CITTÀ METROPOLITANA DI VENEZIA

AREA AMMINISTRAZIONE E TRANSIZIONE DIGITALE

Servizio infrastrutture digitali e SITM

Determinazione N. 3005 / 2024
Responsabile del procedimento: ARMELLIN ROMANO

Oggetto: **APPROVAZIONE DEL PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA ED ATTO D'OBBLIGO AI SENSI DELL'ART. 12 LEGGE 241/90, NELL'AMBITO DEL PNRR NEXT GENERATION EU MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5 CUP B79B21002230006 NO CIG.**

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 stato delegato alla sottoscrizione di tutti gli atti previsti dalla partecipazione al progetto e specificamente alla stipula dell’apposito atto

d’obbligo di accettazione finanziamento concesso dall’Agenzia per la Cybersicurezza Nazionale;

visti inoltre:

i la legge 7 agosto 1990, n. 241, recante “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”, e, in particolare, l’articolo 12, secondo cui la concessione di sovvenzioni, contributi, sussidi ed ausili finanziari e l’attribuzione di vantaggi economici di qualunque genere a persone ed Enti pubblici e privati sono subordinate alla predeterminazione da parte delle Amministrazioni procedenti, nelle forme previste dai rispettivi ordinamenti, dei criteri e delle modalità cui le amministrazioni stesse devono attenersi;

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

iii 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;

iv 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”;

v 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;

vi 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”;

vii 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»)”;

viii 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”;

ix 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”;

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

xi 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;

xii 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";

xiii 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;

xiv 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;

xv 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;

xvi 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;

xvii 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;

xviii 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";

xix 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");

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

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

xxii 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;

xxiii 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”;

xxiv 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”;

xxv 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”;

xxvi 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;

xxvii 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”;

xxviii 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”;

xxix 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”;

xxx 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”;

xxxi 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”;

xxxii 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”;

xxxiii 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”;

xxxiv 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)";

xxxv 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";

xxxvi 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";

xxxvii la circolare del Ministero dell'economia e delle finanze, Dipartimento della Ragioneria generale dello Stato, Servizio Centrale per il PNRR, del giorno 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";

xxxviii 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";

xxxix 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";

xl 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;

xli 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;

xlii 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";

xliii 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;

xliv 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";

xlv 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, mediante lo stanziamento complessivo di € 623.000.000,00;

ii la Misura citata prevede il conseguimento del seguente obiettivo:
- Codice identificativo M1C1-19 “Supporto all’aggiornamento delle misure di sicurezza – 50 strutture di sicurezza adeguate entro dicembre 2024”;

iii il citato accordo tra l’Agenzia per la Cybersicurezza Nazionale e il Dipartimento per la Transizione Digitale DTD del 14 dicembre 2021, prot. ACN n. 896 del 15 dicembre 2021;

iv con Determinazione n. 5959 del 26 febbraio 2024 ACN ha approvato l’avviso pubblico n. 8/2024 finanziato dall’Unione Europea – Next Generation EU recante: “Avviso pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell’ambiente a valere sul piano nazionale di ripresa e resilienza, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity”, riservando una dotazione finanziaria di € 50.000.000,00, aumentata di ulteriori € 50.000.000,00 con propria determinazione prot. 30550 del 23 settembre 2024, successivamente rettificata con determinazione prot. 33707 del 17 dicembre 2024;

v la Città metropolitana di Venezia è compresa tra le PA locali destinatarie dei fondi, quale soggetto attuatore dell’Intervento per la Misura in questione ed ha avviato le adeguate operatività tecniche ed amministrative per la presentazione, entro i termini indicati da ACN del 25 marzo 2024 poi procrastinati al 12 aprile 2024, della domanda di partecipazione, candidando il progetto denominato “CYBERMET - Cybersecurity Metropolitana”, allegato alla presente determinazione, e finalizzato al potenziamento della resilienza cyber dell’Ente;

considerato altresì:

i in data 10 aprile 2024 la Città metropolitana di Venezia ha spedito la domanda di ammissione all’avviso 8/2024 corredata del progetto “CYBERMET – Cybersecurity Metropolitana” riferito ai seguenti interventi di realizzazione:
   a. governance e programmazione cyber;
   b. gestione del rischio cyber e della continuità operativa;
   c. gestione e risposta agli incidenti di sicurezza;
   d. gestione delle identità digitali e degli accessi logici;
   e. sicurezza delle applicazioni, dei dati e delle reti;

ii l’Agenzia per la Cybersicurezza Nazionale con proprio prot. 22731 del giorno 11 luglio 2024 ha comunicato l’ammissione della domanda di partecipazione del progetto CYBERMET disposta con propria determinazione prot. n. 22329 del 9 luglio 2024;

iii appena avuta conoscenza dell’Avviso 8/2024 ed ai sensi del suo paragrafo 4 secondo cui “il progetto si intende avviato anche qualora siano state poste in essere attività propedeutiche all’avvio operativo delle attività,” con determinazione n. 843 del 28 marzo 2024 Città Metropolitana ha determinato di contrarre per l’acquisizione, mediante MePA, del servizio di protezione spam, malware e backup posta elettronica, in riferimento al Progetto CYBERMET -

Cybersecurity Metropolitana – PNRR Next Generation EU Missione 1 - Componente 1 - Investimento 1.5 “Cybersecurity” M1C1I1.5 CUP B79B21002230006;

iv tale servizio, aggiudicato con determinazione n. 1905 del 12 luglio 2024 a seguito di RDO n. 4445364 del 21 giugno 2024 alla ditta Chip Space S.r.l. di Marcon (VE) p. IVA 02179570276 per l’importo di € 93.922,92 IVA inclusa è da considerare quale intervento “in essere”, ai sensi del par. 1.2 dell’Avviso 8/2024, in quanto avviato prima della domanda di ammissione a finanziamento, inviata ad ACN con prot. 23468 del 10 aprile 2024;

v a seguito della valutazione proposte da parte della Commissione contestualmente all’uopo nominata, l’Agenzia per la Cybersicurezza Nazionale in data 23 settembre 2024, tramite la già citata determinazione prot. n. 30550/2024, ha ammesso la proposta progettuale CYBERMET al totale finanziamento di € 1.500.000,00;

dato atto:

i in conseguenza del positivo esito dell’adesione all’Avviso n. 8/2024, comunicato da ACN con propria nota del 25 settembre 2024, nostro prot. 60572 del 26 settembre 2024, risulta necessario dare approvazione al piano operativo “CYBERMET - Cybersecurity Metropolitana” ammesso all’integrale finanziamento;

ii in esecuzione al paragrafo 7.2 dell’Avviso 8/2024 è necessario approvare, ai sensi dell’art. 12 della L. 241/1990 e sottoscrivere, per l’erogazione del contributo indicato, l’atto d’obbligo così come prodotto da ACN per la Cybersicurezza Nazionale, rilasciato in allegato all’avviso 8/2024 e dalla stessa Agenzia inviato con integrazioni in data 21 ottobre 2024, adeguato con le specifiche informazioni riferite alla Città metropolitana di Venezia ed allegato al presente provvedimento;

iii in esecuzione al paragrafo 7.2 dell’Avviso 8/2024 è necessario altresì inoltrare ad ACN, entro i termini colà previsti, l’atto d’obbligo;

iv secondo il par. 4 delle “Linee guida per i soggetti attuatori individuati tramite avvisi pubblici” comunicate da ACN in data 5 ottobre 2024, entro 10 gg dalla sottoscrizione dell’atto d’obbligo la Città metropolitana provvederà alla notifica dell’avvio delle attività afferenti al progetto, avvenuto in data 28 marzo 2024 con la citata determinazione a contrarre n. 843/2024;

v per la particolare rilevanza istituzionale e finanziaria, ai sensi dell’art. 5 della L. 241/1990, è individuato come responsabile di procedimento il sottoscritto dott. Romano Armellin, dirigente dell’Area Amministrazione e transizione digitale;

vi il dirigente firmatario del presente provvedimento e responsabile del procedimento:

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, 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;

visti gli obblighi amministrativo-contabili in capo all’ente attuatore, concernenti la gestione finanziaria del progetto, la Città metropolitana di Venezia:

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 ha 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 il presente provvedimento, procede all’accertamento 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 ha 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”;

v con il presente provvedimento, procede ad impegnare 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;

Determina

1 di approvare il piano operativo “CYBERMET – Cybersecurity Metropolitana” alla presente allegato, ammesso al totale finanziamento di € 1.500.000,00 dall’Agenzia per la Cybersicurezza Nazionale – ACN per la partecipazione al progetto PNRR Next Generation EU Missione 1 – Componente 1 - Investimento 1.5 “Cybersecurity” M1C1I1.5 CUP B79B21002230006, avente ad oggetto i seguenti interventi:
   a. governance e programmazione cyber;
   b. gestione del rischio cyber e della continuità operativa;
   c. gestione e risposta agli incidenti di sicurezza;
   d. gestione delle identità digitali e degli accessi logici;
   e. sicurezza delle applicazioni, dei dati e delle reti;
2 di approvare e sottoscrivere l’atto d’obbligo alla presente allegato, per l’erogazione, ai sensi dell’art. 12 della L. 241/1990, del contributo previsto con determinazione ACN prot. n. 30550/2024 come rettificata con determinazione ACN prot. n. 33707/2024;
3 di notificare, entro 10 gg dalla sottoscrizione dell’atto d’obbligo l’avvio in data 28 marzo 2024 delle attività afferenti al progetto, mediante apposito template fornito a corredo;
4 di nominare, ai sensi dell’art. 5 della L. 241/1990 il sottoscritto dott. Romano Armellin quale Responsabile del procedimento;
5 di accertare la somma in entrata di € 1.500.000,00 relativa alla realizzazione del progetto CYBERMET - Cybersecurity Metropolitana nell’ambito del PNRR Next Generation EU Missione 1 – Componente 1 - Investimento 1.5 “Cybersecurity” M1C1I1.5, sul capitolo n. 420000101326/0 “PNRR PROGETTO M1 C1 INVESTIMENTO 1.5 “CYBERSECURITY” INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006” della corrente annualità 2024 del bilancio 2024-2026;
6 di impegnare la somma complessiva di € 1.500.000,00 per la realizzazione del medesimo progetto PNRR, sul capitolo n. 201080205619/4 “PNRR PROGETTO M1C1 INVESTIMENTO 1.5 “CYBERSECURITY” INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006”” del vigente bilancio 2024,
7 di dare atto che, ai fini dell’articolo 9 del D.lgs. 33/2013, tutte le informazioni relative al presente provvedimento vengono pubblicate sul portale della Città metropolitana di Venezia nella sezione “Amministrazione trasparente”;
8 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

AVVISO PUBBLICO n. 08/2024

per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul

PIANO NAZIONALE DI RIPRESA E RESILIENZA,
Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"

M1C1I1.5

ALLEGATO B1 – SCHEDA DI PROGETTO

TITOLO PROGETTO: CYBERMET – Cybersecurity Metropolitana

SOGGETTO PROPONENTE: CITTÀ METROPOLITANA DI VENEZIA

Sezione 1 – ANAGRAFICA DEL SOGGETTO PROPONENTE

1.A Dati identificativi del Soggetto proponente	
Denominazione	Città metropolitana di Venezia
Codice IPA	**p_ve**
CF/P.IVA	**80008840276**
Posta elettronica certificata (PEC)	informatica.cittametropolitana.ve@pecveneto.it **/** protocollo.cittametropolitana.ve@pecveneto.it
1.B Dati identificativi del titolare del potere di impegnare il Soggetto proponente *(come riportato nell'Allegato A)*	
Nome e Cognome	Luigi Brugnaro
Qualifica	Sindaco metropolitano
Residente in (*indicare Via/Piazza, n. civico e CAP)*	Via Tarù n.2 Mogliano Veneto (TV)
Riferimenti di contatto	Mail: sindaco.metropolitano@cittametropolitana.ve.it N. Telefono: 0412501533-1506
1.C Dati identificativi del Responsabile del Progetto proposto	
Nome e Cognome	Romano Armellin
Qualifica	Dirigente Area amministrazione e transizione digitale
CF	RMLRMN72M30L736D
Nato a *(indicare il luogo e la data di nascita)*	Venezia, 30/08/1972

Residente in (*indicare Via/Piazza, n. civico e CAP)*	Via Bartolomeo Bellocchio, 5 Venezia
Riferimenti di contatto	Mail: romano.armellin@cittametropolitana.ve.it N. Telefono: 041/2501950

Sezione 2 – ANAGRAFICA DEL PROGETTO PROPOSTO

2.A Codice Unico di Progetto (CUP) *Indicare il CUP e la tipologia*	CUP: B79B21002230006 ☒ generato in coerenza con le indicazioni di cui al Template CUP "PNRR" ☐ già in possesso, in quanto progetto già avviato
2.B Costo complessivo del progetto *Indicare il costo complessivo del progetto proposto, inclusivo di eventuali ulteriori fonti finanziarie, come risultante dal CUP*	1.500.000 € (IVA incl.)
2.C Importo contributo richiesto *Indicare l'importo del contributo richiesto a valere sul presente Avviso, come risultante dalla compilazione dell'**Allegato B2***	1.500.000 € (IVA incl.)
2.D Importi derivanti da altre fonti di finanziamento *Eventuale, da compilare esclusivamente se il costo del progetto (2.B) risulta maggiore dell'importo del contributo richiesto (2.C)*	_____, fonte: _____ _____, fonte: _____ _____, fonte: _____
2.E Interventi che si intende realizzare *Indicare gli interventi che si intende realizzare nell'ambito del progetto proposto, finalizzati all'analisi e al potenziamento delle capacità di resilienza cyber in termini di postura di sicurezza, processi e modello organizzativo, competenze, sistemi e tecnologie abilitanti, come descritti nel par. 4.1 dell'Avviso*	☒ 1. Governance e programmazione cyber ☒ 2. Gestione del rischio cyber e della continuità operativa ☒ 3. Gestione e risposta agli incidenti di sicurezza ☒ 4. Gestione delle identità digitali e degli accessi logici ☒ 5. Sicurezza delle applicazioni, dei dati e delle reti

Sezione 3 – DESCRIZIONE DEL SOGGETTO PROPONENTE

3.A Descrizione della struttura organizzativa preposta alla governance ed attuazione del progetto

Illustrare il modello organizzativo, il team preposto alla governance ed attuazione del progetto, e i processi e gli strumenti a disposizione, ai fini dell'attribuzione del criterio di valutazione 1.1 dell'Avviso

Max 200 parole

Il **modello organizzativo** del proponente prevede:

- governance generale affidata all'Area Amministrazione e Transizione Digitale CMVe: definisce linee strategiche, coordina, valida i 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 CMVe esperto nella gestione e rendicontazione, affiancato dall'Unità PMO e Progettazione finanziata di VENIS.

Il modello deriva dall'esperienza del Soggetto Aggregatore Digitale Metropolitano (SAD), con cui CMVe e Comune di Venezia, insieme al partner tecnologico VENIS, dal 2021 guidano la trasformazione digitale dell'area metropolitana di Venezia.

Team e i processi: la Steering Committee definisce le strategie di progetto che vengono raccolte dal Project Manager (PM) e trasformate in piano esecutivo con il supporto del PMO.

Il piano viene sviluppato dal team tecnico, coordinato dal PM e dal Team Manager (esperto funzionale). Il PMO supervisiona la gestione e garantisce la condivisione tra le componenti tecniche e amministrative.

Il team possiede certificazioni di project management, gestione servizi IT, cybersecurity.

Strumenti: Collaboration di progetto strutturato in directory funzionali, GANTT, SAL settimanale, allineamenti di avanzamento e monitoraggio tecnico-amministrativo supportato da Reportistica specifica.

3.B Indicazione di precedenti progetti in ambito IT e cybersecurity gestiti dal Soggetto proponente, similari al progetto presentato per ambito di intervento e per importo gestito, che possano essere a valore aggiunto nell'attuazione del progetto a valere sul presente Avviso

Indicare, per ciascun progetto, l'oggetto, il periodo di riferimento (MM-AAAA di inizio e MM-AAAA di fine) e il relativo valore annuo ai fini dell'attribuzione dei criteri di valutazione 1.2 e 1.3 dell'Avviso

MAX 10 progetti, con riferimento all'ultimo quinquennio (2019 – 2023)

	Nome progetto	Oggetto del progetto	Periodo di riferimento	Valore annuo (IVA incl.)
1	**Con.ME - Convergenza digitale Metropolitana - Azione 2.2.1 Migrazione Data Center Comuni in SAD**	Il progetto Con.ME si inserisce nel percorso di attuazione del processo di transizione digitale avviato nel 2019 da CMVe con il Piano di Digitalizzazione dei Comuni dell'area e risponde all'obiettivo di promuovere la convergenza digitale degli enti attraverso azioni di sistema rese possibili dalle attuali tecnologie digitali. Il progetto ha riguardato il consolidamento e la razionalizzazione delle infrastrutture ICT attualmente in uso presso i Comuni dell'area metropolitana facenti parte dell'aggregazione proponente (21 Comuni), presso il Data Center del Comune di Venezia, gestito dalla in-house VENIS e messo a disposizione del SAD Metropolitano. Il progetto ha consentito di mettere in sicurezza il datacenter dei comuni normalizzando l'infrastruttura ad un modello Saas e attivando procedure di backup e disaster recovery in modalità Baas e Draas elevando l'affidabilità dei servizi, mettendo in sicurezza gli accessi e garantendo sorveglianza ai sistemi.	**02/2021 - 03/2023**	**320.036,67 €**
2	**Adeguamneto Cyber Security 2022**	Percorso di aggiornamento gestionale, procedurale e tecnologico in rispetto alla più recente normativa in ambito cyber sicurezza (PEG 2022 OG0317): • Determina aggiornamento apparati di rete (LAN7): Det 1227 del 10/05/2022 • Determina acquisizione Awingu Checkpoint Netap: Det 3463 del 19/12/2022	**05/2022 - 12/2022**	**146.054,19 €**

3	**Adeguamento Cyber Security 2023**	Piano progettuale di implementazione delle misure di sicurezza: Adeguamento Next Generation Firewall, individuazione EDP, Gestione dei Log • Determina acquisto Darktrace: Det 845 del 27/03/2023 • Det. cambio sistema di posta e passaggio a O365: Det 970 del 28/03/2023 • Determine acquisto Cynet 3560 antivirus: Det 2323 del 20/07/2023 e 4035 del 19/12/2023 • Det. manutenzione Checkpoint: Det 3408 08/11/2023 • Determina acquisto Awingu: Det 3464 del 09/11/2023 • Determina acquisto Log360: Det 3636 del 24/11/2023	**03/2023 - 11/2023**	**403.366,24€**

3.C Indicazione di precedenti progetti gestiti dal Soggetto proponente finanziati da Fondi nazionali, europei o internazionali

Indicare, per ciascun progetto, l'oggetto, il periodo di riferimento (MM-AAAA di inizio e MM-AAAA di fine) e il relativo valore annuo, precisando inoltre la denominazione e la tipologia del fondo (nazionale, europeo o internazionale) ai fini dell'attribuzione del criterio di valutazione 1.4 dell'Avviso

MAX 10 progetti, con riferimento all'ultimo quinquennio (2019 – 2023)

	Nome progetto	Denominazione e tipologia del fondo	Oggetto del progetto	Periodo di riferimento	Valore annuo (IVA incl.)
1	**Con.Me – Convergenza digitale Metropolitana**	**POR FESR Veneto 2014-2020. Asse 2. Azione 2.2.1 Consolidamento data center e creazione Hub regionale, Bando "Agire per la cittadinanza digitale"**	Consolidare e razionalizzare le infrastrutture ICT in uso presso i Comuni dell'area metropolitana di Venezia facenti parte dell'aggregazione proponente, presso il Data Centre pubblico del Comune di Venezia ubicato a Marghera c/o il Parco Scientifico Vega, gestito dalla in-house VENIS e messo a	**02/2021-03/2023**	**320.036,67 €**

			disposizione del SAD Metropolitano.		
2	**Con.Me – Convergenza digitale Metropolitana**	**POR FESR Veneto 2014-2020. Asse 2. Azione 2.2.2 Sviluppo e diffusione dei servizi digitali di e-government (LEDD), Bando "Agire per la cittadinanza digitale"**	Aumentare il numero degli Enti che offrono, a cittadini e imprese, servizi completamente interattivi ed interoperabili, costruendo un catalogo servizi coerente con i LEDD indicati dalla Regione Veneto.	**02/2021-03/2023**	**228.546,26 €**
3	**Con.Me – Convergenza digitale Metropolitana**	**POR FESR Veneto 2014-2020. Asse 2. Azione 2.2.3 Interoperabilità delle infrastrutture abilitanti, Bando "Agire per la cittadinanza digitale"**	Creare un sistema informativo, che assicuri l'interazione e lo scambio di informazioni dalla Piattaforma DiMe verso i sistemi legacy e con la piattaforma CReSCI, attraverso la predisposizione di Interfacce di servizio (API negli standard REST e SOAP) per l'esposizione di servizi digitali.	**02/2021-03/2023**	**47.295,33 €**
4	**Visfrim**	**Interreg Italia Slovenia 2014-2020**	Gestione del Rischio Idraulico per il bacino del fiume Vipacco ed ulteriori bacini transfrontalieri	**01/2019-06/2022**	**38.345,78 €**
5	**CROSSIT SAFER**	**Interreg Italia Slovenia 2014-2020**	Cooperazione transfrontaliera tra Slovenia e Italia per una regione più sicura	**01/2019-09/2022**	**29.425,00 €**
6	**SECAP**	**Interreg Italia Slovenia 2014-2020**	Supporto alle politiche energetiche e di adattamento climatico	**11/2018-04/2022**	**54.354,12 €**
7	**MOVES**	**Programma sperimentale nazionale di**	Mobilità sostenibile nel territorio Veneziano e	**01/2018-**	**260.266,67 €**

		mobilità sostenibile casa-scuola e casa-lavoro (decreto MATTM 208/2016) dal Ministero dell'ambiente e della sicurezza energetica	nelle scuole	**03/2024**	
8	**Programma Life**	**Programma Life EU 2014-2020**	Veneto Adapt Central Veneto Cities netWorking for ADAPTation to Climate Change in a multi-level regional perspective	**07/2017-12/2021**	**35.957,20 €**

3.D Indicazione delle certificazioni relative alla sicurezza informatica e/o alla gestione dei processi e della qualità possedute dal Soggetto proponente

Indicare le certificazioni possedute da parte delle strutture organizzative interne al Soggetto proponente, a qualunque titolo coinvolte nella governance ed attuazione del progetto presentato a valere sul presente Avviso, allegandone una copia, ai fini dell'attribuzione del criterio di valutazione 1.5 dell'Avviso

☐ **Nessuna certificazione**

☒ **Possesso di certificazioni** *(indicare le certificazioni possedute e il riferimento puntuale del relativo allegato a comprova. Eventualmente aggiungere righe)*:

Si illustrano e si documentano le certificazioni della in-house provider VENIS spa, affidataria della Città metropolitana di Venezia per la realizzazione, sviluppo e conduzione tecnica del sistema informativo e della rete di telecomunicazioni dell'Ente, nonché della progettazione e realizzazione del progetto CYBERMET:

1. ISO/IEC 27001:2013 - UNI CEI EN ISO/IEC 27001:2017 (in house VENIS)
2. ISO 9001:2015 (in house VENIS)
3. ANSI/TIA 942-B-2017 (in house VENIS)
4. ISO/IEC 27017:2015 (in house VENIS)
5. ISO/IEC 27018:2019 (in house VENIS)

3.E Indicazione delle certificazioni informatiche e di project management possedute dal team preposto alla governance ed attuazione del progetto

Indicare le certificazioni possedute (allegandone una copia) e le figure professionali interne che le detengono, in coerenza con il modello organizzativo presentato al punto 3.A, ai fini dell'attribuzione del criterio di valutazione 1.6 dell'Avviso

☐ **Nessuna certificazione**

☒ **Possesso di certificazioni** *(indicare le certificazioni possedute e il riferimento puntuale del relativo allegato a comprova. Eventualmente aggiungere righe)*:

Si illustrano e si documentano le certificazioni possedute dalle figure professionali coinvolte nel gruppo di lavoro dell'Ente per la governance e l'attuazione del progetto:

1. ISIPM-Base (Marta Mereu, Lucia Fedrigoni, Ufficio Europa CMVe)
2. ITIL 4 Foundation (Federica Braga, Adrian Trofin, Enrico Boni, Stefano Biondi, Giorgia Comina, VENIS)
3. Prince 2 (Daniela Minto, Enrico Boni, Giorgia Comina, Giacomo Perale, VENIS)
4. PM9001x Project Management Lifecycle (Stefano Biondi, VENIS)
5. NetEye Foundamentals (Andrea Caprioli, VENIS)
6. CompTIA Security+ (Salvatore Gregoraci, team cybersecurity VENIS)
7. Certified Ethical Hacker (Salvatore Gregoraci, Achille Cuccurullo, Cristiana Petrillo, Aurora Cesetti, Rachele De Simone, team cybersecurity VENIS)
8. Certified Network Defender (Salvatore Gregoraci, Cristiana Petrillo, Aurora Cesetti, Rachele De Simone, team cybersecurity VENIS)
9. Computer Hacking Forensic Investigator (Salvatore Gregoraci, Cristiana Petrillo, team cybersecurity VENIS)
10. Kubernetes and Cloud Native Associate (Achille Cuccurullo, team cybersecurity VENIS)
11. CCC Cloud Technology Associate (Achille Cuccurullo, team cybersecurity VENIS)
12. Training Course for Auditor / Lead Auditor Information Security Management Systems - ISO 27001: 2013 standard (Rachele De Simone, team

cybersecurity VENIS)

13. Training Course for auditing ISO Management Systems - ISO 19011:2018 and ISO 17021-1:2015 standards (Rachele De Simone, team cybersecurity VENIS).

Sezione 4 – PROPOSTA PROGETTUALE

4.A Indicazione delle attuali criticità riscontrate sui sistemi informativi

Indicare, per ciascuno degli interventi selezionati nella Sezione 2.E, le criticità riscontrate

1. Governance e programmazione cyber *(da valorizzare solo se scelto)*	Le principali criticità riguardano l'assenza di una Strategia di Cybersecurity documentata, definita e implementata che rispetti le best practice e gli standard del settore (quali, a titolo esemplificativo, ma non esaustivo GDPR e ISO 27001). Tale mancanza, data la centralità dei servizi ICT, può comportare l'esposizione a minacce e rischi che impattano sulla confidenzialità, integrità e disponibilità delle informazioni. In particolare, le criticità riscontrate sono le seguenti: • Assenza di un Piano di Disaster Recovery per i sistemi critici: può comportare malfunzionamenti o interruzioni che causano inefficienze e blocchi operativi; • Necessità di aggiornamento e di strutturazione del processo di formazione del personale interno in tema di cyber security: ciò può comportare un'esposizione critica alle minacce cibernetiche dovuta alla mancanza di consapevolezza dei rischi di sicurezza informatica da parte del personale dipendente, nonché un'eccessiva vulnerabilità delle risorse umane e inconsapevolezza nell'utilizzo di strumenti informatici; • Assenza di un sistema per la gestione delle attività di formazione: un sistema di e-learning consente con dei corsi sempre disponibili contribuirebbe a ridurre l'esposizione alle minacce cibernetiche a causa della mancata conoscenza del personale dei possibili rischi di sicurezza.
2. Gestione del rischio cyber e della continuità operativa *(da valorizzare solo se scelto)*	Le principali criticità riscontrate nell'ambito della gestione del rischio cyber e della continuità operativa riguardano: • Assenza di un Framework di Gestione del Rischio Cyber adeguatamente documentato e definito che consenta di delineare le principali minacce informatiche, la probabilità di accadimento e l'impatto, al fine di prendere decisioni atte a mitigare i rischi e proteggere le risorse e i dati.

	• Mancanza di un Piano e procedure documentate in relazione alla gestione del rischio correlato alle terze parti e ai fornitori. • Necessità di aggiornamento delle Politiche e delle procedure di Backup documentate e definite che consentano di ripristinare i dati, a titolo esemplificato dei sistemi di posta, in caso di incidenti di sicurezza informatica.
3. Gestione e risposta agli incidenti di sicurezza *(da valorizzare solo se scelto)*	Le principali criticità riscontrare nella gestione e risposta agli incidenti di sicurezza sono le seguenti: • Assenza di un piano di gestione di incidenti e di procedure specifiche per i sistemi critici; • Assenza di un processo e di tecnologia volta al monitoraggio costante e proattivo di tutti i dispositivi di rete e degli accessi logici alle risorse di rete che possa supportare l'Amministrazione a individuare anomalie, potenziali o tali, prevenire e gestire gli incidenti di sicurezza.
4. Gestione delle identità digitali e degli accessi logici *(da valorizzare solo se scelto)*	Le principali criticità presenti in riferimento alla gestione delle identità digitali e degli accessi logici sono le seguenti: • Revisione e aggiornamento della politica di uso degli asset; • Necessità di aggiornamento delle politiche di gestione degli accessi logici volta a definire procedure e regole per prevenire e bloccare eventuali accessi non autorizzati (es SW e Wifi; • Necessità di potenziamento delle competenze del personale IT per l'utilizzo di strumenti avanzati di protezione dei dispositivi e della rete; • Potenziamento della tecnologia a supporto della gestione degli accessi logici.

5. Sicurezza delle applicazioni, dei dati e delle reti *(da valorizzare solo se scelto)*	Le criticità rilevate in riferimento alla sicurezza delle applicazioni, dei dati e delle reti riguardano: • Assenza di un Piano di gestione delle vulnerabilità; • Necessità di strutturare e definire il Piano di svolgimento a cadenza periodica di attività di Penetration Test volte a valutare la sicurezza dell'infrastruttura IT; • Necessità di integrare gli strumenti tecnologici volti a supportare la protezione delle applicazioni, dei dati e delle reti.

4.B Indicazione e descrizione delle tipologie di intervento che si intende realizzare per ciascun intervento

Indicare per ciascun intervento selezionato nella Sezione 2.E, una o più tipologie di intervento che si intende realizzare, e fornire descrizione di dettaglio dei contenuti operativi delle specifiche attività previste

1. Governance e programmazione cyber *(da valorizzare solo se scelto)*	**Tipologie di intervento** ☒ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento ☒ B. Miglioramento dei processi e dell'organizzazione ☒ C. Formazione e miglioramento della consapevolezza delle persone ☒ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

(descrizione delle attività di Max 300 parole)

CMVe persegue l'obiettivo di migliorare la sua postura di sicurezza informatica e sostenere le competenze specialistiche per garantire un adeguato livello di cyber resilienza. Al fine di raggiungere l'obiettivo generale si descrivono gli interventi richiesti da CMVe:

1.A - Security Strategy AS-IS:

- ***NIST Maturity Assessment*** – Conduzione di un Assessment basato sul Framework Nazionale della Cybersicurezza (NIST CSF) al fine di

elaborare un security posture profile tramite Information Gathering, Q&A al personale e definizione della Security Architecture As Is Analysis

- ***Gap Analysis*** – Analisi dei gap e delle criticità emerse in fase di assessment rispetto ai benchmark di settore
- ***GDPR Compliance*** – analisi volta a garantire il rispetto dei requisiti della normativa di riferimento per il trattamento dei dati personali nell'UE, nonché il mantenimento ed il miglioramento delle politiche per la gestione efficace della sicurezza delle informazioni dell'Amministrazione

1.B - Security Strategy Plan: Definizione di un piano di miglioramento della postura di cyber security per definire le principali aree di criticità da indirizzare e un piano per l'implementazione di attività operative a supporto del sistema di gestione e delle vulnerabilità tecniche e tecnologiche;

1.C - Formazione Cyber*:*

- ***Definizione della Cyber Situational Awareness e analisi del fabbisogno formativo***
- ***Predisposizione del materiale didattico ed erogazione di security training al personale identificato***
- ***Simulazione di una campagna di phishing***

1.D - Acquisizione ed implementazione di sistemi e tecnologie a supporto dei processi di miglioramento organizzativo:

- ***Analisi dei requisiti tecnici e procedurali*** dall'individuazione delle caratteristiche tecniche di progetto, generali e proprie delle soluzioni di governance e programmazione cyber, quali tecnologia SASE
- ***Scouting e Benchmarking***: individuazione delle tecnologie di interesse presenti sul mercato e comparazione delle soluzioni mediante attribuzione di ciascun requisito secondo un sistema di scoring definito e moltiplicazione dello score per un coefficiente di rilevanza del requisito
- ***Prioritizzazione degli acquisti per aree di emergenza***
- ***Selezione*** *delle soluzioni mediante la stesura di capitolati tecnici o documentazione di gara ove previsto*
- ***Acquisto delle soluzioni selezionate***

2. Gestione del rischio cyber e della continuità	**Tipologie di intervento**

operativa *(da valorizzare solo se scelto)*	☒ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento ☐ B. Miglioramento dei processi e dell'organizzazione ☐ C. Formazione e miglioramento della consapevolezza delle persone ☒ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

(descrizione delle attività di Max 300 parole)

L'obiettivo della gestione del rischio cyber e della continuità operativa è valutare e quantificare il rischio a cui è esposto l'Ente dalle minacce attuali di cyber security. Ciò è fondamentale per preservare la sicurezza e la resilienza dei processi dell'amministrazione, nonché per il mantenimento della sicurezza dei dati, delle informazioni, delle persone e dei loro diritti fondamentali.

Al fine di raggiungere l'obiettivo generale si descrivono gli interventi che CMVe intende mettere in atto:

2.A – 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. Tali processi sono necessari per la comprensione della natura delle minacce identificate consentendo all'Amministrazione di definire le priorità e le strategie di mitigazione delle minacce stesse.

2.D – Acquisizione ed implementazione/sviluppo di sistemi e tecnologie a supporto dei processi di miglioramento dell'organizzazione

- **Analisi dei requisiti tecnici e procedurali** individuando le caratteristiche tecniche di progetto, generali e proprie delle soluzioni di gestione del rischio cyber e della continuità operativa, quali IPS/IDS, Sistemi di Backup, Piattaforme di Threat Intelligence
- **Scouting e Benchmarking**: individuazione delle tecnologie di interesse presenti sul mercato e comparazione delle soluzioni mediante attribuzione di punteggi a ciascun requisito secondo un sistema di scoring definito e moltiplicazione del valore assegnato per un coefficiente di rilevanza del requisito
- ***Prioritizzazione degli acquisti per aree di emergenza***
- ***Selezione*** *delle soluzioni mediante la stesura di capitolati tecnici o documentazione di gara ove previsto*

• ***Acquisto delle soluzioni selezionate***	
3. Gestione e risposta agli incidenti di sicurezza *(da valorizzare solo se scelto)*	**Tipologie di intervento** ☐ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento ☒ B. Miglioramento dei processi e dell'organizzazione ☒ C. Formazione e miglioramento della consapevolezza delle persone ☒ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

(descrizione delle attività di Max 300 parole)

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 raggiungere l'obiettivo generale si descrivono gli interventi che CMVe intende mettere in atto:

***3.B – Definizione di un processo di gestione degli incidenti**:* al fine di implementare un processo che possa garantire la minimizzazione dell'impatto degli eventi malevoli l'individuazione tempestiva di misure di contrasto/contenimento

- ***Supporto specialistico*** nelle attività di ripristino post incident; l'analisi e la produzione di statistiche elaborate dai dati raccolti con lo scopo di aumentare il grado di sensibilità verso il tema della sicurezza attraverso le "lesson learned"
- *Sviluppo di **Playbook** di risposta agli incidenti:* attraverso la predisposizione di passaggi predefiniti e istruzioni operative, consente all'ente di identificare la minaccia ed agire in maniera tempestiva

3.C – Formazione sulle tecniche di hacking: CMVe pubblica servizi sul web per i propri uffici e per enti del territorio. Per garantire l'adeguato livello di sicurezza ai sistemi è fondamentale formare il personale IT a riconoscere attacchi di rete/applicativi grazie ad un percorso specifico su Ethical Hacking/Network Defender

3.D – Acquisizione ed implementazione/sviluppo di sistemi e tecnologie a supporto dei processi di miglioramento dell'organizzazione

- **Analisi dei requisiti tecnici e procedurali** individuando le caratteristiche tecniche di progetto, generali e proprie delle soluzioni di gestione del rischio cyber e della continuità operativa, quali IPS/IDS, Sistemi di Backup, Piattaforme di Threat Intelligence
- **Scouting e Benchmarking**: individuazione delle tecnologie di interesse presenti sul mercato e comparazione delle soluzioni mediante attribuzione di punteggi a ciascun requisito secondo un sistema di scoring definito e moltiplicazione del valore assegnato per un coefficiente di rilevanza del requisito
- ***Prioritizzazione degli acquisti per aree di emergenza***
- ***Selezione** delle soluzioni mediante la stesura di capitolati tecnici o documentazione di gara ove previsto*

- ***Acquisto delle soluzioni selezionate***

4. Gestione delle identità digitali e degli accessi logici *(da valorizzare solo se scelto)*	**Tipologie di intervento** ☐ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento ☐ B. Miglioramento dei processi e dell'organizzazione ☒ C. Formazione e miglioramento della consapevolezza delle persone ☒ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

(descrizione delle attività di Max 300 parole)

L'intervento proposto da CVME si pone come obiettivo generale migliorare le modalità di accesso agli strumenti aziendali rendendo più sicuro l'accesso agli stessi dall'esterno.

Il raggiungimento dell'obiettivo preposto CMVe richiede:

4.C - ***Formazione sull'utilizzo di sistemi di gestione delle identità digitali e degli accessi logici****:* Office 365 offre diverse opzioni per la sicurezza e la gestione degli accessi, nello specifico il modulo "SECURITY E3" fornisce una serie di strumenti avanzati per proteggere i dispositivi e la rete. L'intervento richiede il supporto alla configurazione del modulo di sicurezza. In particolare, deve essere attuata per il personale addetto alla configurazione (IT) un percorso specifico di formazione ai fini dell'utilizzo e dell'implementazione delle principali funzionalità di gestione della piattaforma di gestione Office 365.
Inoltre, si rende necessario regolare gli accessi Wifi tramite l'utilizzo di ClearPass che offre funzionalità avanzate per il controllo degli accessi e la sicurezza delle reti.

4.D – ***Acquisizione ed implementazione/sviluppo di sistemi e tecnologie a supporto dei processi di miglioramento dell'organizzazione***.

- **Analisi dei requisiti tecnici e procedurali** individuando le caratteristiche tecniche di progetto, generali e proprie delle soluzioni di gestione del rischio cyber e della continuità operativa, quali IPS/IDS, Sistemi di Backup, Piattaforme di Threat Intelligence
- **Scouting e Benchmarking**: individuazione delle tecnologie di interesse presenti sul mercato e comparazione delle soluzioni mediante attribuzione di punteggi a ciascun requisito secondo un sistema di scoring definito e moltiplicazione del valore assegnato per un coefficiente di rilevanza del requisito
- ***Prioritizzazione degli acquisti per aree di emergenza***
- ***Selezione*** *delle soluzioni mediante la stesura di capitolati tecnici o documentazione di gara ove previsto*

Acquisto delle soluzioni selezionate

5. Sicurezza delle applicazioni, dei dati e delle reti *(da valorizzare solo se scelto)*	**Tipologie di intervento** ☒ A. Analisi della postura di sicurezza e definizione di un piano di potenziamento B. Miglioramento dei processi e dell'organizzazione ☐ C. Formazione e miglioramento della consapevolezza delle persone ☒ D. Progettazione e sviluppo di nuovi sistemi e tecnologie

(descrizione delle attività di Max 300 parole)

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

Al fine di raggiungere l'obiettivo generale si descrivono gli interventi che CMVe intende porre in essere:

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

- ***Vulnerability Assessment***: Deep Information Gathering, Enumeration e Vulnerability Scan. È tracciata una lista prioritaria delle minacce

esistenti su scoring CVE. Ciò include la raccolta di informazioni su malware, exploit, vulnerabilità e attacchi informatici attivi e potenziali

- ***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 dell'organizzazione

5.D – Acquisizione ed implementazione/sviluppo di sistemi e tecnologie a supporto dei processi di miglioramento dell'organizzazione.

- **Analisi dei requisiti tecnici e procedurali** individuando le caratteristiche tecniche di progetto, generali e proprie delle soluzioni di gestione del rischio cyber e della continuità operativa, quali IPS/IDS, Sistemi di Backup, Piattaforme di Threat Intelligence
- **Scouting e Benchmarking**: individuazione delle tecnologie di interesse presenti sul mercato e comparazione delle soluzioni mediante attribuzione di punteggi a ciascun requisito secondo un sistema di scoring definito e moltiplicazione del valore assegnato per un coefficiente di rilevanza del requisito
- ***Prioritizzazione degli acquisti per aree di emergenza***
- ***Selezione*** *delle soluzioni mediante la stesura di capitolati tecnici o documentazione di gara ove previsto*
- ***Acquisto delle soluzioni selezionate***

4.C Indicazione delle amministrazioni locali coinvolte nel progetto presentato e descrizione delle relative modalità di coinvolgimento

Ai fini dell'attribuzione del criterio di valutazione 3.1 dell'Avviso

Amministrazioni locali coinvolte *(aggiungere eventuali righe ulteriori)*	**Descrizione delle modalità di coinvolgimento dell'amministrazione indicata**

1	**Mirano**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical** • **Piano di Remediation e relative attività di mitigazione**
2	**Jesolo**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical** • **Piano di Remediation e relative attività di mitigazione**
3	**Scorzè**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical** • **Piano di Remediation e relative attività di mitigazione**
4	**Santa Maria di Sala**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical** • **Piano di Remediation e relative attività di mitigazione**
5	**Noale**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical**

		• **Piano di Remediation e relative attività di mitigazione**
6	**Caorle**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical** • **Piano di Remediation e relative attività di mitigazione**
7	**Concordia Sagittaria**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical** • **Piano di Remediation e relative attività di mitigazione**
8	**Fossalta di Piave**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical** • **Piano di Remediation e relative attività di mitigazione**
9	**Gruaro**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical** • **Piano di Remediation e relative attività di mitigazione**

10	**Teglio Veneto**	• **Enumeration delle applicazioni presenti in SAD** • **Mappatura delle applicazioni Business Critical** • **Vulnerability Assessment/Penetration Test delle Applicazioni Business Critical** • **Piano di Remediation e relative attività di mitigazione**

4.D Indicazione dei settori di riferimento della Direttiva NIS impattati dal progetto proposto *Ai fini dell'attribuzione del criterio di valutazione 3.2 dell'Avviso*	
Settori di riferimento della Direttiva NIS impattati	**Descrizione degli impatti del progetto proposto sul potenziamento della resilienza cyber in relazione ai settori di riferimento della Direttiva NIS indicati** *Max 300 parole*

☐ **energia** ☐ **trasporti** ☐ **banche** ☐ **mercati finanziari** ☐ **sanità** ☐ **fornitura e distribuzione di acqua potabile** ☐ **infrastrutture digitali** ☐ **motori di ricerca** ☐ **servizi cloud** ☐ **piattaforme di commercio elettronico**	Il progetto non ha impatti sui settori di riferimento della Direttiva NIS.
4.E Indicazione delle funzioni del Cybersecurity Framework impattate dal progetto proposto *Ai fini dell'attribuzione del criterio di valutazione 3.3 dell'Avviso*	
Funzioni del Cybersecurity Framework	**Descrizione degli impatti del progetto proposto sull'incremento di maturità delle funzioni del Cybersecurity Framework indicate** *Max 300 parole*

Identify **Protect** **Detect** **Respond** **Recover**	Tutti gli interventi richiesti possono essere ricondotti alle 5 funzioni del NIST Cybersecurity Framework, come di seguito riportato: 1.**Identify**: Identificazione e comprensione dei rischi di cybersecurity dell'organizzazione, compresa l'identificazione di asset, sistemi, dati e risorse da proteggere, nonché l'analisi dei rischi e delle potenziali minacce connesse all'infrastruttura dell'Ente. 2.**Protect**: Definizione ed implementazione di controlli e misure di sicurezza volti a mitigare i rischi identificati, compresa l'attuazione di politiche e procedure di sicurezza, l'uso di tecnologie di sicurezza e la gestione degli accessi e delle autorizzazioni. 3.**Detect**: Scouting e supporto alla selezione di soluzioni di tecnologie utili all'identificazione di eventuali violazioni della sicurezza o attività anomale. 4.**Respond**: Predisposizione e definizione di un piano di risposta agli incidenti ben definito, che definisca le azioni da intraprendere per contenere un incidente, ripristinare le normali operazioni e mitigare i danni. 5.**Recover**: Definizione di procedure di ripristino delle normali operazioni a seguito di un incidente di sicurezza.
4.F Indicazione delle finalità perseguite dal progetto proposto e del relativo impatto sulla risoluzione delle criticità dichiarate sui sistemi informativi *Ai fini dell'attribuzione del criterio di valutazione 3.5 dell'Avviso*	

Max 300 parole
Il progetto proposto si pone come obiettivo il potenziamento della resilienza cyber security dell'Amministrazione mediante l'analisi del livello di maturità della postura di sicurezza e la definizione di un piano di rimedio volto a migliorare le lacune presenti, al fine di raggiungere il livello di resilienza desiderato. Il progetto è volto, in particolar modo, a migliorare la strategia di cybersecurity mediante la revisione e quindi il miglioramento del framework documentale e dei processi, soprattutto in riferimento alla gestione dei rischi cibernetici, alla gestione degli incidenti e del ripristino dei dati; la definizione e l'implementazione di attività di formazione al personale dipendente per aumentare la consapevolezza sui rischi di sicurezza informatica e l'utilizzo degli strumenti informatici e prevenire, nonché gestire potenziali attacchi cibernetici; a svolgere attività volte all'acquisizione di nuovi sistemi e tecnologie di supporto all'Amministrazione nel potenziamento della resilienza cyber al fine monitorare e proteggere l'infrastruttura IT. Attraverso l'attuazione degli interventi previsti nel progetto, l'Amministrazione intende rispondere alle criticità evidenziate e note nell'architettura di sicurezza dell'Ente. Tra gli interventi previsti l'Amministrazione intende effettuare attività adeguamento della sicurezza degli applicativi Business Critical individuati all'interno del perimetro SAD.

Ai fini della compilazione del Quadro finanziario e del Cronoprogramma si rimanda all'Allegato B2.

Glossario

Termini	Descrizione esemplificativa
Identify (Identificazione)	Comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati, al fine di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali.
Protect (Protezione)	Implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica.
Detect (Rilevamento)	Definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.
Respond (Risposta)	Definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato, al fine di contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.
Recover (Ripristino)	Definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente, al fine di garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations.

CITTÀ METROPOLITANA DI VENEZIA

AREA ECONOMICO FINANZIARIA

VISTO DI REGOLARITA' CONTABILE ATTESTANTE LA COPERTURA FINANZIARIA

OGGETTO: APPROVAZIONE DEL PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA ED ATTO D'OBBLIGO AI SENSI DELL'ART. 12 LEGGE 241/90, NELL'AMBITO DEL PNRR NEXT GENERATION EU MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5 CUP B79B21002230006 NO CIG.

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
2024	Accertamento 27060	420000101326/0 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006	PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA PNRR NEXT GENERATION EU MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5	€1.500.000,00

2024	Impegno 1661	201080205619/4 - PNRR PROGETTO M1 C1 Investimento 1.5 "CYBERSECURITY" INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER CUP B79B21002230006	PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA PNRR NEXT GENERATION EU MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5	€1.500.000,00

IL DIRIGENTE
ARMELLIN ROMANO

atto firmato digitalmente

CITTÀ METROPOLITANA DI VENEZIA

DICHIARAZIONE DEL RESPONSABILE DEL PROCEDIMENTO

Proposta n. 6049/2024

Oggetto: **APPROVAZIONE DEL PROGETTO CYBERMET - CYBERSECURITY METROPOLITANA ED ATTO D'OBBLIGO AI SENSI DELL'ART. 12 LEGGE 241/90, NELL'AMBITO DEL PNRR NEXT GENERATION EU MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5 CUP B79B21002230006 NO CIG.**

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