COMANDO OPERAZIONI IN RETE
UFFICIO AMMINISTRAZIONE
Sezione Contratti e Acquisti
C.F. 96451060584
Via Stresa 31/B – 00135 ROMA

Posta elettronica: cor@cor.difesa.it
Posta elettronica certificata: cor@postacert.difesa.it

Lettera di Ordinazione n. 137
(da citare in fattura)

Roma, 01/10/2025

Ditta KPMG Advisory S.p.A.
Via Curtatone, 3 00185 Roma
pec:kpmgadvisoryspa.ufficiogare@pec.kpmg.it

Oggetto: Gara 149 – acquisizione percorsi formazione specialistica in ambito progetti Cyber Capacity Building a favore partner internazionali – CIG B7F677D8A7 - CUP D89J25000650001 – Capitolo 1269/2 – E.F. 2025 – Rdo 5572053.

IDV 2050857

Codesta Ditta, si obbliga ad eseguire la sottonotata fornitura/prestazione, comprensiva dei relativi costi per la sicurezza, pari ad €. 523,38 come da citata Rdo.:

Descrizione	Imponibile
acquisizione percorsi formazione specialistica in ambito progetti Cyber Capacity Building a favore partner internazionali, come da requisito tecnico operativo e dettaglio prezzi in allegato.	€. 67.100,00
Totale imponibile	€. 67.100,00
IVA esente ai sensi art. 72 comma 3 punto 2 del D.P.R. 633/72	€. 0,00
TOTALE	€. 67.100,00

1. La presenta commessa, per tutto quanto non previsto nella presente, si svolgerà sotto l'osservanza del D.P.R. 13 marzo 2013, n. 49 (*Regolamento per la disciplina delle attività del Ministero della difesa in materia di lavori, servizi e forniture militari, a norma dell'articolo 4, comma 1, del decreto legislativo 15 novembre 2011, n. 208, recante attuazione della direttiva 2009/81/CE*;
2. La Ditta si impegna ad eseguire la fornitura/prestazione a sua cura, rischio e spese **a decorrere dalla data di consegna/accettazione della presente e dovrà essere conclusa entro il giorno il 31/12/2025**, osservando tutte le norme e disposizioni indicate nella presente lettera di ordinazione.
3. Qualora nel corso di esecuzione del contratto, trascorsi 12 mesi dall'avvio dell'esecuzione, al verificarsi di particolari condizioni di natura oggettiva, si determina una variazione, in aumento o in diminuzione, del costo della fornitura superiore al cinque per cento, dell'importo complessivo, i prezzi sono aggiornati, nella misura dell'ottanta per cento della variazione, in relazione alle prestazioni da eseguire. Ai fini del calcolo della variazione dei prezzi si utilizza l'indice dei prezzi al consumo per le famiglie di operai e impiegati (Foi). In caso di eccessiva onerosità sopravvenuta per il verificarsi di avvenimenti straordinari ed imprevedibili la ditta potrà domandare la risoluzione del contratto ai sensi dell'art. 1467 del codice civile. La risoluzione non può essere domandata se la sopravvenuta onerosità rientra nell'alea normale del contratto così come definita dalle norme civilistiche in materia. La ditta appaltatrice qualora richieda la risoluzione del contratto per eccessiva onerosità sopravvenuta dovrà dimostrare tale situazione alla stazione appaltante con dati inconfutabili. La stazione appaltante si riserva la facoltà di accettare la domanda di risoluzione del contratto o di offrire modifiche eque alle condizioni del contratto.
4. In caso di inadempimento ai patti e agli obblighi contrattuali l'A.D., fatto salvo quanto previsto dal codice dei Contratti in ordine all'esecuzione in danno e alla risoluzione del rapporto contrattuale, applicherà una penalità del 1‰ (uno per mille) dell'importo contrattuale netto per ogni giorno di ritardo, fino al raggiungimento della percentuale massima del 10% (dieci per cento) dell'importo contrattuale netto.
5. **La fattura elettronica dovrà essere obbligatoriamente emessa in data successiva all'ultimazione della fornitura/servizio ovvero successivamente agli esiti positivi delle procedure previste ai fini dell'accertamento della conformità della fornitura/servizio (verbale di verifica conformità) e comunque, previa richiesta di autorizzazione al seguente indirizzo email: uam.sa.sca.cs@cor.difesa.it**, , ogni fattura dovrà essere compilata in maniera analitica nelle modalità richieste, come sopra specificato, e dovrà indicare il numero di protocollo del presente ordinativo e il numero di **CIG** e **CUP**, **la causale come da oggetto presente lettera e l'annotazione "SCISSIONE DEI PAGAMENTI".** La stessa dovrà essere intestata ed inviata a:

COMANDO PER LE OPERAZIONI IN RETE – SERVIZIO AMMINISTRATIVO - Via Stresa, n. 31/b – 00135 ROMA Codice Fiscale 96451060584. **Codice Ufficio ai sensi dell'articolo 3, del Decreto MEF n. 55 del 3 aprile 2013 in materia di emissione, trasmissione e ricevimento della fattura elettronica 2SR075**.

6. La Ditta si obbliga al rispetto dei "Patti di integrità" sottoscritti in sede di presentazione dell'offerta ai sensi dell'art. 1 comma 17 Legge 190/2012. Tali provvedimenti, allegati al presente atto, ne costituiscono parte integrante, sostanziale, e pattizia ed il mancato rispetto degli stessi determinerà la risoluzione del presente atto negoziale.

7. Il pagamento, detratte le eventuali penalità di cui la Ditta si sia resa passibile, verrà effettuato, su presentazione di regolare fattura, dalla **Tesoreria Provinciale dello Stato**, a mezzo di bonifico on-line sul conto corrente bancario/postale che codesta Ditta avrà cura di comunicare nell'ambito della dichiarazione di cui alla legge 136/2010 in materia di tracciabilità dei flussi finanziari, previa verifica di buona esecuzione/collaudo ed accettazione di quanto richiesto; **Si precisa che il pagamento effettuato al netto dell'IVA ove applicabile entro il termine massimo di gg. 60 (sessanta) dalla data di presentazione della fattura. Esso è tuttavia subordinato all'esito positivo dell'accertamento effettuato sulla veridicità di quanto dichiarato in merito alla regolarità contributiva (DURC).**

8. **L'IVA, qualora dovuta, è a carico dell'Amministrazione Difesa e, ai sensi dell'art. 1 comma 629, lettera b), della Legge 190/2014, sarà trattenuta da questa Stazione Appaltante per il successivo versamento all'erario.**

9. Il presente affidamento trova copertura finanziaria con risorse attestate sul **capitolo di bilancio 1269/2 dell'E.F. 2025** mediante apertura di credito a favore del Funzionario Delegato dell'Ufficio Generale Centro di Responsabilità Amministrativa (UGCRA).

10. **La fornitura di eventuali materiali dovrà essere effettuata a cura di codesta Ditta presso il magazzino di questo Comando sito in Viale Castro Pretorio, 57 – 00185 Roma, indicando la codifica NATO dei materiali, previo contatto telefonico con il Mar.Ca. Alfredo MILITANO al seguente numero di telefono 06-46914523 - e-mail: consegnatario2@cor.difesa.it.**

11. **Direttore dell'Esecuzione Contrattuale (D.E.C.): Ten. Col. Davide CANEPARI tel. 01853334545 mail to: davide-canepari@marina.difesa.it.**

12. **Nell'ambito della fornitura oggetto del presente accordo/contratto, la Ditta si impegna ad operare nel rispetto delle politiche e procedure di sicurezza delle informazioni in essere presso l'Amministrazione e la sede stanziale di questa. L'Amministrazione sarà tenuta a mostrare all'operatore economico le predette politiche e procedure in caso di richiesta da parte dello stesso.**

13. La Ditta si impegna a mantenere riservata, anche al termine del presente atto, qualsiasi informazione, sia essa in forma verbale, elettronica o cartacea, di cui venga a conoscenza durante o per l'erogazione del servizio/fornitura oggetto del presente contratto/ordine di acquisto.
La presente obbligazione di riservatezza non si applica alle informazioni che: (1) siano di dominio pubblico al momento della loro comunicazione; (2) siano state sviluppate autonomamente dalla Ditta; (3) siano divenute di dominio pubblico senza alcuna responsabilità da parte della Ditta, successivamente alla loro comunicazione da parte dell'Amministrazione alla Ditta; (4) siano già nella disponibilità della Ditta al momento della loro comunicazione da parte dell'Amministrazione e non siano gravate da alcun obbligo di riservatezza; (5) siano state comunicate a terzi da parte dell'Amministrazione senza alcun obbligo di riservatezza per i terzi; (6) siano state divulgate, per le quali l'Amministrazione ha espresso il suo consenso alla diffusione. In aggiunta a quanto sopra previsto, la Ditta può liberamente comunicare le suddette informazioni in caso di richieste derivanti da un'Autorità Giudiziaria. L'Amministrazione è a conoscenza del fatto che qualora la Ditta dovesse svolgere la propria attività commerciale nella ricerca e nell'analisi dei servizi I.T., la presente obbligazione di riservatezza non si applicherà ad ogni informazione ottenuta dalla Ditta attraverso ricerche, analisi, consulenze provenienti da fonti diverse dall'Amministrazione, ivi compresi i dipendenti che ricevono informazioni ai sensi del presente contratto.

14. **Nella fase di accertamento delle autocertificazioni, rese secondo quanto richiesto dall'articolo 94 del D.Lgs. 36 del 31 marzo 2023, nel caso di discordanza ovvero di dichiarazioni mendaci, il presente atto negoziale si riterrà unilateralmente annullato; inoltre questa stazione appaltante procederà alla prevista segnalazione all'Autorità Competente.**

IL RESPONSABILE UNICO DEL PROGETTO
IN FASE AFFIDAMENTO
Brig. Gen. Maurizio AMBIASE
(Documento firmato digitalmente)

Firmato Digitalmente da/Signed by:
MAURIZIO AMBIASE
RUP AFFIDAM
In Data/On Date:
mercoledì 1 ottobre 2025 10:55:40

ANTONIO CORRADO
03.10.2025 15:55:01
GMT+02:00

PER ACCETTAZIONE
IL LEGALE RAPPRESENTANTE DELLA DITTA
(Documento firmato digitalmente)

KPMG Advisory S.p.A.
Via Curtatone, 3
00185 ROMA RM
Telefono +39 06 80971.1
Email it-fmadvisory@kpmg.it
PEC kpmgadvisoryspa@pec.kpmg.it

ALLEGATO 1

OGGETTO: Tracciabilità dei flussi finanziari - L. 136 del 13 agosto 2010, art. 3 (GURI n. 196 del 23 agosto 2010).

DICHIARAZIONE
(ex D.P.R. N.445 del 28 dicembre 2000)

In relazione a quanto in oggetto, il sottoscritto Antonio Corrado, nato a Lecce il 20/09/1972, residente a Roma in Via Mantova n. 16, in qualità di Procuratore Speciale (giusta procura speciale rilasciata con atto autenticato nella firma dal Notaio Federico Prinetti di Milano in data 30/11/2023, repertorio n. 18.703, raccolta n. 8.978, durata in carica fino alla revoca) della KPMG Advisory S.p.A., sede legale in Milano, Via Vittor Pisani n. 27, Partita IVA/C.F. 04662680158

DICHIARA

- di assumere gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3, commi 7 e 8, della legge 13 agosto 2010, n. 136;

- di assumere gli obblighi connessi con l'identificazione dei lavoratori previsti dall'art. 18, comma 1, lettera n), del D.Lgs. 81/2008, così come integrato dall'art. 5 della legge n. 136/2010.

Istituto bancario: Credito Emiliano S.p.A.;

IBAN: IT41M0303201600010000746867;

ABI: 03032;

CAB: 01600;

C/c: 010000746867;

CIN: M;

GENERALITA' DELEGATO/I AD OPERARE SUL CONTO:

FEDERICO BONANNI	CF BNNFRC66L07L483V
EMANUELE LOLLO	CF LLLMNL70E29A818U
MICHELE PARRAVICINI	CF PRRMHL63D15D416F
RAFFAELE ZINNO	CF ZNNRFL67C20L259N
FRANCESCO PAOLO GAGLIARDI	CF GGLFNC73D21F052T
STEFANO AZZOLARI	CF ZZLSFN65T22A246F

Dichiara infine

che **KPMG Advisory S.p.A.** dispone di più conti correnti dedicati, in modo non esclusivo, alle transazioni soggette alla L.136 del 13/08/10 e vigendo l'obbligo di dichiararli tutti, trasmette il dettaglio allegato.
La società si impegna a comunicare all'Ente ogni eventuale variazione relativa al/i predetto/i conto/i corrente/i e ai soggetti autorizzati ad operare su di esso/i.

La società accetta che l'Ente provveda alla liquidazione del corrispettivo contrattuale, a mezzo bonifico bancario sull'Istituto di credito o su Poste Italiane S.p.A. e sul numero di conto corrente dedicato indicato nella presente clausola, secondo quanto disposto dal contratto in questione, sulla base della consuntivazione dei servizi/forniture effettivamente prestati.

Roma, 03.09.2025

KPMG Advisory S.p.A.

Antonio Corrado

Procuratore Speciale

(Firmato digitalmente)

CONTI CORRENTI DEDICATI, IN MODO NON ESCLUSIVO, ALLE TRANSAZIONI SOGGETTE ALLA L. 136 DEL 13/08/10 PER KPMG ADVISORY SPA.

1) **BANCO BPM SPA- Conto attivo dal 10.09.2010**
Fil. 00670 – Piazza Duca D'Aosta, 8/2
20124 Milano
CONTO CORRENTE N. 000000019233
IBAN: IT59W0503401741000000019233
SWIFT: BAPPIT21670

DELEGATI:	RAFFAELE ZINNO	CF ZNNRFL67C20L259N
	FEDERICO BONANNI	CF BNNFRC66L07L483V
	EMANUELE LOLLO	CF LLLMNL70E29A818U
	FRANCESCO PAOLO GAGLIARDI	CF GGLFNC73D21F052T
	MICHELE PARRAVICINI	CF PRRMHL63D15D416F
	STEFANO AZZOLARI	CF ZZLSFN65T22A246F

2) **BANCO BPM SPA – Conto attivo dal 24/07/1997**
Fil. 00670 – Piazza Duca D'Aosta, 8/2
20124 Milano
CONTO CORRENTE N. 000000016300
IBAN: IT42I0503401741000000016300
SWIFT: BAPPIT21670

DELEGATI:	RAFFAELE ZINNO	CF ZNNRFL67C20L259N
	FEDERICO BONANNI	CF BNNFRC66L07L483V
	EMANUELE LOLLO	CF LLLMNL70E29A818U
	FRANCESCO PAOLO GAGLIARDI	CF GGLFNC73D21F052T
	MICHELE PARRAVICINI	CF PRRMHL63D15D416F
	STEFANO AZZOLARI	CF ZZLSFN65T22A246F

3) **BANCO DI DESIO E DELLA BRIANZA – conto attivo da 24.08.2004**
Fil. 59 – Via Pergolesi, 20
20124 Milano
CONTO CORRENTE N. 000000362700
IBAN: IT54F0344001603000000362700
SWIFT: BDBDIT22

DELEGATI:	RAFFAELE ZINNO	CF ZNNRFL67C20L259N
	FEDERICO BONANNI	CF BNNFRC66L07L483V
	EMANUELE LOLLO	CF LLLMNL70E29A818U
	FRANCESCO PAOLO GAGLIARDI	CF GGLFNC73D21F052T
	MICHELE PARRAVICINI	CF PRRMHL63D15D416F

4) **BANCA NAZIONALE DEL LAVORO – conto attivo dal 07/02/1994**
Succ. Metropolitana - MILANO
Piazza Lina Bo Bardi, 3
20124 Milano

CONTO CORRENTE N. 000000016530

IBAN: IT61E0100501612000000016530
SWIFT: BNLIITRR

DELEGATI:	RAFFAELE ZINNO	CF ZNNRFL67C20L259N
	FEDERICO BONANNI	CF BNNFRC66L07L483V
	EMANUELE LOLLO	CF LLLMNL70E29A818U
	FRANCESCO PAOLO GAGLIARDI	CF GGLFNC73D21F052T
	MICHELE PARRAVICINI	CF PRRMHL63D15D416F
	STEFANO AZZOLARI	CF ZZLSFN65T22A246F

5) <u>UNICREDIT SPA – conto attivo dal 20.03.2014</u>
Corporate Operations & Customer Care Italy

CONTO CORRENTE N. 000103123277
IBAN: IT57W0200805364000103123277
SWIFT: UNCRITMMOMM

DELEGATI:	RAFFAELE ZINNO	CF ZNNRFL67C20L259N
	FEDERICO BONANNI	CF BNNFRC66L07L483V
	FRANCESCO PAOLO GAGLIARDI	CF GGLFNC73D21F052T
	EMANUELE LOLLO	CF LLLMNL70E29A818U
	MICHELE PARRAVICINI	CF PRRMHL63D15D416F
	CARMELO MARIANO	CF MRNCML72L24Z133Z
	ANDREA CAPPELLETTI	CF CPPNDR70T29H501E
	MARCO DUCCIO PERRONE	CF PRRMCD77B24L219R
	ALESSANDRO BELLIA	CF BLLLSN81A14G914P
	STEFANO AZZOLARI	CF ZZLSFN65T22A246F

6) <u>CREDIT AGRICOLE – CARIPARMA – conto attivo dal 17.05.2017</u>
Ag. 3 Milano
Via Pirelli-Ang. Via Fara, 20
20124 Mlano

CONTO CORRENTE N. 0000043923521
IBAN: IT12G0623001630000043923521
SWIFT: CRPPIT2P230

DELEGATI:	EMANUELE LOLLO	CF LLLMNL70E29A818U
	MICHELE PARRAVICINI	CF PRRMHL63D15D416F
	RAFFAELE ZINNO	CF ZNNRFL67C20L259N
	FEDERICO BONANNI	CF BNNFRC66L07L483V
	FRANCESCO PAOLO GAGLIARDI	CF GGLFNC73D21F052T
	STEFANO AZZOLARI	CF ZZLSFN65T22A246F

7) <u>INTESA SANPAOLO – conto attivo dal 25.06.2021</u>
Ag. 01876 Milano
Via G. Verdi, 8
20121 Milano

CONTO CORRENTE N. 100000071675
IBAN: IT87S0306909400100000071675
SWIFT: BCITITMM

DELEGATI:	EMANUELE LOLLO	CF LLLMNL70E29A818U

KPMG

MICHELE PARRAVICINI	CF PRRMHL63D15D416F
RAFFAELE ZINNO	CF ZNNRFL67C20L259N
FEDERICO BONANNI	CF BNNFRC66L07L483V
FRANCESCO PAOLO GAGLIARDI	CF GGLFNC73D21F052T
STEFANO AZZOLARI	CF ZZLSFN65T22A246F

8) <u>CREDITO EMILIANO– conto attivo dal 27.04.2022</u>
Sede di Milano
Via Andegari, 14
20121 Milano

CONTO CORRENTE N. 010000746867
IBAN: IT41M0303201600010000746867
SWIFT: BACRIT22XX

DELEGATI:	FEDERICO BONANNI	CF BNNFRC66L07L483V
	EMANUELE LOLLO	CF LLLMNL70E29A818U
	MICHELE PARRAVICINI	CF PRRMHL63D15D416F
	RAFFAELE ZINNO	CF ZNNRFL67C20L259N
	FRANCESCO PAOLO GAGLIARDI	CF GGLFNC73D21F052T
	STEFANO AZZOLARI	CF ZZLSFN65T22A246F

Nome e Cognome	Luogo e data di nascita	Residenza Luogo e indirizzo	Codice Fiscale	Carica
RAFFAELE ZINNO	Torre Del Greco (NA) 20 marzo 1967	Roma (RM), Via Nizza n. 51	ZNNRFL67C20L259N	Presidente del CdA
FEDERICO BONANNI	Udine (UD) 07 luglio 1966	Verona (VR), Via Rovereto n. 5	BNNFRC66L07L483V	Amministratore Delegato
EMANUELE LOLLO	Besana in Brianza (MB) 29 maggio 1970	Inverigo (CO) Via Curcetto 29	LLLMNL70E29A818U	Amministratore
FRANCESCO PAOLO GAGLIARDI	Matera (MT) 21 aprile 1973	Milano (MI), Viale Ergisto Bezzi n. 2	GGLFNC73D21F052T	Vice Presidente del CdA
MICHELE PARRAVICINI	Erba (CO) 15 aprile 1963	Albavilla (CO), Via Mentana n. 4	PRRMHL63D15D416F	Procuratore Speciale
CARMELO MARIANO	Zurigo (Svizzera) 24 luglio 1972	Casalecchio di Reno (BO), Via Bazzanese n. 2/15	MRNCML72L24Z133Z	Procuratore Speciale
ANDREA CAPPELLETTI	Roma (RM) 29 dicembre 1970	Roma (RM), Via Giovanni Paisiello n. 12	CPPNDR70T29H501E	Procuratore Speciale
STEFANO AZZOLARI	Alzano Lombardo (BG) 2 dicembre1965	Bergamo (BG), Viale Papa Giovanni XXIII n. 72	ZZLSFN65T22A246F	Procuratore Speciale
MARCO DUCCIO PERRONE	Torino (TO) 24 febbraio 1977	Torino (TO) Corso Giuseppe Siccardi n. 15	PRRMCD77B24L219R	Procuratore Speciale

KPMG

Nome e Cognome	Luogo e data di nascita	Residenza Luogo e indirizzo	Codice Fiscale	Carica
ALESSANDRO BELLIA	Portogruaro (VE) 14 gennaio 1981	Padova (PD) Via Antonio Pertile n. 46/A	BLLLSN81A14G914P	Procuratore Speciale

Allegato 2

MINISTERO DELLA DIFESA
COMANDO PER LE OPERAZIONI IN RETE
PATTO DI INTEGRITA'

OGGETTO Gara 149 – acquisizione percorsi formazione specialistica in ambito progetti Cyber Capacity Building a favore partner internazionali – CUP D89J25000650001 – Capitolo 1269/2 – E.F. 2025.

tra

il Comando per le Operazioni in Rete - Ufficio Amministrazione

e

la Ditta KPMG Advisory S.p.A. (di seguito denominata Ditta), sede legale in Milano, via Vittor Pisani n. 27 codice fiscale/P.IVA 04662680158, rappresentata da Antonio Corrado in qualità di Procuratore Speciale (giusta procura speciale rilasciata con atto autenticato nella firma dal Notaio Federico Prinetti di Milano in data 30/11/2023, repertorio n. 18.703, raccolta n. 8.978, durata in carica fino alla revoca)

Il presente documento deve essere obbligatoriamente sottoscritto e presentato insieme all'offerta da ciascun partecipante alla gara in oggetto. La mancata consegna del presente documento, debitamente sottoscritto, comporterà l'esclusione automatica dalla gara.

VISTO

- la legge 6 novembre 2012 n. 190, art. 1, comma 17 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
- il decreto legislativo 14 marzo 2013, n. 33 avente per oggetto il "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- il decreto del Presidente della Repubblica 16 aprile 2013, n. 62 con il quale è stato emanato il "Regolamento recante il codice di comportamento dei dipendenti pubblici";
- il Protocollo d'intesa siglato tra il Ministero dell'Interno e l'Autorità Nazionale Anticorruzione il 15 luglio 2014;
- il decreto-legge 24 giugno 2014, n. 90 recante "Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari" convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114;
- il Protocollo d'intesa siglato tra il Ministero dell'Interno e l'Autorità Nazionale Anticorruzione il 15 luglio 2014;
- il "Regolamento in materia di esercizio del potere sanzionatorio dell'Autorità Nazionale Anticorruzione per l'omessa adozione dei Piani triennali di prevenzione della corruzione, dei Programmi triennali di trasparenza, dei Codici di comportamento" emanato dall'Autorità Nazionale Anticorruzione con delibera del 9 settembre 2014;

- il "Codice di comportamento dei dipendenti del Ministero della Difesa" approvato dal Ministro della Difesa il 22 marzo 2018;
- il Piano Nazionale Anticorruzione (P.N.A.) emanato dall'Autorità Nazionale Anticorruzione approvato con Delibera n. 1064 del 13 novembre 2019, e relativi allegati;
- il Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT) 2023-2025 del Ministero della Difesa;

SI CONVIENE QUANTO SEGUE

Art. 1 - Il presente Patto d'integrità stabilisce la formale obbligazione della Ditta che, ai fini della partecipazione alla gara in oggetto, si impegna:

- a conformare i propri comportamenti ai principi di lealtà, trasparenza e correttezza, a non offrire, accettare o richiedere somme di denaro o qualsiasi altra ricompensa, vantaggio o beneficio, sia direttamente che indirettamente tramite intermediari, al fine dell'assegnazione del contratto e/o al fine di distorcerne la relativa corretta esecuzione;
- a segnalare alla stazione appaltante qualsiasi tentativo di turbativa, irregolarità o distorsione nelle fasi di svolgimento della gara e/o durante l'esecuzione dei contratti, da parte di ogni interessato o addetto o di chiunque possa influenzare le decisioni relative alla gara in oggetto;
- ad assicurare che non si è accordata e non si accorderà con altri partecipanti alla gara per limitare o eludere la concorrenza e, comunque, di non trovarsi in altre situazioni ritenute incompatibili con la partecipazione alle gare dal Codice degli Appalti, dal Codice Civile o dalle altre disposizioni normative vigenti;
- ad informare puntualmente tutto il personale, di cui si avvale, del presente Patto di integrità e degli obblighi in esso contenuti;
- a vigilare affinché gli impegni sopra indicati siano osservati da tutti i collaboratori e dipendenti nell'esercizio dei compiti loro assegnati;
- a denunciare alla Pubblica Autorità competente ogni irregolarità o distorsione di cui sia venuta a conoscenza per quanto attiene l'attività di cui all'oggetto della gara in causa.

Il legale rappresentante della Ditta, inoltre, dichiara: - di non aver conferito incarichi ai soggetti di cui all'art. 53, comma 16- ter, del D.Lgs.. n. 165 del 30 marzo 2001, così come integrato dall'art. 21 del D.Lgs. 8 aprile 2013 n. 39 e di non aver stipulato contratti di lavoro subordinato o autonomo con i medesimi soggetti; - di essere consapevole che, qualora emerga la violazione del suddetto divieto verrà disposta l'immediata esclusione dalla partecipazione alla procedura di affidamento.

Art. 2 - La Ditta prende nota e accetta che nel caso di mancato rispetto degli impegni anticorruzione assunti con il presente Patto di integrità, comunque accertato dall'Amministrazione, potranno essere applicate le seguenti sanzioni:

- esclusione del concorrente dalla gara;
- escussione della cauzione di validità dell'offerta;
- risoluzione del contratto;
- escussione della cauzione di buona esecuzione del contratto;
- esclusione del concorrente dalle gare indette dalla stazione appaltante per 5 anni.

Art. 3 – Fermo restando quanto previsto dai precedenti articoli 1 e 2, in aderenza alle prescrizioni in materia di anticorruzione contenute nel d.l. 90/2014 convertito dalla l. 114/2014 e ss.mm.ii.:

- la Ditta si impegna a dare comunicazione tempestiva alla Stazione appaltante di tentativi di concussione che si siano, in qualsiasi modo, manifestati nei confronti dell'imprenditore, degli organi sociali o dei dirigenti di impresa. Il predetto adempimento ha natura essenziale ai fini della esecuzione del contratto. Ne consegue, pertanto, che il relativo inadempimento darà luogo alla risoluzione espressa del contratto stesso, ai sensi dell'art. 1456 c.c., qualora la mancata

comunicazione del tentativo di concussione subito risulti da una misura cautelare o dal disposto rinvio a giudizio, nei confronti di pubblici amministratori che abbiano esercitato funzioni relative alla stipula ed esecuzione del contratto, per il delitto previsto dall'art. 317 c.p.;

- la Stazione appaltante si impegna ad avvalersi della clausola risolutiva espressa, di cui all'art. 1456 c.c., ogni qualvolta nei confronti dell'imprenditore o dei componenti la compagine sociale, o dei dirigenti dell'impresa, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli arti. 317 c.p., 318 c.p., 319 c.p., 319-bis c.p., 319- ter c.p., 319-quater c.p., 320 c.p., 322 c.p., 322-bis c.p., 346-bis c.p., 353 c.p. e 353-bis c.p..

Nei casi di cui al presente articolo, l'esercizio della potestà risolutoria da parte della Stazione appaltante è subordinato alla previa intesa con l'Autorità Nazionale Anticorruzione. La Stazione appaltante, pertanto, comunicherà la propria volontà di avvalersi della clausola risolutiva espressa al Responsabile per la prevenzione della corruzione che ne darà comunicazione all'Autorità Nazionale Anticorruzione. Quest'ultima potrà valutare se, in alternativa all'ipotesi risolutoria, ricorrano i presupposti per la prosecuzione del rapporto contrattuale tra Stazione appaltante ed impresa aggiudicataria, alle condizioni di cui al d.l. 90/2014.

Art. 4 - Il contenuto del Patto di integrità e le relative sanzioni applicabili resteranno in vigore sino alla completa esecuzione del contratto. Il presente Patto dovrà essere richiamato dal contratto quale allegato allo stesso onde formarne parte integrante, sostanziale e pattizia.

Art. 5 - Il presente Patto deve essere obbligatoriamente sottoscritto in calce ed in ogni sua pagina, dal legale rappresentante della Ditta partecipante ovvero, in caso di consorzi o raggruppamenti temporanei di imprese, dal rappresentante degli stessi e deve essere presentato unitamente all'offerta. La mancata consegna di tale Patto debitamente sottoscritto comporterà l'esclusione dalla gara.

Art. 6 - Ogni controversia relativa all'interpretazione ed esecuzione del Patto d'integrità fra la Stazione appaltante ed i concorrenti e tra gli stessi concorrenti sarà risolta dall'Autorità Giudiziaria competente.

Luogo e data Roma, 03.09.2025

Per la Ditta:

Il Procuratore Speciale
(sottoscrizione digitale)

KPMG

ALLEGATO 4

Ai fini della validità dell'offerta, la stessa va presentata seguendo lo schema seguente.

Per informazioni a carattere amministrativo-procedurale:

SCHEMA DI OFFERTA

Allo **COMANDO OPERAZIONI IN RETE**
Ufficio Amministrazione - Sezione Gestione
Finanziaria e Contratti
Via Stresa, 31/B

Oggetto: **Gara 149 – acquisizione percorsi formazione specialistica in ambito progetti Cyber Capacity Building a favore partner internazionali – CUP D89J25000650001 – Capitolo 1269/2 – E.F. 2025 – Importo massimo previsto €. 117.647,06 (centodiciassettemilaseicentoquarantasette/06) IVA N/A.**

Il sottoscritto Antonio Corrado nella sua qualità di Procuratore Speciale (giusta procura speciale rilasciata con atto autenticato nella firma dal Notaio Federico Prinetti di Milano in data 30/11/2023, repertorio n. 18.703, raccolta n. 8.978, durata in carica fino alla revoca) della Ditta KPMG Advisory S.p.A., pec kpmgadvisoryspa.ufficiogare@pec.kpmg.it, residente in Roma, Via Mantova n. 16, Codice fiscale/partita I.V.A. n. 04662680158, sede legale in Milano, Via Vittor Pisani n. 27, sede operativa per la presente procedura di gara in Roma, Via Curtatone n. 3, presenta la seguente offerta:

TIPOLOGIA	Qtà richieste	Prezzo unitario	TOTALE COMPRENSIVO COSTI SICUREZZA, come da offerta MEPA (A)
acquisizione percorsi formazione specialistica in ambito progetti Cyber Capacity Building a favore partner internazionali come da Requisito Tecnico Operativo in allegato.	come da RTO in allegato	**€ 67.100,00**	€ 67.100,00
N.B. ALLEGARE DETTAGLIO ANALITICO PREZZI OFFERTI SUDDIVISO PER COSTO UNITARIO DEI MATERIALI E/O ATTIVITA' DA SVOLGERE COME DA RTO IN ALLEGATO		ONERI DELLA SICUREZZA (a cura stazione appaltante qualora previsti non soggetti a ribasso) (B)	€ 0,00
		COSTI SICUREZZA a cura Ditta indicazione obbligatoria (solo da indicare) *	€ 523,38
		IMPORTO IMPONIBILE	€ 67.100,00
		IVA N/A	*******
		Totale Offerta	**€ 67.100,00**

*** Ai sensi dell'art. 26, comma 6, del D.Lgs. 9 aprile 2008, n.81 e del D.L. n. 70/2011 "Decreto sviluppo", è obbligatoria l'indicazione dei costi per la sicurezza.**

La presente offerta ha validita fino al 31/12/2025.

L'OFFERENTE

KPMG Advisory S.p.A. - Antonio Corrado - Procuratore Speciale
firma digitale

SCUOLA TELECOMUNICAZIONI FF.AA.
Direzione Corsi

CAPITOLATO PER LA FORNITURA DI PERCORSI FORMATIVI AREA CYBER PER PERSONALE STRANIERO – ESIGENZA SMD VI REPARTO

Edizione giugno 2025

Capitolato

1. **Amministrazione appaltante**
   Comando per le Operazioni in Rete.

2. **Oggetto della prestazione**
   Oggetto della prestazione è lo svolgimento di corsi formativi, afferenti all'area *Cyber Security*, a favore di personale straniero individuato da SMD III Reparto e con il supporto di SMD VI Reparto, **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:
   - Corso "**CISO (*Chief Information Security Officer*)**";
   - Corso "***Cybersecurity Governance, Risk and Compliance***";
   - Corso "***Digital Transformation & Emerging Technologies***".

   I *Syllabus* dei corsi sono riportati in annesso al presente capitolato.

   I corsi dovranno essere erogati IN LINGUA INGLESE per il seguente numero di frequentatori:

   - Corso **CISO: 16 frequentatori per ciascuna sessione;**
   - Corso **"*Cybersecurity Governance, Risk and Compliance*": 20 frequentatori per ciascuna sessione;**
   - Corso **"*Digital Transformation & Emerging Technologies*": 20 frequentatori per ciascuna sessione.**

   Al fine di poter condurre in modo adeguato i previsti coordinamenti tra la ditta aggiudicataria e i responsabili della esecuzione dell'attività, **il\I docente\i individuato\i e il responsabile del prestatore di servizi aggiudicatario dovranno avere una buona capacità comunicativa anche in lingua italiana, almeno di livello scolastico.**

   La formazione in parola dovrà essere svolta in modalità **"live sincrona a distanza"** come di seguito specificato:
   1. **"CISO":**
      - Prima sessione: dal 13 ottobre al 24 ottobre 2025;
      - Seconda sessione: dal 10 novembre al 21 novembre 2025.
   2. **"*Cybersecurity Governance, Risk and Compliance*":**
      - Prima sessione: dal 29 settembre al 3 ottobre 2025;
      - Seconda sessione: dal 27 ottobre al 31 ottobre 2025;
   3. **"*Digital Transformation & Emerging Technologies*":**
      - Prima sessione: dal 6 ottobre al 10 ottobre 2025;
      - Seconda sessione: dal 3 novembre al 7 novembre 2025.

COD	CORSI	Durata GG	SETTEMBRE					OTTOBRE				NOVEMBRE			
	Data inizio settimana		1	8	15	22	29	6	13	20	27	3	10	17	24
International Portfolio															
TBD	Cybersecurity Governance, Risk e Compliance	5					■ 20				■ 20				
TBD	Digital Transformation & Emerging Technologies	5						■ 20				■ 20			
TBD	CISO (Chief Information Security Officer)	5							■ 16	■ 16			■ 16	■ 16	

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

3. Obiettivi

3.1. Tipologia di formazione

Le attività formative a distanza dovranno tenersi da lunedì a venerdì per un totale di **256 ore complessive** come di seguito specificato:

4. **CISO**: **64 ore complessive per ciascuna sessione** (5 gg per 2 settimane – 32 ore a settimana);
5. ***Cybersecurity Governance, Risk and Compliance*: 32 ore complessive per ciascuna sessione** (5 gg per 1 settimane – 32 ore a settimana);
6. ***Digital Transformation & Emerging Technologies*: 32 ore complessive per ciascuna sessione** (5 gg per 1 settimane – 32 ore a settimana).

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.

Al termine di ogni sessione di ciascun corso la Ditta aggiudicataria, su indicazioni e in coordinamento con i referenti (RUP, DEC), dovrà prevedere una prova valutativa, fornendo un set di almeno nr. 30 domande a risposta multipla 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.

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.

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

4. Responsabili del prestatore di servizi aggiudicatario

Il prestatore di servizi aggiudicatario, entro 7gg dalla firma del contratto, dovrà nominare e comunicare al RUP e DEC il nominativo di 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 il certificato ISO 9001:2015, settore EA37 istruzione (allegare sul MEPA relativa documentazione attestante);
- Per la verifica dei requisiti richiesti la Ditta aggiudicataria dovrà pertanto presentare e allegare sul MEPA in sede di offerta, 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;
  - 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.
- La ditta aggiudicataria deve comunicare eventuali personalizzazioni dei contenuti.

ANNESSO

Syllabus

Corso CISO *(Chief Information Security Officer):*

Prima sessione: dal 13 ottobre al 24 ottobre 2025
Seconda sessione: dal 10 novembre al 21 novembre 2025
Durata 2 settimane per un totale di 64 ore (7 ore al giorno dal lunedì al giovedì - 4 ore il venerdì).
Modalità: e-learning sincrono.

COURSE OVERVIEW

The course aims to develop the necessary skills to define security strategies, implement policies, and manage resources, personnel, processes, and tasks within an organization concerning cybersecurity aspects.

COURSE OBJECTIVES

- Manage the implementation of cyber policies within an organization.
- Develop, define, manage, and communicate security measures for the protection of networks and IT systems.
- Ensure information exchange and relationship management with various stakeholders.

TARGET AUDIENCE

- CISOs & Security Executives – Leaders responsible for shaping and implementing security policies at an organizational level.
- Risk & Compliance Officers – Experts overseeing regulatory requirements and governance frameworks.
- Security Architects & IT Managers
- Incident Response & Crisis Managers
- Government & Military Cybersecurity Personnel

PREREQUISITES

- Fundamental understanding of cybersecurity concepts
- Basic knowledge of network security, cloud computing, and identity management
- Familiarity with risk management frameworks (e.g., NIST, ISO 27001)

COURSE MODULES

1. Security Risk Management, Controls, Audit Management

This module focuses on the identification and evaluation of cybersecurity risks, including assessment methodologies, impact analysis, and mitigation strategies. Participants will also explore identity and access management, cryptographic techniques, and advanced security architectures.

KEY TOPICS

- Risk Assessment Methodologies and Impact Analysis

- Authentication and Authorization Methods
- Cloud Security and Shared Responsibility
- Emerging Architectures: Microservices, Containers, IoT
- Cryptographic Principles and Secure Key Exchange
- TOR Network

2. Cyber Threats and Attack Techniques

Participants will gain insight into various cyber threats, including APT (Advanced Persistent Threat) groups, malware classifications, botnet operations, and DDoS mitigation strategies.

KEY TOPICS

- Threat Landscape and Attack Objectives
- Lockheed Martin Kill Chain, MITRE ATT&CK Framework
- Malware Analysis and Evasion Techniques
- Botnets, Command and Control Mechanisms
- DDoS Attack Types and Countermeasures

3. Incident Response and Crisis Management

This module covers the essentials of incident response, including stakeholder management, forensic analysis, and emergency communication strategies to handle security breaches effectively.

KEY TOPICS

- Incident Response Plans and Mitigation Tactics
- Digital Forensics and Threat Attribution
- Emergency Communication and Stakeholder Coordination
- Security Audit and Monitoring

4. Business Continuity & Disaster Recovery

Students will learn how to ensure operational resilience through business continuity planning and disaster recovery strategies.

KEY TOPICS

- Business Impact Analysis and Recovery Planning
- Strategies for Data Redundancy and Backup Protection
- Testing and Validating Disaster Recovery Plans

5. Cyber Threat Intelligence & Risk Mitigation

In this module, participants will explore intelligence gathering methods, analyzing emerging hacker techniques, and using threat intelligence to improve security posture.

KEY TOPICS

- Intelligence Sources: Big Data, Open Source, Dark Web
- Trend Analysis of Cyber Threats
- Sharing Threat Intelligence with External Partners
- Updating Security Controls Based on Emerging Threats

COURSE DURATION

Two weeks in **live/synchronous remote** format.

Corso *"Cybersecurity Governance, Risk and Compliance":*

Prima sessione: dal 29 settembre al 03 ottobre 2025
Seconda sessione: dal 27 ottobre al 31 ottobre 2025
Durata 1 settimana per un totale di 32 ore (7 ore al giorno dal lunedì al giovedì - 4 ore il venerdì).
Modalità: e-learning sincrono.

COURSE OVERVIEW

The course offers comprehensive training and an integrated approach to addressing cybersecurity challenges, risk management, and regulatory compliance. The program focuses on the creation and management of effective frameworks and aims to provide guidelines and best practices for effectively managing risks and implementing appropriate data and information protection measures to establish and oversee an efficient governance system.

COURSE OBJECTIVES

- Provide an in-depth overview of cybersecurity, current threats, and fundamental governance concepts in this field.
- Illustrate the importance of building a cybersecurity culture and engaging management and stakeholders in information protection.
- Explore cybersecurity regulations and laws.
- Examine international security standards and frameworks.
- Introduce risk management concepts and provide practical tools for risk identification, analysis, evaluation, and mitigation.

TARGET AUDIENCE

- Cybersecurity Managers & Risk Analysts
- IT & Security Consultants
- Legal & Compliance Officers
- Executives & Business Leaders
- Government & Military Cybersecurity Personnel

PREREQUISITES

- Understanding of basic cybersecurity principles, threats, and risk mitigation strategies.
- Basic knowledge of network security, cloud computing, and identity management
- Familiarity with risk management frameworks (e.g., NIST, ISO 27001, CIS controls)
- Awareness of regulatory compliance and standards in data protection and security governance.

COURSE MODULES

1. Cybersecurity Governance

This module introduces cybersecurity governance, covering fundamental principles, roles, and responsibilities in security management. Participants will explore how to develop security policies and resilience strategies.

KEY TOPICS

- Introduction to cybersecurity and current threats
- Basic principles of cybersecurity governance
- Organizational governance frameworks and Security policies
- Defining and measuring cybersecurity resilience

2. International Security Standards and Frameworks
This module introduces globally recognized security standards and compliance frameworks, equipping participants with best practices for cybersecurity implementation.

KEY TOPICS
- Overview of security standards and certifications
- Overview of ISO, NIST, CIS Controls, and other standards
- Certifications relevant to cybersecurity compliance
- Emerging global security frameworks

3. Compliance and Regulations
This module examines international cybersecurity regulations, helping participants understand and implement compliance requirements.

KEY TOPICS:
- ISO 27001 and International standard for Information Security Management Systems (ISMS)
- Global cybersecurity frameworks and regulatory laws
- Audit and certification procedures for cybersecurity governance
- Business continuity and disaster recovery strategies

4. Risk Management
Effective cybersecurity risk management requires systematic identification, assessment, and mitigation of cyber threats. This module focuses on international risk standards, frameworks, and assessment methodologies to secure digital environments.

KEY TOPICS:
- International standards for risk management and assessment
- Identifying, analyzing, and evaluating security risks
- Mitigation and risk treatment strategies

5. Operational Security
Cybersecurity operational security focuses on incident response, security monitoring, and technical defense strategies. This section explores the tools, methodologies, and best practices used by cybersecurity teams to protect digital assets.

KEY TOPICS:
- Incident Monitoring and detection techniques (SIEM, SOC, CSIRT)
- Standard Operating Procedures (SOPs)
- Service & Application Security Mapping

6. Information Security Management
This module explores data security strategies, emphasizing classification, encryption, and access control policies for information protection.

KEY TOPICS:
- Data Classification Models
- Access Control & Identity Management
- Document Management & Security Policies
- Data Encryption & Cyber Resilience Measures

7. Managing Future Cyber Risks
Cybersecurity risks are continuously evolving, driven by AI-powered threats, smart technologies, and cloud security vulnerabilities. This module provides a forward-looking approach to cybersecurity, preparing participants for future challenges.

KEY TOPICS:

- AI & Machine Learning in Cybersecurity
- Smart Societies & Cybersecurity Challenges
- Advanced Threat Landscapes
- Cloud Security Best Practices for data protection in cloud environments

COURSE DURATION
One week in **live/synchronous remote** format.

Corso" *Digital Transformation & Emerging Technologies*":

Prima sessione: dal 06 ottobre al 10 ottobre 2025
Seconda sessione: dal 03 novembre al 07 novembre 2025
Durata 1 settimana per un totale di 32 ore (7 ore al giorno dal lunedì al giovedì - 4 ore il venerdì).
Modalità: e-learning sincrono

COURSE OVERVIEW

The course will provide a general overview of the phenomenon of digital transformation and innovative digital tools, as well as an architectural understanding of technologies, applications, and processes for collecting and managing large amounts of data.
Additionally, emerging digital technologies and the broader concept of the digital revolution will be introduced. The development of new digital tools is also changing the way information is processed; thus, the course will offer knowledge on the primary dynamics of digital transformation and an overview of digital tools, methods, and techniques.

COURSE OBJECTIVES

- Understand emerging digital trends and the importance of the digital revolution.
- Gain knowledge of relevant and emerging digital technologies.
- Apply a technical approach and digital tools.
- Utilize terminology and communication typical of digitalization and technology.
- Foster the development of interpersonal skills in international contexts.

TARGET AUDIENCE

- Cybersecurity Managers & Risk Analysts
- IT & Digital Professionals
- Executives & Business Leaders
- Government & Military Cybersecurity Personnel

PREREQUISITES

- Familiarity with **modern computing concepts**
- Basic knowledge of **data analytics, machine learning, and artificial intelligence**.

COURSE MODULES

1. Introduction to Cyber Security Attacks Analysis
This module provides a foundational understanding of cybersecurity threats and attack methodologies, emphasizing their role in digital transformation. Participants will explore how cyber threats impact modern technological systems and how organizations develop defense strategies.

KEY TOPICS

- Definition and importance of cybersecurity attack analysis
- Understanding attack vectors and methodologies
- Cyber defense strategies and the significance of incident response

2. Digitalization Trends

The digital revolution is reshaping industries through agile innovation and design thinking methodologies. This module covers strategies for digital transformation and the application of cutting-edge innovation frameworks.

KEY TOPICS

- Design Thinking – A user-centric approach to digital innovation.
- Agile Development & Open Innovation – Methods for adapting to rapid technological changes.
- Emerging trends shaping digital business models.

3. Blockchain and Distributed Ledger Technologies

Blockchain and distributed ledgers are revolutionizing data security, financial transactions, and business ecosystems. This module explores how decentralized technologies impact industries and introduces smart contracts and decentralized applications.

KEY TOPICS:

- The fundamentals of blockchain technology.
- Smart contracts – Their role in automation and security.
- Decentralized applications

4. Digital Platforms and Ecosystems

Digital platforms create new economic models and shift business operations towards network-driven ecosystems. This module examines how platform-based businesses thrive in modern industries.

KEY TOPICS:

- Platform economy – How digital platforms redefine industries.
- Digital ecosystems – Interconnected business models enabling innovation.

5. Change Management and Leadership

This module focuses on leadership strategies for successful digital transformation initiatives, emphasizing cultural shifts and skill development.

KEY TOPICS:

- Digital Leadership – Driving change in modern organizations.
- Organizational Change – Overcoming resistance in digital transitions.
- Skills Development & Training – Fostering innovation-ready teams.
- Cultural Transformation – Establishing digital-first mindsets.

6. The Role of Data in Digital Transformation

Data is the backbone of technological evolution, influencing decisions, automation, and business strategies. This module covers data processing and governance frameworks for digital transformation.

KEY TOPICS:

- How data-driven insights influence digital innovation.
- Data governance policies for businesses.

7. Data Analysis and Artificial Intelligence

AI and data analytics power predictive insights, enabling organizations to make strategic decisions based on machine learning algorithms.

KEY TOPICS:

- Big Data Architecture – Managing massive information flows.
- Machine Learning Applications – AI-driven automation strategies.
- Predictive Analytics – Forecasting trends through AI models.

8. Virtual Reality (AR/VR/MR)
Immersive technologies like augmented reality (AR), virtual reality (VR), and mixed reality (MR) are shaping new user experiences. This module explores their applications across industries.

KEY TOPICS
- Extended Reality (XR) – Combining multiple immersive technologies.
- Digital Twin Technology – Real-world simulation models.
- Future of Human-Computer Interaction – AI-driven interfaces.

9. Quantum Cryptography and Quantum Computing
Quantum technology is set to revolutionize encryption methods and computational speed. This module covers its potential impact on cybersecurity and business applications.

KEY TOPICS
- Quantum cryptography – Future-proof security protocols.
- Quantum computing applications in finance and research.

10. Internet of Things (IoT)
IoT is driving smart solutions, integrating connected devices across industries to enhance automation and efficiency.

KEY TOPICS:
- IoT Architecture & Platforms – How interconnected devices operate.
- Industrial IoT Applications – Automation in manufacturing.
- Connected ecosystems – The role of IoT in smart cities.

11. Digital Transformation and Its Impact on Organizations
Digital transformation reshapes corporate structures, affecting decision-making, enterprise systems, and user-focused design.

KEY TOPICS:
- Decision Support Systems – AI-driven business strategies.
- Enterprise Information Systems – Automation in corporate environments.
- User-Centered Design – Improving usability through digital enhancements.

12. Ethics and Technological Innovation
With rapid digital innovation comes ethical concerns regarding data privacy, AI ethics, and societal impact.

KEY TOPICS:
- AI ethics – Addressing biases in algorithm development.
- Responsible digital transformation – Ensuring ethical tech adoption.

13. Risk Management and Security
This module focuses on cybersecurity strategies, ensuring organizations can safeguard digital transformation initiatives against cyber threats.

KEY TOPICS:
- Cybersecurity Frameworks – Industry security models.
- Risk Assessment & Mitigation – Evaluating vulnerabilities.
- Privacy Considerations & Compliance – Regulatory requirements in digital technologies.

COURSE DURATION
One week in **live/synchronous remote** format.

Allegato "B"

Corsi per il *Cyber Capacity Building* – Anno 2025

1. **Da finanziare con fondi ACN (attestati al COR, *online*, in inglese):**

   - ***Cybersecurity Governance, Risk and Compliance***
     - dal 29 settembre al 03 ottobre 2025 (1^ sessione, 20 unità max)
     - dal 27 al 31 ottobre 2025 (2^ sessione, 20 unità max)

   - ***Digital Transformation & Emerging Technologies***
     - dal 6 al 10 ottobre 2025 (1^ sessione, 20 unità max)
     - dal 3 al 7 novembre 2025 (2^ sessione, 20 unità max)

   - ***Chief Information Security Officer***
     - dal 13 al 24 ottobre 2025 (1^ sessione, 16 unità max)
     - dal 10 al 21 novembre 2025 (2^ sessione, 16 unità max)

2. **Già finanziati nell'ambito delle attività di SMD III (in presenza, in inglese):**

   Cyber Threat Hunting
   dal 01 al 12 dicembre: sessione unica, 15 unità max di cui 8 dedicati agli stranieri (restanti 7 da AD selezionati con adeguata conoscenza di inglese)

3. **Previsti per personale italiano, con la presenza di n.1 frequentatore straniero (*online*, in italiano):**

   - ***Malware Analysis***
     dal 08 al 26 settembre 2025 (n.1 frequentatore straniero);

   - ***Digital Forensics***
     dal 06 al 24 ottobre 2025 (n.1 frequentatore straniero).