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 IV.

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

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

115. CORSO 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;
- installazione di Linux: dalla teoria alla pratica;
- i *desktop manager* Linux;
- procedura di autenticazione;
- *login/logout*;
- struttura del *filesystem*;
- la *shell* e i comandi;
- *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 *background* e *foreground*;
- compressione e archiviazione;
- backup incrementale con il tar;
- RPM (*redhat package manager*);
- installazione del software con yum e dnf;
- ambiente grafico (Desktop Gnome Kde);

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 25.

DURATA DEL CORSO:

2 settimane in modalità *e-learning* asincrono (40 ore in piattaforma).

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

All'atto dell'iscrizione sarà inviata al candidato una *password* per l'accesso iniziale ai contenuti della piattaforma *e-learning* della Scuola. Il corso sarà interamente tenuto in modalità *on-line*. Gli iscritti attraverso le proprie credenziali, potranno collegarsi ed accedere alla piattaforma di studio *on-line*, partecipando/seguendo le lezioni in modalità a-sincrona o, quando stabilito dalla Scuola, attraverso *forum* e *chat*.

È PREVISTO UN ESAME FINALE

116. CORSO ELEMENTI DI VIRTUALIZZAZIONE - COD. ET24B

OBIETTIVI DEL CORSO

Fornire ai frequentatori le conoscenze generali sulle tecnologie di virtualizzazione descrivendone le caratteristiche, le funzionalità e i principali vantaggi del suo utilizzo.

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;
- 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* (15 ore in piattaforma).

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

È PREVISTO ESAME FINALE

AREA INFOSEC E INFORMATION ASSURANCE

117. CORSO SICUREZZA IT¹³: 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

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 75.

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

¹³ Contenuti tratti dal modulo "sicurezza IT" del corso "IT Specialist cod. ET18B.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV. Gli iscritti attraverso le proprie credenziali potranno collegarsi e accedere alla piattaforma di studio *on-line*, partecipando/seguendo le lezioni in modalità asincrona o, quando stabilito dalla Scuola, attraverso *forum* e *chat*.

È PREVISTO ESAME FINALE

AREA CYBER DEFENCE, FORENSICS & LAW

118. CORSO FONDAMENTI DI INTELLIGENZA ARTIFICIALE (IA) – COD. Y453B

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

Cyber Defence, Forensics & Law.

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:

- a. Frequenza preventiva: N.N.;
- b. Conoscenze basiche richieste: N.N.;
- c. Studio preventivo sinossi / testi propedeutici: N.N..

2. Di segretezza:

NOS non richiesto.

3. Di grado:

Ufficiali, Sottufficiali, Sergenti, Graduati e personale civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: fino ad un massimo di 12.

DURATA DEL CORSO:

1 settimana.

Per esigenze logistiche/sanitarie, il corso potrà essere svolto a distanza in modalità *e-learning* sincrono.

È PREVISTO UN ESAME FINALE.

119. CORSO 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, Forensics & Law

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;
- sarà, inoltre, effettuato a discrezione dell'istruttore, uno o più *webinar* le cui modalità saranno comunicate dall'istruttore stesso sulla chat di piattaforma.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva:
Modulo informativo per la CD;
- 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 25.

DURATA DEL CORSO: 1 settimana in modalità *e-learning* sincrone (20 ore in piattaforma).

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

È PREVISTO ESAME FINALE

120. CORSO FONDAMENTI DI DIGITAL FORENSICS - COD. EY446B

OBIETTIVI DEL CORSO

Fornire ai frequentatori le conoscenze generali per gestire e condurre attività di Digital Forensics su supporti digitali o su reti di computer di interesse della Difesa, a seguito di incidente o di reato informatico, ivi compresa l'eventuale cooperazione con le Autorità e gli organismi preposti in ambito forense.

AREA

Cyber Defence, Forensics & Law

PROGRAMMA/ARGOMENTI TRATTATI

- introduzione ai crimini informatici
- teoria della *Digital Forensics* (Procedure e *Best Practices*)
- *Computer Forensics* (Acquisizione ed Analisi con strumenti *Open Source*);
- laboratorio

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva:
Moduli Informativi di Fondamenti di Informatica Giuridica e di Cyber Defence e Corso Fondamenti di Cyber Defence;
- b. Conoscenze basiche richieste:
 - conoscenze generali sull'utilizzo e la gestione di sistemi operativi Windows e Linux;
 - conoscenza di base dei principali concetti legati alla 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: 2 settimane (da lunedì a venerdì per 32 ore a settimana) in modalità *e-learning* sincrona/asincrona, su piattaforma *e-learning* della Difesa e con modalità di apprendimento individuali e di gruppo.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV 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 TEST D'INGRESSO NON SBARRANTE ED UN ESAME FINALE.

121. CORSO FONDAMENTI DI INFORMATICA GIURIDICA PER IL PERSONALE DELLA DIFESA - COD. EY450B

OBIETTIVI DEL CORSO

Fornire le conoscenze fondamentali per un approccio corretto all'uso delle tecnologie e per una comprensione delle problematiche giuridiche ad esse connesse, soprattutto con riferimento alle vulnerabilità di sicurezza ed ai crimini informatici ed alla luce dell'evoluzione normativa nazionale, europea ed internazionale.

AREA

Cyber Defence, Forensics & Law

PROGRAMMA/ARGOMENTI TRATTATI

- l'informatica giuridica tra informatica del diritto e diritto dell'informatica;
- nozioni elementari di informatica (*hardware, software*, le reti ed il *world wide web*);
- la protezione dei dati personali;
- l'evoluzione della normativa in tema di "sicurezza cibernetica";
- cenni su reati informatici e informatica forense;
- Codice dell'Amministrazione digitale;
- cenni su intelligenza artificiale e diritto;
- cenni su *blockchain* ed i registri distribuiti.

CARATTERISTICHE E PREREQUISITI DEI PARTECIPANTI

1. Professionali:

- a. Frequenza preventiva:
Modulo Informativo di Informatica Giuridica;
- 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 20.

DURATA DEL CORSO: 2 settimane (da lunedì a venerdì per 32 ore a settimana) in modalità *e-learning* sincrona/asincrona, su piattaforma *e-learning* della Difesa e con modalità di apprendimento individuali e di gruppo.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV 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 TEST D'INGRESSO NON SBARRANTE ED UN ESAME FINALE.

122. CORSO SU TRATTAMENTO DEI DATI PERSONALI PER IL PERSONALE DELLA DIFESA - COD. EY451B

OBIETTIVI DEL CORSO

Fornire al personale militare e civile della Difesa le conoscenze fondamentali per trattare in modo adeguato i dati personali.

Analizzare gli strumenti per adeguare processi e comportamenti alle disposizioni in vigore e fornire le indicazioni su come redigere i principali documenti richiesti dal GDPR.

Approfondire le basi del funzionamento di un sistema di gestione della privacy.

AREA

LAW & FORENSICS

PROGRAMMA / ARGOMENTI TRATTATI

- L'evoluzione del concetto di protezione dei dati personali;
- Le normative in tema di protezione dei dati personali in Italia, in Europa e nel mondo;
- Regolamento Generale sulla Protezione dei Dati (UE) 2016/679;
- Le diverse tipologie di illeciti connesse al trattamento dei dati personali;
- La figura di Amministratore di sistema, in relazione al trattamento dei dati personali;
- Cenni su Sistema di Gestione Privacy.

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

1 settimana (da lunedì a venerdì per 32 ore a settimana) in modalità *e-learning* sincrona/asincrona, su piattaforma *e-learning* della Difesa e con modalità di apprendimento individuali e di gruppo.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV 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 ESAME FINALE.

123. MODULO INFORMATIVO SULLA CYBER DEFENCE – COD. EY430B

OBIETTIVI

Fornire al personale le competenze necessarie per identificare e trattare le minacce associate all'uso delle tecnologie digitali al fine di incrementare la capacità di gestire i dati in modo sicuro. Questo modulo informativo, di livello basico, sarà sempre accessibile nella piattaforma *e-learning* della Scuola e non necessita di iscrizione.

AREA

Cyber Defence, Forensics & Law

PROGRAMMA/ARGOMENTI TRATTATI

- riconoscere le minacce e proteggersi;
- gestire le *e-mail* in sicurezza;
- *login* e *password*;
- la navigazione sicura sul *web*;
- proteggere i dati e i *file*;
- come proteggersi dal *social engineering*;
- la sicurezza fisica dei dispositivi mobili;
- uso consapevole dei *social network*;
- *information disclosure*;
- furto d'identità digitale;
- crittografia;
- certificati digitali;
- accesso al Wi-Fi;
- accesso a internet da stazioni pubbliche.

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:

Tutto il personale militare e civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: modulo ad accesso libero in piattaforma.

DURATA DEL CORSO: 15 ore in piattaforma *e-learning*.

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

NON È PREVISTO ESAME FINALE

NON È PREVISTA LA TRASCRIZIONE A MATRICOLA.

124. MODULO INFORMATIVO SULL'INFORMATICA GIURIDICA - COD. EY431B

OBIETTIVI DEL CORSO

Fornire al personale della Difesa le conoscenze volte a garantire l'adozione di idonee misure organizzative nel trattamento dei dati personali e ad affrontare le problematiche di carattere giuridico-legale connesse alla creazione, alla conservazione ed alla circolazione dei dati e delle informazioni, con particolare riguardo alla protezione dagli illeciti interni ed esterni. Questo modulo informativo, di livello basico, sarà sempre accessibile nella piattaforma *e-learning* della Scuola e non necessita di iscrizione.

AREA

Cyber Defence, Forensics & Law

PROGRAMMA/ARGOMENTI TRATTATI

- a. Introduzione normativa e legislativa:
 - concetti normativi fondamentali comunitari e nazionali;
 - diritto d'autore.
- b. La tutela dei dati personali:
 - la Privacy: principi generali e ambiti di applicazione nell'Amministrazione Difesa;
 - le misure di sicurezza;
 - aspetti sanzionatori.
- c. La disciplina sugli amministratori di sistema:
 - analisi della disciplina vigente in materia;
 - redazione di documentazione dedicata.
- d. Cyberspace:
 - cenni sulla dottrina nazionale ed internazionale inerente il c.d. "CYBERSPACE" ed analisi delle principali minacce.
- e. REATI INFORMATICI:
 - cenni sui reati informatici principali.
- f. PROVA DIGITALE:
 - la Convenzione di Budapest del 2001 e le caratteristiche della prova digitale;
 - elementi di Computer Forensics.

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:

Tutto il personale militare e civile della Difesa.

NUMERO FREQUENTATORI AMMESSI: Modulo ad accesso libero in piattaforma.

DURATA DEL CORSO: 15 ore in piattaforma *e-learning*;

MODALITÀ DI SVOLGIMENTO

Le attività a distanza sono disciplinate nell'Annesso IV.

NON È PREVISTO ESAME FINALE

NON È PREVISTA LA TRASCRIZIONE A MATRICOLA.

ANNESI

**ANNESSO I - INFORMAZIONI PER GLI ENTI
PROGRAMMATORI**

NOTIZIE LOGISTICHE/AMMINISTRATIVE

1. ONERI DI VIAGGIO

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

Il personale designato alla frequenza di Corsi dovrà presentarsi munito di Foglio di Viaggio che comprenda tutto il periodo di durata dell'attività, così come definito nel messaggio di convocazione dei Master/Corsi universitari e 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 la concessione di licenze al frequentatore a cura di questo Istituto.

Le fasi frontali dei corsi erogati presso questa 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 rese disponibili nel Calendario dei Corsi, per i corsi erogati dagli Istruttori della Scuola, o attraverso una specifica comunicazione, a mezzo messaggio telegrafico o lettera, per i frequentatori dei Master/Corsi Universitari.

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.

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:

	1^ Colazione	Pranzo	Cena
Lunedì – giovedì	07.20 – 07.50	12.55 – 14.00	19.00 – 20.00
Venerdì		12.30 – 13.00	
Sabato	08.00 – 08.20	12.00 – 13.00	
Domenica			

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., presso la Cassa della Scuola, sita in Palazzina A, che emetterà un'apposita quietanza.

La Scuola non fornisce ai frequentatori effetti di vestiario e materiali per l'igiene personale.

Le tipologie delle sistemazioni alloggiative per i frequentatori sono:

- Camere multiple con bagno in comune al piano;
- Camere doppie con bagno in comune in camera;
- Camere singole con bagno in camera.

Le assegnazioni dei precitati alloggi, con particolare riferimento alle loro tipologie, sono effettuate 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 DELLE FFAA

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. 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) *I metodi di segnalazione ai corsi potranno essere modificati nel corso dell'AA e ne sarà data opportuna comunicazione agli Enti Programmatori.*
- (3) Per i Master/Corsi di Formazione Specialistica in convenzione con le Università, la domanda di iscrizione dovrà essere inviata, dal personale designato dalla F.A. alla frequenza del Corso/Master, direttamente alle segreterie degli atenei indicate sugli

appositi messaggi telegrafici emanati da questo Istituto. La documentazione per l'immatricolazione del frequentatore è riportata sui bandi rettorali pubblicati dagli atenei. Il frequentatore, una volta completato l'iter di iscrizione con gli atenei, dovrà segnalare alla Scuola l'avvenuta iscrizione. Si rammenta che la Scuola non può in nessun modo intervenire nei processi di iscrizione dei frequentatori alle università che rimangono sotto la diretta responsabilità degli atenei stessi.

- (4) 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 in Scheda A al presente Annesso.

Per alcuni Corsi è previsto un test iniziale, non sbarrante, per la verifica del grado di conoscenza nella specifica materia.

c. Requisiti per l'ammissione ai corsi/master di Alta formazione universitaria

(1) Master di I e II livello e Corsi di Perfezionamento di Alta formazione universitaria

I requisiti per l'ammissione sono indicati nei singoli decreti rettorali di attivazione degli atenei in convenzione e descritti nelle schede dei Master e Corsi universitari erogati dagli Atenei in convenzione (Annesso III).

(2) Uditori ai Master e Corsi universitari di Alta formazione universitaria

È ammesso alla frequenza il personale non in possesso dei titoli accademici previsti dal Corso/Master universitario indicati sul bando rettorale che possono comunque frequentare tali corsi in qualità di "Uditori" (senza obbligo di frequenza continuativa e di effettuare gli esami intermedi/finali del corso/master). Al termine del percorso formativo l'Uditore riceverà un attestato di frequenza redatto dalla Scuola che non ha alcun valore accademico.

(3) Annullamento dei corsi non a carattere universitario

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

- mancato raggiungimento del numero minimo necessario all'attivazione di un corso (5 discenti);
- esigenze organizzative della Scuola (indisponibilità dell'istruttore, aspetti di carattere logistico, ecc.).

4. ADEMPIMENTI DEGLI ENTI PROGRAMMATORI IN PERIODO DI PANDEMIA COVID19

In esito all'applicazione delle linee guida sanitarie anti-COVID 19 dettate dalle SS.AA., questo Istituto ha introdotto i sotto elencati adempimenti che dovranno essere fatti assolvere dai discenti entro il giovedì antecedente l'inizio del corso pena l'esclusione d'autorità dai corsi:

- compilare ed inviare a stelmilit.corsi@marina.difesa.it la **scheda anagrafica** scaricabile dal link [20210310_SCHEDA_ANAGRAFICA_STELMILIT.pdf \(difesa.it\)](#);
- compilare ed inviare per email a stelmilit.corsi@marina.difesa.it (tel. 722 8510 o 0185-3334510 e 722 8567 o 0185-3334567) e a stelmilit.dottore@marina.difesa.it (tel. 722 8466 o 0185-3334466) l'**Autocertificazione** scaricabile dal link [20201007_Allegato_2_Autocertificazione.pdf \(difesa.it\)](#);
- prima di intraprendere il viaggio per Chiavari, il frequentatore dovrà controllare la propria temperatura corporea e, in caso di riscontro di temperatura superiore a 37,5° C, quest'ultimo sarà tenuto a rimanere presso il proprio domicilio dandone tempestiva comunicazione alle autorità sanitarie competenti, al proprio Ente/Comando di appartenenza e a questo Istituto (per email a stelmilit.corsi@marina.difesa.it e a stelmilit.dottore@marina.difesa.it).

Il discente continuerà ad essere avviato alla frequenza dei corsi presso questo Istituto in missione (in regime di aggregazione completa con vitto e alloggio presso la Scuola) e, a parziale variante dell'iter di presentazione previsto dall'Annesso II del Catalogo dei Corsi, quest'ultimo dovrà raggiungere l'Istituto il lunedì dell'inizio del corso, dalle ore 08.00 alle ore 14.00, munito di mascherina. Una volta al Corpo di Guardia, sarà sottoposto alla misurazione della temperatura corporea e, in caso di riscontro di temperatura superiore a 37.5°C non potrà accedere al sedime della Scuola.

Il frequentatore sarà successivamente avviato all'Infermeria di questa Scuola dove verrà sottoposto, previo consenso informato, al test antigenico rapido per la diagnosi da infezione da Sars-Cov2 mediante tampone rinofaringeo. Qualora tale test risulti negativo, il discente sarà sottoposto a visita medica che si concluderà con il rilascio, da parte del Capo Servizio Sanitario della Scuola, del "Nulla Osta alla frequenza dei corsi".

Nel caso in cui il discente dovesse risultare positivo ad uno dei sopracitati controlli/test, sarà sottoposto ad ulteriori accertamenti sanitari e posto in isolamento presso una struttura logistica della Scuola appositamente allestita.

I discenti saranno sottoposti quotidianamente al controllo della temperatura corporea prima dell'inizio delle attività didattiche in aula.

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 e per Conoscenza a SMD I Rep, 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 prenda visione di quanto riportato al seguente link:
www.difesa.it/SMD /EntiMI/STELMILIT/Pagine/vita_istituto.aspx

**ANNESSO II - INFORMAZIONI PER I
FREQUENTATORI**

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 (0185-3334510) o, fuori 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 ED ALLOGGIAMENTO

Allo scopo di disporre del tempo necessario per la sistemazione logistica, i frequentatori devono presentarsi presso la Scuola entro il giorno antecedente l'inizio del Corso. Il personale di Guardia all'ingresso della Scuola, effettuate le procedure di riconoscimento, fornirà ai frequentatori il *pass* personale e quello per l'autovettura, i talloncini pasto per la mensa e le chiavi dell'alloggio assegnato.

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 Unificata con bar gestito da ditta civile.

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 esclusivamente nelle versioni con giacca, maglione, camicia o giubbino.

Non è consentito indossare:

- tute da combattimento;
- vestiario di navigazione;
- combinazioni di volo;
- vestiario speciale di FA.

Il personale frequentatore dovrà avere al seguito la Divisa Ordinaria da utilizzare in occasione di cerimonie organizzate dalla Scuola. Nei periodi prossimi al cambio divisa stagionale, il personale frequentatore dovrà avere al seguito le due versioni delle predette divise.

Al di fuori dell'orario di servizio, per la frequenza della Mensa e della Sala Convegno Unificata 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 e Sala Convegno, 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. L'eventuale concessione di licenza comporta la sospensione del trattamento economico di missione.

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.

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 erogate dal personale istruttore della Scuola e per le percentuali indicate dagli Atenei in convenzione per i Corsi/Master Universitari;
- 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. Dimissioni volontarie: 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. ASSISTENZA SANITARIA

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. SPORT E TEMPO LIBERO

Le strutture della Scuola disponibili per l'attività ginnico-sportiva e del tempo libero includono:

- una palestra attrezzata;
- una sala TV (Piano terra - Palazzina Comando).

Per la frequenza della palestra il frequentatore dovrà presentare un “certificato medico” attestante l'idoneità alla *pratica sportiva non agonistica* oppure il certificato di idoneità alle PEF.

Da giugno a settembre, è disponibile, a pagamento, per i frequentatori ed i loro familiari (con le stesse modalità) lo stabilimento elioterapico della Scuola situato a Cavi di Lavagna. Tale struttura offre anche un servizio bar e di ristorazione.

12. DISPOSIZIONI PER LA FREQUENZA DI CORSI SUPERIORI AI 60 GIORNI

Il discente che parteciperà a Corsi di lunghezza superiori ai 60 giorni, dovrà arrivare presso l'Istituto munito di:

- statino licenze/ore spettanti non ancora fruite;
- scheda individuale di controllo efficienza fisica.

13. VITA D'ISTITUTO IN PERIODO DI PANDEMIA COVID19

In esito all'applicazione delle linee guida sanitarie anti-COVID 19 dettate dalle SS.AA., questo Istituto ha introdotto i sotto elencati adempimenti che dovranno essere assolti dai discenti entro il giovedì antecedente l'inizio del corso pena l'esclusione d'autorità dai corsi:

- compilare ed inviare a stelmilit.corsi@marina.difesa.it la **scheda anagrafica** scaricabile dal link [20210310_SCHEDA_ANAGRAFICA_STELMILIT.pdf](#) (difesa.it);
- compilare ed inviare per email a stelmilit.corsi@marina.difesa.it (tel. 722 8510 o 0185-3334510 e 722 8567 o 0185-3334567) e a stelmilit.dottore@marina.difesa.it (tel. 722 8466 o 0185-3334466) l'**Autocertificazione** scaricabile dal link [20201007_Allegato_2_Autocertificazione.pdf](#) (difesa.it);
- prima di intraprendere il viaggio per Chiavari, il frequentatore dovrà controllare la propria temperatura corporea e, in caso di riscontro di temperatura superiore a 37,5° C, quest'ultimo sarà tenuto a rimanere presso il proprio domicilio dandone tempestiva comunicazione alle autorità sanitarie competenti, al proprio Ente/Comando di appartenenza e a questo Istituto (per email a stelmilit.corsi@marina.difesa.it e a stelmilit.dottore@marina.difesa.it).

Il discente continuerà ad essere avviato alla frequenza dei corsi presso questo Istituto in missione (in regime di aggregazione completa con vitto e alloggio presso la Scuola) e, a parziale variante dell'iter di presentazione previsto al para. 3, quest'ultimo dovrà raggiungere l'Istituto il lunedì dell'inizio del corso, dalle ore 08.00 alle ore 14.00, munito di mascherina. Una volta al Corpo di Guardia, sarà sottoposto alla misurazione della temperatura corporea e, in caso di riscontro di temperatura superiore a 37.5°C non potrà accedere al sedime della Scuola.

Il frequentatore sarà successivamente avviato all'Infermeria di questa Scuola dove verrà sottoposto, previo consenso informato, al test antigenico rapido per la diagnosi da infezione da Sars-Cov2 mediante tampone rinofaringeo. Qualora tale test risulti negativo, il discente sarà sottoposto a visita medica che si concluderà con il rilascio, da parte del Capo Servizio Sanitario della Scuola, del "Nulla Osta alla frequenza dei corsi".

Nel caso in cui il discente dovesse risultare positivo ad uno dei sopracitati controlli/test, sarà sottoposto ad ulteriori accertamenti sanitari e posto in isolamento presso una struttura logistica della Scuola appositamente allestita.

I discenti saranno sottoposti quotidianamente al controllo della temperatura corporea prima dell'inizio delle attività didattiche in aula.

**ANNESSO III - INFORMAZIONI MASTER E
CORSI UNIVERSITARI**

MASTER II LIVELLO**1. INTRODUZIONE**

Quanto riportato di seguito è valido per i soli frequentatori dei Corsi/Master Universitari ad eccezione di quelli dell'Area Cyber, Digital Forensics & Law le cui caratteristiche sono riportate a partire da pagina 245.

2. CARATTERISTICHE E REQUISITI DEI FREQUENTATORI

I titoli di studio richiesti sono:

- Laurea in Fisica, Ingegneria, Informatica e Matematica conseguita secondo l'ordinamento previgente o titoli equipollenti.
- Laurea Magistrale in Fisica (classe LM-17), Informatica (classe LM-18), Ingegneria aerospaziale e astronautica (classe LM-20), Ingegneria biomedica (classe LM-21), Ingegneria chimica (classe LM-22), Ingegneria civile (classe LM-23), Ingegneria dell'automazione (classe LM-25), Ingegneria delle telecomunicazioni (classe LM-27), Ingegneria elettrica (classe LM-28), Ingegneria elettronica (classe LM-29), Ingegneria energetica e nucleare (classe LM-30), Ingegneria gestionale (classe LM-31), Ingegneria informatica (classe LM-32), Ingegneria meccanica (classe LM-33), Ingegneria navale (classe LM-34), Ingegneria per l'ambiente e il territorio (classe LM-35), Matematica (classe LM-40), Modellistica matematico-fisica per l'ingegneria (classe LM-44) e Scienza e ingegneria dei materiali (classe LM-53) conseguita secondo l'ordinamento vigente o titoli equipollenti.

Possono accedere, altresì, coloro che, in possesso di un titolo di studio di secondo livello diverso da quello specificato, abbiano conoscenze e comprovata esperienza professionale ritenute affini al profilo del Master.

3. PERIODICITÀ E DURATA DEI MASTER

I master si svolgono una volta l'anno e le relative attività di didattica frontale hanno una durata di circa 19 settimane (400 ore di lezione frontale).

Le attività di compilazione della tesi finale sono svolte presso l'EDR di appartenenza.

La discussione della tesi sarà effettuata entro 12 mesi dall'inizio del master presso STELMILIT.

4. VERIFICHE

È previsto un esame di valutazione del livello di apprendimento raggiunto e di verifica per l'attribuzione dei relativi crediti formativi universitari al termine di ciascun modulo

didattico.

L'esame consisterà in un test scritto nella forma più consona al modulo e decisa dal docente titolare dell'insegnamento (domande a risposta aperta, test a risposta multipla, esercizi).

In media il test si articolerà su due ore e si svolgerà una settimana dopo la chiusura del modulo, al fine di permettere agli allievi di prepararsi al meglio.

Per ogni esame di fine modulo sarà formata una Commissione d'esame composta da due persone: il docente titolare del modulo (o suo delegato) e un esperto della materia scelto dalla Scuola (come il tutor o suo delegato). I membri della Commissione saranno presenti in aula al momento dell'esame. La votazione attribuita sarà in trentesimi.

5. CONSEGUIMENTO DEL TITOLO

Al termine delle attività formative gli studenti del Master dovranno preparare e discutere una tesi finale, relativa alle attività svolte. L'attività potrà essere:

- di ricerca, sia teorica sia sperimentale, tipicamente relativa all'analisi critica di uno o più argomenti trattati nei moduli oppure allo studio di tematiche di ricerca e alla produzione di risultati sperimentali innovativi;
- di approfondimento, tipicamente relativa all'approfondimento di argomenti trattati nei moduli oppure all'applicazione di metodi studiati nei moduli per la soluzione di particolari problemi e casi specifici e all'eventuale produzione di risultati sperimentali;
- di indagine bibliografica (ricerca bibliografica su argomenti specifici relativi alle tematiche studiate nel Master).

L'attività svolta verrà documentata in una relazione che introduce l'argomento e il problema affrontato, delinea il metodo seguito per la soluzione ovvero il percorso seguito per estendere le metodologie, descrive i risultati ottenuti.

Ogni tesi sarà seguita, come relatore, da un docente del Master afferente all'Università di Genova. Eventuali eccezioni (relatori non docenti del Master e/o esterni all'Università) dovranno essere approvate dal Comitato di Gestione.

Ogni candidato si presenterà alla discussione dell'elaborato finale, in sessione plenaria, con un voto di partenza risultante dalla media dei voti ottenuti durante gli esami intermedi, ponderata sui crediti formativi universitari corrispondenti a ciascun modulo didattico.

Al voto di partenza sarà sommato il voto della tesi, deciso dalla Commissione in sede d'esame in base alla qualità dell'elaborato, al tipo di attività svolta (ricerca, approfondimento o indagine bibliografica) e all'esposizione discussa.

La Commissione d'esame sarà composta da tre membri del Comitato di Gestione, due afferenti all'Università e uno alla Scuola. Eventuali eccezioni dovranno essere approvate dal

Comitato di Gestione.

Al termine ogni candidato consegnerà una votazione finale complessiva espressa in centodecimi.

A conclusione del Master, a tutti gli studenti che abbiano superato con esito positivo le prove, sarà rilasciato il diploma di Master universitario II livello come previsto dall'art. 19 del Regolamento dei Corsi di Perfezionamento, di aggiornamento professionale e di formazione permanente e dei corsi per Master universitari di primo e secondo livello dell'Università degli Studi di Genova.

6. POSTI DISPONIBILI

Ogni Master sarà attivato al raggiungimento di almeno 5 frequentatori ed il numero massimo di frequentatori è fissato in 12 unità.

7. MODALITÀ D'ISCRIZIONE

La domanda di ammissione deve essere presentata mediante la procedura *on-line* disponibile all'indirizzo <http://servizionline.unige.it/studenti/post-laurea>, con le tempistiche che sono definite con la pubblicazione del bando disponibile nel sito www.unige.it

8. STAGE

Al termine del Master, potrà essere svolto uno STAGE presso Istituti, Enti Pubblici, Enti della Difesa o nell'industria privata nazionale. L'Ente verrà individuato su indicazione del Collegio dei Docenti e dei rappresentanti dell'A.D

CORSI DI FORMAZIONE UNIVERSITARI

1. CARATTERISTICHE E REQUISITI DEI FREQUENTATORI

I titoli di studio richiesti sono:

- Laurea in Fisica, Ingegneria, Informatica e Matematica conseguita secondo l'ordinamento previgente o titoli equipollenti.
- Laurea in Ingegneria Civile e Ambientale (classe 8), Ingegneria dell'Informazione (classe 9), Ingegneria Industriale (classe 10), Scienze e Tecnologie Fisiche (classe 25), Scienze e Tecnologie Informatiche (classe 26) Scienze Matematiche (classe 32) conseguita secondo l'ordinamento vigente o titoli equipollenti.
- Eventuali altri requisiti: possono accedere altresì coloro che, in possesso di un titolo di studio universitario diverso da quello specificato o del solo diploma di scuola media superiore, abbiano conoscenze e comprovata esperienza professionale affini al profilo del Corso.

Occorre in ogni caso essere in possesso di diploma di scuola secondaria superiore.

2. VERIFICHE

Al termine della fase d'aula è previsto un esame di verifica e di valutazione del livello di apprendimento raggiunto. L'esame consisterà in un test scritto nella forma più consona al Corso e decisa dal docente titolare dell'insegnamento (domande a risposta aperta, test a risposta multipla, esercizi). In media il test si articolerà su due ore e sarà somministrato da una Commissione d'esame composta da due persone: il docente titolare (o suo delegato) e un esperto della materia scelto dalla Scuola (come il tutor o suo delegato).

La votazione attribuita sarà in trentesimi.

3. ATTESTATI

A conclusione del Corso, a tutti i frequentatori che abbiano superato con esito positivo l'esame, verrà rilasciato dall'Università il relativo attestato di frequenza.

4. POSTI DISPONIBILI

Il corso verrà effettuato al raggiungimento di minimo 5 frequentatori. Il numero massimo di frequentatori per ogni singolo corso è fissato in 12 unità.

5. MODALITÀ D'ISCRIZIONE

La domanda di ammissione deve essere presentata mediante la procedura *on-line* disponibile all'indirizzo indicato sul bando rettorale dell'Ateneo e apposito messaggio di STELMILIT.

AREA CYBER DEFENCE, DIGITAL FORENSICS & LAW**MASTER I LIVELLO****1. INTRODUZIONE**

Quanto riportato di seguito è valido per i soli frequentatori dei Corsi/Master Universitari dell'Area Cyber Defence, Digital Forensics & Law.

2. CARATTERISTICHE E REQUISITI DEI FREQUENTATORI

Saranno ammessi al Corso di Master:

- Per il conseguimento del titolo di Master: laureati di primo livello, laureati magistrali, laureati vecchio ordinamento didattico in qualsiasi classe che, sulla base del curriculum formativo e/o dell'esperienza pregressa, abbiano comprovate competenze informatiche.
- Come uditore senza il conseguimento del titolo di Master: diplomati che, pur non in possesso di titolo accademico, abbiano comprovate competenze informatiche attinenti al Master. A questi partecipanti, verrà rilasciato dalla Direzione Corsi di Chiavari un attestato di frequenza al termine del Corso.

A tutti i partecipanti è richiesta una presenza pari ad almeno il 70% delle ore di lezioni frontali.

3. PERIODICITÀ E DURATA DEL CORSO

Il Master si svolge una volta all'anno, comporta 1.500 ore di impegno complessivo, di cui 300 ore di didattica frontale, 350 ore di laboratorio e progetti assistiti, 650 ore di studio individuale, 200 per la preparazione della tesi e della discussione finale.

Le attività di predisposizione della tesi finale saranno svolte presso il Reparto di appartenenza, e la discussione della tesi dovrà essere effettuata entro 12 mesi dall'inizio dei corsi. Nel corso del master sarà possibile usufruire di licenze e permessi nei limiti indicati nel precedente paragrafo.

4. VERIFICHE

Sono previsti esami intermedi di accertamento per l'attribuzione dei relativi Crediti Formativi Universitari (CFU) per ciascun modulo didattico.

L'esame consisterà di un colloquio orale o di un test o di un progetto da discutere con il docente. Ciascuna prova dovrebbe articolarsi al massimo su di un'ora e dovrebbe essere svolta dopo una settimana dalla chiusura del modulo, al fine di permettere agli allievi di studiare/assimilare i contenuti.

Per ogni esame di modulo sarà formata una commissione d'esame composta da un minimo di due persone, di cui una è il titolare del modulo (o suo delegato) e l'altra è un esperto della materia scelto dalla Scuola (come il tutor o suo delegato). I membri della commissione saranno presenti in aula al momento dell'esame.

La votazione attribuita sarà in trentesimi.

5. CONSEGUIMENTO DEL TITOLO

Al termine delle attività formative, il partecipante al Master dovrà preparare e discutere un elaborato (tesi finale) relativo alle attività svolte nell'ambito del Project Work successivo al periodo di didattica frontale.

L'attività potrà essere sia teorica sia sperimentale e relativa all'approfondimento di argomenti trattati nell'ambito dei moduli, allo studio di tematiche innovative o alla produzione di risultati sperimentali ottenuti mediante applicazione di strumenti e metodologie studiati nell'ambito dei moduli.

L'attività svolta verrà documentata in una relazione che introduce l'argomento e il problema affrontato, delinea il metodo seguito per la soluzione ovvero il percorso intrapreso per l'applicazione delle metodologie, descrive i risultati ottenuti. Ogni progetto di tesi sarà seguito da un relatore, di norma docente del Master, eventualmente in collaborazione con un correlatore dell'Ente di appartenenza. Eventuali eccezioni di relatori non docenti del Master dovranno essere preventivamente approvate dal Comitato di Gestione.

Ogni candidato si presenterà alla discussione dell'elaborato finale, in sessione plenaria, con un voto di partenza risultante dalla media dei voti ottenuti durante gli esami intermedi, ponderata sui Crediti Formativi Universitari corrispondenti ai vari moduli didattici. Per determinare il voto di discussione la Commissione esaminatrice potrà attribuire alla prova finale un punteggio che varierà tra 0 e 6 punti a seconda della qualità dell'elaborato, dipendente anche dal tipo di attività svolta (ricerca, approfondimento, o sperimentazione) e della capacità di esposizione dello stesso.

Al termine, ogni candidato conseguirà una votazione finale complessiva espressa in centodecimi.

A conclusione del Master, agli iscritti che a giudizio del Comitato abbiano superato con esito positivo la prova finale, verrà rilasciato il diploma di Master Universitario di I livello in "Cyber Defence Governance".

Agli uditori verrà rilasciato dalla Scuola Telecomunicazioni di Chiavari un attestato di frequenza.

6. POSTI DISPONIBILI

Il Master verrà effettuato se i frequentatori designati raggiungono il numero minimo di 5 unità, mentre il numero massimo di frequentatori è fissato in 12 unità.

La Scuola Telecomunicazioni delle FF.AA. regolerà le esclusioni in caso di domande eccedenti le disponibilità, e le assegnazioni di eventuali posti non utilizzati dagli assegnatari.

7. MODALITÀ D'ISCRIZIONE

La domanda di ammissione deve essere presentata mediante la procedura *on-line* secondo modalità e tempistiche che saranno definite nell'ambito del bando.

CORSI UNIVERSITARI

1. CARATTERISTICHE E PREREQUISITI DEI FREQUENTATORI

Sono ammessi al corso:

- Prioritariamente: laureati in Fisica, Matematica ed Ingegneria (laurea di secondo livello o specialistica secondo il vecchio ordinamento);
- Personale della Pubblica Amministrazione che, pur non in possesso di titolo accademico, abbia comprovata professionalità attinente al corso;

Tale condizione sarà valutata da apposita commissione dell'AD e del Corpo Docenti.

2. PERIODICITÀ E DURATA DEL CORSO

Il Corso si svolge una volta all'anno e comporta le ore indicate nelle varie schede corsi di impegno complessivo.

3. VERIFICHE

Esame finale.

4. POSTI DISPONIBILI

Ogni singolo corso viene effettuato se i frequentatori designati raggiungono il numero minimo di 5 unità.

Il numero massimo di frequentatori per ogni singolo corso è fissato in 12 unità.

5. MODALITÀ D'ISCRIZIONE

La domanda di ammissione deve essere presentata mediante la procedura *on-line* secondo le modalità e tempistiche che saranno definite nell'ambito del bando.

**ANNESSO IV - EROGAZIONE DEI CORSI IN
DIDATTICA A DISTANZA (D.A.D.)**

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 (D.A.D.)

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

- *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* sincrone: 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'accesso remoto in VPN ai laboratori della Scuola.

Infine, nell'area "Autoformazione" della piattaforma *e-learning* sono disponibili dei Moduli Informativi ad accesso libero, la cui fruizione non richiede la prevista iscrizione per il personale dell'A.D..

Utilizzando il link <https://elearning.difesa.it/course/index.php?categoryid=171>, si potrà accedere alle istruzioni riportate nella piattaforma stessa, senza alcuna ulteriore comunicazione alla Scuola.

2. MODALITÀ DI FRUIZIONE

Il personale iscritto dovrà svolgere il corso da una postazione che gli EDR dovranno mettere a disposizione dei discenti presso la sede di servizio, con hardware, software e connettività adeguata, come previsto dalla pubblicazione "Linee guida in materia di formazione in modalità *e-learning*" ed. 2012 dello Stato Maggiore Difesa.

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.

La piattaforma è raggiungibile all'indirizzo <https://elearning.difesa.it>¹⁴ sia dalle reti intranet 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.

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.

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 predefinita 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.

¹⁴ Eventuali Link/URL/Portali, differenti dalla Piattaforma e utili allo svolgimento delle attività di laboratorio effettuate a distanza, saranno comunicati ai frequentatori dai Referenti/Docenti dei relativi corsi.

5. SEGNALAZIONI ED INIZIO CORSO E-LEARNING

I percorsi formativi che prevedono una fase *e-learning* preventiva e/o che sono erogati totalmente in *e-learning* sono indicati all'interno del presente Catalogo dei Corsi.

Per tali corsi formativi (*blended e-learning*), gli EDR deputati alla segnalazione dei frequentatori dovranno comunicare alla Scuola i dati di ciascuno di essi, comprensivi della mail istituzionale, almeno 3 settimane prima dell'inizio della fase in questione.

Si evidenzia che le *policy* di utilizzo della Piattaforma non consentono la registrazione di utenti con e-mail che NON siano istituzionali.

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 evidenzino delle problematiche nella fruizione dei contenuti, il tutor/docente interagirà direttamente con il frequentatore per trovare soluzioni adeguate. Nel caso di difficoltà di livello tale da compromettere il raggiungimento degli obiettivi formativi del corso (mancato completamento della fase a *e-learning* nel periodo definito), 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.

7. ESAME DI FINE CORSO E RICONOSCIMENTO DELLE ATTIVITÀ SVOLTE

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

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

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

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

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

Per accedere alla sessione d'esame il discente dovrà:

- aver completato tutti i moduli del corso e superato i relativi accertamenti intermedi;
- aver caricato in piattaforma l'atto di nomina della Commissione di controllo locale;
- al termine dell'esame la Commissione di controllo dovrà inviare via mail alla Segreteria corsi della Scuola (stelmilit.corsi@marina.difesa.it) copia dell'atto di nomina e del verbale d'esame, redatto secondo il modello allegato e debitamente compilato e firmato.

Lo stesso verbale dovrà essere inoltre caricato a cura del discente sulla piattaforma stessa che, a seguito della sua acquisizione, rilascerà copia dell'attestato di partecipazione con indicazione dell'esito finale e del punteggio conseguito.

FAC-SIMILE - ORDINE DEL GIORNO/ATTO DI NOMINA/ORDINE DI SERVIZIO¹⁵

Nomina commissione di sorveglianza – Esame fine corso “Nome del Corso” (Cod. CORSO) del/dei “Grado – Cognome - Nome” (discente/i che sosterranno la prova)

VISTI: Le linee guida in materia di formazione in modalità *e-learning* Ed. 2012 dello Stato Maggiore della Difesa;
L’ Annesso IV - EROGAZIONE DEI CORSI IN MODALITÀ A DISTANZA – del Catalogo Corsi della Scuola Telecomunicazioni
“EVENTUALI ULTERIORI NORME/CIRCOLARI/DISPOSIZIONI”

DISPONGO

Il “giorno – mese - anno” la sottonotata Commissione si riunisca nell’orario previsto di svolgimento della prova al fine di garantire il corretto svolgimento del test di fine corso “Nome del Corso” a favore del “Grado – Cognome - Nome” (discente/i che sosterranno la prova):

- “Grado – Cognome - Nome” – Presidente
- “Grado – Cognome - Nome” – Membro
- “Grado – Cognome - Nome” – Membro/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 (a meno di diversa indicazione degli Istruttori del Corso).

Al termine dell’esame la suddetta Commissione dovrà inviare alla Segreteria Corsi della Scuola Telecomunicazioni di Chiavari – STELMILIT CHIAVARI – (stelmilit.corsi@marina.difesa.it) il verbale d’esame¹⁶ redatto secondo il modello previsto dal Catalogo Corsi della Scuola, debitamente compilato e firmato.

Località e data _____

IL COMANDANTE

¹⁵ Per accedere alla sessione d’esame il discente dovrà caricare in piattaforma, nell’apposita area del relativo corso, l’atto di nomina della Commissione di controllo locale;

¹⁶ Si rammenta che una copia del verbale d’esame dovrà essere caricata dal discente, nell’apposita area del relativo corso, per il rilascio dell’Attestato del Corso che avverrà unicamente e direttamente in Piattaforma.

VERBALE D'ESAME DEI CORSI SVOLTI A DISTANZA

Corso:	
Data esame:	
Ora inizio:	
Ora fine:	

ELENCO CANDIDATI		
n.	Grado, Cognome, Nome	Numero CMD
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