CITTÀ METROPOLITANA DI VENEZIA

AREA AMMINISTRAZIONE E TRANSIZIONE DIGITALE
Servizio infrastrutture digitale e SITM

Determinazione N. 1918 / 2025
Responsabile del procedimento: ARMELLIN ROMANO

Oggetto: **FINANZIAMENTO DI INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER IN CONTINUITÀ AL PROGETTO PNRR 1.5 "CYBERMET - CYBERSICUREZZA METROPOLITANA".**

Il dirigente

Visti:

i il D.lgs. 18 agosto 2000, n. 267, "Testo unico delle leggi sull'ordinamento degli enti locali" e, in particolare:
   a. l'art. 107 che definisce le funzioni e le responsabilità dei dirigenti;
   b. gli articoli 182 e seguenti che regolano il procedimento di spesa;
   c. l'art 192 che stabilisce che la stipulazione dei contratti deve essere preceduta da apposita determinazione a contrattare;

ii la Legge 7 aprile 2014, n. 56, contenente le disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni;

iii lo Statuto della Città metropolitana di Venezia, approvato con deliberazione della Conferenza dei sindaci n. 1 del 20 gennaio 2016, con particolare riferimento all'art. 28 "Dirigenti ed altri responsabili";

iv il Regolamento sull'ordinamento degli uffici e dei servizi della Città metropolitana di Venezia, approvato con Decreto del Sindaco metropolitano n. 1 del 3 gennaio 2019 da ultimo modificato con Decreto n. 34 del 16 giugno 2022, in particolare l'articolo n. 13 che individua i compiti dei dirigenti;

v il Regolamento di contabilità della Città metropolitana di Venezia, approvato il 24 settembre 2019 con deliberazione n. 18 del Consiglio metropolitano ed entrato in vigore il 22 ottobre 2019, in particolare gli articoli 19 e 20 sulle modalità d'impegno degli stanziamenti di spesa;

vi la Deliberazione n. 22 del Consiglio metropolitano del 20 dicembre 2024, con la quale è stato approvato l'aggiornamento del DUP Documento Unico di Programmazione 2025/2027 e del bilancio di previsione per gli esercizi 2025/2027;

vii il Piano Integrato di Attività e Organizzazione (P.I.A.O.) di cui al Decreto del Sindaco metropolitano n. 6 del 31 gennaio 2025 "Approvazione del Piano Integrato di Attività e Organizzazione e del Piano esecutivo di gestione – parte finanziaria - 2025 – 2027", contenente il Piano Esecutivo di Gestione, il Piano dettagliato degli Obiettivi, il Piano della Performance, il Piano Triennale per la Prevenzione della Corruzione e la Trasparenza;

viii il Decreto del Sindaco metropolitano n. 82 del giorno 29 dicembre 2023 con il quale è stato attribuito l'incarico dirigenziale relativo all'Area Amministrazione e transizione digitale;

visti inoltre:

i il decreto legislativo 18 maggio 2018, n. 65, “Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell’Unione”;
ii il Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, “relativo all’ENISA, l’Agenzia dell’Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell’informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»)”;
iii il Decreto-Legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla Legge 18 novembre 2019, n. 133, recante “Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica”;
iv la Strategia Nazionale di Cybersicurezza 2022-2026, adottata unitamente al relativo Piano di Implementazione, con Decreto del Presidente del Consiglio dei Ministri del 17 maggio 2022;
v Il Regolamento (UE) n. 1303/2013 del Parlamento europeo e del Consiglio del 17 dicembre 2013, recante disposizioni comuni sui fondi europei di finanziamento, in particolare l’obbligo quinquennale di non alterare la natura, gli obiettivi o le condizioni di attuazione dell’operazione finanziata;
vi il D.L. 19 agosto 2016, n. 175, e s.m.i. recante il “Testo unico in materia di società a partecipazione pubblica” e, in particolare, gli articoli 2, comma 1, lett. c) ed o), comma 4 e comma 16, in tema di società *in house*;
vii il Regolamento sul sistema dei controlli interni della Città metropolitana, approvato con Deliberazione consiliare n. 6 del giorno 8 gennaio 2013 e modificato con Deliberazione del Presidente della Provincia n. 52 del 28 ottobre 2014, applicabile in base al principio di continuità amministrativa, e, in particolare l’art. 13 relativo al controllo sulle società *in house*;
viii le più recenti Linee guida sulla sicurezza nel procurement ICT, approvate con determinazione AgID n. 220 del 17 maggio 2020, elaborate in collaborazione coi Ministeri degli Affari Esteri, dell’Interno, della Giustizia, della Difesa, dell’Economia e delle Finanze, dello Sviluppo Economico, con il Dipartimento Informazioni per la Sicurezza della Presidenza del Consiglio, con il Dipartimento della Protezione Civile della Presidenza del Consiglio e con CONSIP S.p.A.;
ix il piano triennale per l’informatica AgID 2024-2026, aggiornamento 2025;
x il regolamento per le infrastrutture digitali e per i servizi cloud per le PPAA, di cui al decreto direttoriale ACN n. 21007 del 27 luglio 2024;
xi la L. n. 90 del 28 giugno 2024 che prevede una specifica disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici dal punto di vista della cybersicurezza;
xii il D.lgs. n. 138 del 4 settembre 2024 di recepimento in Italia della Direttiva (UE) 2022/2555 “Direttiva NIS2”, contenente misure per un livello comune elevato di cybersicurezza nell’Unione;
xiii la Determinazione ACN n.164179 del 14 aprile 2025 che definisce le misure di sicurezza di base che i “soggetti importanti” devono adottare;
xiv il Regolamento del Parlamento Europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull’intelligenza artificiale (Legge sull’intelligenza artificiale) e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale);

considerato:
i per dare attuazione alla Strategia Nazionale di Cybersicurezza, le pubbliche amministrazioni possono far ricorso a fondi dedicati attraverso la legge di bilancio per il 2023 n. 197 del 29 dicembre 2022; oppure ricorrendo alle risorse rese disponibili dal PNRR 1.5. “Cybersecurity” Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” M1C1I1.5; ovvero ricorrendo a fondi propri;

ii con Decreto del Sindaco metropolitano n. 16 del 18 marzo 2024 la Città metropolitana di Venezia ha aderito all'Avviso n. 8/2024 dell'Agenzia per la Cybersicurezza Nazionale, finalizzato al finanziamento di progetti tesi al potenziamento della resilienza cyber;

iii in seguito alla presentazione, all'approvazione ed all'avvio del proprio progetto "CyberMet – Cybersicurezza Metropolitana" a valere sul PNRR 1.5 "Cybersecurity", l'ente ha affidato alla propria società *in house* Venezia Informatica Soluzioni - Venis S.p.A. di Venezia, p. IVA 02396850279 l'esecuzione delle principali attività approvate, tramite determinazione n. 3421 del 18 dicembre 2024 e sottoscrizione del contratto prot. 2098 del 14 gennaio 2025 ratificato con prot. 12665 del 25 febbraio 2025;

iv lo spiegamento delle attività oggetto di intervento prevede l'adesione di Venis S.p.A. a diverse iniziative contrattuali, con durata eccedente il 31 dicembre 2025, termine del progetto CyberMet, imposto dall'Avviso ACN citato;

v la scelta, condivisa con la Città metropolitana, di contrarre obbligazioni eccedenti il termine temporale di chiusura progetto, risponde esclusivamente all'interesse dell'ente di trarre legittimo vantaggio dalla maggiore durata degli impegni contrattuali, in un'ottica di contenimento dei costi nel settore normativo e tecnologico della cybersicurezza, intesa come potenziamento delle capacità di resilienza cyber dell'ente, in termini di postura di sicurezza, processi e modello organizzativo, competenze e, infine, sistemi e tecnologie abilitanti;

dato atto:

vi Venis S.p.A. ha avviato le procedure per aderire al lotto 1 dell'Accordo Quadro Consip ID 2296 "SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI" per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo;

vii i servizi implementati attraverso lo strumento dell'AQ citato, della durata di tre anni dal perfezionamento del Contratto esecutivo, in una col Piano operativo comunicato per condivisione alla Città metropolitana di Venezia con prot. 47822 del 15 luglio 2025, sono di seguito elencati:
   a. analisi, implementazione e gestione degli eventi di sicurezza in tempo reale e relativi servizi professionali annessi (L1 S1);
   b. implementazione di un servizio di "Web Application Firewall" e relativi servizi professionali annessi (L1 S3 ed L1 S15);
   c. implementazione e gestione continuativa delle vulnerabilità (Vulnerability Management) e relativi servizi professionali annessi (L1 S4 ed L1 S15);
   d. servizi professionali Trasversali (L1 S15);

viii il modello operativo proposto prevede il monitoraggio continuo delle informazioni prodotte dalle sorgenti di log (eventi di sicurezza) identificati come perimetro di monitoraggio ed in uso presso il data center dell'Amministrazione. Il servizio, nel suo complesso, consente di:
   a. controllare in maniera attiva il perimetro infrastrutturale soggetto al servizio di monitoraggio, attraverso attività di "monitoring real-time" così da anticipare per quanto possibile eventuali incidenti di sicurezza;
   b. produrre specifici allarmi e reportistica sugli eventi raccolti;
   c. identificare e comunicare le possibili azioni correttive da intraprendere nell'immediato, per contenere l'attacco e prevenirne la propagazione;
   d. acquisire e trasmettere eventuali evidenze digitali da utilizzare nella ricostruzione di quanto accaduto in seguito all'incidente;
   e. effettuare una valutazione post incidente, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza;

ix i servizi descritti rientrano nelle cinque linee di intervento previste dal Piano progettuale CyberMet – Cybersicurezza Metropolitana di seguito elencate, a valere sul finanziamento PNRR 1.5, qualificati da Venis S.p.A. con prot. 44208 del 27 giugno 2025 "acquisti in sistemi e

tecnologie", riservando agli stessi il budget di finanziamento PNRR massimo di € 330.000,00 IVA esclusa;

x le cinque linee di intervento previste dal progetto CyberMet sono le seguenti:
   1. Governance e programmazione cyber;
   2. Gestione del rischio cyber e della continuità operativa;
   3. Gestione e risposta agli incidenti di sicurezza;
   4. Gestione delle identità digitali e degli accessi logici;
   5. Sicurezza delle applicazioni, dati e delle reti;

xi la fornitura in sistemi e tecnologie, elaborata dal Servizio infrastrutture digitali e SITM dell'ente in collaborazione con i fornitori di Venis S.p.A., si inserisce all'interno dell'attività di progettazione e sviluppo a supporto dell'evoluzione della postura di cybersicurezza dell'Ente, contribuendo in modo sinergico al raggiungimento degli obiettivi delineati nelle citate cinque linee di intervento del progetto CyberMet:
   a. Il Security Operation Center (SOC) rappresenta il fulcro per la Gestione e risposta agli incidenti di sicurezza (rif. Intervento 3.), fornendo capacità proattive di monitoraggio, identificazione e coordinamento delle azioni di contenimento e ripristino attraverso l'analisi avanzata degli eventi raccolti via SIEM. Il servizio è strettamente integrato con le altre componenti, contribuendo all'evoluzione continua delle politiche di sicurezza, e supporta la Governance cyber (rif. Intervento 1.), grazie al coinvolgimento attivo nella gestione e nella consultazione degli alert prodotti;
   b. Il Web Application Firewall (WAF) rafforza la Sicurezza delle applicazioni, dei dati e delle reti (rif. Intervento 5.), agendo come strumento di difesa contro minacce veicolate da traffico HTTP e proteggendo i sistemi da attacchi web-based, elemento chiave per la gestione del rischio, la prevenzione di incidenti e la salvaguardia delle informazioni (rif. Intervento 2.);
   c. Il servizio di Vulnerability Management, attraverso scansioni automatiche e aggiornate, consente l'individuazione e valutazione sistematica del rischio cyber, supportando la pianificazione di contromisure efficaci e aumentando la resilienza del perimetro digitale dell'Ente in ottica di continuità operativa (rif. Intervento 2.). In parallelo, la classificazione tecnica delle vulnerabilità e l'indicazione delle misure di mitigazione supportano l'implementazione di policy di protezione dell'infrastruttura applicativa e dei dati (rif. Intervento 5.);
   d. I Servizi Specialistici garantiscono un supporto professionale per l'adozione e il mantenimento dei servizi SOC, WAF e di Vulnerability Management e, al contempo, contribuiscono in modo trasversale al coordinamento strategico degli interventi cyber, allineandosi alla linea di intervento di Governance e programmazione (rif. Intervento 1.). Tra le attività chiave, il servizio di Cyber Threat Intelligence contribuisce sia alla gestione e risposta agli incidenti di sicurezza (rif. Intervento 3.), grazie all'identificazione tempestiva di minacce e compromissioni, sia alla gestione del rischio e continuità operativa (rif. Intervento 2.), abilitando capacità predittive tramite l'analisi del Dark Web, dei domini e dei profili VIP. Il monitoraggio degli utenti VIP e la rilevazione di utilizzi impropri di riferimenti aziendali rafforzano, inoltre, la gestione delle identità digitali e degli accessi logici (rif. Intervento 4.), garantendo il controllo sull'autenticazione e sulle autorizzazioni in base ai principi di riservatezza e privilegio minimo. Infine, le attività di Attack Surface Management, ricomprese nel servizio, supportano la sicurezza delle applicazioni, dei dati e delle reti (rif. Intervento 5.), grazie alla classificazione e all'analisi continua di asset noti, sconosciuti e rogue, migliorando la capacità di prevenzione, risposta e protezione dell'infrastruttura ICT dell'Ente;

xii il piano operativo dell'AQ oggetto di adesione da parte di Venis S.p.A. si presenta come un insieme coerente e integrato di azioni che potenziano la postura di sicurezza dell'Ente, intervenendo su più livelli per assicurare prevenzione, rilevamento, risposta e recupero efficaci nell'ambito cyber, in consonanza col progetto CyberMet PNRR 1.5 "Cybersecurity";

xiii la quantificazione dei servizi descritti è espressa dalla seguente tabella che, secondo il listino disponibile al link pubblico: https://www.consip.it/sites/default/files/ID%202296%20Allegato%20C%20-%20Lotto%201%20-%20Corrispettivi%20e%20tariffe%20PAL.pdf presentato dal RTI Accenture S.p.A., Fastweb S.p.A., Fincantieri Nex Tech S.p.A., Difesa e Analisi Sistemi S.p.A., operatore individuato da Venis S.p.A. quale fornitore, prevede un importo totale di € 621.488,00 IVA esclusa, pari a € 758.215,36 IVA inclusa;

Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**
L1.S1	Security Operation Center	Device equivalente/annuo	Canone	Fascia 3 (fino a 1200 EPS)	150	150	150
L1.S15	Servizi specialistici	Giorni/Persona del Team ottimale	Canone/A corpo	gg/p Team ottimale	469	56	56
L1.S3	WAF	Mbps	Canone	Fascia 1 (fino a 500 Mbps)	1	1	1
L1.S15	Servizi specialistici	Giorni/Persona del Team ottimale	Canone/A corpo	gg/p Team ottimale	60	0	0
L1.S4	Vulnerability Management	IP	Canone	Fascia 1 (fino a 50IP)	50	50	50
L1.S15	Servizi specialistici	Giorni/Persona del Team ottimale	Canone/A corpo	gg/p Team ottimale	181	0	0
L1.S15	Servizi specialistici	Giorni/Persona del Team ottimale	Canone/A corpo	gg/p Team ottimale	857	289	89

Codice	**Costo unitario**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**TOTALE**
L1.S1	€ 239,40	150	150	150	€ 107.730,00
L1.S3	€ 2.800,00	1	1	1	€ 8.400,00
L1.S4	€ 23,00	50	50	50	€ 3.450,00
L1.S15	€ 244,00	1.567	345	145	€ 501.908,00
TOTALE		**€ 514.208,00**	**€ 124.040,00**	**€ 75.240,00**	**€ 621.488,00**

xiv la quantità di servizi erogabili dal RTI, eccedente la data di fine progetto, non è remunerabile attraverso il contributo PNRR quantificato in via previsionale da Venis S.p.A. nell'ambito del progetto PNRR 1.5 e corrisponde alle seguenti quantità:

Codice	**Costo unitario**	**Q.tà 2025 PNRR 1.5**	**Q.tà 2026**	**Q.tà 2027**	**Q.tà 2028**	**TOTALE**
L1.S1	€ 239,40	75	150	150	75	€ 107.550,00
L1.S3	€ 2.800,00	1	1	1	/	€ 8.400,00
L1.S4	€ 23,00	50	50	50	/	€ 3.450,00
L1.S15	€ 244,00	1262	478	245	72	€ 501.908,00
TOTALE		**€ 329.833,00**	**€ 156.492,00**	**€ 99.640,00**	**€ 35.523,00**	**€ 621.488,00**

xv risulta opportuno prevedere a bilancio i necessari fondi IVA inclusa per il supporto finanziario alle azioni di cybersicurezza oggetto del presente provvedimento e, specificamente:

RESILIENZA CYBER IN CONTINUITÀ AL PROGETTO PNRR 1.5 "CYBERMET – CYBERSICUREZZA METROPOLITANA"	2026	2027	2028	TOTALE
101080305702/0 "ADOZIONE MISURA DI CYBERSICUREZZA"	€ 190.920,24	€ 121.560,80	€ 43.338,06	€ 355.819,10

xvi ai sensi del punto 2.5 della Determinazione ANAC n. 4 del 7 luglio 2011 recante Linee guida sulla tracciabilità dei flussi finanziari ai sensi dell'articolo 3 della legge 13 agosto 2010, n. 136, aggiornata con delibera n. 556 del 31 maggio 2017, con delibera n. 371 del 27 luglio 2022 e con delibera n. 585 del 19 dicembre 2023, sono escluse dall'ambito di applicazione della legge n. 136/2010 (tracciabilità dei movimenti finanziari – CIG) le movimentazioni di danaro derivanti da prestazioni eseguite in favore di pubbliche amministrazioni da soggetti, giuridicamente distinti dalle stesse, ma sottoposti ad un controllo analogo a quello che le medesime esercitano sulle proprie strutture (cd. affidamenti *in house*);

xvii Venis S.p.A. fatturerà alla Città metropolitana di Venezia le spettanze riconducibili ai precedenti argomenti, in concomitanza con il ciclo di fatturazione riferibile al proprio rapporto contrattuale con il RTI Accenture S.p.A., Fastweb S.p.A., Fincantieri Nex Tech S.p.A., Difesa e Analisi Sistemi S.p.A.. e per i medesimi importi;

Determina

1 di approvare il modello operativo proposto e disporre i necessari impegni a bilancio, a favore della società *in house* Venezia Informatica e Sistemi - Venis S.p.A. di Venezia p. IVA 02396850279, per l'adesione all'Accordo Quadro Consip ID 2296 "Servizi applicativi in ottica Cloud e servizi di demand e PMO per le PAL" per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo, a garanzia del finanziamento degli interventi successivi alla scadenza del progetto CyberMet PNRR 1.5 fissata al 31 dicembre 2025 e dallo stesso previsti;

2 di impegnare l'importo totale massimo di € 355.819,10 IVA inclusa come di seguito specificato:

RESILIENZA CYBER IN CONTINUITÀ AL PROGETTO PNRR 1.5 "CYBERMET – CYBERSICUREZZA METROPOLITANA"	2026	2027	2028	**TOTALE**
101080305702/0 "ADOZIONE MISURA DI CYBERSICUREZZA"	€ 190.920,24	€ 121.560,80	€ 43.338,06	**€ 355.819,10**

3 in attuazione del comma 629 dell'art. 1 legge 190/2014, si provvederà a pagare solo l'imponibile fatturato dalla ditta, mentre l'IVA verrà trattenuta e versata all'erario dall'Area Economico Finanziaria, secondo le modalità indicate dal D.M. 23 gennaio 2015;

4 di dare atto che ai pagamenti sarà provveduto con atto del dirigente responsabile ai sensi dell'art. 107 D.lgs. 267/2000 tramite il servizio di ragioneria e su presentazione di regolare fattura, previa verifica dei costi esposti e nei limiti della spesa autorizzata;

5 le somme IVA inclusa saranno esigibili entro ciascun anno di competenza;

6 ai fini dell'articolo 9 del D.lgs. 33/2013, tutte le informazioni relative all'assegnazione in oggetto e al presente provvedimento vengono pubblicate sul portale della Città metropolitana di Venezia nella sezione "Amministrazione trasparente" (mis. Z02 del P.I.A.O. 2025-2027) e nell'apposita sezione di Amministrazione Trasparente relativa agli atti PNRR (mis. Z09 del P.I.A.O. 2025-2027);

7 le somme citate saranno esigibili entro ciascun anno di competenza;

la presente determinazione concerne l'ambito delle funzioni istituzionali della Città metropolitana assegnate all'Area Amministrazione e transizione digitale.

Si dichiara che l’operazione oggetto del presente provvedimento non presenta elementi di anomalia tali da proporre l’invio di una delle comunicazioni previste dal provvedimento del Direttore dell'Unità di informazione finanziaria (U.I.F.) per l’Italia del 23 aprile 2018.

Si attesta, ai sensi dell’art. 147-bis, comma 1, del D.LGS n. 267/2000, la regolarità e la correttezza dell’azione amministrativa relativa al presente provvedimento.

IL DIRIGENTE
ARMELLIN ROMANO

atto firmato digitalmente