COMUNE DI FIRENZE

PROVVEDIMENTO DIRIGENZIALE

Numero: **DD/2024/06246**
Del: **19/08/2024**
Proponente: **Direzione Sistemi Informativi - Servizio Sicurezza, Infrastruttura e Architettura IT dell'Ente**

OGGETTO:
MATICMIND SPA - Acquisto di apparati e dispositivi di sicurezza informatica sul Mercato Elettronico della Pubblica Amministrazione (MEPA) per gli Enti partecipanti al progetto Metrowide - Avviso 3/2022 della Agenzia per la Cybersicurezza Nazionale - Piano Nazionale di Ripresa e Resilienza (PNRR) Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” finanziato dall’Unione europea – Next generation EU – Progetto Metrowide - CUP H11C22001670006 – CIG B261E74FC8

IL DIRIGENTE

Premesso che

- in data 29/01/2024 è stata approvata la Deliberazione del Consiglio Comunale n. 5 avente ad oggetto “Documenti di programmazione 2024-2026: approvazione note di aggiornamento al Dup – bilancio finanziario, nota integrativa e piano triennale investimenti”;

- in data 27/02/2024 è stata approvata dalla Giunta la deliberazione n. 49 avente ad oggetto "Piano Esecutivo di Gestione (PEG) 2024-2026. Approvazione”.

- con Decreto del Sindaco n. 2022/DEC/00015 del 1/4/2022 è stato attribuito al sottoscritto l’incarico di Dirigente del Servizio Sicurezza, Infrastruttura e Architettura IT dell’Ente;

- in data 26.03.24, è stata approvata dalla Giunta la deliberazione n. 111 avente ad oggetto "Piano Integrato di Attività e Organizzazione 2024 -2026. Approvazione."

- il Piano di Prevenzione della Corruzione 2024/2026, a seguito del DL n. 80 del 9.6.2021, convertito con modificazioni dalla Legge n. 113 del 6.8.2021, e del DM n.132 del 30.6.2022, è confluito nella Sezione n. 2 “Valore pubblico, Performance e Anticorruzione” del Piano integrato di attività e organizzazione (PIAO) approvato con la citata Delibera di Giunta n. 111/2023;

Dato atto che

- il Piano Nazionale di Ripresa e Resilienza (PNRR) è lo strumento che, grazie ai fondi del Next Generation EU, renderà l'Italia più equa, sostenibile e inclusiva;

- la Commissione Europea ha lanciato nel luglio 2020 “Next Generation EU” (NGEU), un pacchetto di misure e stimoli economici per i Paesi membri in risposta alla crisi pandemica da Covid-19, individuando con il regolamento UE 2021/241 sei grande aree (pilastri) di intervento sui quali i PNRR si dovranno focalizzare: transizione verde, trasformazione digitale, crescita intelligente e inclusiva, coesione sociale e territoriale, salute e resilienza economica, politiche per le nuove generazioni;

- al fine di accedere ai fondi di Next Generation EU (NGEU), ciascuno Stato membro ha dovuto predisporre un Piano nazionale per la ripresa e la resilienza (PNRR - Recovery and Resilience Plan) per definire un pacchetto coerente di riforme e investimenti per il periodo 2021-2026;

- il “Piano Nazionale di Ripresa e Resilienza” (“PNRR”) è stato presentato dall’Italia alla Commissione europea in data 30 aprile 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;

- il PNRR, che prevede investimenti e riforme in relazione a tre settori strategici – digitalizzazione e innovazione, transizione ecologica e inclusione sociale – si sviluppa in sei missioni, la prima delle quali, denominata “Digitalizzazione, Innovazione, Competitività, Cultura”, ha l’obiettivo di promuovere la trasformazione digitale del Paese e sostenere l’innovazione del sistema produttivo.

- il decreto-legge 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108, recante “Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure” definisce il quadro normativo nazionale finalizzato a semplificare e agevolare la realizzazione dei traguardi e degli obiettivi stabiliti dal PNRR;

- mediante il decreto del Ministero dell’Economia e delle Finanze in data 6 agosto 2021 (pubblicato sulla G.U. n. 229 del 24 settembre 2021) sono state assegnate le risorse finanziarie previste per l’attuazione dei singoli interventi del PNRR alle Amministrazioni centrali e corrispondenti milestone e target;

- mediante il decreto del Presidente del Consiglio dei ministri del 15 settembre 2021 sono stati individuati gli

strumenti per il monitoraggio del PNRR;

- mediante il decreto del Ministro dell'economia e delle finanze 11 ottobre 2021, pubblicato sulla Gazzetta Ufficiale n. 279 del 23 novembre 2021 sono state rese note le procedure per la gestione del PNRR in merito alle risorse messe in campo;

- al fine di supportare le Amministrazioni centrali titolari di interventi previsti nel PNRR nelle attività di presidio e vigilanza nell'esecuzione dei progetti/interventi di competenza che compongono le misure del Piano e di fornire indicazioni comuni a livello nazionale è stata emanata la circolare del Ministero dell'economia e delle finanze 14 ottobre 2021, n. 21, recante "Piano Nazionale di Ripresa e Resilienza (PNRR) - Trasmissione delle Istruzioni Tecniche per la selezione dei progetti PNRR";

Visto l'Avviso pubblico 03/2022 della Agenzia per la Cybersicurezza Nazionale (ACN) in qualità di soggetto attuatore dell'Investimento 1.5 "Cybersecurity" – Missione 1 Componente 1 del PNRR a titolarità del Ministro Innovazione Tecnologia e Transizione Digitale e Presidenza del Consiglio dei Ministri - Dipartimento per la trasformazione digitale per la presentazione di proposte di interventi di potenziamento della resilenza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul "Piano Nazionale di Ripresa e Resilienza – Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity", finanziato dall'Unione Europea – Next generation EU;

Rilevato che il Comune ha risposto all'avviso presentando tre domande di finanziamento, fra le quali la proposta (prot. 347581 del 14/10/2022) "Metrowide" per € 999.180,00 – CUP H11C22001670006

Dato atto che il progetto "Metrowide" presentato dall'Ente ha il fine di rafforzare il governo e la maturità di sicurezza e privacy di tutto l'ecosistema comunale, ossia è volto a garantire la riservatezza, l'integrità e la disponibilità del patrimonio informativo, con particolare riferimento ai dati personali, nel contesto della digitalizzazione dei servizi dell'ecosistema oggetto del progetto;

Considerato che, nello specifico dell'ecosistema esistente e soprattutto in funzione dei dati trattati, è fondamentale che il tema della cybersecurity sia affrontato su una scala più ampia, metropolitana, che coinvolge anche altri interlocutori istituzionali. Per questo, nell'ambito del progetto "Metrowide", che ha conseguito il finanziamento proprio per la sua impostazione multiente, il Comune con le altre amministrazioni individuate sul territorio, cioè Città Metropolitana di Firenze, Comune di Scandicci, Unione di Comuni Circondario Empolese-Valdelsa, Comune di Bagno a Ripoli, Unione di Comuni del Chianti Fiorentino, svilupperà la gestione della sicurezza delle informazioni e l'adeguamento alle disposizioni previste dalla vigente normativa in materia di dati personali e di cybersecurity;

Vista la Determinazione n. 3429 del 20/01/2023 dell'Agenzia per la Cybersicurezza Nazionale con la quale sono state individuate le proposte progettuali ammesse al finanziamento a valere sull'Avviso di cui sopra;

Vista, inoltre, la Determinazione n. 7591 del 23/02/2023 dell'Agenzia per la Cybersicurezza Nazionale per la rettifica della graduatoria finale;

Preso atto che la proposta progettuale del Comune di Firenze "Metrowide" CUP H11C22001670006 è stata finanziata per € 999.180,00;

Richiamati

- il Provvedimento dirigenziale DD/2023/03708 del 8/5/2023 avente oggetto "*Avviso 3/2022 della Agenzia per la Cybersicurezza Nazionale - Piano Nazionale di Ripresa e Resilienza (PNRR) Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" - finanziato dall'Unione europea – Next generation EU - Accertamento di entrata e correlato impegno di spesa*";

- il Provvedimento dirigenziale DD/2023/06484 del 3/8/2023 avente oggetto "*Avviso 3/2022 della Agenzia per la Cybersicurezza Nazionale - Piano Nazionale di Ripresa e Resilienza (PNRR) Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" finanziato dall'Unione europea – Next generation EU – Progetto Metrowide - CUP H11C22001670006 - Modifica accertamento e impegni di spesa correlati*";

- il Provvedimento dirigenziale DD/2023/1172 del 28/12/2023 avente oggetto "*Avviso 3/2022 della Agenzia per la Cybersicurezza Nazionale - Piano Nazionale di Ripresa e Resilienza (PNRR) Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" finanziato dall'Unione europea – Next generation EU – Progetto Metrowide - CUP H11C22001670006 - Annullamento accertamento e impegni di spesa correlati*";

- Il provvedimento dirigenziale DD/2024/3614 del 09/05/2024 avente ad oggetto "Avviso 3/2022 della Agenzia per la Cybersicurezza Nazionale - Piano Nazionale di Ripresa e Resilienza (PNRR) Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" finanziato dall'Unione europea – Next generation EU – Progetto Metrowide - CUP H11C22001670006 – Accertamento entrata e impegni di spesa correlati";

Dato atto che con il citato provvedimento dirigenziale DD/2024/3614 si è provveduto, fra l'altro, ad

- accertare per l'anno 2024 sul capitolo di 46309 "CONTRIBUTI STATALI PER PROGETTO "CYBERSECURITY METROWIDE" - PNRR M.1- C.1 – Inv.1.5 CUP H11C22001670006" l'importo di € 158.600,00 quale finanziamento per il Piano Nazionale di Ripresa e Resilienza – Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" (codice debitore 76581);
- assumere un impegno di spesa di € 158.600,00 sul capitolo correlato 59936 "PROGETTO "CYBERSECURITY METROWIDE" - FINANZIATO DALLO STATO - PNRR M.1- C.1 – Inv.1.5 CUP H11C22001670006" anno 2024 – codice opera 230106;

Ritenuto pertanto necessario, al fine di raggiungere i target previsti per il progetto Metrowide, procedere all'approvazione del Piano acquisti per il codice opera afferente la Misura 1.4.5. del PNRR e specificatamente

tale progetto;

Visto il Piano acquisti relativo al Codice Opera 230106 (Missione 01, Programma 08, Responsabile Procedura C9, Tipo finanziamento: 5), “Avviso Cybersecurity 03/2022 - PNRR M.1- C.1 – Inv.1.5 progetto "Cybersecurity Metrowide" - CUP H11C22001670006”, predisposto dal sottoscritto Dirigente e allegato al presente provvedimento come parte integrante e sostanziale, contenente l’indicazione dei costi complessivi presunti, I.V.A. inclusa, pari a € 158.600,00, per l’acquisto delle apparecchiature necessarie per la protezione della rete interna e/o esterna degli enti coinvolti nel progetto multiente Metrowide;

Dato atto della volontà dell’Amministrazione di rafforzare il governo e la maturità di sicurezza e privacy di tutto l’ecosistema comunale in collaborazione con gli altri enti partecipanti al progetto, ossia incrementare il livello di riservatezza, integrità e disponibilità del patrimonio informativo, con particolare riferimento ai dati personali, nel contesto della digitalizzazione dei servizi;

Preso atto che

- il Comune di Firenze è il capofila del progetto multiente di cybersecurity, denominato Metrowide, finanziato con fondi PNRR in risposta al bando n. 3/2022 pubblicato dall’Agenzia per la Cybersicurezza Nazionale (ACN);
- quale capofila, il Comune necessita di affrontare la sicurezza informatica anche in una prospettiva più ampia, prevedendo la partecipazione di più Enti locali del territorio metropolitano fiorentino che, dovendo collaborare per il perseguimento dei propri fini istituzionali, implementano forme di interoperabilità o addirittura condividono alcune delle risorse informatiche o degli ambienti in cui queste sono dispiegate (ad esempio il datacenter di Regione Toscana denominato TIX); pertanto si richiede di implementare adeguate policy di sicurezza su servizi, credenziali e dati afferenti agli ambienti di tutti gli enti coinvolti nel progetto, tramite lo svolgimento di alcune attività specialistiche di verifica e controllo in ambito sicurezza informatica (compromise assessment, active directory assessment, password strenght assesment, dark web assesment), nell'ottica di condividere tali migliori pratiche e conseguire un livello omogeneo di sicurezza, almeno in alcuni ambiti specifici;
- sono necessari nuovi apparati di protezione, configurazioni di sicurezza e prevedere interventi in alcuni ambiti specifici per condividere una visione organica della cybersicurezza negli Enti coinvolti e identificare ed attuare azioni coordinate, omogenee e condivise per garantire la protezione automatizzata e duratura di servizi ed infrastrutture digitali, nonché l’integrità e confidenzialità del patrimonio informativo delle Amministrazioni interessate;
- gli interventi sopra elencati sono oltretutto attività in risposta e motivati dall'attuazione di quanto richiesto nel Piano Triennale per l'Informatica nella Pubblica Amministrazione, dalle Misure Minime di Sicurezza ICT per le pubbliche amministrazioni, dalle linee guida e dalle circolari emanate dall'Agenzia per l'Italia Digitale (AgID), prima, e da ACN, adesso;

Considerato che si rende necessario individuare, definire ed implementare soluzioni tecnologiche per

rafforzare la cybersicurezza di processi, risorse e servizi e applicazioni necessari per il perseguimento dei fini istituzionali, ponendo gli enti in condizione di fronteggiare adeguatamente il rischio cyber nel prossimo futuro;

Preso atto che, in base alle valutazioni tecniche condotte con i referenti dei diversi enti, le soluzioni individuate sono Firewall NGFW (Next Generation FireWall) e Anti -APT (Advanced Persistent Threat), come meglio descritte nel parere tecnico del 03/07/2024 ns prot.227463, allegato al presente provvedimento;

Visto l'articolo 1 comma 512 ss. della legge 28 dicembre 2015, n. 208 che obbliga il ricorso agli strumenti di acquisto e di negoziazione disponibili su Consip e soggetti aggregatori per procedere all'acquisizione dei servizi informatici;

Rilevato che le soluzioni tecnologiche idonee a soddisfare le esigenze sopra descritte erano presenti nell'Accordo Quadro (AQ) CONSIP con ID 2367 – Lotto 3 PAL Centro Sud, a cui non è stato possibile aderire in quanto il massimale a disposizione è stato esaurito; pertanto, è stata effettuata un'ulteriore ricerca su MEPA (Mercato Elettronico della Pubblica Amministrazione) per reperire i prodotti in questione, che risultano disponibili con i seguenti codici prodotto e quantità, ad un prezzo anche inferiore a quanto previsto nell'AQ CONSIP ID 2367:

- cod. MM-99920-FPR2110-BUN - mod. CISCO-FPR2110 – Q. tà 4 per € 20.152,00;
- cod. MM-99920-FPR2130-BUN – mod. CISCO- FPR2130 – Q. tà 2 per € 24.030,00;
- cod. MM-99920-AXZZE5XL-B1 – mod. TRENDMICRO Deep, Discovery Analyzer e Deep Discovery Inspector – Q. tà 4 per € 85.268,00.

come meglio dettagliati nelle schede prodotto MEPA, allegate quali parti integranti al presente provvedimento;

Dato atto che è necessario acquistare i suddetti apparati e che l'offerta è ritenuta economicamente congrua e tecnologicamente vantaggiosa, come da parere tecnico del 03/07/2024 ns prot.227463;

Ritenuto pertanto necessario ricorrere all'affidamento diretto, ai sensi dell'art. 50, comma 1, lett. b) del D. Lgs. 36/2023, utilizzando lo strumento telematico MEPA (Mercato Elettronico della Pubblica Amministrazione) mediante ordine diretto di acquisto e di affidare alla società MATICMIND SPA con sede in via Roberto Bracco 6, 20159 (MI) – P. IVA 05032840968 la fornitura dei suindicati apparati e dispositivi di sicurezza informatica per un importo totale di € 129.450,00 IVA esclusa, pari a € 157.929,00 IVA inclusa;

Dato atto che

- trattandosi di appalto d'importo inferiore ad € 140.000 e, fermi restando gli obblighi di utilizzo di strumenti di acquisto e di negoziazione previsti dalle vigenti disposizioni in materia di contenimento della spesa, questa Amministrazione può, ai sensi dell'art. 62, comma 1, del D. Lgs. 36/2023, procedere direttamente e

autonomamente all'acquisizione della fornitura in oggetto;

- l’art. 50, comma 1, lett. b del D. Lgs. 36/2023 stabilisce che per gli affidamenti di contratti di servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo inferiore a € 140.000, si debba procedere ad affidamento diretto, anche senza consultazione di più operatori economici;

Considerato che è intenzione di questa amministrazione perseguire i principi definiti dal Codice dei contratti pubblici (Libro I, Parte I) e in ossequio a quanto previsto dall'art.25 del D. Lgs. 36/2023 avvalersi a tal fine degli strumenti di acquisto e di negoziazione disponibili su Consip e soggetti aggregatori;

Ritenuto pertanto opportuno di affidare alla società MATICMIND SPA, con sede in via Roberto Bracco 6, 20159 (MI) – P. IVA 05032840968, la fornitura di apparati e dispositivi di sicurezza informatica per gli Enti partecipanti al progetto Metrowide - Avviso 3/2022 della Agenzia per la Cybersicurezza Nazionale - Piano Nazionale di Ripresa e Resilienza (PNRR) Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” finanziato dall’Unione europea – Next generation EU – Progetto Metrowide - CUP H11C22001670006 – CIG B261E74FC8, per un importo di € 129.450,00 IVA esclusa, pari a € 157.929,00 IVA inclusa;

Dato atto che

- non sussiste nel presente affidamento un interesse transfrontaliero certo;
- è rispettato il principio di rotazione ex art.49 del D. Lgs. 36/2023;
- la spesa suddetta grava sul Capitolo 59936 – codice opera 230106
- che il CIG è B261E74FC8;
- che il CUP è H11C22001670006;
- della regolarità tecnica del presente provvedimento e della congruità della spesa;
- dell’avvenuta verifica della regolarità contributiva ed assicurativa ai sensi della normativa vigente in materia di DURC – Documento Unico di Regolarità Contributiva;
- l’art. 15 del D. Lgs. n. 36/2023 prevede la nomina del Responsabile Unico del Progetto anche per gli appalti relativi a forniture e servizi, e che, pertanto, con atto del 31/05/2024 ns prot. 187455 è stato nominato quale Responsabile Unico del Progetto, il sottoscritto Dirigente del Servizio Sicurezza, Infrastruttura e Architettura IT dell’Ente, il quale dichiara con nota del 06/08/2024 ns prot. 265817, che non sussistono conflitti di interesse che lo riguardano in relazione all’oggetto dell’affidamento e dell’affidatario;

Preso atto della nomina del gruppo di supporto al RUP per l’esecuzione del contratto del 31/05/2024 ns prot. 187455, i cui componenti dichiarano che non sussistono conflitti di interesse che li riguardano in relazione all’oggetto dell’affidamento né nei confronti dell’affidatario;

Individuato in Maurizio Marini della E.Q. Data Center, Sistemi e Cloud, la figura che per competenze

professionali meglio può svolgere il compito di Direttore dell'esecuzione del contratto (DEC) in oggetto, come da nomina del gruppo di supporto al RUP già citata;

Visto l'art. 53 comma 4 del D. Lgs. 36/2023 che in relazione ai contratti di importo inferiore alle soglie di rilevanza europea, attribuisce la facoltà alla stazione appaltante, in casi debitamente motivati, di non richiedere la garanzia definitiva per l'esecuzione dei contratti di cui alla Parte I del codice;
- il parere del Presidente dell'Anac n. 3541/2023 con cui si ritiene di non potere escludere che l'articolo 53, comma 4, del decreto legislativo n. 36 del 2023, consenta di addurre il miglioramento del prezzo come motivazione alla base dell'esonero dalla prestazione della garanzia definitiva;

Rilevato che l'affidamento a Maticmind SpA si concretizza nella fornitura di apparati hardware dedicati per fornire soluzioni di protezione informatica per la durata prevista contrattualmente che si può rilevare in modo certo e che sarà immediatamente verificabile dal portale del produttore stesso;

Dato atto che, una volta attivati gli apparati, le successive ed eventuali interazioni sui sistemi avverranno con i produttori degli apparati stessi, non con il partner se non in modalità solo accidentale e residuale;
- che gli apparati previsti in fornitura sono prodotti da Cisco e Trend Micro, cioè aziende multinazionali che esistono da oltre 30 anni sul mercato, quindi di comprovata stabilità ed affidabilità nel mondo ICT e anche la stessa Maticmind SpA è presente sullo stesso mercato da circa 20 anni;

Pertanto, in considerazione di quanto sopra, della natura della fornitura e della società affidataria che ha già collaborato in numerose occasioni con questa stazione appaltante non vi è motivo di credere che disattenderà alle prestazioni richieste e non si ravvedono gli estremi per richiedere la cauzione;

Preso atto che, in sede di verifica dei requisiti di ordine generale, l'Agenzia delle Entrate Direzione Provinciale di Milano con pec del 01/08/2024 ns prot. 260958 ha dato riscontro attestante la presenza di una violazione non definitivamente accertata a carico dell'affidatario risultante dal Sistema Informativo dell'Anagrafe Tributaria;

Dato atto che la società Maticmind con la presentazione del DGUE e delle altre dichiarazioni, ha dichiarato quanto emerso in sede di verifica con l'Agenzia delle Entrate presentando altresì le proprie osservazioni e controdeduzioni in merito al debito tributario;

Valutate tali osservazioni e controdeduzioni e preso atto che nessuna contestazione al momento è giunta in sede giudiziaria al giudizio definitivo;

Vista la giurisprudenza del Consiglio di Stato, sia pure pronunciatosi nell'ambito del vecchio Codice (D.Lgs 50/2016), secondo cui: "*la rilevata sussistenza a carico dell'operatore economico di "violazioni non definitivamente accertate", pur se quantitativamente superiori alla soglia di gravità fissata dal legislatore ai*

fini della loro rilevanza escludente, rapportata come si è visto al valore dell'appalto (siccome "pari o superiore al 10%" dello stesso), non genera un effetto espulsivo automatico, ma subordinato ad una espressa e motivata valutazione espressa dalla stazione appaltante in ordine alla sua incidenza negativa sulla affidabilità del concorrente" (cfr. Consiglio di Stato, sez. III, sentenza del 24 luglio 2023, n. 7219);

Rilevato pertanto che la Stazione Appaltante, dopo aver accertato la gravità delle violazioni non definitivamente accertate, è tenuta ad effettuare due ulteriori valutazioni: una sulla moralità del concorrente e l'altra relativa alla sua "*capacità di fare fronte agli oneri economici connessi alla esecuzione dell'appalto, tenuto conto, da un lato, dell'esposizione debitoria da cui è gravato nei confronti dell'Erario* [...] *dall'altro lato, della sua dimostrata inclinazione a non assolvere gli obblighi assunti (o, come per quelli di carattere fiscale, generatisi ex lege a suo carico)*".

Considerato che la società ha dimostrato di essere finanziariamente e professionalmente solida in numerose occasioni con questa appaltante, oltre ad essere tuttora anche affidataria in RTI di diverse convenzioni/accordi quadro CONSIP (ID 2367, 2181, ...), si ritiene di poter comunque procedere con l'affidamento in questione;

Visto l'art. 28 del D. Lgs. 36/2023 che prevede l'obbligo di pubblicazione e aggiornamento di tutti gli atti relativi alle procedure di affidamento di appalti pubblici di servizi, forniture, lavori e opere sul profilo del committente e nella sezione "Amministrazione trasparente", con l'applicazione delle disposizioni di cui al decreto legislativo 14 marzo 2013, n. 33;

Visti

- il D. Lgs. 36/2023;

- gli artt. 107 – 183 e 192 del D. Lgs. 267/2000;

- il vigente Regolamento per l'attività contrattuale;

- l'art. 81, comma 3, dello Statuto del Comune di Firenze;

Ravvisata la propria competenza ai sensi dell'art. 58 dello Statuto del Comune di Firenze, nonché l'art. 21 del Regolamento sull'Ordinamento dei Servizi e degli Uffici;

DETERMINA

Per le motivazioni espresse in narrativa, che integralmente si richiamano:

1) di approvare il Piano acquisti, allegato al presente provvedimento quale parte integrante, relativo al Codice Opera 230106, il cui importo complessivo ammonta a € 158.600,00, IVA inclusa – CUP H11C22001670006;

2) di affidare, in attuazione dell'Avviso 3/2022 della Agenzia per la Cybersicurezza Nazionale - Piano Nazionale di Ripresa e Resilienza (PNRR) Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" finanziato dall'Unione europea – Next generation EU – Progetto Metrowide - CUP H11C22001670006, la fornitura di apparati e dispositivi di sicurezza informatica per gli Enti partecipanti al progetto Metrowide alla società **MATICMIND SPA** con sede in via Roberto Bracco 6, 20159 (MI) – P. IVA 05032840968 per una spesa complessiva di € **157.929,00 IVA inclusa**, come da schede prodotto MEPA allegate al presente provvedimento quali parti integranti - **CIG B261E74FC8**;

3) di sub impegnare a favore di MATICMIND SPA (codice beneficiario **37584**) la somma complessiva di € 157.929,00 IVA inclusa per l'affidamento di cui al precedente punto 1) sul Capitolo 59936 - Impegno 2024/7102 - Codice opera 230106 – CUP H11C22001670006;

4) di dare atto che il RUP è il sottoscritto Ing. Luca Bertelli Dirigente del Servizio Sicurezza Infrastruttura e Architettura IT dell'Ente della Direzione Sistemi Informativi, come da atto di nomina sopra indicato, il quale dichiara che non sussistono conflitti di interesse che lo riguardano in relazione all'oggetto dell'affidamento e dell'affidatario

5) di pubblicare la presente Determinazione Dirigenziale nella sezione Amministrazione Trasparente e nel Profilo del Committente del sito web Comune di Firenze

ALLEGATI INTEGRANTI

20240703_PROT. 227463 _Parere Metrowide IDS-IPS-AntiAPT_signed - 2c054403d86ba2f66c922f81078ee155ee24519c4f12138ae5e35a1aa8e8a501
Piano acquisti cod. op. 230106_signed - 2b4077e5792bd83d7449757c80148866befcc666bbbf22b4ea3c2b1b5d119a14
Scheda MEPA_prodotto AXZZE5XL.pdf - 698abdd0cf1f02939a4e8ff432f14eb97b9e7e29a9a381d4648d941c82cdd7e5
Scheda MEPA_prodotto FPR2130.pdf - 01a4c7009f192b6394fc575a6e266aac966574299331a42147a90b7364bd1d8e
Scheda MEPA_prodotto_FPR2110 (2).pdf - e5c059770072185bc32fc8ad12c32de16c5701d8ae57dd527d052c39c9c02759

Sottoscritto digitalmente da

Responsabile regolarità tecnica
Luca Bertelli

Elenco Movimenti

N°	Tipo Mov.	Esercizio	Capitolo	Articolo	Impegno/ Accertamento	Sub Impegno/Sub Accertamento	Importo	Beneficiario
1)	U	2024	59936		2024/7102	1	€ 157.929,00	37584 - MATICMIND S.P.A.

VISTO DI REGOLARITÀ CONTABILE ATTESTANTE LA COPERTURA FINANZIARIA

Responsabile Ragioneria