REGIONE DEL VENETO
giunta regionale

Allegato B **al Decreto n.** 16156 **del** 22/07/2026

REGIONE DEL VENETO

PROCEDURA APERTA TELEMATICA, AI SENSI DELL'ART. 71 DEL D.LGS. N. 36/2023 E SS.MM.II, PER L'ACQUISTO DI SERVIZI DI SICUREZZA PER IL CSIRT REGIONALE DELLA DURATA DI 48 MESI, IN DUE LOTTI.

CODICE GARA APPTEL: **G03944**

Lotto 1 CUI: **S80007580279202600043**

Lotto 2 CUI:

S80007580279202600044 - **S80007580279202400040** - **S80007580279202400043** - **S80007580279202500049**

PROGETTO DI GARA

ALLEGATO B al Decreto n. 16156 del 22/07/2026

1. PREMESSA

Regione del Veneto promuove una procedura aperta telematica, ai sensi dell'articolo 71 del D.Lgs. 36/2023, per l'acquisto di servizi di sicurezza a supporto del CSIRT Regionale e degli Enti che ne compongono la Constituency, articolata in **due lotti** e della durata di **48 mesi**.

I servizi sono forniti con logica «chiavi in mano» ed End-to-End, con gestione unitaria e coordinata di persone, processi e piattaforme.

Il presente documento costituisce il progetto di gara e descrive il contesto di riferimento, l'oggetto dell'affidamento, le motivazioni sottese alle scelte progettuali adottate, la stima dei fabbisogni e la determinazione del valore dell'appalto.

2. ACRONIMI E DEFINIZIONI

Acronimo	**Definizione**
ACN	Agenzia per la Cybersicurezza Nazionale
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
Constituency	Insieme degli Enti destinatari dei servizi del CSIRT Regionale
EPS	Events Per Second
FTE	Full-Time Equivalent
IoC	Indicator of Compromise
MISP	Malware Information Sharing Platform
RUAC	Responsabile Unico delle Attività Contrattuali
RV	Regione del Veneto
SBOM	Software Bill of Materials
SDP	Security Data Platform
SOAR	Security Orchestration, Automation and Response

Acronimo	Definizione
SOC	Security Operation Center
TPRM	Third Party Risk Management

Per l'elenco completo si rinvia al paragrafo 1.3 del Capitolato Tecnico.

3. RELAZIONE TECNICO-ILLUSTRATIVA DI CONTESTO

3.1 Il CSIRT Regionale del Veneto

Il CSIRT Regionale del Veneto è la struttura di cui Regione del Veneto si è dotata quale presidio di coordinamento e supporto in materia di cybersicurezza a favore degli Enti del territorio. Il percorso istitutivo si è articolato nei seguenti atti:

Atto	Data	Oggetto
D.G.R. n. 1174	27 settembre 2022	Approvazione del progetto di istituzione del CERT regionale
D.G.R. n. 1024	22 agosto 2023	Approvazione del progetto esecutivo e avvio operativo
Ammissione a finanziamento	novembre 2024	Proposta «Attivazione CERT-CSIRT Regionale» — Avviso 06/2023
D.d.r. n. 1025	24 gennaio 2025	Approvazione della versione 2.1 del progetto esecutivo

Nel marzo 2026 è stata avviata la procedura per il cambio di denominazione da CERT a **CSIRT Regionale del Veneto**, alla data di redazione del presente documento in attesa di formale approvazione.

Il modello dei servizi è definito sulla base dei modelli di riferimento ENISA e si articola in quattro ambiti: servizi di gestione della qualità della sicurezza, servizi reattivi, servizi di gestione degli artefatti e servizi proattivi.

3.2 Modello di funzionamento e governance

Il modello operativo adottato è di tipo **«Campus»**: un approccio ibrido e federato in cui il CSIRT eroga centralmente i servizi e definisce linee guida standardizzate, mentre ciascun Ente mantiene la responsabilità operativa sul proprio perimetro. Il modello si fonda su tre principi: standardizzazione e linee guida centralizzate, responsabilità operativa distribuita e condivisione delle risorse tra gli Enti.

La governance è strutturata su tre livelli:

- **Livello Strategico** — Comitato Strategico, presieduto dalla Regione e partecipato dai referenti degli Enti principali e dalle autorità nazionali; definisce il piano pluriennale e funge da punto di escalation per gli incidenti di massima gravità;
- **Livello Direttivo** — Comitato Direttivo, guidato dal Responsabile del CSIRT e dai CISO/CIO degli Enti aderenti; traduce la strategia in processi operativi;
- **Livello Operativo Locale** — Referenti di Sicurezza degli Enti, quale interfaccia unica verso il CSIRT centrale.

La struttura centrale del CSIRT è articolata in tre team specializzati: Team Governance, Team Security Strategy e Team Esperti Cyber.

3.3 La Constituency

La Constituency è composta da **41 Enti**, suddivisi in **cinque Gruppi con livelli di rischio differenziati**. Ne fanno parte le Strutture Sanitarie e Sociali coordinate da Azienda Zero, gli Enti pubblici regionali strumentali, le Società a partecipazione regionale maggioritaria, il Consiglio regionale del Veneto e gli ulteriori enti autorizzati nel tempo dal Comitato Strategico.
L'elenco completo è riportato nell'Appendice A al Capitolato Tecnico.

L'adesione ai singoli servizi non è attualmente uniforme sull'intera Constituency, pertanto si riporta di seguito uno spaccato delle attuali adesioni:

Servizio	**Enti aderenti**
Security Operation Center (SOC)	35
Cyber Threat Intelligence e MISP	33
Vulnerability Management	34
Gestione del rischio e Business continuity	39
Sensibilizzazione e formazione	39 (circa 75.000 utenti)
Formazione Apicali e SME	circa 140 utenti

4. METODO DI ANALISI

La definizione del presente progetto di gara è scaturita da un'attenta attività di ricognizione, condotta in sinergia con la governance del CSIRT Regionale e gli Enti della Constituency, finalizzata ad adeguare i servizi di cybersicurezza alle mutate esigenze del panorama tecnologico e normativo. L'evoluzione del progetto trae origine dalla necessità di superare i limiti riscontrati nella precedente configurazione, integrando soluzioni all'avanguardia per garantire una resilienza superiore.

A ciò si aggiunge l'inderogabile necessità di allineamento agli obblighi normativi vigenti, quali la conformità alla direttiva NIS2 e l'integrazione con la piattaforma HyperSOC dell'ACN, oltre all'estensione del perimetro di monitoraggio alle infrastrutture cloud, garantendo così un presidio di sicurezza sempre più integrato, scalabile e proattivo.

In particolare, rispetto alla precedente procedura sono state quindi introdotte novità, di cui di seguito si riportano le principali.

Servizi di Governance, controllo e supporto normativo (L1)

- estensione del supporto normativo alla disciplina in materia di intelligenza artificiale (AI Act e Legge 132/2025) e alla sua integrazione con il quadro NIS2;
- linee guida per l'aggiornamento annuale sul portale ACN, con indicazioni operative per l'individuazione dei fornitori rilevanti;
- introduzione del principio di indipendenza tra il soggetto che svolge funzioni di governance e controllo e i soggetti che erogano i servizi tecnici sottoposti a tale controllo.

SOC, Incident Management e Cyber Threat Intelligence (L2)

- adozione di un'architettura **trimodale** della Security Data Platform (Cloud, Ibrida, On-Premise), con facoltà per il concorrente di proporre la modalità ritenuta più idonea;
- requisiti stringenti in materia di **anti-lock-in e portabilità degli artefatti** e completamento della transizione dalla tecnologia proprietaria in licenza a soluzione open source;
- **contestualizzazione della threat intelligence** sull'inventario degli asset e sugli SBOM degli Enti, quale elemento distintivo rispetto alla distribuzione di intelligence generica;
- valorizzazione dell'impiego reale dell'**intelligenza artificiale** per il triage, la riduzione dei falsi positivi e la correlazione laterale tra Enti;
- introduzione della figura del **Service Manager** quale punto di riferimento contrattuale unico;
- accreditamento obbligatorio alla piattaforma **HyperSOC di ACN** e supporto agli Enti per le notifiche al CSIRT Italia ai sensi del D.Lgs. 138/2024;
- estensione del perimetro di monitoraggio alle **sorgenti cloud** degli Enti;
- introduzione del **Medical SOC** per il monitoraggio dei dispositivi IoMT in ambito sanitario.

Vulnerability Management (L3)

- passaggio da un modello di esecuzione a un modello di **gestione forte** del ciclo di vita della vulnerabilità, con presidio assistito della remediation;
- ampliamento del perimetro di Vulnerability Assessment fino a **13.000 indirizzi IP** per anno;
- introduzione del **purple teaming** accanto al penetration test tradizionale;
- introduzione della gestione degli **SBOM** e della conformità al Cyber Resilience Act;
- estensione ai processi **DevSecOps** e alla sicurezza della supply chain software.

Gestione del Rischio, TPRM e Business Continuity (L4)

- introduzione di un **modello evoluto per gli Enti del perimetro NIS2**, con presidio continuativo in luogo della sola esecuzione periodica dell'assessment;
- introduzione del **Third Party Risk Management** quale processo strutturato;
- estensione alla **Business Continuity e al Disaster Recovery** con strategia di resilienza avanzata.

Formazione e Security awareness (L5)

- adozione di piattaforma **qualificata ACN**;
- formazione **segmentata e role-based** in luogo del percorso indifferenziato;
- introduzione delle **campagne di phishing etico** multicanale;
- introduzione dello **«zainetto formativo»** per la conservazione del percorso in caso di trasferimento del personale;
- integrazione tra formazione e monitoraggio SOC.

5. OGGETTO DELL'APPALTO

L'appalto ha per oggetto la conduzione operativa, l'evoluzione e il miglioramento continuo di una serie di servizi integrati di cybersecurity a supporto degli Enti facenti parte della Constituency del CSIRT Regionale.

I servizi oggetto della fornitura, suddivisi per Lotto, sono i seguenti:

Lotto	ID Servizio	Servizio
Lotto 1	L1.1.	Governance, controllo e supporto normativo
	L1.2	Servizio di Reperibilità in caso di Crisi
Lotto 2	L2.1	SOC, Incident Management e Cyber Threat Intelligence

Lotto	ID Servizio	Servizio
	L2.2	Vulnerability Management
	L2.3	Gestione del Rischio, TPRM e Business Continuity
	L2.4	Formazione e Security awareness

Gli Aggiudicatari di ciascun Lotto sono tenuti a presentare un'offerta che distingua i costi per ciascun servizio a copertura dell'intera Constituency, con ripartizione per Gruppo di appartenenza. Tale strutturazione è funzionale a consentire alla Stazione Appaltante l'identificazione della spesa relativa a eventuali Enti inclusi nella Constituency successivamente all'aggiudicazione.

5.1 Modalità di esecuzione

I servizi sono erogati:

- **on-site**, presso le sedi della Stazione Appaltante o degli Enti destinatari, con oneri di trasporto, viaggio, trasferta e missione a carico del Fornitore.
- **da remoto**, presso i Centri Servizi del Fornitore;

L'orario di svolgimento è dal lunedì al venerdì, dalle 9:00 alle 18:00, per tutti i giorni lavorativi dell'anno, a eccezione dei servizi **L1.1 — Reperibilità in caso di Crisi** e **L2.1 — SOC, Incident Management e CTI**, per i quali è prevista copertura continuativa secondo quanto dettagliato nei rispettivi paragrafi del Capitolato Tecnico.

6. SUDDIVISIONE IN LOTTI

In ottica di definizione della modalità di affidamento dei servizi previsti, è stata svolta un'attenta analisi da parte dell'Amministrazione, basata anche sull'esperienza dei precedenti affidamenti, che ha portato a individuare la suddivisione in **due lotti**, distinti per natura delle prestazioni:

- il **Lotto 1** raggruppa i servizi di governance, controllo e supporto normativo, di natura prevalentemente consulenziale e organizzativa, unitamente al servizio di reperibilità in caso di crisi;
- il **Lotto 2** raggruppa i servizi tecnico-operativi di sicurezza (SOC e Incident Management, Cyber Threat Intelligence, Vulnerability Management, Gestione del Rischio e Business Continuity, Formazione e Security awareness).

Tale separazione risponde all'esigenza di garantire:

- l'**indipendenza** tra il soggetto che svolge funzioni di governance, controllo e monitoraggio della qualità dei servizi e i soggetti che erogano i servizi tecnici sottoposti a tale controllo;
- l'esigenza di un **presidio centralizzato** di Governance, punto di raccordo tra l'Amministrazione e la Constituency;
- maggiore **efficacia operativa.**

Alla luce di tali considerazioni, si ritiene che l'affidamento mediante la suddivisione in 2 lotti distinti rappresenti la modalità più idonea a garantire l'efficacia, la qualità e la sostenibilità del servizio richiesto, nel rispetto dei principi di buon andamento, economicità ed efficienza dell'azione amministrativa.

7. IMPATTO ECONOMICO-ORGANIZZATIVO

L'introduzione di recenti normative di settore da parte di ACN e di ulteriori organismi regolatori (quali la direttiva NIS2 e il Cybersecurity Act) ha richiesto, nell'ambito del nuovo appalto, una profonda riorganizzazione delle attività e una spiccata specializzazione dei servizi. Parallelamente, al fine di ottimizzare l'efficienza gestionale complessiva, e ottimizzare i costi si è provveduto al ridimensionamento e all'accorpamento di quelle prestazioni che, nel corso del precedente progetto, si erano rivelate meno efficaci.

Nel complesso, tra gli elementi che hanno contribuito alla determinazione della base d'asta possiamo considerare:

- aggiornamento dei costi e dei prezzi;
- estensione della copertura dei servizi agli Enti attualmente non aderenti (il SOC copre oggi 35 Enti su 40, la CTI 33 su 40);
- introduzione di nuovi servizi e di nuove figure professionali;
- impatti organizzativi sulla struttura del CSIRT e sui referenti degli Enti.

8. STIMA DEI FABBISOGNI ED EVENTUALI OPZIONI

Al fine di determinare l'effettivo fabbisogno è stata svolta un'attività di ricognizione condotta in collaborazione con diversi attori coinvolti nella gestione e utilizzo dei servizi in perimetro, inclusa l'analisi dei risultati del monitoraggio dei contratti ICT. L'obiettivo è stato quello di individuare i punti critici e gli asset strategici dell'attuale servizio/contratto, identificando eventuali margini di efficienza o necessità di ampliamento della copertura.

Quest'attività ha permesso di determinare le quantità di servizi da richiedere (a titolo esemplificato FTE, ecc.) e di valutare l'integrazione di nuove attività per adeguarsi all'evoluzione tecnologica e dimensionale registrata negli ultimi anni, anche in seguito all'evoluzione delle normative in ambito Cyber security e di individuare elementi critici

dell'attuale contratto da risolvere, nonché di definire alcuni elementi specifici del contratto e servizio.

In particolare, si specificano i seguenti elementi:

- Necessità di prevedere un **periodo di subentro** per il fornitore entrante. La mancata previsione di un periodo di affiancamento nel contratto vigente e le conseguenti difficoltà relative al necessario prolungamento dei contratti in essere (ove possibile), ha spinto l'Amministrazione a prevedere nel nuovo contratto un periodo iniziale di affiancamento a titolo gratuito per i nuovi fornitori entranti della durata di 3 mesi;
- Necessità di estendere la **durata complessiva del contratto** a 48 mesi in totale (3 + 45) al fine di conseguire economie di apprendimento e garantire una presa in carico adeguata in raccordo con le necessità degli Enti della Constituency;
- Necessità di prevedere delle **figure specialistiche** che fungano da Responsabili dei servizi oltre ad una maggiore **presenza on site** sia presso l'Amministrazione che presso gli Enti della Constituency;
- **Estensione degli Enti della Constituency** e la possibilità di ulteriore inserimento di nuovi enti nel previa approvazione del Comitato Strategico e compatibilmente con le risorse economiche disponibili.
- Prosecuzione del percorso di **miglioramento dell'efficienza operativa.**

8.1 Metodo di determinazione del valore stimato

Ai sensi dell'articolo 14 del D.Lgs. 36/2023, il valore stimato dell'appalto è stato determinato sulla base di:

- analisi dei costi sostenuti nei contratti in essere;
- esigenze emerse dalla fase di ricognizione e previsioni di evoluzione dei servizi nel periodo di riferimento;
- analisi delle efficienze perseguibili;
- benchmark con procedure assimilabili per ambito e dimensione, tra cui la Gara Consip ID 2737, per l'affidamento di servizi di Managed Security Services gestiti da remoto, Governance, Analisi del Rischio e Controllo per le Pubbliche Amministrazioni (pubblicata ma non ancora attiva);
- andamento generale dei prezzi del settore di riferimento.

Il benchmark ha osservato i profili e i servizi richiesti, le tariffe poste a base d'asta, le formule di valutazione offerta economica e le eventuali tariffe di aggiudicazione

Tale valutazione è stata effettuata in conformità ai principi di economicità, efficienza e sostenibilità finanziaria.

8.2 Opzioni

In conformità all'art. 120 comma 9 del D.Lgs. 36/2023, è previsto l'istituto del **quinto d'obbligo**, che consente all'Amministrazione di modificare l'importo del contratto fino al 20% dell'importo iniziale, garantendo la flessibilità necessaria per adeguarsi a eventuali variazioni di fabbisogno o a nuove esigenze operative. Questo strumento rappresenta un elemento di garanzia per la continuità e l'evoluzione dei servizi, assicurando la capacità di adattamento dell'amministrazione alle dinamiche del settore ICT.

8.3 Importi

Il valore complessivo stimato dell'appalto ammonta a Euro **€ 29.110.716,75** (IVA esclusa) di cui per il Lotto 1 € 808,794,10 (IVA esclusa), ed per il Lotto 2 € 4.042.992,02 (IVA esclusa) per l'opzione di cui all'art. 120 comma 9 del D.lgs. 36/2023 e ss.mm.ii.

L'importo a base di gara è pari ad Euro **€ 24.258.930,63** iva esclusa.

Voce	**Importo (IVA esclusa)**
Lotto 1	€ 4.043.970,51
Lotto 2	€ 20.214.960,12
Importo a base di gara	**€ 24.258.930,63**
Opzioni Lotto 1	€ 808,794,10
Opzioni Lotto 2	€ 4.042.992,02
Valore complessivo stimato dell'appalto	**€ 29.110.716,75**

9. TIPO DI PROCEDURA E CRITERIO DI AGGIUDICAZIONE

Nell'ambito delle attività preliminari volte alla definizione della modalità di affidamento dei servizi dei Lotti 1 e 2, è stata condotta un'analisi comparativa tra diverse opzioni contrattuali, con l'obiettivo di individuare la soluzione maggiormente rispondente alle esigenze operative, tecnologiche e temporali dell'Amministrazione e rispondente agli elementi migliorativi individuati.

Considerata anche l'attuale mancanza di un accordo quadro attivo, l'affidamento avviene mediante **procedura aperta telematica** ai sensi dell'articolo 71 del D.Lgs. 36/2023.

L'appalto è aggiudicato in base al criterio dell'offerta economicamente più vantaggiosa individuata sulla base del miglior rapporto qualità/prezzo.

La valutazione dell'offerta tecnica e dell'offerta economica è effettuata in base ai seguenti punteggi:

	ELEMENTI DI VALUTAZIONE	PUNTEGGIO MASSIMO
1	Offerta Tecnica	80
2	Offerta Economica	20
	TOTALE	**100**

9.1 Metodo di attribuzione del coefficiente per il calcolo del punteggio dell'offerta economica

Il punteggio attribuito all'elemento economico è determinato tramite la seguente formula:

PEi = 20 x CEi

dove:
PERichiesta di anticipo nella consegna dei nuovi aggiornamenti/moduli software per gli apparati di sicurezza di rete.i = Punteggio economico attribuito al concorrente i-esimo;
20 = Punteggio massimo economico assegnabile;
CEi = Coefficiente economico attribuito al concorrente i-esimo;

Per determinare il coefficiente del punteggio economico (CEi), variabile da zero a uno, viene adottata la seguente formula **non lineare "Concava a punteggio assoluto" al rialzo:**

$CEi = 1 - (1 - Ri)^{n}$

dove:
CEi = Coefficiente economico attribuito al concorrente i-esimo
Ri = ribasso dell'offerta del concorrente i-esimo,
^{n}=parametro che determina la concavità della curva di punteggio:10

10. DURATA DEL CONTRATTO E SUBENTRO

Il Contratto spiega i suoi effetti dalla data della sua sottoscrizione ed avrà termine allo spirare di 45 mesi decorrenti dalla data di avvio delle attività (data di inizio dell'erogazione dei servizi) successiva al periodo di subentro/presa in carico, non retribuito, dei servizi della durata di 3 mesi.

Pertanto, dalla data di sottoscrizione del contratto, sarà previsto:

- **Periodo di subentro/presa in carico**, non retribuito, della durata di **3 mesi** dalla data di sottoscrizione del contratto.
- **Periodo di erogazione di 45 mesi** a partire dalla data di avvio delle attività, comunicata a mezzo PEC dall'Amministrazione Contraente al Fornitore a conclusione del periodo di subentro;
- **Trasferimento del know-how** a fine fornitura, il Fornitore deve garantire un supporto alla transizione per almeno **3 mesi**, collaborando al trasferimento delle competenze verso l'Amministrazione o un nuovo Fornitore, secondo un Piano di Trasferimento approvato (per il dettaglio si veda il par. 4.4 Piano di Trasferimento Know-How del Capitolato Tecnico). Tale attività deve concludersi entro il termine del contratto.

11. QUADRO ECONOMICO DELL'APPALTO E COSTRUZIONE DELLA BASE D'ASTA

L'importo a base di gara dei servizi oggetto dell'affidamento è di complessivi euro **24.258.930,63 (iva esclusa)** così come dettagliato nella tabella che segue:

Lotto 1

n.	Descrizione servizio	CPV	P (principale) S (secondaria)	Importo per 48 mesi
1	Servizio di Governance e supporto normativo	72000000-5	P	€ 3.740.579,50
2	Servizio di reperibilità	72000000-5	P	€ 303.391,01
A) Importo a base di gara per 48 mesi (Iva esclusa)				**€ 4.043.970,51**
B) Oneri per la sicurezza da interferenze non soggetti a ribasso				€ 0,00

Lotto 2

n.	Descrizione servizio	CPV	P (principale) S (secondaria)	Importo per 48 mesi

1	Servizio Soc, incident management e Cyber Threat Intelligence	72510000-3	P	€ 6.611.427,01
2	Servizio di vulnerability management	72000000-5	P	€ 5.146.972,73
3	Servizio di gestione del rischio, TPRM e-business continuity	72000000-5	P	€ 4.686.841,38
4	Servizio di formazione	72000000-5	P	€ 880.719,00
5	Servizio di Security awareness	72000000-5	P	€ 2.889.000,00
A) Importo a base di gara per 48 mesi (Iva esclusa)				**€ 20.214.960,12**
B) Oneri per la sicurezza da interferenze non soggetti a ribasso				€ 0,00

Il valore complessivo stimato della procedura ai sensi dell'art. 14, comma 4 del D. Lgs. n. 36/2023 e ss.mm.ii è pari ad euro **29.110.716,75** al netto di Iva, così suddiviso:

Lotto 1

A) Importo complessivo a base di gara IVA esclusa	€ 4.043.970,51
B) Importo massimo del quinto, in caso di variazioni in aumento ex art. 120 co. 9 del D.lgs.36/2023	€ 808.794,10
VALORE COMPLESSIVO STIMATO (A+B)	**€ 4.852.764,61**

Lotto 2

A) Importo complessivo a base di gara IVA esclusa	€ 20.214.960,12
B) Importo massimo del quinto, in caso di variazioni in aumento ex art. 120 co. 9 del D.lgs.36/2023	€ 4.042.992,02
VALORE COMPLESSIVO STIMATO (A+B)	**€ 24.217.952,14**

Conformemente a quanto previsto dall'articolo 108, comma 9, del D.Lgs. 36/2023 n.6, trattandosi di una procedura di gara avente ad oggetto servizi di natura intellettuale, non standardizzabili,

non sarà richiesta all'operatore economico di indicare i costi della manodopera e gli oneri aziendali per l'adempimento delle disposizioni in materia di salute e sicurezza sui luoghi di lavoro.

12. INDICAZIONI E DISPOSIZIONI PER LA STESURA DEI DOCUMENTI INERENTI ALLA SICUREZZA

In considerazione della natura del servizio oggetto della presente procedura, non sussiste, ai sensi dell'art. 26 del D.Lgs. 9 aprile 2008 n. 81, l'obbligo di procedere alla predisposizione dei documenti di cui all'art. 26 commi 3 e 3 ter del predetto decreto.

13. NORMATIVA DI RIFERIMENTO

Fermo il rispetto del Codice dei contratti pubblici e l'ulteriore normativa tecnica e/o di settore, si dà atto che i documenti di gara sono stati redatti nel rispetto del bando tipo ANAC n.1/2023, aggiornato con Delibera n.148, approvata dal Consiglio dell'Autorità del 1° aprile 2026.