ALLEGATO
Prot 05/DID
del 05/03/2026

SCUOLA TELECOMUNICAZIONI FF.AA.
Direzione Corsi

CAPITOLATO PER LA FORNITURA DI PERCORSI FORMATIVI CYBER

Edizione febbraio 2026

Capitolato

1. Amministrazione appaltante

Scuola Telecomunicazioni delle Forze Armate (denominata in seguito "Scuola") sita in Via Parma, 34 16043 Chiavari (GE) – C.F. 82004050108.

2. Oggetto della prestazione

Oggetto della prestazione è lo svolgimento di un percorso formativo a favore del personale della Difesa in ambito *cyber*, mediante lezioni live sincrone a distanza e attività pratica/esperienziale attraverso l'utilizzo di laboratori su infrastruttura tecnica remota.

I corsi oggetto del percorso formativo sono riportati di seguito:

- Nr 1 sessione "**Corso di *Malware Analysis***";
- Nr 1 sessione "**Corso di *Chief Information Security Officier*** (CISO)";
- Nr 1 sessione "**Corso di *Big Data Analysis***";
- Nr 1 sessione "**Corso di *Digital Forensics***".

I *Syllabus* del percorso formativo sono riportati in annesso al presente capitolato.

I percorsi formativi dovranno essere erogati per un minimo di 8 ed un massimo di 16 discenti.

La formazione in parola dovrà essere svolta in modalità "**live sincrona a distanza**" come di seguito specificato:

- ***Malware Analysis***: dal 18 maggio al 5 giugno 2026;
- **CISO**: dal 08 al 19 giugno 2026;
- ***Big Data Analysis***: dal 22 giugno al 10 luglio 2026;
- ***Digital Forensics***: dal 13 al 31 luglio 2026.

La Ditta aggiudicataria, a seguito di coordinamento con la Scuola ed in tempo utile per l'erogazione del percorso formativo, dovrà predisporre e mettere a disposizione del personale partecipante idonei laboratori e sistemi di *Online Training*.

3. Obiettivi

3.1. Tipologia di formazione

Le attività formative a distanza e/o in presenza dovranno tenersi da lunedì a venerdì per un totale di **352 ore complessive** come di seguito specificato:

- *Malware Analysis*: **96 ore** complessive (5 gg per 3 settimane – 32 ore a settimana) dal 18 maggio al 5 giugno 2026;
- CISO: **64 ore** complessive (5 gg per 2 settimane – 32 ore a settimana) dal 8 al 19 giugno 2026;
- *Big Data Analysis*: **96 ore** complessive (5 gg per 3 settimane – 32 ore a settimana) dal 22 giugno al 10 luglio 2026;
- *Digital Forensics*: **96 ore** complessive (5 gg per 3 settimane – 32 ore a settimana) dal 13 al 31 luglio 2026.

La Ditta aggiudicataria dovrà mettere a disposizione dei discenti il necessario materiale didattico, slide/libri/dispense/*e-book* ed i relativi *Software*, *Virtual Machine,* Laboratori (Guide ai Lab), da utilizzare nell'attività pratica/esperienziale di laboratorio.

Si precisa che non è possibile utilizzare riproduzioni fotostatiche di alcun tipo di testi pubblicati. Nel corso dovranno essere svolti i periodi di laboratorio e attività pratiche (riferiti ai contenuti nei moduli richiesti e riportati in annesso) come di seguito riportato:

- attraverso formazione a distanza da svolgere in spazi ed infrastruttura tecnica remota resi disponibili dalla ditta aggiudicataria e necessari al corretto svolgimento dell'intervento formativo.
- I laboratori dovranno garantire isolamento completo degli ambienti per ciascun frequentatore e l'accesso contemporaneo per tutti gli utenti, nonché la disponibilità continuativa H24 7/7 per tutta la durata del corso.
- I discenti non dovranno installare alcun software, componente o plug-in sui propri dispositivi: l'accesso ai laboratori dovrà avvenire esclusivamente tramite browser o client remoto fornito dalla Ditta.
- per le lezioni *live*, le attività si potranno tenere su "stanze virtuali" fornite dalla Scuola o, in alternativa, in spazi virtuali che dovranno essere messi a disposizione dalla ditta aggiudicatrice, secondo la discrezionalità della Scuola; in entrambi i casi la ditta erogatrice è tenuta ha verificare l'effettiva presenza dei frequentatori utilizzando un registro presenze, oppure attraverso i log di accesso nel caso in cui la stanza virtuale venga fornita e gestita dalla ditta stessa.
- Allo scopo di aumentare il coinvolgimento e incentivare la partecipazione attiva dei frequentatori, l'attività *live* di erogazione dei contenuti teorici dovrà essere alternata ad attività esercitativa e di laboratorio (quest'ultima NON inferiore al 25% delle ore di lezione), condotta applicando la strategia didattica della *Gamification* dove possibile. Tali attività esperienziali, che non saranno oggetto di valutazione sommativa finale, si terranno di massima nella fase pomeridiana della giornata e dovranno prevedere, all'interno di laboratori ed esercitazioni, un sistema di sfide e punteggi da assegnare al singolo frequentatore o a squadre di frequentatori che il docente formerà. Per queste attività il feedback dovrà essere immediato in modo da correggere gli errori in tempo reale, facilitando e stimolando l'apprendimento. In alternativa, per le attività che non si prestano a esperienze laboratoriali, la ditta aggiudicatrice dovrà prevedere nelle ore pomeridiane attività di studio\esercizi\consegne individuali\di gruppo, sotto la supervisione del docente.

Al termine di ogni corso la Ditta aggiudicatrice, su indicazioni e in coordinamento con i referenti della Scuola, dovrà prevedere una prova valutativa finale[1] con punteggio espresso in trentesimi, fornendo un set di almeno nr. 40 domande a risposta multipla (in formato Aiken o altro compatibile con la piattaforma LMS in uso presso la Scuola) da svolgersi sulla piattaforma e-Learning della Difesa e dovrà rilasciare, per ogni frequentatore, un attestato di frequenza del corso svolto.

3.2. Luogo di esecuzione dei servizi

L'attività di **formazione live sincrona a distanza** dovrà essere garantita in modalità *Online Training*, attraverso lezioni *online* (*live web streaming*), con Istruttore qualificato, in classi virtuali e attività guidate di laboratorio, svolte su infrastrutture remote e secondo quanto previsto dal presente capitolato e dai relativi *Lab Training*;

3.3. Data e orari

Fermo restando quanto riportato al punto 2 del presente documento in merito all'inizio e termine erogazione del corso, gli orari delle attività didattiche dovranno rispettare quanto di seguito stabilito:

- dalle 8.00 alle 13.00 (5 ore) e dalle 14.30 alle 16.30 (2 ore) dal lunedì al giovedì;
- dalle 8.00 alle 12.00 (4 ore) il venerdì.

[1] La Scuola Telecomunicazioni, al raggiungimento da parte di ogni discente del punteggio minimo di 18/30 nel test finale del percorso formativo, consegnerà un ulteriore e proprio attestato di frequenza ad ognuno di essi.

Eventuali variazioni in funzione di esigenze non preventivabili potranno essere concordate tra le parti.

Le ore di lezione previste in eventuali festivi infrasettimanali dovranno essere recuperate di massima nella stessa settimana, prevedendo una estensione dell'orario giornaliero.

A titolo di esempio, la giornata festiva di martedi 2 giugno 2026, all'interno della sessione del Corso *Malware Analysis*, dovrà essere recuperata come segue:

- Lun 1 giugno: dalle 08:00 alle 13:00 (5 ore) e dalle 14:30 alle 17:30 (3 ore)
- Merc 3 e Gio 4 giugno: dalle 08:00 alle 13:00 (5 ore) e dalle 14:30 alle 17:30 (3 ore)
- Ven 5 giugno: dalle 08:00 alle 13:00 (5 ore) e dalle 14:30 alle 17:30 (3 ore)

4. Responsabili del prestatore di servizi aggiudicatario

Il prestatore di servizi aggiudicatario, entro 7gg dalla firma del contratto, dovrà nominare e comunicare alla Scuola una persona cui sarà affidata la responsabilità ed il coordinamento di tutte le attività previste come precisato nel precedente punto 3 del presente documento.

5. Condizioni di fornitura

- La ditta aggiudicataria deve avvalersi di figure professionali esperte nel settore e nella docenza per l'esecuzione della presente prestazione
- l'azienda deve aver ottenuto (allegare in sede di offerta\gara) il certificato ISO 9001:2015 nel settore della formazione, preferibilmente "EA37 istruzione" o certificazione equipollente; si specifica che rimane in carico alla ditta l'onere di dimostrare tale equipollenza o superiorità
- Per la verifica dei requisiti richiesti la ditta aggiudicataria dovrà pertanto presentare e allegare in sede di offerta\gara, i "Curricula Vitae" (CV) di tutte le risorse professionali proposte, predisposti in formato standard "Europass" attestanti le caratteristiche professionali ed in particolare:
  - Esperienza professionale, sia complessiva che specifica
  - Certificazioni conseguite in corso di validità alla data della presentazione dell'offerta
  - Competenze professionali maturate in contesti analoghi a quello in esame, sia per tematiche (servizi) che per complessità
  - Metodologie, strumenti e tools di supporto conosciuti per lo svolgimento delle attività specifiche richieste nell'ambito della presente prestazione
- Il possesso di tali requisiti deve essere riscontrabile nei curricula dei singoli specialisti
- I curricula di ogni docente e le relative certificazioni devono essere attinenti all'area tematica oggetto di insegnamento
- I docenti indicati in sede di offerta dovranno essere gli stessi che erogheranno i rispettivi corsi. Eventuali sostituzioni saranno ammesse esclusivamente per cause di forza maggiore e dovranno essere preventivamente comunicate e concordate con la Stazione appaltante, che si riserva la facoltà di approvarle o respingerle
- Per la verifica dei requisiti richiesti la ditta, in fase di offerta\gara, dovrà allegare una scheda di sintesi che descriva come intende condurre le attività esercitative, pratiche e di studio individuale\di gruppo, con l'elenco dei *tools*, piattaforme, metodologie, ect. Dovrà inoltre specificare, in caso di non applicabilità di attività didattiche condotte secondo la strategia della *Gamification,* in quali corsi intende avvalersi della possibilità di impiegare le ore pomeridiane per studio individuale\di gruppo con consegne specifiche
- La ditta aggiudicataria deve comunicare eventuali personalizzazioni dei contenuti.

Il Responsabile del procedimento per la fase di programmazione, progettazione ed esecuzione (R.P.P.E.)
IL DIRETTORE DEI CORSI
Col. t.(tlm.) t.ISSMI Alessandro EZZIS

Firmato Digitalmente da/Signed by:
ALESSANDRO EZZIS

In Data/On Date:

Syllabus

Corso Malware Analysis: dal 18 maggio al 05 giugno 2026

Durata 3 settimane per un totale di 96 ore (7 ore al giorno dal lunedì al giovedì - 4 ore il venerdì).

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.

PROGRAMMA

Introduzione e Setup

- Panoramica delle minacce malware attuali
- Classificazione dei malware (virus, worm, trojan, ransomware, ecc.)
- Strumenti essenziali per l'analisi del malware

Fondamenti di Assembly x86/x64

- Architettura Intel x86/x64
- Registri, istruzioni e stack
- Struttura dei file PE (Portable Executable)
- Debugging di base
- Esercitazione: Analisi di semplici programmi in assembly

Analisi Statica di Base

- Estrazione di metadati e stringhe
- Identificazione di funzioni importate/esportate
- Riconoscimento di pattern sospetti
- Calcolo e verifica di hash
- Esercitazione: Analisi statica di campioni di malware semplici

Analisi Comportamentale

- Monitoraggio di processi e risorse di sistema
- Analisi del traffico di rete
- Tracciamento delle API Windows
- Analisi comportamentale di documenti/eseguibili Windows malevoli;
- Sandboxing e automazione dell'analisi
- Esercitazione: Analisi comportamentale di malware reale

Tecniche di Packing e Unpacking

- Identificazione di malware packed
- Riconoscimento dei packer comuni
- Individuazione dell'Original Entry Point (OEP)
- Tecniche di unpacking manuale
- Strumenti automatizzati per l'unpacking
- Esercitazione: Unpacking di campioni reali

Tecniche Anti-Analisi

- Rilevamento di macchine virtuali e strumenti di debug
- Offuscamento del codice
- Anti-disassembly e anti-debugging
- Tecniche di evasione temporale
- Esercitazione: Superamento delle difese anti-analisi

Analisi di Codice Malevolo

- Analisi di malware a livello di codice

- Esame di proprietà statiche di documenti/eseguibili Windows sospetti;
- Analisi statica e dinamica del codice di eseguibili Windows malevoli;
- Reverse engineering di algoritmi critici
- DLL injection e function hooking
- Tecniche di keylogging e cattura di credenziali
- Comunicazione HTTP/HTTPS e command-and-control
- Esercitazione: Analisi approfondita di malware complesso

Malware su Piattaforme Multiple

- Malware per Linux e macOS
- Malware per dispositivi mobili (Android/iOS)
- Esercitazione: Analisi comparativa di malware multi-piattaforma

Casi di Studio

- Analisi di campagne APT recenti
- Studio di ransomware significativi
- Esercitazione: Analisi di un caso reale end-to-end

STRUMENTI UTILIZZATI:

- Disassembler/Debugger: IDA Pro, Ghidra, x64dbg, OllyDbg
- Analisi statica: PEiD, PEStudio, PPEE, Detect It Easy
- Analisi dinamica: Process Monitor, Process Explorer, Regshot
- Analisi di rete: Wireshark, NetworkMiner
- Sandbox: Cuckoo Sandbox, ANY.RUN, VMware/VirtualBox
- Strumenti di scripting: Python, PowerShell

Gli STRUMENTI UTILIZZATI elencati sopra sono a titolo esemplificativo. Può essere concesso alla ditta aggiudicatrice, a seguito di proposta e di valutazione vincolante della Scuola, di utilizzare strumenti con analoghe potenzialità di raggiungere gli obiettivi didattici prefissati nel presente capitolato\annesso.

Corso Chief Information Security Officer (CISO): dal 08 al 19 giugno 2026

Durata 2 settimane per un totale di 64 ore (7 ore al giorno dal lunedì al giovedì - 4 ore il venerdì).

Il corso mira a creare le necessarie competenze in grado di definire le strategie di sicurezza, implementare la policy e gestire le risorse, il personale, i processi e i compiti nell'ambito di un'organizzazione per gli aspetti di sicurezza informatica.

PROGRAMMA

***Governance* e strategia della cybersecurity in Italia**

- Architettura Nazionale di Cybersicurezza/Agenzia per la Cybersicurezza Nazionale (ACN)
- Sistema Nazionale di Cybersicurezza/Strategia Nazionale di Cybersicurezza
- Framework Nazionale per la Cybersecurity
- CSIRT Italia
- Incident Response
- Crisis Management/Gestione delle Minacce
- Threat Intelligence nazionale
- Analisi del rischio cyber
- Capacità di risposta
- Standard tecnici
- Misure minime di sicurezza
- CAD/Linee Guida AGID/Linee guida ACN
- Best practice nazionali

Security Risk Management, Controls, Audit Management

- Identificazione e valutazione dei rischi di sicurezza informatica
- Metodologie di risk assessment
- Analisi dell'impatto
- Determinazione del rischio residuo
- Identity and Access Management/Metodi di autenticazione
- Tecnologie di controllo accessi
- Modelli di autorizzazione
- I sistemi di gestione degli accessi
- Protocolli di autenticazione e autorizzazione
- Cloud e modelli di servizio
- La responsabilità condivisa nell'era del cloud computing
- Le nuove architetture
- Microservizi/I container
- IoT
- Edge, Fog e Cloud computing
- Il Grid computing
- La crittografia/Crittografica a chiave simmetrica-asimmetrica
- Lo scambio sicuro di chiavi
- Hash
- Firme crittografiche
- Crittografia quantistica

- La rete TOR
- Navigare in incognito
- I servizi nascosti
- Attacchi a TOR
- Sforzi per rendere TOR sicuro
- I gruppi APT/La minaccia APT
- Gli obiettivi degli attacchi APT
- Gruppi statali vs Gruppi criminali
- Convenzioni di denominazione
- Gli attacchi
- La Kill Chain Lockheed Martin
- Unified Kill Chain di Paul Pols
- MITRE ATT&CK/MITRE D3FEND
- I malware/La classificazione dei malware
- Le tecniche di evasione
- I Ransomware/Le botnet
- I componenti principali di una botnet
- Architettura del C&C
- Utilizzo delle botnet
- I meccanismi di protezione
- Takedown
- Attacchi DDoS/ Evoluzione degli attacchi DDoS
- Tipologia di attacchi
- Mitigazione
- Addendum
- I documenti nello sviluppo e deploy del software
- Termini e Condizioni nei contratti di acquisto
- L'outsourcing/I processi di innovazione
- Selezione e implementazione di controlli di sicurezza adeguati
- Framework di riferimento (NIST CSF, CIS Controls)
- Identificazione dei controlli tecnici, organizzativi e procedurali
- Gestione del rischio residuo e piani di mitigazione
- Strategie per il trattamento del rischio (accettazione, mitigazione, trasferimento)
- Audit e monitoraggio continuo della sicurezza
- Metodologie di audit/Indicatori di performance/Dashboard di monitoraggio
- Report periodici
- Principali normative e standard di riferimento
- GDPR/NIS2/EU Cybersecurity Act/CER (Critial Entities Resilience)
- Direttiva (UE) 2022/2557/ISO 27001
- NIST Cybersecurity Framework

Security Program Management & Operations

- Progettazione e implementazione di un programma di sicurezza
- Definizione della roadmap/Pianificazione delle attività/Allocazione delle risorse
- Strategie di Resilienza delle Infrastrutture Critiche
- Zero Trust Strategy
- Gestione delle risorse, del personale e dei processi di sicurezza
- Organizzazione del team di sicurezza
- Definizione di ruoli e responsabilità
- Gestione delle competenze
- Incident response e gestione delle crisi di sicurezza/Piani di risposta agli incidenti

- Coinvolgimento degli stakeholder/Comunicazione in situazioni di emergenza
- Business Continuity e Disaster Recovery
- Analisi degli impatti aziendali
- Strategie di business continuity/Piani di disaster recovery

Cyber Threat Intelligence

- Raccolta e analisi delle informazioni sulle minacce cyber
- Fonti di intelligence (big data, open source, dark web, feeds)
- Tecniche di analisi e correlazione dei dati
- Individuazione e comprensione delle nuove tecniche degli hacker
- Analisi delle tendenze
- Metodologie e strumenti utilizzati
- Condivisione delle informazioni sulla minaccia con gli stakeholder
- Modalità di condivisione, tempistiche, formati, piattaforme
- Integrazione della threat intelligence nella strategia di sicurezza
- Utilizzo delle informazioni per l'aggiornamento dei controlli, dei piani di mitigazione e della
- postura di sicurezza

Corso Big Data Analysis: dal 22 giugno al 10 luglio 2026

Durata 3 settimane per un totale di 96 ore (7 ore al giorno dal lunedì al giovedì - 4 ore il venerdì).

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.

PROGRAMMA

- Introduzione ai 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
- Intelligenza artificiale e machine learning
- Machine Learning e famiglie di algoritmi
- Data Mining con sviluppo ed utilizzo di metodologie specifiche (regressione, clustering, associazioni)
- Identificazione di modelli finalizzati all'interpretazione dei dati anche con capacity predittiva
- Social Media Analysis
- Marketing analytics
- Google Cloud Platform per i Big Data e Google Analytics e Dispositivi di IoT
- Strumenti di visualizzazione dei dati: Google Data Studio
- Laboratorio: Esercitazioni pratiche mediante la discussione di casi reali

Corso Digital Forensics: dal 13 al 31 luglio 2026

Durata 3 settimane per un totale di 96 ore (7 ore al giorno dal lunedì al giovedì - 4 ore il venerdì).

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.

PROGRAMMA

Quadro normativo e giuridico

- Normativa nazionale e internazionale sui reati informatici
- GDPR e implicazioni per la Digital Forensics
- Catena di custodia: requisiti legali e best practices
- Ammissibilità delle prove digitali in tribunale
- Casi giurisprudenziali rilevanti

Fondamenti tecnici

- Architettura hardware e software dei sistemi informatici
- Sistemi operativi: Windows, macOS, Linux
- Archiviazione dei dati: file system, supporti di memorizzazione

Acquisizione forense dei dati

- Metodologie di acquisizione forense
- Strumenti hardware e software per l'acquisizione
- Acquisizione di memorie volatili (RAM)
- Acquisizione di memorie di massa
- Imaging forense e verifica dell'integrità dei dati

Digital Forensics su dispositivi mobili

- Architettura dei dispositivi mobili
- Tecniche di acquisizione per iOS, Android e altri sistemi
- Bypass delle protezioni e accesso ai dati
- Analisi delle app e dei dati di social media
- Geolocalizzazione e timeline delle attività

Network Forensics

- Monitoraggio e cattura del traffico di rete
- Analisi dei log di sistema e di rete
- Ricostruzione delle comunicazioni
- Identificazione di attacchi e intrusioni

Memory Forensics

- Analisi della memoria volatile
- Estrazione di artefatti dalla RAM
- Identificazione di malware in memoria
- Ricostruzione delle attività dell'utente
- Utilizzo di Volatility e altri framework

Digital Forensics antiforense e avanzata

- Tecniche di antiforensics: cancellazione sicura, crittografia
- Recupero dati da dispositivi danneggiati
- Analisi forense di database

- Indagini sulle criptovalute e blockchain
- Dark web e investigazioni anonime

Automazione e strumenti avanzati

- Utilizzo di OSINT nelle indagini digitali
- Analisi timeline e correlazione degli eventi
- Data visualization per le indagini
- Intelligenza artificiale applicata alla Digital Forensics

Simulazione di un caso completo

- Esercitazione pratica su un caso complesso
- Discussione e analisi dei risultati

METODOLOGIA DIDATTICA

- Laboratori pratici con strumenti forensi professionali
- Casi di studio reali
- Esercitazioni di gruppo

STRUMENTI E SOFTWARE

- EnCase Forensic
- FTK (Forensic Toolkit)
- Autopsy/The Sleuth Kit
- Cellebrite UFED
- XRY
- Oxygen Forensic
- Volatility Framework
- NetworkMiner
- Wireshark
- OSINT Framework

Gli STRUMENTI E SOFTWARE elencati sopra sono a titolo esemplificativo. Può essere concesso alla ditta aggiudicatrice, a seguito di proposta e di valutazione vincolante della Scuola, di utilizzare strumenti con analoghe potenzialità di raggiungere gli obiettivi didattici prefissati nel presente capitolato\annesso.