

COMANDO OPERAZIONI IN RETE

UFFICIO AMMINISTRAZIONE

Sezione Gestione Finanziaria e Contratti

C. F. 96451060584

Via Stresa 31/B – 00135 ROMA

Posta elettronica: cor@cor.difesa.it

Posta elettronica certificata: cor@postacert.difesa.it

Roma, 27/05/2025

FRRR S.R.L.

Via Borgo dei Leoni, 70/C Ferrara

(pec: frrrsrl2021@pec.it)

Lettera di Ordinazione n. 56

Oggetto: GARA 60 Acquisto vouchers per corsi formazione specialistica Cyber per il personale militare del COR. – Cap. 2265/1 EF 2025. – CIG B6D8C6E080 - CUP D89J25000050001 – RDO 5357751.
IDV 1986452-1920233

1. Codesta Ditta, si obbliga ad eseguire la sottonotata fornitura/prestazione, comprensiva dei relativi costi per la sicurezza, pari a euro 0,00 come da citata R.D.O.:

Descrizione	Quantità	Prezzo Unitario	Imponibile
Acquisto vouchers per corsi formazione specialistica Cyber per il personale militare del COR come da Requisiti Tecnici in allegato.			€ 9.696,00
Esonero deposito cauzionale -1%			€ 96,96
Totale Imponibile			€ 9.599,04
Iva ESENTE ai sensi art. 72 comma 3 punto 2 del D.P.R. 633/72			*****
Totale			€ 9.599,04

2. La presenta commessa, per tutto quanto non previsto nella presente, si svolgerà sotto l'osservanza del Codice dei contratti di cui al **decreto legislativo 31 marzo 2023, nr. 36**;
3. 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 30/10/2025**, osservando tutte le norme e disposizioni indicate nella presente lettera di ordinazione.
4. 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.
5. 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.
6. **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**.

7. 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.
8. 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/collaudato 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).
9. 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.
10. Il presente affidamento trova copertura finanziaria con risorse attestate sul capitolo di bilancio 2265/1 dell’E.F. 2025 mediante apertura di credito a favore del Funzionario Delegato dell’Ufficio Generale Centro di Responsabilità Amministrativa (UGCRA).
11. 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.
12. Direttori dell’Esecuzione Contrattuale (D.E.C.): Cap. Antonino MATASSA tel. 06/469124677 mail to: scd.uis.sacs.asva.cn@cor.difesa.it (RTO1) S.T.V. Sara RUFFO tel. 06/469124590 mail to: scd.cert.dthvii.add02@cor.difesa.it (RTO2).
13. 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.
14. 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.
15. 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 CAPO SERVIZIO AMMINISTRATIVO

Col. com. Maurizio LAMBIASE

(Documento firmato digitalmente)

Firmato Digitalmente da/Signed by:

MAURIZIO LAMBIASE

RUP AFF

In Data/On Date:

martedì 27 maggio 2025 10:53:26

FIRMA PER ACCETTAZIONE

IL LEGALE RAPPRESENTANTE DELLA DITTA

(Documento firmato digitalmente)

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 Monterumici Matteo, nato a Bondeno il 19/03/1976, residente a Bondeno in via Matteotti n.42, in qualità di legale rappresentante della FRRR SRL, sede legale in Ferrara, via Borgo dei Leoni 70/C, Partita IVA/C.F. 02098830389

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: La Cassa di Ravenna;

IBAN: IT73J0627013001cc0980282387

GENERALITA' DELEGATO/I AD OPERARE SUL CONTO:

- Nome Matteo _____ cognome Monterumici _____ cod. fisc. MNTMTT76C19A965Y

- Nome _____ cognome _____ cod. fisc. _____

- Nome _____ cognome _____ cod. fisc. _____

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.

Località, Ferrara

Timbro e firma

FRRR s.r.l.
Via Borgo dei Leoni, 70/c5
41121 FERRARA
Partita IVA 02098830389

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

OGGETTO: GARA 60 – II ESPERIMENTO Acquisto vouchers per corsi formazione specialistica Cyber per il personale militare del COR. CUP D89J25000050001 – Cap. 2265/1 EF 2025.

tra

il Comando per le Operazioni in Rete - Ufficio Amministrazione

e

la Ditta FRRR S.R.L...... (di seguito denominata Ditta),
sede legale in Ferrara....., via Borgo dei Leoni.....n. 70/C codice
fiscale/P.IVA 02098830389....., rappresentata da Monterumici Matteo
..... in qualità di legale rappresentante.....

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) 2022-2024 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 artt. 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

Per la Ditta:

**Il legale rappresentante
(sottoscrizione digitale)**

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 60 - II ESPERIMENTO Acquisto vouchers per corsi formazione specialistica Cyber per il personale militare del COR.
CUP D89J25000050001 – Cap. 2265/1 EF 2025 - Importo massimo previsto €. 16.210,00 (sedicimiladuecentodieci/00) iva esente .

Il sottoscritto Matteo MOnterumici nella sua qualità di amministratore unico della Ditta FRRR srl , pec frrrsrl2021@pec.it residente in Ferrara, Via Borgo dei Leoni 70 Codice fiscale/partita I.V.A. n. 02098830389 presenta la seguente offerta:

TIPOLOGIA	Qtà richieste	Prezzo unitario	TOTALE COMPRENSIVO COSTI SICUREZZA, come da offerta MEPA (A)
Acquisto vouchers per corsi formazione specialistica Cyber per il personale militare del COR. Come da RTO 1 e RTO 2 in allegato	come da requisito Tecnico Operativo 1 E 2 in allegato	€ 9.696,00	€ 9.696,00
N.B. ALLEGARE DETTAGLIO ANALITICO PREZZI OFFERTI SUDDIVISO PER COSTO UNITARIO DEI MATERIALI E/O ATTIVITA' DA SVOLGERE COME DA REQUISITO TECNICO 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) *	€ 0,00
		IMPORTO IMPONIBILE	€ 9.696,00
		IVA ESENTE	ESENTE
		Totale Offerta	€ 9.696,00

* 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 validità fino al 31/12/2025.

FRRR s.r.l.
Via Borgo dei Leoni, 70/c5
44121 FERRARA
Partita IVA 02098830389

L'OFFERENTE

timbro e firma

Spett.le COMANDO PER LE OPERAZIONI IN RETE

Ufficio Amministrazione

Sezione Gestione Finanziaria e Contratti

Via Stresa 31b – 00135 Roma

PEC: cor@postacert.difesa.it

Oggetto: Corsi di formazione specialistici per il potenziamento delle capacità operative del personale dell'Ufficio Infrastrutture di Sicurezza del COR

Facendo seguito alla Vs. cortese richiesta telefonica, vi inviamo qui di seguito il dettaglio dei corsi quotati:

Codice	Descrizione	Modalità	Periodo	N. discenti	Certificazione	Mat. Didattico	N. ore	Quantità	Costo IVA esclusa
OES002	Vulnerability Assessment Basics	A distanza	Non specificato	1	No	No	16	1	1.385,14 €
OWASP	Sicurezza delle Web Application - OWASP Testing Guide	A distanza	Non specificato	2	No	No	16	2	1.385,14 €
CISSP	Certified Information Systems Security Professional	A distanza	31/03/2025 – 08/04/2025	1	No	Si	16	1	1.385,14 €
	Computer Hacking Forensic Investigator (CHFI) - EC COUNCIL	A distanza	Non specificato	1	No	No	16	1	1.385,14 €
	Certified Threat Intelligence Analyst (CTIA) - EC COUNCIL	A distanza	Non specificato	1	No	No	16	1	1.385,14 €
	Malware Development - Maldev Academy	A distanza	Non specificato	1	No	No	16	1	1.385,14 €

Cordiali saluti.

Ferrara, 26/5/2025

FRRR s.r.l.
Via Borgo del Leone, 70/c5
44121 FERRARA
Partita IVA 02096830369



COMANDO PER LE OPERAZIONI IN RETE



REQUISITO TECNICO OPERATIVO

RELATIVO A

**Corsi di formazione specialistici per il potenziamento
delle capacità operative del personale dell'Ufficio
Infrastrutture di Sicurezza del COR**

Edizione Marzo 2025

PREDISPOSIZIONE DEL DOCUMENTO

Redatto da	Data
Comando per le Operazioni in Rete Reparto Sicurezza e <i>Cyber Defence</i> Ufficio Infrastrutture di Sicurezza Sezione Architetture e Configurazioni di Sicurezza	12/03/2025

LISTA REVISORI

Ufficio/Sezione/Nominativo

REGISTRO DELLE REVISIONI

Revisione	Data	Capitoli/paragrafi modificati	Osservazioni

QUESTO DOCUMENTO È COSTITUITO DA 6 PAGINE TOTALI

INDICE

1. OBIETTIVI.....	4
2. NORMATIVA DI RIFERIMENTO	4
3. SITUAZIONE “AS IS”	4
4. SITUAZIONE “TO BE”	4
5. GAP ANALYSIS	4
6. OGGETTO DELLA FORNITURA	4
7. PIANO ATTUATIVO	5
8. ESIGENZA FINANZIARIA	5

1. OBIETTIVI

Il presente documento è finalizzato al potenziamento delle capacità operative del personale dell'Ufficio Infrastrutture di Sicurezza (UIS) del Reparto Sicurezza e *Cyber Defence* (RSCD) del Comando per le Operazioni in Rete (COR) nello svolgimento dei precipui compiti istituzionali, attraverso l'erogazione di corsi specialistici non erogati o garantiti dagli istituti di formazione militari.

2. NORMATIVA DI RIFERIMENTO

Non applicabile.

3. SITUAZIONE "AS IS"

Nell'ambito dei precipui compiti istituzionali, il COR, tramite l'Ufficio IS, effettua periodicamente delle attività di controllo di sicurezza sugli *asset* ICT presenti nell'infrastruttura ICT della Difesa (DIFENET); ciò, al fine di mantenerne un adeguato livello di postura di sicurezza. Al riguardo, si rende necessario elaborare ed applicare uno specifico piano di formazione per il personale incaricato di svolgere le citate attività di controllo, per potenziarne le capacità operative.

4. SITUAZIONE "TO BE"

Al fine di potenziare le capacità operative del personale di UIS, responsabile di svolgere le attività di controllo di sicurezza sugli *asset* ICT presenti nell'infrastruttura ICT della Difesa (DIFENET) volto a mantenerne un adeguato livello di postura di sicurezza, è necessario far svolgere specifici corsi non erogati o garantiti dagli istituti di formazione militari, conferendo il mandato ad Enti/Società esterni/e alla Difesa specializzati/e anche nella formazione.

5. GAP ANALYSIS

Al fine di potenziare le capacità operative del personale del COR, è necessario svolgere:

Attività	Da realizzare	In realizzazione	Realizzata
Fabbisogno formativo per l'anno 2025 per il personale del COR erogato dalla società di formazione specializzata OverNet.	X		

6. OGGETTO DELLA FORNITURA

Per colmare il *Gap* formativo, descritto nella suindicata tabella, è necessaria la fornitura da parte della società OverNet dei corsi di seguito indicati (consultabili nel catalogo del sito <https://overnet.education/catalogo>):

Codice	Descrizione	Sede	Periodo	N. persone	Certificazione	Materiale didattico
OES002	Vulnerability Assessment Basics	A distanza	Non specificato	1	No	No
OWASP	Sicurezza delle Web Application – OWASP Testing Guide	A distanza	Non specificato	2	No	No
CISSP	Certified Information Systems Security Professional	A distanza	31/03/2025 – 08/04/2025	1	No	Si

7. PIANO ATTUATIVO

Il piano attuativo della citata fornitura dovrà prevedere:

- ricezione di n. 4 *voucher* utili alla partecipazione ai corsi indicati nel paragrafo precedente;
- erogazione dei corsi di formazione attraverso la piattaforma *online* messa a disposizione dal fornitore, utilizzando i *voucher* al precedente alinea.

8. ESIGENZA FINANZIARIA

Nella tabella seguente viene fornita la stima degli oneri finanziari necessari per la fornitura:

Codice	Descrizione	Quantità	Costo stimato (IVA esente)	Capitolo di spesa
OES002	Vulnerability Assessment Basics	1		
OWASP	Sicurezza delle Web Application – OWASP Testing Guide	2		
CISSP	Certified Information Systems Se- curity Professional	1		
TOTALE				



COMANDO PER LE OPERAZIONI IN RETE

Reparto Sicurezza e Cyber Defence

CERT Difesa



REQUISITO TECNICO OPERATIVO

Relativo a

Corsi di Formazione del personale

Edizione 2025

Indice

1. Obiettivi	3
2. Riferimenti	3
3. Situazione "AS IS"	3
4. Situazione "TO BE"	3

1. Obiettivi

Il Comando per le Operazioni in Rete (COR), in accordo con le disposizioni discendenti dalle decretazioni emesse nel contesto del "Board Direttivo per il conseguimento degli obiettivi tecnologici funzionali all'evoluzione della nuova *Governance* di sicurezza della Difesa", ha identificato il CERT quale accentratore, gestore e valutatore di tutte le informazioni tecniche riguardanti le minacce cibernetiche nei confronti dell'intero comparto Difesa; ciò al fine di sviluppare una efficace azione di prevenzione e pronta reazione alle minacce attraverso l'impiego di adeguati strumenti di raccolta ed analisi delle informazioni relative ad attori malevoli e caratteristiche degli strumenti e delle modalità operative impiegate dagli stessi.

Per poter adeguatamente sviluppare le funzioni sopra sommariamente descritte, l'elemento umano rimane focale, secondo il paradigma per cui "l'uomo e le macchine lavorano meglio insieme". Il personale in servizio presso il CERT Difesa deve, pertanto, essere in possesso di adeguate competenze e conoscenze che gli permettano di garantire l'espletamento dei propri compiti istituzionali confrontandosi quotidianamente con la minaccia, la quale è in continua evoluzione.

2. Riferimenti

- SMD-G-137/R - Tabelle Ordinarie del Comando COR;
- SMD-I-013 - Procedure di risposta agli incidenti informatici riguardanti le reti telematiche della Difesa. Ed. 2008;
- SMD-I-024 - Procedure sulla gestione in sicurezza dei servizi informatici non-classificati dell'amministrazione difesa. Ed.2017 – aggiornata alle varianti 2020.
- Resoconto riunione Board attuativo del 07 marzo 2019;

3. Situazione "AS IS"

Il personale attualmente in forza presso il CERT Difesa necessita di formazione strutturata e continua per acquisire e mantenere aggiornate le proprie conoscenze e competenze, indispensabili per lo svolgimento delle proprie attività, in quanto un disallineamento o una obsolescenza delle stesse si tradurrebbe irrimediabilmente in ripercussioni negative sull'efficienza operativa del CERT. La formazione del personale riveste infatti un ruolo cruciale per garantire un'efficace gestione delle minacce informatiche, il tempestivo rilevamento e la mitigazione degli incidenti di sicurezza, nonché l'applicazione delle *best practices* di settore. La mancanza di un aggiornamento adeguato può comprometterne la capacità di rispondere in modo adeguato alle minacce emergenti, con potenziali impatti sulla sicurezza dell'infrastruttura Difesa. Pertanto è necessario dotare il personale di una formazione specifica e aggiornata per garantire il corretto funzionamento e la protezione efficace degli *asset* informatici.

4. Situazione "TO BE" / Oggetto della fornitura

Il presente requisito è mirato all'acquisizione dei corsi di formazione riepilogati nella seguente tabella e, ove applicabile, la relativa certificazione.

Nello specifico i corsi dovranno essere:

- erogati preferibilmente *on-line*, in modalità *e-learning* asincrona;
- corredati dei rispettivi laboratori, ove previsti;

Qualora compresa, dovrà essere fornita la certificazione prevista per il completamento del corso.

n.	Corso da fornire	Certificazione	Modalità di erogazione	Prezzo unitario stimato	Quantità
1	Computer Hacking Forensic Investigator (C HFI) - EC COUNCIL	C HFI	E-Learning		
2	Certified Threat Intelligence Analyst (C TIA) - EC COUNCIL	C TIA	E-Learning		
3	Malware Development - Maldev Academy	-	E-Learning		

L'impegno presumibile per l'acquisto dei sopracitati corsi è quantificabile complessivamente in circa 6.650 € IVA esente (IVA non applicabile ai sensi del Decreto del Presidente della Repubblica 26 ottobre 1972, n. 633).