# CITTÀ METROPOLITANA DI VENEZIA

## AREA AMMINISTRAZIONE E TRANSIZIONE DIGITALE

*Servizio infrastrutture digitali e SITM*

Determinazione N. 3421 / 2024
Responsabile del procedimento: ARMELLIN ROMANO

Oggetto: **DETERMINAZIONE A CONTRATTARE PER L'ACQUISIZIONE, MEDIANTE AFFIDAMENTO DIRETTO IN HOUSE, DEL SERVIZIO DI REALIZZAZIONE PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA NELL'AMBITO DEL PNRR NEXT GENERATION EU MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5 CUP B79B21002230006.**

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, in particolare l'art. 1;

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. 31 del Consiglio metropolitano del 15 dicembre 2023, con la quale è stato approvato l'aggiornamento del DUP Documento Unico di Programmazione 2024/2026 e del bilancio di previsione per gli esercizi 2024/2026;

vii il Piano Integrato di Attività e Organizzazione (P.I.A.O.) di cui al Decreto del Sindaco metropolitano n. 5 del 31 gennaio 2024 "Approvazione del Piano Integrato di Attività e Organizzazione e del Piano esecutivo di gestione – parte finanziaria - 2024 – 2026" aggiornato con Decreto del Sindaco n. 32 del 10 giugno 2024, 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;

ix il Decreto del Sindaco metropolitano n. 16 del 18 marzo 2024 con cui, tra l'altro, il dirigente dell'Area Amministrazione e transizione digitale è delegato alla sottoscrizione di tutti gli atti

previsti dalla partecipazione al progetto e specificamente alla stipula dell'apposito accordo di collaborazione con AgID;

visti inoltre:

i il Codice dell'amministrazione digitale (CAD) emanato con decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni e integrazioni;

ii il Regolamento di esecuzione (UE) n. 821/2014 della Commissione del 28 luglio 2014, recante modalità di applicazione del Regolamento (UE) n. 1303/2013 del Parlamento europeo e del Consiglio per quanto riguarda le modalità dettagliate per il trasferimento e la gestione dei contributi dei programmi, le relazioni sugli strumenti finanziari, le caratteristiche tecniche delle misure di informazione e di comunicazione per le operazioni e il sistema di registrazione e memorizzazione dei dati;

iii il decreto del Presidente della Repubblica 5 febbraio 2018, n. 22, "Regolamento recante i criteri sull'ammissibilità delle spese per i programmi cofinanziati dai Fondi strutturali di investimento europei (SIE) per il periodo di programmazione 2014/2020";

iv il Regolamento (UE) 2018/1046 del Parlamento europeo e del Consiglio del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i Regolamenti (UE) n. 1296/2013, n. 1301/2013, n. 1303/2013, n. 1304/2013, n. 1309/2013, n. 1316/2013, n. 223/2014, n. 283/2014 e la decisione n. 541/2014/UE e abroga il Regolamento (UE, Euratom) n. 966/2012;

v 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";

vi 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»)";

vii 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";

viii la Legge 16 gennaio 2003 n. 3, istitutiva del CUP Codice Unico di Progetto, come modificata dall'art. 41, comma 1, della L. 120/2020, secondo cui "Gli atti amministrativi anche di natura regolamentare adottati dalle Amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, che dispongono il finanziamento pubblico o autorizzano l'esecuzione di progetti d'investimento pubblico, sono nulli in assenza dei corrispondenti codici di cui al comma 1 che costituiscono elemento essenziale dell'atto stesso";

ix la Delibera del Comitato per la programmazione economica (CIPE) del 26 novembre 2020, n. 63, che introduce la normativa attuativa della riforma CUP;

x la legge 30 dicembre 2020, n.178, recante "Bilancio di previsione dello Stato per l'anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023", in particolare l'articolo 1:
   a. comma 1042 ai sensi del quale con uno o più decreti del Ministro dell'economia e delle finanze sono stabilite le procedure amministrativo-contabili per la gestione delle risorse di cui ai commi da 1037 a 1050, nonché le modalità di rendicontazione della gestione del Fondo di cui al comma 1037;
   b. comma 1043, secondo periodo ai sensi del quale, al fine di supportare le attività di gestione, di monitoraggio, di rendicontazione e di controllo delle componenti del Next Generation EU, il Ministero dell'economia e delle finanze - Dipartimento della Ragioneria generale dello Stato sviluppa e rende disponibile un apposito sistema informatico;

xi il decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n.131, recante "Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133";

xii il Regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza, in particolare l'art. 5, comma 2 che, come modificato dall'art. 1 comma 2 del Regolamento (UE) 435/2023, prevede unicamente il finanziamento di misure che rispettano il principio "non arrecare un danno significativo",applicabile anche alle misure incluse nei capitoli dedicati al piano REPowerEU;

xiii il D.L. 6 maggio 2021, n. 59, recante "Misure urgenti relative al Fondo complementare al Piano nazionale di ripresa e resilienza e altre misure urgenti per gli investimenti", convertito con modificazioni dalla legge 1° luglio 2021, n.101;

xiv il decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, recante "Governance del Piano nazionale di ripresa e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure" e, in particolare:

a. l'art. 9, primo comma, che attualmente prevede che "Alla realizzazione operativa degli interventi previsti dal PNRR provvedono le Amministrazioni centrali, le Regioni, le Province autonome di Trento e di Bolzano e gli enti locali, sulla base delle specifiche competenze istituzionali, ovvero della diversa titolarità degli interventi definita nel PNRR, attraverso le proprie strutture, ovvero avvalendosi di soggetti attuatori esterni individuati nel PNRR, ovvero con le modalità previste dalla normativa nazionale ed europea vigente";
b. l'articolo 47 che ha previsto il rispetto di specifiche clausole negli affidamenti di procedure PNRR in tema di Pari opportunità di genere e generazionali nonché le Linee guida "Linee guida volte a favorire la pari opportunità di genere e generazionali, nonché l'inclusione lavorativa delle persone con disabilità nei contratti pubblici finanziati con le risorse del PNRR e del PNC" adottate con decreto interministeriale del 7 dicembre 2021;

xv il Piano Nazionale di Ripresa e Resilienza (di seguito anche "PNRR") - presentato alla Commissione in data 30 giugno 2021 e valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021, notificata all'Italia dal Segretariato generale del Consiglio con nota LT161/21, del 14 luglio 2021 e modificata dall'Allegato della proposta di Decisione di esecuzione del Consiglio del 24 novembre 2023 - e, in particolare, le indicazioni contenute relativamente al raggiungimento di Milestone e Target;

xvi gli ulteriori principi trasversali previsti dal paragrafo 5.2.1 del PNRR, quali, tra l'altro, il principio del contributo all'obiettivo climatico e digitale (c.d. tagging), il principio di parità di genere, l'obbligo di protezione e valorizzazione dei giovani e del superamento dei divari territoriali;

xvii il decreto del Ministro dell'economia e delle finanze del 6 agosto 2021, recante "Assegnazione delle risorse finanziarie previste per l'attuazione degli interventi del Piano nazionale di ripresa e resilienza (PNRR) e ripartizione di traguardi e obiettivi per scadenze semestrali di rendicontazione", che individua il DTD della Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante "Cybersecurity";

xviii il Regolamento (UE) 2020/852 del Parlamento europeo e del Consiglio del 18 giugno 2020, relativo all'istituzione di un quadro che favorisce gli investimenti sostenibili e recante modifica del Regolamento (UE) 2019/2088, e, in particolare, l'articolo 17, che definisce gli obiettivi ambientali, tra cui il principio del "non arrecare un danno significativo" (DNSH, "Do no significant harm");

xix la Comunicazione della Commissione UE 2021/C 58/01, recante "Orientamenti tecnici sull'applicazione del principio non arrecare danno significativo a norma del regolamento sul dispositivo per la ripresa e la resilienza";

xx gli obblighi di assicurare il conseguimento di target e milestone e degli obiettivi finanziari stabiliti nel PNRR;

xxi il decreto del Presidente del Consiglio dei ministri del 15 settembre 2021, con il quale sono stati individuati gli strumenti per il monitoraggio del PNRR;

xxii il decreto ministeriale del giorno 11 ottobre 2021, recante “Procedure relative alla gestione finanziaria delle risorse previste nell’ambito del PNRR di cui all’articolo 1, comma 1042, della legge 30 dicembre 2020, n. 178”;

xxiii la circolare del Ministero dell’economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, 14 ottobre 2021, n. 21, recante “Piano Nazionale di Ripresa e Resilienza Trasmissione alle Amministrazioni centrali dello Stato delle Istruzioni tecniche per la selezione dei progetti PNRR”;

xxiv il decreto-legge 6 novembre 2021, n. 152, convertito, con modificazioni, dalla legge 29 dicembre 2021, n. 233, recante “Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose”;

xxv la circolare del Ministero dell’economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, 30 dicembre 2021, n. 32, recante “Piano Nazionale di Ripresa e Resilienza – Guida operativa per il rispetto del principio di non arrecare danno significativo all’ambiente (DNSH)”, aggiornata con la circolare del 13 ottobre 2022, n. 33 errata corrige del 24 ottobre 2022 e circolare n. 22 del 14 maggio 2024;

xxvi la circolare del Ministero dell’economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 31 dicembre 2021, n. 33, recante “Piano Nazionale di Ripresa e Resilienza (PNRR) - Nota di chiarimento sulla Circolare del 14 ottobre 2021, n. 21 - Trasmissione delle Istruzioni Tecniche per la selezione dei progetti PNRR - Addizionalità, finanziamento complementare e obbligo di assenza del c.d. doppio finanziamento”;

xxvii il decreto del Presidente del Consiglio dei ministri 15 giugno 2021, recante “Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell’articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133”;

xxviii la circolare del Ministero dell’economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 21 giugno 2022, n. 27, recante “Piano Nazionale di Ripresa e Resilienza (PNRR) - Monitoraggio delle misure PNRR”;

xxix la circolare del Ministero dell’economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, del 18 gennaio 2022, n. 4, recante “Piano Nazionale di Ripresa e Resilienza (PNRR) - articolo 1, comma 1, del decreto-legge n. 80 del 2021 - Indicazioni attuative”;

xxx la circolare del Ministero dell’economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 24 gennaio 2022, n. 6, recante “Piano Nazionale di Ripresa e Resilienza (PNRR) – Servizi di assistenza tecnica per le Amministrazioni titolari di interventi e soggetti attuatori del PNRR”;

xxxi la circolare del Ministero dell’economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 10 febbraio 2022, n. 9, recante “Piano Nazionale di Ripresa e Resilienza (PNRR) - Trasmissione delle Istruzioni tecniche per la redazione dei sistemi di gestione e controllo delle amministrazioni centrali titolari di interventi del PNRR”;

xxxii la circolare del Ministero dell’economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, 29 aprile 2022, n. 21, recante “Piano nazionale di ripresa e resilienza (PNRR) e Piano nazionale per gli investimenti complementari - Chiarimenti in relazione al riferimento alla disciplina nazionale in materia di contratti pubblici richiamata nei dispositivi attuativi relativi agli interventi PNRR e PNC”;

xxxiii il decreto-legge 30 aprile 2022, n. 36, convertito, con modificazioni, dalla legge 29 giugno 2022, n. 79, recante “Ulteriori modifiche urgenti per l’attuazione del Piano nazionale di ripresa e resilienza (PNRR)”;

xxxiv la circolare del Ministero dell’economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio centrale per il PNRR, del 4 luglio 2022, n. 28, recante “Controllo di regolarità amministrativa e contabile dei rendiconti di contabilità ordinaria e di contabilità

speciale. Controllo di regolarità amministrativa e contabile sugli atti di gestione delle risorse del PNRR - prime indicazioni operative";

xxxv la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 26 luglio 2022, n. 29, recante "Circolare delle procedure finanziarie PNRR";

xxxvi la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, dell'11 agosto 2022, n. 30, recante "Circolare sulle procedure di controllo e rendicontazione delle misure PNRR", con la quale sono state emanate le "Linee guida di controllo e rendicontazione delle Misure PNRR di competenza delle Amministrazioni centrali e dei Soggetti Attuatori", aggiornate con la circolare del 14 aprile 2023, n. 16 e la circolare 15 settembre 2023, n. 27 recante l'adozione della "Appendice tematica Rilevazione delle titolarità effettive ex art. 22 par. 2 lett. d) Reg. (UE) 2021/241 e comunicazione alla UIF di operazioni sospette da parte della Pubblica amministrazione ex art. 10, d.lgs. 231/2007";

xxxvii la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 2 gennaio 2023, n. 1, recante "Controllo preventivo di regolarità amministrativa e contabile di cui al decreto legislativo 30 giugno 2011, n. 123. Precisazioni relative anche al controllo degli atti di gestione delle risorse del Piano Nazionale di Ripresa e Resilienza";

xxxviii la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, 13 marzo 2023, n. 10, recante "Interventi PNRR. Ulteriori indicazioni operative per il controllo preventivo ed il controllo dei rendiconti delle Contabilità Speciali PNRR aperte presso la Tesoreria dello Stato";

xxxix la Strategia Nazionale di Cybersicurezza 2022-2026, adottata unitamente al relativo Piano di Implementazione (di seguito anche "Piano"), con decreto del Presidente del Consiglio dei ministri del 17 maggio 2022;

xl l'Accordo stipulato, in data 14 dicembre 2021, tra l'Agenzia e il Dipartimento per la trasformazione digitale, ai sensi dell'articolo 5, comma 6, del d.lgs. n. 50/2016, di cui al prot. ACN n. 896 del 15 dicembre 2021, disciplinante lo svolgimento in collaborazione delle attività di realizzazione dell'"Investimento 1.5", registrato dalla Corte dei Conti il 18 gennaio 2022 al n. 95, e modificato dall'atto aggiuntivo del 14 luglio 2023, registrato dalla Corte dei Conti il 5 settembre 2023 al n. 2425;

xli il Sistema di Gestione e Controllo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri che illustra la struttura organizzativa, gli strumenti operativi e le procedure definite per la gestione, il monitoraggio, la rendicontazione e il controllo degli interventi previsti nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) di competenza del DTD, tra cui l'investimento 1.5 "Cybersecurity";

xlii le Linee guida per i Soggetti Attuatori versione 3 del 6 marzo 2023, adottate dall'Unità di Missione PNRR del Dipartimento per la trasformazione digitale, Amministrazione Centrale titolare per l'investimento 1.5;

xliii le circolari emanate dall'Unità di Missione PNRR del DTD e, in particolare, la circolare n. 1 "Politica per il contrasto alle frodi e alla corruzione e per prevenire i rischi di conflitti di interesse e di doppio finanziamento", la circolare n. 2 "Tutela della sana gestione finanziaria – Indicazioni ai fini dell'attuazione degli interventi", la circolare n. 3 "Indicatori per il monitoraggio e la valutazione del PNRR" e la circolare n. 5 "Ulteriori indicazioni ai fini della rilevazione dei titolari effettivi";

xliv le "Linee guida per i soggetti attuatori individuati tramite avvisi pubblici" per la realizzazione degli interventi a valere su M1M1I1.5 del PNRR comunicate da ACN in data 5 ottobre 2024 ai soggetti attuatori dell'avviso pubblico n. 8/2024 aggiornate alla versione 5.0;

considerato:

i nell'ambito delle procedure di attuazione degli interventi di cui al PNRR, la Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo", Componente 1 "Digitalizzazione, Innovazione e Sicurezza della P.A.", Investimento 1.5 "Cybersecurity" del PNRR prevede interventi per la digitalizzazione delle infrastrutture tecnologiche e dei servizi della P.A., rafforzando le difese cyber nazionali;

ii la Misura citata persegue l'aggiornamento delle misure di sicurezza cibernetica per n. 50 strutture, tra cui è stata individuata la Città metropolitana di Venezia;

iii la Città metropolitana di Venezia ha presentato entro i termini indicati da ACN del 25 marzo 2024 poi procrastinati dall'Agenzia al 12 aprile 2024, la domanda di partecipazione, candidando il progetto denominato "CYBERMET - Cybersecurity Metropolitana";

iv con determina ACN n. 22329 del 9 luglio 2024 è stata disposta l'ammissione della domanda di partecipazione della Città metropolitana e, a seguito della positiva valutazione del progetto, l'Agenzia per la Cybersicurezza Nazionale, con propria determina prot. 30550 del 23 settembre 2024 ha approvato la graduatoria finale dei progetti e ha ammesso a completo finanziamento "CYBERMET - Cybersecurity Metropolitana";

v con determinazione n. 3005 del 25 ottobre 2024 l'Area Amministrazione e transizione digitale, in conseguenza del positivo esito dell'adesione all'Avviso n. 8/2024, ha approvato i contenuti e gli obiettivi del progetto "CYBERMET - Cybersecurity Metropolitana" e l'atto d'obbligo definito da ACN per l'erogazione, ai sensi dell'art. 12 della L. 241/1990, del contributo previsto a finanziamento, inoltrato entro i termini ad ACN in data 25 ottobre 2024 con prot. 69165;

vi l'avvio del progetto, avvenuto in data 28 marzo 2024 con la determinazione a contrarre n. 843/2024 per l'acquisizione mediante MePA del servizio di protezione spam, malware e backup posta elettronica Hornet Security, già in riferimento al Progetto CYBERMET - Cybersecurity Metropolitana – PNRR Next Generation EU Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5 CUP B79B21002230006 CIG B2332081C7, è stato comunicato ad ACN entro il termine previsto con prot. 70148 del 30 ottobre 2024, nel rispetto delle modalità di comunicazione dell'avvio degli interventi qualificati "in essere" contenute nell'Avviso 8/2024 e nelle Linee guida di realizzazione;

vii l'aggiudicazione del servizio acquistato, di seguito identificato anche come "Contratto Hornet CIG B2332081C7", è avvenuta con determinazione n. 1905 del 12 luglio 2024 a seguito di RDO n. 4445364 del 21 giugno 2024 a favore della ditta Chip Space S.r.l. di Marcon (VE) p. IVA 02179570276 per l'importo di € 93.922,92 IVA inclusa ed è tuttora in esecuzione;

viii col medesimo prot. 70148/2024 di comunicazione avvio del progetto, Città metropolitana ne ha contestualmente comunicato la modifica, per meglio aderire alle necessità dell'ente in considerazione del diminuito ambito temporale a disposizione e delle migliori soluzioni disponibili, in termini di efficacia ed efficienza;

considerato altresì:

i il progetto "CYBERMET - Cybersecurity Metropolitana" prevede il seguente modello organizzativo:
   - governance generale affidata all'Area Amministrazione e Transizione Digitale della Città metropolitana di Venezia per la definizione delle linee strategiche, per il coordinamento e la validazione dei risultati;
   - progettazione e realizzazione affidata a Venis S.p.A., *in house* per i servizi informativi che dispone del team qualificato "cybersecurity", composto da figure interne specializzate e da figure esterne stabilmente inserite nel team per la sicurezza;
   - gestione amministrativa affidata all'Ufficio Europa della Città metropolitana, esperto nella gestione e rendicontazione, affiancato dall'Unità PMO e Progettazione finanziata di Venis S.p.A.;

ii la società Venezia Informatica Soluzioni - Venis S.p.A. di Venezia, p. IVA 02396850279 è posseduta per il 65,1% dal Comune di Venezia e per il 10% dalla Città metropolitana di Venezia che, ai sensi dell'art. 4 "Oggetto sociale" dello Statuto, ha nel tempo affidato contratti per la

produzione di beni e servizi strumentali alla propria attività, anche nell'interesse della collettività e del territorio metropolitano, attraverso:

- la progettazione, la realizzazione, la messa in opera e la gestione operativa di sistemi di informatica e di sistemi e reti di telecomunicazione, anche in qualità di operatore di telecomunicazioni, ed in generale di qualsiasi sistema di elaborazione e comunicazione elettronica attraverso tutti i mezzi e forme consentiti dalle tecnologie e dalla loro evoluzione;
- la razionalizzazione di sistemi già in esercizio;
- la produzione di sistemi operativi, procedure e programmi elettronici sia di base che applicativi;
- la progettazione, la messa in opera e la gestione operativa di strutture logistiche attrezzate, impianti speciali, apparecchiature elettroniche necessarie alla realizzazione e il funzionamento di impianti informatici e di telecomunicazione;
- l'installazione e la manutenzione dei sistemi di informatica e delle reti di telecomunicazione, ivi inclusa la effettuazione di controlli e diagnostiche di efficienza, la rimessa in servizio dei sistemi sia per quanto attiene le procedure che le apparecchiature;
- la realizzazione e la gestione di prodotti e l'erogazione di servizi di "Information and Communication Technology", compresa l'attività di formazione del personale richiesta da dette attività;
- la realizzazione e gestione di banche dati connesse al governo del territorio, nonché all'erogazione di servizi nel medesimo;
- l'esecuzione di lavori, la gestione e la realizzazione di opere, quali strutture mobili o immobili, impianti, infrastrutture o altre dotazioni patrimoniali strumentali e funzionali al sistema informativo ed alla rete di telecomunicazioni della Città metropolitana;
- l'erogazione di ogni altra attività e servizio connessi a quelli forniti, che non rientrano nelle fattispecie precedenti;

iii ai sensi dell'art. 7 comma 2 del D.lgs. 36/2023 la Città metropolitana intende affidare a Venis S.p.A. la progettazione e la realizzazione del progetto "CYBERMET - Cybersecurity Metropolitana", valutandone la congruità economica in relazione al perseguimento soprattutto degli obiettivi di economicità e celerità del procedimento;

iv per le correnti attività, oggetto statutario di Venis S.p.A., il Comune di Venezia ha reso disponibile la "Relazione per la valutazione della congruità economica" PG 603661 del 19 dicembre 2023, da cui si evince che le proposte commerciali di Venis S.p.A. concretano uno scostamento medio di benchmark pari al 3,8%, al netto dei costi di funzionamento della struttura aziendale e dell'IVA e comprensivo dei costi stimati in caso di affidamento del servizio a soggetti terzi (*mark up*);

v la citata valutazione di congruità economica è applicabile per estensione ed analogia anche alle attività oggetto del presente provvedimento, in riferimento alla proposta prot. n. 73171 del 12 novembre 2024 con cui Venis S.p.A. ha comunicato l'offerta per l'esecuzione entro il 31 ottobre 2025 dei servizi richiesti;

vi l'offerta tecnico- economica di Venis S.p.A., allegata al presente provvedimento, prevede:

| **DESCRIZIONE** | **IMPORTO** |
|---|---|
| 1. Governance e programmazione cyber | € 399.073,08 |
| 2. Gestione del rischio cyber e della continuità operativa | € 159.836,07 |
| 3. Gestione e risposta agli incidenti di sicurezza | € 221.311,47 |
| 4. Gestione delle identità digitali e degli accessi logici | € 143.442,62 |
| 5. Sicurezza delle applicazioni, dei dati e delle reti | € 148.423,84 |
| **TOTALE IVA ESCLUSA** | **€ 1.072.087,08** |

| | |
|---|---|
| **IVA 22%** | **€ 235.859,16** |
| **TOTALE IVA INCLUSA** | **€ 1.307.946,24** |

vii Limitatamente all'intervento 5 – Sicurezza delle applicazioni, dei dati e delle reti - le seguenti attività:
   a. Enumeration delle applicazioni presenti in SAD Venezia (Soggetto Aggregatore Digitale, ai sensi del Decreto del Direttore della Direzione ICT e Agenda Digitale della Regione Veneto n. 117 del 4 novembre 2019, in BUR Veneto n. 129 del 15 novembre 2019) e mappatura delle applicazioni business critical;
   b. Vulnerability assessment/Penetration test delle applicazioni business critical;
   c. Piano di remediation e relative attività di mitigazione;

   verranno eseguite anche sugli applicativi delle seguenti dieci amministrazioni che in fase di candidatura hanno dato parere favorevole alla propria adesione al progetto, concorrendo in modo significativo all'approvazione dello stesso e al riconoscimento del contributo nella sua interezza;
   1. Comune di Mirano;
   2. Comune di Jesolo;
   3. Comune di Scorzè;
   4. Comune di Santa Maria di Sala;
   5. Comune di Noale;
   6. Comune di Caorle;
   7. Comune di Concordia Sagittaria;
   8. Comune di Fossalta di Piave;
   9. Comune di Gruaro;
   10. Comune di Teglio Veneto;

viii a seguito della applicazione della metodologia DNSH di cui ai richiamati regolamenti unionali e circolari del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, la società esecutrice, anche in funzione del tagging climatico, assicura il rispetto dei principi DNSH nelle procedure di acquisizione dei servizi e dei beni oggetto dell'appalto;

ix come chiarito nella determinazione ANAC n. 4/2011, aggiornata da ultimo con delibera n. 585 del 19 dicembre 2023, gli affidamenti *in house* non sono sottoposti agli obblighi di tracciabilità dei flussi finanziari. Restano però valide le ulteriori cause per l'acquisizione del CIG, e cioè:
   a. l'identificazione univoca di una procedura di affidamento ed il suo monitoraggio, a garanzia della pubblicità e della trasparenza;
   b. l'adempimento degli obblighi contributivi;

x in applicazione al precedente alinea, le attività oggetto di contratto di servizio con Venis S.p.A. saranno affidate mediante PAD in uso nell'ente e, in concomitanza con la procedura di acquisto, saranno richiesti:
   a. il Documento Unico di Gara Europeo;
   b. le dichiarazioni e la documentazione specificamente richiesta dalle "Linee guida per i soggetti attuatori individuati tramite avvisi pubblici" per la realizzazione degli interventi a valere su M1C1I1.5 del PNRR, versione 5.0;
   c. il rispetto degli obblighi documentali di cui al commi 2, 3, 3-bis dell'art. 47 del decreto legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, che dispone in merito alle pari opportunità, generazionali e di genere nei contratti pubblici PNRR e PNC;
   d. l'autocertificazione sugli obblighi di condotta previsti dal D.P.R. 16 aprile 2013, n. 62 "Codice di comportamento dei dipendenti pubblici", dal codice interno, dalla disciplina dell'istituto del whistleblowing per la segnalazione degli illeciti, dalla disciplina della tutela del segnalante (di cui alle relative sezioni del P.I.A.O. citato);

e. il codice identificativo di gara CIG;

xi è stata accertata la regolarità del DURC in corso di validità;

xii pur trattandosi di affidamento di contratto di servizio *in house*, l'ente richiede di effettuare il controllo e le opportune verifiche in tema di antiriciclaggio mediante l'utilizzo della check list 1 a, b, di cui alla Circolare 02/2024 del 22 ottobre 2024;

xiii tenuto conto della rilevanza strategica ed economica dell'affidamento, ai sensi dell'art. 15 D.lgs. 36/2023 è nominato Responsabile unico di progetto il sottoscritto dott. Romano Armellin dirigente dell'Area Amministrazione e transizione digitale;

xiv il dirigente firmatario del presente provvedimento nonché responsabile di progetto:

a. non si trova in posizione di conflitto d'interessi rispetto all'adozione dello stesso provvedimento e, pertanto, non è tenuto all'obbligo di astensione come previsto dall'art. 6-bis della legge n. 241/1990, dall'art. 16 del D.lgs. 36/2023 nonché dagli artt. 6 e 7 del Codice di comportamento dei dipendenti pubblici;

b. non si trova in alcuna delle condizioni previste dall'art. 35 bis del D.lgs. 165/2001 e dall'art. 6 della L. 114/2014, nella misura in cui sono applicabili;

xv per quanto riguarda il rispetto delle norme previste dal P.I.A.O. nella sezione P.T.P.C.T.:

a. il presente provvedimento sarà pubblicato nella sezione Amministrazione Trasparente sul sito istituzionale dell'Ente, nel rispetto degli obblighi di pubblicazione vigenti (mis. Z02 del P.I.A.O. 2024-2026);

b. vista la natura di affidamento *in house*, non ricorre l'obbligo di recepimento del protocollo di legalità della Prefettura di Venezia (mis. Z18 del PIAO 2024-2026), come modificato ed integrato dalla circolare CMVE n. 1 del 23 marzo 2023;

xvi i rapporti e le relazioni previste dai citati commi 2, 3 e 3-bis dell'art. 47 del decreto legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108 saranno pubblicati sul profilo del committente, sia nella sezione "Amministrazione trasparente", sia nella sottosezione "Bandi di gara e contratti - dal 01/01/2024" e comunicati alla Presidenza del Consiglio dei Ministri ovvero ai Ministri o alle autorità delegati per le pari opportunità e della famiglia e per le politiche giovanili e il servizio civile universale;

visti gli obblighi amministrativo-contabili concernenti la gestione finanziaria del progetto, posti in capo alla Città metropolitana di Venezia in qualità di soggetto attuatore dell'Intervento:

i come previsto dal coordinato disposto dell'art. 10 comma 1 lettera c) e art. 161 comma 6-bis del D.P.R. n. 207 del 5 ottobre 2010 "Schema di regolamento di esecuzione e attuazione del Decreto Legislativo 12 Aprile 2006, n. 163, recante codice dei contratti pubblici relativi a lavori, servizi e forniture"; e dell'art. 1, commi 1 e 5 della L. n. 144 del 17 maggio 1999 "Misure in materia di investimenti, delega al Governo per il riordino degli incentivi all'occupazione e della normativa che disciplina l'INAIL, nonché disposizioni per il riordino degli enti previdenziali"; e dell'art. 28, commi 3 e 5 della L. n. 289 del 27 dicembre 2002 "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2003)"; e dell'art. 11 della L. n. 3 del 16 gennaio 2003 "Disposizioni ordinamentali in materia di pubblica amministrazione" è stato acquisito il CUP: B79B21002230006;

ii è stato attivato a bilancio il capitolo specifico di entrata n. 420000101326/0 "PNRR PROGETTO M1 C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006";

iii con determinazione n. 3005 del 25 ottobre 2024 si è proceduto all'accertamento nel 2024 delle somme in entrata relative alla realizzazione del progetto PNRR Missione 1, Componente 1, Asse 1, Misura 1.5 "Cybersecurity", piano operativo CMVE: "CYBERMET – Cybersecurity Metropolitana" CUP B79B21002230006 per € 1.500.000,00 IVA inclusa;

iv necessita riaccertare in competenza anno 2025 l'importo di € 1.468.692,36, risultante dal complessivo contributo di ACN, dedotta:

a. la somma di € 31.307,64 IVA inclusa, quale remunerazione, già fatturata nel corso del 2024, per la prima annualità del "Contratto Hornet CIG B2332081C7";

b. la somma di € 600,00 IVA esente, per il contributo ANAC sul contratto di servizio Venis S.p.A., così quantificato in relazione al valore del futuro contratto, compreso tra € 1.000.000,00 e € 5.000.000,00;

v necessita ridurre per l'intero ammontare l'accertamento n. 27060/2024 dal capitolo specifico di entrata n. 420000101326/0 "PNRR PROGETTO M1 C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006" dell'anno 2024 trattenendo esclusivamente la somma di € 600,00 IVA esente, a copertura del contributo ANAC citato;

vi è stato attivato a bilancio il capitolo specifico di spesa n. 201080205619/4 "PNRR PROGETTO M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006";

vii con medesima determinazione n. 3005/2024 si è proceduto ad impegnare nel 2024 le somme relative alla realizzazione del progetto PNRR Missione 1, Componente 1, Asse 1, Misura 1.5 "Cybersecurity", piano operativo CMVE: "CYBERMET – Cybersecurity Metropolitana" CUP B79B21002230006 per € 1.500.000,00 IVA inclusa;

viii necessita reimputare su annualità 2025 la spesa di € 1.468.692,36, risultante dal complessivo contributo di ACN, dedotta:

a. la somma di € 31.307,64 IVA inclusa, quale remunerazione, già fatturata nel corso del 2024, per la prima annualità del "Contratto Hornet CIG B2332081C7";

b. la somma di € 600,00 IVA esente, per il contributo ANAC sul contratto di servizio Venis S.p.A., così quantificato in relazione al valore del futuro contratto, compreso tra € 1.000.000,00 e € 5.000.000,00;

ix necessita ridurre per l'intero ammontare l'impegno n. 1661/2024 del capitolo specifico di spesa n. 201080205619/4 "PNRR PROGETTO M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006" dell'anno 2024, trattenendo esclusivamente la somma di € 600,00 IVA esente, a copertura del contributo ANAC citato, che si procede a sub impegnare. Detto importo è considerato parte delle spese generali, fino ad un massimo del 7% dei costi diretti ammissibili a progetto, ai sensi dell'art. 54, lettera A) del Reg. (UE) 2021/1060;

x con il presente provvedimento, si procede a impegnare sul capitolo n. 201080205619/4 "PNRR PROGETTO M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006" del bilancio 2025:

a. € 1.307.946,24 IVA inclusa a favore della società Venis S.p.A. per l'esecuzione dei servizi afferenti al progetto PNRR Missione 1, Componente 1, Asse 1, Misura 1.5 "Cybersecurity", piano operativo CMVE "CYBERMET – Cybersecurity Metropolitana" CUP B79B21002230006;

b. € 31.307,64 IVA inclusa, quale remunerazione per la seconda annualità del "Contratto Hornet CIG B2332081C7", completamente riducendo l'impegno n. 151/2025 su capitolo n. 101080305512/0 - SERVIZI DI HOUSING E RELATIVA CONNETTIVITÀ/HOSTING/SICUREZZA giusta determinazione n. 1905/2024;

c. la somma a copertura degli incentivi per le funzioni tecniche ai sensi dell'art. 45 D.lgs. 36/2023, essenziali e strumentali all'attuazione dell'intervento e per il perseguimento degli obiettivi di progetto. Gli incentivi ammissibili per le funzioni tecniche ai sensi dell'art. 45 D.lgs. 36/2023, ai sensi della normativa nazionale e comunitaria di riferimento vigente, riguardano il "Contratto Hornet CIG B2332081C7", per un importo di € 1.231,78, pari al 2% del valore contrattuale dei servizi citati, diminuito del 20% per le finalità di cui ai commi 6 e 7 del D.lgs. 36/2023, non dovuto. Gli incentivi ammissibili per le funzioni tecniche ai sensi dell'art. 45 D.lgs. 36/2023 sono considerati parte delle spese generali, fino ad un massimo del 7% dei costi diretti ammissibili a progetto, ai sensi dell'art. 54, lettera A) del Reg. (UE) 2021/1060;

Determina

1 di adottare la decisione di contrarre per l'acquisizione del servizio di realizzazione Progetto CYBERMET - Cybersecurity Metropolitana nell'ambito del PNRR Next Generation EU Missione 1 – Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5 CUP B79B21002230006 dalla società Venezia Informatica e Sistemi S.p.A. di Venezia p. IVA 02396850279 ai sensi dell'art. 7 comma 2 del D.lgs. 36/2023, per un importo complessivo di € 1.072.087,08 IVA esclusa;

2 di stipulare il contratto di servizio *in house* con le modalità, le condizioni e le forme previste dalla PAD della Città metropolitana di Venezia;

3 di ridurre completamente l'accertamento n. 27060/2024 sul capitolo specifico di entrata n. 420000101326/0 "PNRR PROGETTO M1 C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006" dell'anno 2024 giusta determinazione n. 3005/2024, trattenendo esclusivamente la somma di € 600,00 IVA esente, a copertura del contributo ANAC;

4 di riaccertare in competenza anno 2025 l'importo di € 1.468.692,36 sul capitolo specifico di entrata n. 420000101326/0 "PNRR PROGETTO M1 C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006";

5 di ridurre completamente l'impegno n. 1661/2024 su capitolo n. 201080205619/4 "PNRR PROGETTO M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006" del bilancio 2024 giusta determinazione n. 3005/2024, trattenendo esclusivamente la somma di € 600,00 IVA esente, a copertura del contributo ANAC;

6 di sub impegnare la somma di € 600,00 IVA esente per il contributo ANAC su impegno n. 1661/2024 del capitolo n. 201080205619/4 "PNRR PROGETTO M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006" del bilancio 2024, giusta determinazione n. 3005/2024;

7 di imputare alla competenza anno 2025 l'importo di € 1.468.692,36 sul capitolo specifico di spesa n. 201080205619/4 "PNRR PROGETTO M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006";

8 di impegnare la somma complessiva di € 1.307.946,24 IVA inclusa per il servizio in oggetto, sul capitolo n. 201080205619/4 "PNRR PROGETTO M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006" del bilancio 2025 a favore della società Venezia Informatica e Sistemi S.p.A. di Venezia p. IVA 02396850279;

9 di impegnare la somma complessiva di € 31.307,64 IVA inclusa quale remunerazione per la seconda annualità del "Contratto Hornet CIG B2332081C7", sul capitolo n. 201080205619/4 "PNRR PROGETTO M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006" del bilancio 2025 a favore della società Chip Space S.r.l. di Marcon (VE), p. IVA 02179570276;

10 di impegnare la somma complessiva di € 1.231,78, pari al 2% del valore contrattuale del "Contratto Hornet CIG B2332081C7", diminuito del 20% per le finalità di cui ai commi 6 e 7 del D.lgs. 36/2023, non dovuto, sul capitolo n. 201080205619/4 "PNRR PROGETTO M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006" del bilancio 2025;

11 di prendere atto che, 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;

12 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;

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

14 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. 2024-2026) e nell’apposita sezione di Amministrazione Trasparente relativa agli atti PNRR (mis. Z09 del P.I.A.O. 2024-2026);

15 ai fini del comma 9 dell’art. 47 del D.lgs. 77/2021 convertito con modifiche in Legge 29 luglio 2021 n. 108:

a. in caso l’operatore economico dichiari di occupare più di 50 dipendenti, sarà pubblicato il rapporto di cui all’art. 47 comma 2 del citato D.L. 77/2021;

b. in caso l’operatore economico dichiari di occupare da 15 a 50 dipendenti, verrà richiesta la consegna, entro sei mesi dalla data di stipulazione del contratto, della documentazione di cui al comma 3 e 3 bis dell’art. 47 del citato D.L. 77/2021 per la relativa pubblicazione su “Amministrazione trasparente” e, contestualmente, per la trasmissione ai Ministeri o autorità delegati per le pari opportunità e la famiglia per le politiche giovanili ed il servizio civile universale, per le politiche in favore della disabilità;

c. la pubblicazione degli atti avverrà anche nella sottosezione “Bandi di gara e contratti - dal 01/01/2024” di “Amministrazione trasparente”;

16 in merito all’assenza di conflitto di interesse, così come previsto dalla Circolare MEF n. 30 Determinazione n. 81 del 26 gennaio 2024, in relazione alle procedure di controllo e rendicontazione delle misure PNRR, si allega al presente atto, in modalità riservata in quanto contenenti dati personali non ostensibili, le dichiarazioni rilasciate dal RUP.;

17 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

venezia informatica e sistemi

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

Venezia, 11novembre 2024
Sigla: 610_DM_241111

Al Dirigente
Area Amministrazione e Supporto alla Transizione Digitale
Città metropolitana di Venezia
Dott. Romano ARMELLIN

E, p.c.

Al Responsabile
Servizio Infrastrutture Digitali e SITM
Area Amministrazione e Transizione Digitale
Ing. Luca CELEGHIN

informatica.cittametropolitana.ve@pecveneto.it
protocollo.cittametropolitana.ve@pecveneto.it

Oggetto: Progetto PNRR M1C1 - 1.5 Cybersecurity “CYBERMET – Cybersecurity Metropolitana”, Città Metropolitana di Venezia, CUP B79B21002230006
**Trasmissione dell'offerta tecnico-economica v.01.**

Egr. Dott. Armellin,

Si fa seguito alle intercorse comunicazioni di cui in oggetto relative alla nostra proposta tecnico-economica per la realizzazione del progetto CYBERMET – CYBERSECURITY METROPOLITANA" NELL’AMBITO DEL PNRR NEXTGENERATION EU MISSIONE 1 – COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY", per precisare quanto segue in merito ai “tempi di realizzazione” rif. p. 2 dell’Offerta e “articolazione temporale del progetto” rif. p. 4 della Proposta di Piano Operativo:

*Le attività avranno avvio a partire dal perfezionamento dell’affidamento a Venis da parte di Città Metropolitana di Venezia e verranno completate entro il 31/10/2025 (da intendersi come data di conclusione dell’affidamento); in coerenza con la data di fine progetto fissata dall’Avviso n. 08 al 31/12/2025 (salvo proroghe eventualmente concesse da ACN), proseguiranno le sole attività di supporto all’Ente per la finalizzazione della rendicontazione.*

A tal fine si riportano nel prosieguo i contenuti dell’Offerta v. 01 e si riallega la Proposta di Piano Operativo vers 0.1 in recepimento della suddetta precisazione.

## 1. CONTENUTI DELLA PROPOSTA

Il progetto *"CYBERMET – Cybersecurity Metropolitana* si pone come obiettivo prioritario il potenziamento della resilienza cyber dell'Ente, coerentemente con quanto previsto dalla normativa relativa al Perimetro di Sicurezza Cibernetica Nazionale ed al GDPR.

Le attività proposte da Venis in qualità di esecutore, si sviluppano lungo cinque linee di intervento:

1. Delineare l'attuale stato di maturità cyber di Città Metropolitana di Venezia con particolare focus sulla postura di sicurezza dei servizi esposti in rete Internet e Intranet, alle postazioni di lavoro e dei principali processi di sicurezza previsti nei *framework* di riferimento;

2. Definire una strategia di miglioramento per la gestione del rischio e della continuità operativa di specifici processi e strumenti adottati per la gestione della sicurezza ICT e degli eventi di sicurezza;

3. Incrementare la Cybersecurity Awareness dei dipendenti dell'Ente e potenziare le competenze del personale tecnico attraverso piani di formazione base e specializzanti, nonché simulazione di attacchi (ad esempio: simulazione di campagna di phishing) dotando l'Ente di adeguante competenze e procedure standard utili alla prevenzione e alla gestione di incidenti di sicurezza.

4. Potenziare la gestione delle identità digitali e degli accessi logici attraverso il trasferimento di competenze specialistiche al personale tecnico attraverso piani specializzanti e l'implementazione di nuove tecnologie a supporto;

5. Rafforzare la Sicurezza delle applicazioni, dei dati e delle reti attraverso l'analisi della postura di sicurezza dal punto di vista tecnologico di Città Metropolitana di Venezia individuando soluzioni e strumenti tecnologici da acquistare per il potenziamento dell'infrastruttura di protezione dell'Ente.
Specificatamente in ambito SAD Metropolitano, elaborare Piani di Remediation per le eventuali applicazioni Business Critical che verranno rilevate, da proporre alle 10 amministrazioni aderenti al progetto.

## 2. TEMPI DI REALIZZAZIONE

Le attività avranno avvio a partire dal perfezionamento dell'affidamento a Venis da parte di Città Metropolitana di Venezia e verranno completate entro il 31/10/2025 (da intendersi come data di conclusione dell'affidamento); in coerenza con la data di fine progetto fissata dall'Avviso n. 08 al 31/12/2025 (salvo proroghe eventualmente concesse da ACN), proseguiranno le sole attività di supporto all'Ente per la finalizzazione della rendicontazione.

Per i dettagli del nuovo cronoprogramma si rimanda al cap. 4 dell'allegato Proposta di Piano Operativo.

## 3. DETTAGLIO DEI COSTI

Il seguente quadro economico è stato elaborato tenendo conto del raggiungimento delle Milestone e dei Target stabiliti nel progetto, al netto dei costi già affidati da Città Metropolitana e di progressiva maturazione (spese generali e servizi di protezione “Hornet”).

La tabella esposta riassume i costi di realizzazione imputati per ogni linea d’intervento, considerando il coinvolgimento di un team di lavoro misto, composto da risorse professionali Venis e da servizi specialistici esterni da acquisire attraverso l’adesione ad Accordi Quadro Consip.

Per ogni linea d’intervento è stata prevista, inoltre, un’attività specifica di “acquisizione e implementazione di sistemi e tecnologie” finalizzata all’attuazione delle azioni di mitigazione del rischio che dovessero emergere dalla gap analysis.

| Descrizione | Valorizzazione economica complessiva |
|---|---|
| 1. Governance e programmazione cyber | 399.073,08 € |
| 2. Gestione del rischio cyber e della continuità operativa | 159.836,07 € |
| 3. Gestione e risposta agli incidenti di sicurezza | 221.311,47 € |
| 4. Gestione delle identità digitali e degli accessi logici | 143.442,62 € |
| 5. Sicurezza delle applicazioni, dei dati e delle reti | 148.423,84 € |
| **Costi IVA ESCL.** | **1.072.087,08 €** |
| **IVA 22%** | **235.859,16 €** |
| **TOTALE PROGETTO IVA INCL.** | **1.307.946,24 €** |

Complessivamente la presente offerta ammonta a **euro 1.072.087,08 € (iva esclusa)** pari a euro **1.307.946,24 € (iva inclusa)**. Per i dettagli delle attività e dei relativi costi, si rimanda al cap. 5 della proposta di Piano Operativo qui allegato.

Resta inteso che, a valle della fase di progettazione esecutiva o comunque in corso d’opera, alla luce delle contrattualizzazioni effettive dei servizi nonché delle acquisizioni di tecnologie che si renderanno necessarie, ogni eventuale economia realizzata rispetto alla proposta economica qui presentata, sarà tempestivamente comunicata e ritornerà nella piena disponibilità di Città Metropolitana di Venezia.

## 4. CONDIZIONI DI FORNITURA

Il referente tecnico di Venis per il progetto è:

- **Adrian Trofin**, tel 041 2744826, e-mail venis@venis.it

Modalità di fatturazione: a deliverables rilasciati per stati avanzamento lavori, attraverso la elaborazione di Relazioni Intermedie di Avanzamento sottoposte a validazione dell'Ente attuatore CMVE, nel rispetto delle formalità previste dal programma PNRR e specificatamente dall'avviso pubblico n. 08 di riferimento.

Pagamento: 30 giorni data fattura.

Validità della presente offerta tecnico-economica: **10 giorni** dalla data di protocollazione della stessa.

## 5. TRATTAMENTO DATI PERSONALI

Con riferimento ai dati personali, presenti e/o strettamente connessi alla presente offerta, Venis effettua il trattamento nel rispetto della normativa vigente in materia di protezione dati (Reg. UE 2016/679 e D. Lgs. 196/2003 e s.m.i.) applicando adeguate misure di sicurezza tecnologiche e organizzative. Con l'accettazione dell'offerta, anche il cliente si impegna a effettuare il trattamento in conformità alla normativa vigente per le sole finalità gestionali e amministrative connesse.

Restando in attesa di un Vostro riscontro, si coglie l'occasione per porgere cordiali saluti.

Venis S.p.A.
Marco Bettini
Condirettore Generale
**FIRMATO DIGITALMENTE**

**Allegato**: Citato

# PROPOSTA DI PIANO OPERATIVO

*CYBERMET – Cybersecurity Metropolitana*

Città Metropolitana di Venezia
Misura PNRR 1.5 - " Cybersecurity"

08/11/2024 v. 0.1

| | |
|---|---|
| **Redatto:** | **Daniela Minto 08/11/2024** |
| **Visto:** | **Adrian Trofin 08/11/2024** |
| **Visto:** | **Federica Braga 08/11/2024** |
| **Approvato:** | **Marco Bettini 08/11/2024** |

venezia informatica e sistemi

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

# Sommario

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

# 1 Introduzione

L'obiettivo della misura PNRR M1C1 – Investimento 1.5 "*Cybersecurity*" è quello di rafforzare la capacità del Paese di prevenire e gestire gli attacchi cibernetici, al fine di garantire la sicurezza del sistema Paese e tutelare i cittadini, le imprese e le infrastrutture critiche dal rischio di attacchi informatici. L'Agenzia per la Cybersicurezza Nazionale **(ACN**) è stata individuata come Soggetto Attuatore dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri **(DTD)** per promuove Avvisi Pubblici per l'attuazione degli investimenti finalizzati alla realizzazione di interventi di potenziamento della resilienza cyber per la Pubblica Amministrazione.

Nell'ambito del Piano Operativo per l'attuazione del citato investimento e ai fini del raggiungimento di milestone e target (M&T) assegnati, ACN prevede la selezione di progetti a titolarità di **Altri Soggetti Attuatori** pubblici o privati che provvedono alla realizzazione degli interventi previsti dal PNRR e che sono responsabili dell'avvio, dell'attuazione e della funzionalità dei singoli interventi di competenza, della regolarità delle procedure e delle spese rendicontate, nonché del monitoraggio circa il conseguimento dei valori definiti per gli indicatori associati ai propri progetti. In quest'ultima fattispecie rientrano anche le **Città Metropolitane**, le quali grazie all'**Avviso Pubblico n. 08** hanno candidato progetti per il potenziamento della resilienza *cyber.*

L'Avviso era volto a supportare la realizzazione di un percorso virtuoso di gestione del rischio cyber in linea con le migliori pratiche nazionali e internazionali ed in particolare riguardava:

- il finanziamento per la realizzazione di un censimento dei livelli di maturità della postura di sicurezza dei servizi e delle infrastrutture digitali della PA;
- il finanziamento per la realizzazione di un piano programmatico di potenziamento, sia a breve che a medio-lungo termine, delle capacità cyber, volto a supportare il percorso di trasformazione digitale sicura della PA;
- il finanziamento per la realizzazione di interventi di potenziamento cyber a breve-medio termine dei servizi e delle infrastrutture in essere della PA.

**Con Domanda di Ammissione del 10/04/2024 all'Avviso Pubblico n. 08/2024, Città Metropolitana di Venezia ha candidato il progetto CYBERMET per la realizzazione dei seguenti interventi da attuare entro il 31/12/2025**:

1. Governance e programmazione cyber: coordinamento, supervisione e gestione olistica e integrata della cybersecurity attraverso la programmazione strategica di investimenti e iniziative;
2. Gestione del rischio cyber e della continuità operativa: individuazione, valutazione e trattamento sistematico dei rischi associati all'ambito cyber, e implementazione di un piano volto a garantire la resilienza di funzioni e servizi critici in caso di eventi avversi;
3. Gestione e risposta agli incidenti di sicurezza: monitoraggio, identificazione e gestione degli incidenti cyber, e ripristino dei sistemi impattati;
4. Gestione delle identità digitali e degli accessi logici: governo delle identità e definizione dei permessi di accesso alle risorse al fine di autenticare e autorizzare correttamente persone, gruppi e servizi in base agli attributi specifici e ai principi di "need to know", "least privilege" e "segregation of duties";

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

5. Sicurezza delle applicazioni, dei dati e delle reti: protezione dell'infrastruttura applicativa e di rete, e regolamentazione dei processi di protezione dei dati riservati, al fine di prevenire l'occorrenza di potenziali incidenti cyber e ridurne gli impatti.

**Gli interventi proposti da Città Metropolitana di Venezia sono finalizzati all'analisi e al potenziamento delle capacità di resilienza cyber dell'Ente** in termini di: postura di sicurezza, processi, modello organizzativo, competenze e consapevolezza del personale, acquisizione di sistemi e tecnologie. Nell'ambito del SAD Metropolitano, inoltre, sono stati previsti alcuni interventi specifici di cybersecurity che **coinvolgono n. 10 Amministrazioni Locali,** e che mirano alla formulazione di Piani di Remediation per gli applicativi che risulteranno Business Critical.

ACN con nota di trasmissione del 25/09/2024 ha comunicato l'ammissione in graduatoria e finanziamento del progetto "***CYBERMET – Cybersecurity Metropolitana***" come da Determina prot. n. 30550 del 23/09/2024.

Con riferimento alla richiesta di Città Metropolitana del 22 ottobre scorso (PG/2024/2567), **Venis** in qualità di inhouse dell'Ente e chiamato quale **Soggetto Esecutore**, formula la **Proposta di Piano Operativo** del progetto dettagliando le attività che intende erogare, nonché i relativi tempi e costi per il raggiungimento di milestone e target (M&T) fissati con il progetto.

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

# 2 Descrizione del progetto

Il progetto "***CYBERMET – Cybersecurity Metropolitana***" si pone come obiettivo prioritario il potenziamento della resilienza cyber dell'Ente, coerentemente con quanto previsto dalla normativa relativa al Perimetro di Sicurezza Cibernetica Nazionale ed al GDPR, nonché di supportare il processo di transizione digitale della Città Metropolitana di Venezia attraverso cinque linee di intervento.
Il progetto si articola lungo cinque linee di intervento che Venis è chiamata a sviluppare:

1. Delineare l'attuale **stato di maturità cyber di Città Metropolitana di Venezia**, con particolare focus sulla postura di sicurezza dei servizi esposti in rete Internet e Intranet, alle postazioni di lavoro e dei principali processi di sicurezza previsti nei *framework* di riferimento;
2. Definire una **strategia di miglioramento** per la gestione del rischio e della continuità operativa di specifici processi e strumenti adottati per la gestione della sicurezza ICT e degli eventi di sicurezza;
3. Incrementare la **Cybersecurity Awareness** dei dipendenti e potenziare le **competenze del personale tecnico** attraverso piani di formazione base e specializzanti, nonché simulazione di attacchi (ad esempio: simulazione di campagna di phishing) dotando l'Ente di adeguante competenze e procedure standard utili alla prevenzione e alla gestione di incidenti di sicurezza.
4. Potenziare la gestione delle identità digitali e degli accessi logici attraverso il trasferimento di **competenze specialistiche al personale tecnico** attraverso piani specializzanti e l'implementazione di nuove tecnologie a supporto;
5. Rafforzare la **Sicurezza delle applicazioni**, dei **dati** e delle **reti** attraverso l'analisi della postura di sicurezza dal punto di vista tecnologico individuando soluzioni e strumenti tecnologici da acquistare per il potenziamento dell'infrastruttura di protezione dell'Ente**.**
Specificatamente in ambito SAD, elaborare piani di remediation per le eventuali applicazioni Buisiness Critical da proporre alle 10 amministrazioni aderenti al progetto.

## 2.1 Intervento 1 – Governance e programmazione cyber

Per l'intervento in analisi, Venis attuerà l'analisi della postura di sicurezza dell'Ente al fine di delineare una **Strategia di Cybersecurity** che rispetti le best practice e gli standard del settore (quali, a titolo esemplificativo, ma non esaustivo GDPR e ISO 27001). Venis prevede specificatamente di sviluppare le seguenti attività:

- ***Security Strategy AS-IS***: L'attività permette di delineare lo stato di maturità Cyber consentendo di individuare eventuali lacune nella sicurezza informatica attraverso una fase di **Gap Analysis** e di adottare misure di sicurezza appropriate per proteggere le informazioni sensibili e i dati personali dei cittadini, mantenendo così un alto livello di fiducia e trasparenza. Inoltre, la definizione del profilo di sicurezza AS-IS è volta a garantire il rispetto dei requisiti della normativa di riferimento per il trattamento dei dati personali nell'UE (GDPR), nonché il mantenimento ed il miglioramento delle politiche per la gestione efficace della sicurezza delle informazioni dell'Amministrazione;
- ***Security Strategy Plan***: L'attività prevede la definizione di un piano di miglioramento della postura di cyber security per consentire l'individuazione delle principali aree di criticità e delle azioni di remediation da attuare;

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

- ***Formazione e Cyber**:* A partire dai risultati ottenuti dall'Assessment sulla postura di sicurezza e attraverso un'attenta analisi dei fabbisogni formativi, l'intervento mira alla definizione di un piano formativo in tema cyber ad-hoc sulle esigenze dell'Ente.
- ***Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo:*** A seguito dei risultati ottenuti dall'Assessment sulla postura di sicurezza e in relazione alle esigenze dell'Ente, Venis condurrà una fase di Scouting e Benchmarking di nuovi strumenti e tecnologie volta al potenziamento dell'infrastruttura tecnologica tramite l'implementazione di nuovi sistemi quali, a titolo esemplificativo, piattaforme SASE o piattaforme per la formazione del personale (un sistema integrato di e-learning può contribuire alla riduzione dell'esposizione alle minacce cibernetiche).

  Le soluzioni/strumenti identificati saranno sottoposti alla validazione dell'Ente.

## 2.2 Intervento 2 – Gestione del rischio cyber e della continuità operativa

L'intervento ha l'obiettivo di valutare e quantificare il rischio a cui è esposto l'Ente dalle minacce cyber security in relazione alla postura di sicurezza AS-IS. Ciò è fondamentale per preservare la continuità operativa e la resilienza dei processi dell'Ente, nonché per il mantenimento della sicurezza dei dati, delle informazioni, delle persone e dei loro diritti fondamentali.

Al fine di raggiungere l'obiettivo, Venis propone la realizzazione delle seguenti attività:

- ***Analisi dei rischi cyber:*** Analisi della gestione del rischio cyber e della continuità operativa al fine di raccogliere, analizzare e interpretare informazioni relative alle minacce e alle vulnerabilità del sistema informatico attualmente in essere. Tali processi sono necessari per la comprensione della natura delle minacce identificate e al calcolo del livello di rischio a cui l'Ente è esposto. La definizione di tale livello di rischio consente poi di delineare un Piano di trattamento volto alla mitigazione del rischio residuo e di contribuire al potenziamento della resilienza cyber dell'intera infrastruttura.
- ***Acquisizione ed implementazione/sviluppo di sistemi e tecnologie a supporto dei processi di miglioramento dell'organizzazione: A seguito di un'attenta* analisi dei requisiti tecnici e procedurali** derivanti dall'analisi al punto precedente, sarà possibile individuare le soluzioni e gli strumenti da integrare nell'infrastruttura al fine di consentire una più ampia gestione del rischio cyber e della continuità operativa, quali a titolo esemplificativo Sistemi di Backup e di Data Loss Prevention.

## 2.3 Intervento 3 – Gestione e risposta agli incidenti di sicurezza

L'obiettivo dell'intervento della gestione e della risposta agli incidenti di sicurezza si identifica nel monitoraggio, identificazione e gestione degli incidenti cyber, e ripristino dei sistemi impattati.

Al fine di consentire all'Ente di traguardare l'obiettivo generale, Venis prevede la realizzazione delle seguenti attività:

- **Definizione di un processo di gestione degli incidenti**: Redazione e standardizzazione di un processo efficace e sistematico da adottare in caso di incidente, che possa garantire la

Venis S.p.A.
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
protocollo@pec.venis.it - venis@venis.it - www.venis.it

minimizzazione dell'impatto degli eventi malevoli l'individuazione tempestiva di misure di contrasto e contenimento. Oltre alla procedura di gestione incidenti di carattere tecnico-organizzativo, saranno prodotti una serie di **Playbook di risposta agli incidenti** su diversi scenari, contenenti una serie di misure predefinite e istruzioni operative, per consentire all'Ente di identificare la minaccia ed agire in maniera tempestiva. Contestualmente verranno svolte delle **sessioni di formazione ad-hoc sulle Tecniche di hacking** per permettere al personale specializzato di comprendere al meglio gli scenari di attacco e di rispondere in modo tempestivo, attraverso un percorso formativo specifico basato su Ethical Hacking/Network Defender. Si prevede un'attività formativa da erogare a circa 30 dipendenti (profili e ruoli da identificare), da somministrare con differenti strumenti: formazione frontale in presenza, da remoto su piattaforma e-learning, attraverso pillole registrate/ricorsive e simulazioni di attacco etc. (il piano verrà proposto e concordato con CMVE).

- ***Acquisizione ed implementazione/sviluppo di sistemi e tecnologie a supporto dei processi di miglioramento dell'organizzazione:*** A seguito di un'attenta analisi dei requisiti tecnici e procedurali derivanti dall'analisi della postura di sicurezza dal punto di vista di Risposta e ripristino, Venis individuerà le soluzioni e gli strumenti da integrare nell'infrastruttura al fine di consentire una più efficace azione di risposta agli incidenti di natura cyber, quali a titolo esemplificativo IPS/IDS, Sistemi di e Piattaforme di Threat Intelligence. Le soluzioni individuare saranno sottoposte a validazione da parte di Città Metropolitana.

## 2.4 Intervento 4 – Gestione delle identità digitali e degli accessi logici

L'intervento si pone come obiettivo generale quello di potenziare la sicurezza delle modalità di accesso agli strumenti e dotazioni aziendali normando e rendendo più sicuro l'accesso agli stessi dall'esterno.

Per il raggiungimento dell'obiettivo Venis prevede:

- **Acquisizione ed implementazione/sviluppo di sistemi e tecnologie a supporto dei processi di miglioramento dell'organizzazione**: Al fine di consentire il rafforzamento delle misure di sicurezza in relazione al controllo Accessi, Venis prevede l'acquisizione, l'installazione e il supporto alla configurazione di un software specifico per la sicurezza (es. "SECURITY E3" di Office365 già segnalato come fabbisogno da Città Metropolitana). Inoltre, l'intervento mira a normare e regolare gli accessi anche in relazione alla rete Wi-fi tramite l'analisi e valutazione di strumenti per il controllo degli accessi e la sicurezza delle reti, quali a titolo esemplificativo ClearPass.
- **Formazione sull'utilizzo di sistemi di gestione delle identità digitali e degli accessi logici**: In relazione alle nuove tecnologie che saranno adottate ed introdotte dall'Ente, Venis prevede un percorso di affiancamento formativo per il personale addetto alla configurazione (IT) per consentire loro il corretto utilizzo dello strumento e la corretta implementazione delle principali funzionalità delle soluzioni acquisite.

Venis S.p.A.
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
protocollo@pec.venis.it - venis@venis.it - www.venis.it

## 2.5 Intervento 5 – Sicurezza delle applicazioni, dei dati e delle reti

L'intervento proposto si pone come obiettivo generale quello di assicurare la sicurezza delle applicazioni, dei dati e della rete e di identificare le minacce, esistenti o potenziali, al sistema informatico dell'Ente.

Per consentire il raggiungimento dell'obiettivo generale Venis prevede la realizzazione delle seguenti attività:

- **Security Posture and Security Scoring: attività di analisi delle criticità uomo/macchina –** L'attività prevede un Assessment tecnologico composto da tre macro tipologie di test dell'infrastruttura tecnologica e delle terze parti che interagiscono con essa:
    - ***Vulnerability Assessment***, Deep Information Gathering, Enumeration e Vulnerability Scan. Vengono effettuate delle scansioni di vulnerabilità con degli strumenti automatizzati e tracciata manualmente una lista prioritaria delle minacce esistenti su scoring CVE. L'Attività include la raccolta di informazioni su malware, exploit, vulnerabilità e attacchi informatici attivi e potenziali in riferimento al perimetro oggetto di analisi;
    - ***Penetration Testing***, attività mirata a testare la sicurezza di un sistema, una rete o un'applicazione attraverso simulazioni di attacchi reali, durante il quale si cerca di sfruttare vulnerabilità individuate per valutarne l'effettivo impatto sull'organizzazione.
    - ***Deep Scanning sul Dark & Deep Web***: Attività di ***OSINT (Open Source Intelligence)*** al fine di definire reputation, sentiment, data leaking e shadow IT dei principali fornitori dell'Ente. Tale attività consente di valutare la postura di sicurezza delle terze parti e di individuare in maniera tempestiva potenziali vulnerabilità e minacce alla Città Metropolitana di Venezia.
- **Acquisizione ed implementazione/sviluppo di sistemi e tecnologie** a supporto del potenziamento dei sistemi per la mitigazione rischio cyber; Venis prevede un processo di selezione e acquisizione di nuove tecnologie volte a proteggere il patrimonio informativo e le risorse dell'Ente. La valutazione dei sistemi per la protezione delle applicazioni, dei dati e della rete porterà allo Scouting e Benchmarking di nuovi strumenti e tecnologie (ad es. Sistemi di Vulnerability Management o Piattaforme di monitoraggio), che verranno sottoposti a validazione a Città Metropolitana.

### 2.5.1 Altre Amministrazioni locali coinvolte nel progetto

In relazione all'esigenza dell'Ente di analizzare, adeguare e mettere in sicurezza eventuali applicativi Business Critical presenti all'interno del SAD – Soggetto Aggregatore Digitale, Venis prevede i seguenti interventi:

- **Enumeration delle applicazioni presenti in SAD e Mappatura delle applicazioni Business Critical:** estrazione del nome delle applicazioni, della tipologia e dei servizi erogati. Attraverso questa prima fase di analisi sarà possibile raccogliere informazioni sugli applicativi che rientrano nel perimetro SAD. Dopo aver enumerato suddetti applicativi, sarà condotta un'analisi mirata all'individuazione delle applicazioni business critical per l'Amministrazione al fine di identificare le applicazioni target che saranno oggetto di test nella fase successiva.

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

- **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical**: Le attività di test saranno condotte sugli applicativi target su identificati per ciascuna delle Amministrazioni locali coinvolte nel progetto, ritenuti ad alta criticità per l'Amministrazione stessa e per il servizio erogato ai cittadini.
- **Piano di Remediation e relative attività di mitigazione:** A seguito di ciascun test, oltre alle evidenze raccolte, sarà rilasciato un Piano di Remediation contenente le attività di mitigazione proposte e i consigli di implementazione, pensati per la risoluzione delle vulnerabilità e/o mitigazione delle criticità riscontrati nel corso dell'attività.

Gli interventi su indicati, verranno eseguiti sugli applicativi presenti nel SAD delle seguenti 10 amministrazioni che Città Metropolitana ha coinvolto in fase di candidatura del progetto:

1. Comune di Mirano;
2. Comune di Jesolo:
3. Comune di Scorzè;
4. Comune di Santa Maria di Sala;
5. Comune di Noale;
6. Comune di Caorle;
7. Comune di Concordia Sagittaria;
8. Comune di Fossalta di Piave;
9. Comune di Gruaro;
10. Comune di Teglio Veneto.

**Le suddette Amministrazioni dovranno essere attivamente coinvolte da Città Metropolitana di Venezia, per la condivisione delle informazioni utili alla conduzione delle attività di enumeration e per l'ottenimento delle necessarie autorizzazioni allo svolgimento delle attività di Vulnerability Assessment/Penetration Test da parte di Venis.**
**Le eventuali attività di mitigazione derivanti dal Piano di Remediation, che verrà prodotto da Venis per ogni Amministrazione, saranno a carico degli amministratori di sistema delle rispettive Amministrazioni coinvolte.**

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

# 3 Piano progettuale di dettaglio

Si riporta di seguito la struttura di progetto, articolata in Interventi, Tipologia di interventi, Attività in coerenza con le milestone e i target (M&T) fissati con il progetto.

Si precisa che, on top, è prevista da parte di Venis **un'attività trasversale di coordinamento e governance di progetto** rafforzativa rispetto a quella dell'Ente.

## 3.1 Intervento 1 – Governance e programmazione cyber

Le tipologie di intervento e le relative attività previste per la realizzazione dell'intervento sono le seguenti:

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento
   1A – Security Strategy AS-IS

B. Miglioramento dei processi e dell'organizzazione
   1B – Security Strategy Plan

C. Formazione e miglioramento della consapevolezza delle persone
   1C – Formazione Cyber

D. Progettazione e sviluppo di nuovi sistemi e tecnologie
   1D – Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo

## 3.2 Intervento 2 – Gestione del rischio cyber e della continuità operativa

Le tipologie di intervento e le relative attività previste per la realizzazione dell'intervento sono le seguenti:

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento
   2A – Analisi dei rischi cyber

D. Progettazione e sviluppo di nuovi sistemi e tecnologie

   2D – Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo

## 3.3 Intervento 3 – Gestione e risposta agli incidenti di sicurezza

Le tipologie di intervento e le relative attività previste per la realizzazione dell'intervento sono le seguenti:

B. Miglioramento dei processi e dell'organizzazione

   3B – Definizione di un processo di gestione degli incidenti (Supporto specialistico, Sviluppo di Playbook)

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

C. Formazione e miglioramento della consapevolezza delle persone

3C – Formazione sulle tecniche di hacking

D. Progettazione e sviluppo di nuovi sistemi e tecnologie

3D – Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo

## 3.4 Intervento 4 – Gestione delle identità digitali e degli accessi logici

Le tipologie di intervento e le relative attività previste per la realizzazione dell'intervento sono le seguenti:

C. Formazione e miglioramento della consapevolezza delle persone

4C – Formazione sull'utilizzo di sistemi di gestione delle identità digitali e degli accessi logici

D. Progettazione e sviluppo di nuovi sistemi e tecnologie

4D – Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo

## 3.5 Intervento 5 – Sicurezza delle applicazioni, dei dati e delle reti

Le tipologie di intervento e le relative attività previste per la realizzazione dell'intervento sono le seguenti:

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

5A – Security Posture and Security Scoring: attività di analisi delle criticità uomo/macchina. Il perimetro viene analizzato

D. Progettazione e sviluppo di nuovi sistemi e tecnologie

5D – Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo

venezia informatica e sistemi

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

# 4 Articolazione temporale del Progetto

Le attività proposte avranno avvio a partire dalla data di affidamento a Venis da parte di Città Metropolitana di Venezia e si concluderanno **entro il 31 ottobre 2025;** in coerenza con la data di fine progetto fissata dall'Avviso n. 08 al **31 dicembre 2025** (salvo proroghe eventualmente concesse), proseguiranno le sole attività di supporto all'Ente per la finalizzazione della rendicontazione.

Di seguito si riporta la pianificazione delle attività proposte su base trimestrale:

| ID Intervento | Intervento | ID Tipologia Intervento | Tipologia Intervento | ID Attività | Attività | 2024 | | | | 2025 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 |
| | | | | 0 | Coordinamento e governance di progetto | | | | | | | | |
| 1 | Governance e programmazione cyber | A | Analisi della postura di sicurezza e definizione di un piano di potenziamento | 1A | Security Strategy AS-IS (NIST Maturity Assessment, Gap Analysis, GDPR Compliace) | | | | | | | | |
| | | B | Miglioramento dei processi e dell'organizzazione | 1B | Security Strategy Plan | | | | | | | | |
| | | C | Formazione e miglioramento della consapevolezza delle persone | 1C | Formazione Cyber (Definizione della Cyber Situational Awareness e analisi del fabbisogno formativo, Predisposizione del materiale didattico ed erogazione di security training al personale selezionato, Simulazione di una campagna di phishing) | | | | | | | | |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 1D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | | | | | | | | |
| 2 | Gestione del rischio cyber e della continuità operativa | A | Analisi della postura di sicurezza e definizione di un piano di potenziamento | 2A | Analisi dei rischi cyber | | | | | | | | |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 2D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | | | | | | | | |
| 3 | Gestione e risposta agli incidenti di sicurezza | B | Miglioramento dei processi e dell'organizzazione | 3B | Definizione di un processo di gestione degli incidenti (Supporto specialistico, Sviluppo di Playbook) | | | | | | | | |
| | | C | Formazione e miglioramento della consapevolezza delle persone | 3C | Formazione sulle tecniche di hacking | | | | | | | | |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 3D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | | | | | | | | |
| 4 | Gestione delle identità digitali e degli accessi logici | C | Formazione e miglioramento della consapevolezza delle persone | 4C | Formazione sull'utilizzo di sistemi di gestione delle identità digitali e degli accessi logici | | | | | | | | |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 4D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | | | | | | | | |
| 5 | Sicurezza delle applicazioni, dei dati e delle reti | A | Analisi della postura di sicurezza e definizione di un piano di potenziamento | 5A | Security Posture and Security Scoring: attività di analisi delle criticità uomo/macchina. Il perimetro viene analizzato (Vulnerability Assessment, Penetration Testing, Deep Scanning sul Dark & Deep Web) | | | | | | | | |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 5D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | | | | | | | | |

Si precisa che il progetto risulta avviato nel Q1 2024 da parte di Città Metropolitana con l'attività 5D. Le attività proposte da Venis si prevede verranno avviate a partire dal Q4 2024.

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

# 5 Costi del progetto

La tabella seguente illustra sinteticamente il quadro economico di partenza per la formulazione della proposta tecnico-economica di Venis.

Rispetto al totale di progetto finanziato, sono stati evidenziati i costi già affidati da Città Metropolitana e di progressiva maturazione (spese generali strettamente correlate all'attività del soggetto Attuatore CMVE e servizi di protezione "Hornet" aggiudicati con determinazione n. 1905/2024).

| QUADRO ECONOMICO DEL PROGETTO | Costo Imponibile | Costo IVA Incl. |
|---|---|---|
| **TOTALE PROGETTO FINANZIATO (a)** | 1.229.508,20 € | 1.500.000,00 € |
| **SPESE GENERALI CMVE (valorizzazione MAX 7% dei costi diretti ammissibili) (b)** | 80.435,11 € | 98.130,84 € |
| **COSTI DI ACQUISTO SERVIZI DI PROTEZIONE HORNET (Determinazione CMVE N. 1905 /2024, valorizzazione del totale acquisto) (c)** | 76.986,00 € | 93.922,92 € |
| **TOTALE DA AFFIDARE IN ESECUZIONE (a-b-c)** | **1.072.087,08 €** | **1.307.946,24 €** |

venezia informatica e sistemi

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

Tenuto conto di quanto sopra e del raggiungimento delle Milestone e dei Target stabiliti nel progetto, si riporta nella tabella seguente il dettaglio della proposta Venis evidenziando i costi di progetto suddivisi per Intervento, Tipologia di intervento, Attività e Tipologia di costo.

| ID Intervento | Intervento | ID Tipologia intevento | Tipoligia intervento | ID Attività | Attività | Tipologia di costo | Costo Imponibile | IVA | Costo IVA Incl. | Totale Costi IVA Incl. per Intervento |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Governance e programmazione cyber | A | Analisi della postura di sicurezza e definizione di un piano di potenziamento | 1A | Security Strategy AS-IS (NIST Maturity Assessment, Gap Analysis, GDPR Compliace) | *Servizi professionali* | 98.360,66 € | 21.639,34 € | 120.000,00 € | **486.869,16 €** |
| | | B | Miglioramento dei processi e dell'organizzazione | 1B | Security Strategy Plan | *Servizi professionali* | 81.967,21 € | 18.032,79 € | 100.000,00 € | |
| | | C | Formazione e miglioramento della consapevolezza delle persone | 1C | Formazione Cyber (Definizione della Cyber Situational Awareness e analisi del fabbisogno formativo, Predisposizione del materiale didattico ed erogazione di security training al personale selezionato, Simulazione di una campagna di phishing) | *Servizi professionali* | 99.892,75 € | 21.976,41 € | 121.869,16 € | |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 1D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | *Servizi professionali e acquisto di sistemi e tecnologie* | 118.852,46 € | 26.147,54 € | 145.000,00 € | |
| 2 | Gestione del rischio cyber e della continuità operativa | A | Analisi della postura di sicurezza e definizione di un piano di potenziamento | 2A | Analisi dei rischi cyber | *Servizi professionali* | 40.983,61 € | 9.016,39 € | 50.000,00 € | **195.000,00 €** |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 2D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | *Servizi professionali e acquisto di sistemi e tecnologie* | 118.852,46 € | 26.147,54 € | 145.000,00 € | |
| 3 | Gestione e risposta agli incidenti di sicurezza | B | Miglioramento dei processi e dell'organizzazione | 3B | Definizione di un processo di gestione degli incidenti (Supporto specialistico, Sviluppo di Playbook) | *Servizi professionali* | 90.163,93 € | 19.836,07 € | 110.000,00 € | **270.000,00 €** |
| | | C | Formazione e miglioramento della consapevolezza delle persone | 3C | Formazione sulle tecniche di hacking | *Servizi professionali* | 12.295,08 € | 2.704,92 € | 15.000,00 € | |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 3D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | *Servizi professionali e acquisto di sistemi e tecnologie* | 118.852,46 € | 26.147,54 € | 145.000,00 € | |
| 4 | Gestione delle identità digitali e degli accessi logici | C | Formazione e miglioramento della consapevolezza delle persone | 4C | Formazione sull'utilizzo di sistemi di gestione delle identità digitali e degli accessi logici | *Servizi professionali* | 24.590,16 € | 5.409,84 € | 30.000,00 € | **175.000,00 €** |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 4D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | *Servizi professionali e acquisto di sistemi e tecnologie* | 118.852,46 € | 26.147,54 € | 145.000,00 € | |
| 5 | Sicurezza delle applicazioni, dei dati e delle reti | A | Analisi della postura di sicurezza e definizione di un piano di potenziamento | 5A | Security Posture and Security Scoring: attività di analisi delle criticità uomo/macchina. Il perimetro viene analizzato (Vulnerability Assessment, Penetration Testing, Deep Scanning sul Dark & Deep Web) | *Servizi professionali* | 106.557,38 € | 23.442,62 € | 130.000,00 € | **181.077,08 €** |
| | | D | Progettazione e sviluppo di nuovi sistemi e tecnologie | 5D | Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo (Analisi dei requisiti tecnici e procedurali, Scouting e Benchmarking, Prioritizzazione degli acquisti per aree di emergenza, Selezione delle soluzioni, Acquisto delle soluzioni selezionate) | *Servizi professionali e acquisto di sistemi e tecnologie* | 41.866,46 € | 9.210,62 € | 51.077,08 € | |
| | | | | | | **TOTALE GENERALE** | **1.072.087,08 €** | **235.859,16 €** | **1.307.946,24 €** | **1.307.946,24 €** |
| | | | | | | ***di cui TOTALE Servizi professionali (Tipologia intervento A,B,C)*** | **554.810,78 €** | **122.058,38 €** | **676.869,16 €** | |
| | | | | | | ***di cui TOTALE Servizi professionali e acquisto di sistemi e tecnologie (Tipologia intervento D)*** | **517.276,30 €** | **113.800,78 €** | **631.077,08 €** | |

**Venis S.p.A.**
San Marco, 4934 - Palazzo Ziani - 30124 Venezia
tel. 041 2744800 fax 041 5238899
**protocollo@pec.venis.it - venis@venis.it - www.venis.it**

La presente tabella espone i costi di realizzazione imputati per ogni linea d'intervento, tenuto conto del coinvolgimento di un team di lavoro misto, composto da risorse professionali Venis e da servizi specialistici esterni da acquisire attraverso l'adesione ad Accordi Quadro Consip.

Per ogni linea d'intervento è stata, inoltre, prevista un'attività specifica di "acquisizione e implementazione di sistemi e tecnologie" (rif. Lett. D), finalizzata alle azioni di mitigazione del rischio che dovessero emergere dalla gap analysis.

L'offerta di Venis per l'esecuzione del progetto ammonta complessivamente a **euro 1.072.087,08 € iva esclusa**.

# ***CHECK LIST ANTIRICICLAGGIO***

**Check list n. 1**

**attività**

**CONTRATTI PUBBLICI (APPALTI E CONCESSIONI)**

Le Pubbliche Amministrazioni sono tenute a comunicare dati e informazioni relative a operazioni sospette, a prescindere da:

- rilevanza e importo
- operazioni rifiutate o interrotte o eseguite da altri operatori.

Il sospetto deve essere basato su una valutazione di elementi oggettivi e soggettivi acquisiti sulla base dell'istruttoria normalmente avviata.

La presente checklist fornisce un ausilio all'identificazione delle attività a forte rischio di riciclaggio in base ai seguenti **indicatori di anomalia.**

**OGGETTO: SERVIZIO DI REALIZZAZIONE PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA NELL'AMBITO DEL PNRR NEXT GENERATION EU MISSIONE 1 – COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5**

Cod. CUP: B79B21002230006 - cod. CIG: /
Compilatore ALESSANDRO BOTTOS
Dirigente Responsabile ROMANO ARMELLIN
Responsabile del Procedimento – RUP ROMANO ARMELLIN

**A - ANOMALIE DEL SOGGETTO PARTECIPANTE O AFFIDATARIO**

| INDICATORE DI ANOMALIA | | VALORE | dati rilevabili dall'istruttoria | |
|---|---|---|---|---|
| A) Residenza, sede, cittadinanza in: | A.1 Paesi terzi o zone ad alto rischio di infiltrazione criminale, economia sommersa, degrado economico-istituzionale | 1 | SI | ~~NO~~ |
| | A.2 Paesi la cui legislazione non consente di identificare i nominativi che ne detengono la proprietà e il controllo | 1 | SI | ~~NO~~ |
| | A.3 Aree di conflitto o Paesi (o zone limitrofe e di transito) che notoriamente finanziano il terrorismo | 1 | SI | ~~NO~~ |
| B) Controparti con cui opera (es: professionisti, intermediari, società, ecc..) provenienti da: | B.1 Paesi terzi o zone ad alto rischio di infiltrazione criminale, economia sommersa, degrado economico-istituzionale | 1 | SI | ~~NO~~ |
| | B.2 Paesi la cui legislazione non consente di identificare i nominativi che ne detengono la proprietà e il controllo | 1 | SI | ~~NO~~ |
| | B.3 Aree di conflitto o Paesi (o zone limitrofe e di transito) che notoriamente finanziano il terrorismo | 1 | SI | ~~NO~~ |
| C) Reticenza nel fornire: | C.1 documenti d'identità | 4 | SI | ~~NO~~ |
| | C.2 documenti o informazioni inerenti l'operazione | 4 | SI | ~~NO~~ |
| | C.3 documenti o informazioni atti a individuare l'effettivo beneficiario dell'operazione | 4 | SI | ~~NO~~ |
| D) Scarsa conoscenza dell'operazione che richiede in merito a: | D.1 natura | 4 | SI | ~~NO~~ |
| | D.2 oggetto | 2 | SI | ~~NO~~ |
| | D.3 ammontare | 2 | SI | ~~NO~~ |
| | D.4 scopo | 4 | SI | ~~NO~~ |

| | | | | |
|---|---|---|---|---|
| E) Documentazione che sembra falsa o dubbia: | E.1 con elementi difformi o forti elementi di criticità o dubbio | 5 | SI | ~~NO~~ |
| | E.2 attesta esistenza di cospicue disponibilità economiche o finanziarie in Paesi ad alto rischio | 2 | SI | ~~NO~~ |
| | E.3 attesta garanzie reali o personali rilasciate da soggetti con residenza, cittadinanza o sede o relativi a beni ubicati in Paesi terzi ad alto rischio | 2 | SI | ~~NO~~ |
| F) Indirizzo o domiciliazione fiscale anomali: | F.1utilizzato da più soggetti legati fra loro che operano in attività non coerenti con l'operazione richiesta | 3 | SI | ~~NO~~ |
| | F.2 diversi dal domicilio, dalla residenza o dalla sede che sembrano domiciliazioni di comodo | 4 | SI | ~~NO~~ |
| G) Collegamenti con organizzazioni no profit o non governative con: | G.1 connessioni nell'indirizzo, dei rappresentanti o del personale, non giustificate | 2 | SI | ~~NO~~ |
| | G.2 titolarità di rapporti riconducibili a nominativi ricorrenti | 4 | SI | ~~NO~~ |
| H) Ripetute domande di partecipazione | H.1 nonostante società in perdita o in forte difficoltà finanziaria, ma senza aver operato modifiche agli assetti gestionali e operatività | 5 | SI | ~~NO~~ |
| I) Sembra agire per conto di altri: | I.1accompagnato da altri soggetti non direttamente coinvolti, ma molto interessati all'operazione | 4 | SI | ~~NO~~ |
| | I.2 privo di necessarie disponibilità economiche o patrimoniali | 3 | SI | ~~NO~~ |
| | I.3 PEC o email di un soggetto diverso da chi ha presentato la richiesta | 2 | SI | ~~NO~~ |
| | I.4 rilascio di deleghe o procure per evitare contatti diretti, frequente ed inconsueto | 1 | SI | ~~NO~~ |
| L) Assetti societari anomali: | L.1 caratterizzati da presenza di trust, fiduciarie, fondazioni, international business company | 2 | SI | ~~NO~~ |
| | L.2 con ripetute e/o improvvise modifiche dell'assetto proprietario, manageriale o di controllo dell'impresa | 3 | SI | ~~NO~~ |
| | L.3 costituita di recente,<br>- con intensa operatività finanziaria, ma poi cessata improvvisamente l'attività<br>- controllata o amministrata da soggetti prestanomi. | 5 | SI | ~~NO~~ |

| | | | | |
|---|---|---|---|---|
| M) Mancanza di requisiti per partecipare con: | M.1 rilevanti mezzi finanziari privati anche di incerta provenienza o non compatibili con il profilo economico patrimoniale dell'impresa | 4 | SI | ~~NO~~ |
| | M.2 forte disponibilità di anticipazione finanziarie e garanzie prive di idonea giustificazione | 4 | SI | ~~NO~~ |
| N) Contiguità o operatività o rapporti finanziari rilevanti o connessione a imprese, fondazioni, associazioni, organizzazioni no profit o non governative con soci o amministratori | N.1 persone sottoposte a procedimenti penali e/o misure di prevenzione patrimoniale | 5 | SI | ~~NO~~ |
| | N.2 persone sottoposte ad altri provvedimenti di sequestro | 5 | SI | ~~NO~~ |
| | N.3 soggetti o enti coinvolti nel finanziamento del terrorismo o vicini ad ambienti radicalizzati | 5 | SI | ~~NO~~ |
| | N.4 persone che rivestono importanti cariche pubbliche | 2 | SI | ~~NO~~ |
| | N.5 persone con importanti cariche pubbliche e improvvisamente registra un notevole aumento di fatturato | 4 | SI | ~~NO~~ |
| O) Avvalimento plurimo o frazionato con: | O.1 concorrente che non dimostra effettiva disponibilità dei mezzi facenti capo all'impresa avvalsa e necessari all'esecuzione dell'appalto | 3 | SI | ~~NO~~ |
| | O.2 eccessiva onerosità o irragionevolezza dell'avvalimento desunti dal contratto stesso o da altri elementi assunti nel corso del procedimento | 4 | SI | ~~NO~~ |
| | TOTALE | 0 | | |

| 0-30 ↓ | 31-90 ↓ | 91-118 ↓ |
|---|---|---|
| NON SEGNALARE | AVVIO ALLA SEGNALAZIONE | |

| B- ANOMALIE DELL'APPALTO | | | | |
|---|---|---|---|---|
| INDICATORE DI ANOMALIA | | VALORE | dati rilevabili dall'istruttoria | |
| A) la procedura di gara è indetta come: | A.1 affidamento diretto sotto soglia tra l'80 % e il 100% del limite di valore previsto (ad es. tra €112.000 e €140.000) | 1 | SI | ~~NO~~ |
| | A.2 Affidamento successivo a gara deserta | 2 | SI | ~~NO~~ |
| | A.3 offerta economicamente più vantaggiosa | 2 | SI | ~~NO~~ |
| | A.4 gara con un'unica offerta valida | 2 | SI | ~~NO~~ |
| | A.5 procedura negoziata con invito di meno di cinque operatori economici | 3 | SI | ~~NO~~ |
| B) Presentazione di un'unica offerta nell'ambito di procedure di gara con: | B.1 aggiudicazione al prezzo più basso | 1 | SI | ~~NO~~ |
| | B.2 offerta anormalmente bassa | 1 | SI | ~~NO~~ |
| | B.3 contratto caratterizzato da complessità elevata | 1 | SI | ~~NO~~ |
| C) Offerta con ribasso elevato in gare al prezzo più basso con: | C.1 contratto caratterizzato da complessità elevata | 2 | SI | ~~NO~~ |
| | C.2 appalto con caratteristiche di ripetitività | 2 | SI | ~~NO~~ |
| D) Soggetti estranei molto interessati o che sollecitano l'operazione: | D.1 PEP (Persone Politicamente Esposte) | 2 | SI | ~~NO~~ |
| E) Numero di partecipanti al raggruppamento temporaneo sproporzionato: | E.1 rispetto al valore economico e prestazioni oggetto del contratto | 2 | SI | ~~NO~~ |
| | E.2 partecipante singolo a suo volta raggruppato o consorziato | 2 | SI | ~~NO~~ |
| F) Disponibilità economiche sospette senza plausibili giustificazioni | F.1 sproporzionate rispetto al profilo economico patrimoniale del partecipante | 2 | SI | ~~NO~~ |
| | F.2 operazioni di importo ingente effettuate da società costituite di recente o con oggetto sociale generico o incompatibile con l'attività del soggetto richiedente | 1 | SI | ~~NO~~ |
| | F.3 garanzie personali da parte di soggetti che sembrano operare in via professionale senza essere autorizzati a prestare garanzie | 4 | SI | ~~NO~~ |
| | F.4 copertura dell'esposizione del soggetto, con pagamento effettuato in un'unica soluzione invece che rateizzato come concordato, effettuata con intervento di un terzo | 2 | SI | ~~NO~~ |
| G) Assenza di convenienza economica all'esecuzione del contratto per: | G.1 dimensione aziendale | 2 | SI | ~~NO~~ |
| | G.2 località di svolgimento della prestazione distante dalla residenza, domicilio o sede del soggetto | 2 | SI | ~~NO~~ |
| | G.3 assenza di legami con il luogo in cui si svolge l'attività (residenza, sede) | 1 | SI | ~~NO~~ |
| | G.4 presuppone modifica delle condizioni o modalità di svolgimento dell'attività, con ulteriori oneri a carico del richiedente | 2 | SI | ~~NO~~ |
| | G.5 acquisto o vendita di beni o servizi di valore a prezzi palesemente sproporzionati rispetto al mercato o alla loro stima | 2 | SI | ~~NO~~ |
| | G.6 ripetuto ricorso a contratti a favore di terzo, per persona da nominare o a intestazioni fiduciarie, specie se aventi oggetto diritti su immobili o partecipazioni societarie | 3 | SI | ~~NO~~ |

| | | | | |
|---|---|---|---|---|
| H) Sponsorizzazione tecnica con: | H.1 utilità e/o valore complessivo indeterminato o difficilmente determinabile | 3 | SI | ~~NO~~ |
| | H.2 individuazione da parte dello sponsor di uno o più soggetti esecutori, che magari coincidono con raggruppamenti numerosi o costituiti da singoli a loro volta raggruppati o consorziati e privi dei requisiti di qualificazione per la progettazione e l'esecuzione | 4 | SI | ~~NO~~ |
| I) Sponsorizzazione eseguita con ricorso a subappalti | I.1 oltre i limiti imposti per i contratti pubblici | 4 | SI | ~~NO~~ |
| | I.2 mediante ripetuto ricorso a sub affidamenti | 2 | SI | ~~NO~~ |
| | I.3 con reiterata violazione degli obblighi contrattuali e delle prescrizioni impartite in ordine alla progettazione, direzione ed esecuzione | 5 | SI | ~~NO~~ |
| L) Concessione o finanza di progetto che, con anticipazioni finanziarie fatte dal concessionario o promotore: | L.1 per importo superiore alle norme comunitarie | 2 | SI | ~~NO~~ |
| | L.2 con termine di realizzazione superiore a 4 anni | 1 | SI | ~~NO~~ |
| M) l'aggiudicatario dell'appalto è figura ricorrente negli ultimi tre anni | M.1 se in procedura aperta | 1 | SI | ~~NO~~ |
| | M.2 se in affidamento diretto o procedura negoziata | 3 | ~~SI~~ | NO |
| | TOTALE | 3 | | |

| 0-19 ↓ | 20-35 ↓ | 36-55 ↓ |
|---|---|---|
| NON SEGNALARE | AVVIO ALLA SEGNALAZIONE | |

Data compilazione

14/11/2024

ROMANO ARMELLIN

# CITTÀ METROPOLITANA DI VENEZIA

***AREA ECONOMICO FINANZIARIA***

***VISTO DI REGOLARITA' CONTABILE ATTESTANTE LA COPERTURA FINANZIARIA***

***OGGETTO: DETERMINAZIONE A CONTRATTARE PER L'ACQUISIZIONE, MEDIANTE AFFIDAMENTO DIRETTO IN HOUSE, DEL SERVIZIO DI REALIZZAZIONE PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA NELL'AMBITO DEL PNRR NEXT GENERATION EU MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5 CUP B79B21002230006.***

*Ai sensi e per gli effetti dell'art. 151, comma 4, del T.U. delle leggi sull'ordinamento degli enti locali, D.Lgs 267/2000, si attesta la copertura finanziaria relativamente alla determinazione.*

| ANNO | MOVIMENTO | CAPITOLO | DESCRIZIONE | IMPORTO |
|---|---|---|---|---|
| 2025 | Sub-Impegno 72 Impegno 2025/280 | 201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | 80% INCENTIVI PERSONALE TECNICO CONTRATTO HORNET COMMI 6 e 7 ART. 45 D.LGS 36/2023 | €1.231,78 |

| | | | | |
|---|---|---|---|---|
| 2025 | Sub-Impegno 70 Impegno 2025/280 | 201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | AFFIDAMENTO DIRETTO IN HOUSE, DEL SERVIZIO DI REALIZZAZIONE PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA NELL'AMBITO DEL PNRR NEXT GENERATION EU MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5 CUP B79B21002230006 | €1.307.946,24 |
| 2025 | Sub-Impegno 71 Impegno 2025/280 | 201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | SECONDA ANNUALITA' CONTRATTO HORNET | €31.307,64 |
| 2024 | Sub-Impegno 684 Impegno 2024/1661 | 201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | contributo ANAC_esecuzione progetto Cybermet - Cybersecurity metropolitana - | €600,00 |
| 2024 | Var. Accertamento 27060 | 420000101326/0 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | ECONOMIA ACCERTAMENTO CORRELATA ALLA CORRISPONDENTE SPESA | -€30.707,64 |
| 2024 | Var. Accertamento 27060 | 420000101326/0 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | VARIAZIONE ESIGIBILITA' AL 2025 | -€1.468.692,36 |

| | | | | |
|---|---|---|---|---|
| 2024 | Var. Bilancio 26194 | 201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | MIN. ENTR. E MIN SPE. | -€1.468.692,36 |
| 2024 | Var. Bilancio 26193 | 420000101326/0 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | MIN. ENTR. E MIN SPE. | -€1.468.692,36 |
| 2024 | Var. Bilancio 26192 | 201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | MIN. ENTR. E MIN SPE. | -€30.707,64 |
| 2024 | Var. Bilancio 26191 | 420000101326/0 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | MIN. ENTR. E MIN SPE. | -€30.707,64 |
| 2025 | Var. Bilancio 26190 | 201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | VARIAZIONE ESIGIBILITA' | €1.468.692,36 |
| 2025 | Var. Bilancio 26189 | 420000101326/0 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | VARIAZIONE ESIGIBILITA' | €1.468.692,36 |

| | | | | |
|---|---|---|---|---|
| 2024 | Var. Impegno 1661 | 201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | ECONOMIA DI SPESA CORRELATA ALLA RISPETTIVA ENTRATA | -€30.707,64 |
| 2024 | Var. Impegno 1661 | 201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006 | VARIAZIONE ESIGIBILITA' SPESA | -€1.468.692,36 |

IL DIRIGENTE
ARMELLIN ROMANO

atto firmato digitalmente

# CITTÀ METROPOLITANA DI VENEZIA

## DICHIARAZIONE DEL RESPONSABILE DEL PROCEDIMENTO

Proposta n. 6643/2024

Oggetto: **DETERMINAZIONE A CONTRATTARE PER L'ACQUISIZIONE, MEDIANTE AFFIDAMENTO DIRETTO IN HOUSE, DEL SERVIZIO DI REALIZZAZIONE PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA NELL'AMBITO DEL PNRR NEXT GENERATION EU MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5 CUP B79B21002230006.**

Il R.U.P./responsabile di procedimento dichiara che il presente schema di provvedimento è conforme alle risultanze istruttorie, attestandone il giusto procedimento

IL DIRIGENTE
ARMELLIN ROMANO

atto firmato digitalmente