CITTA' DI TORINO

DIPARTIMENTO SERVIZI INTERNI
DIVISIONE SISTEMI INFORMATIVI
S. INFRASTRUTTURE E CYBERSECURITY

ATTO N. DD 3516 **Torino, 27/06/2023**

DETERMINAZIONE DIRIGENZIALE

OGGETTO: PNRR – MISURA M1C1 - DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA - INVESTIMENTO 1.5 "CYBERSECURITY" - NUOVA ADESIONE AD ACCORDO QUADRO CONSIP PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PA - ID 2296 LOTTO 2 - SERVIZI DI COMPLIANCE E CONTROLLO PA LOCALI - APPROVAZIONE DEL PIANO OPERATIVO E AUTORIZZAZIONE ALLA STIPULA DEL CONTRATTO ESECUTIVO PER € 893.534,10 (IVA 22% COMPRESA) - CUP C17H22002830006 E CUP C17H22002840006 CIG PADRE 8884642E81 CIG DERIVATO 9816963E22 - FINANZIATO DALL'UNIONE EUROPA - NEXTGENERATIONEU.

Premesso che:
- 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», pubblicato nella Gazzetta Ufficiale della Repubblica Italiana il 24 settembre 2021, n. 229, ha individuato la Presidenza del Consiglio dei ministri quale amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante «Cybersicurezza».
- L'Agenzia per la Cybersicurezza Nazionale, in qualità di Soggetto Attuatore della misura, ha pubblicato l'Avviso Pubblico n. 03/2022 con il quale si prevedeva la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane e delle Province autonome a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5 finanziato dall'Unione Europea – NextGenerationEU.Visto il comma 512 dell'art. 1 della L. 208/2015 (legge di stabilità 2016) che prevede che le amministrazioni pubbliche provvedano ai propri approvvigionamenti di beni e servizi informatici tramite Consip S.p.A., principio formalmente ribadito anche dall'Amministrazione;

Alla luce di tale Avviso di invito a manifestare interesse per la selezione di proposte di intervento

come sopra descritte, la Città di Torino ha inoltrato, in data 14/10/2022, domanda di partecipazione per l'Investimento 1.5 “Cybersecurity” e, a seguito dell’istruttoria della domanda di partecipazione, è stata emanata la Determina di Approvazione (N. Registro 3429.20-01-2023.I) della Graduatoria Finale del Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri, con la quale è stato approvata la graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziabili presentate dai Comuni in adesione all’Avviso, e dalla quale risulta l'ammissione al finanziamento del Comune di Torino per entrambi i progetti presentati, assegnato in data 25 gennaio 2023, Ns. Prot. n. 88 del 25 gennaio 2023, per un totale di € 1.990.200,00.

Dato atto inoltre che in riferimento al paragrafo n. 5.2 “Spese ammissibili” dell’Avviso pubblico recante “Avviso Pubblico per la presentazione di proposte per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity”M1C1I1.5”, si specifica che il Soggetto attuatore dell’intervento potrà presentare esclusivamente costi strettamente connessi allo svolgimento delle attività previste nel Piano di Progetto coerenti e pertinenti con le finalità dell’intervento 1.5, Missione M1C1, e successivamente comprovabili con opportuna documentazione giustificativa.

Con Deliberazione n. 74 del 21/02/2023 la Città di Torino prendeva atto dell'ammissione al finanziamento nell'ambito del PNRR M1C1 - Digitalizzazione, Innovazione e Sicurezza nella PA” - Investimento 1.5 "Cybersecurity", dei due progetti denominati “Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino” - CUP C17H22002830006 - per euro 995.100,00 e “Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino” - CUP C17H22002840006 - per euro 995.100,00; con la stessa Deliberazione sono stati approvati gli schemi di Atto d'Obbligo, uno per ciascuna progettualità, con i quali la Città si impegna a garantire il rispetto dei tempi, delle modalità e degli obblighi relativi all'attuazione delle proposte progettuali. Gli atti d’obbligo sono stati successivamente sottoscritti dal Sindaco in data 08/03/2023.

La Città di Torino, come ogni Ente di medio-grandi dimensioni, si trova a fronteggiare ogni giorno decine di migliaia di attacchi informatici, per lo più automatici, ma talora anche mirati e preparati con competenza e risorse dedicate. Per questo, da alcuni anni la Città investe sulla sicurezza del sistema informativo nel suo complesso, a partire dalla rete e dalla server farm che ospita gli applicativi e i data base centrali, ma senza trascurare la cosiddetta periferia del sistema, ossia le postazioni di lavoro e le aree condivise.

Nel corso del 2022, il Comune di Torino ha avviato una serie di interventi finalizzati al miglioramento della postura di sicurezza. Tali iniziative si inseriscono nel contesto dell’adesione al sopracitato "Avviso pubblico per la presentazione di proposte di interventi di potenziamento della resilienza 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” M1C1I1.5. WP-9";

Come parte integrante di uno dei due progetti è stato eseguito un assessment in ambito Cybersecurity effettuato nel periodo compreso tra Novembre e Dicembre 2022 e relativo alla valutazione dello stato di maturità della sicurezza delle informazioni nell’Ente, con principale focus sui processi trasversali del Comune e con un approfondimento verticale su tre ambiti di servizi al cittadino. Sono quindi emerse una serie di azioni prioritarie da indirizzare con priorità al fine di definire un programma sulla sicurezza delle informazioni ed innalzare il livello di maturità in ambito Cyber dell’Ente. Le azioni riguardano principalmente la definizione e redazione di regolamenti, politiche e procedure per la formalizzazione dei processi di sicurezza individuati,

nonché interventi atti a migliorare le competenze digitali degli utenti e la capacità di reazione a situazioni di emergenza.

Per la Città di Torino, aumentare il know-how e la consapevolezza sui rischi inerenti alla propria organizzazione e ai propri servizi riveste un'importanza centrale, così come programmare le azioni da attuare per mitigare i rischi e per contrastare eventi di cybercrime.

In tale contesto l'Ente si propone di attuare degli interventi finalizzati all'incremento complessivo e progressivo del livello di sicurezza della Città, in coerenza con quanto previsto dalle linee di azione indicate nel Piano Triennale AgID per la PA e finalizzati a contrastare il costante aumento delle minacce informatiche, anche in considerazione degli accadimenti che hanno avuto risvolti sulle PA italiane.

L'obiettivo principale del Comune di Torino è la realizzazione delle azioni di rimedio identificate nell'ambito del Piano strategico e della Roadmap evolutiva delle iniziative in ambito Cybersecurity definite a seguito dell'assessment trasversale sulla Cyber Posture effettuato e in accordo con i Piani di Progetto approvati dall'Agenzia Nazionale per la Cybersicurezza e finanziati con fondi del PNRR.

Le misure nazionali a favore della cyber-security rappresentano un tassello della più complessa vision di un unico mercato digitale che assicuri un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione, adottato come criterio ispiratore della Direttiva NIS. In ottemperanza agli obblighi imposti a livello sovranazionale dall'art. 7 Direttiva NIS (Direttiva (UE) 2016/1148 secondo cui "Ogni Stato membro adotta una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi che definisce gli obiettivi strategici e le opportune misure strategiche e regolamentari al fine di conseguire e mantenere un livello elevato di sicurezza delle reti e dei sistemi informativi e contempla almeno i settori di cui all'allegato II e i servizi di cui all'allegato III", rispettivamente, di Operatori di Servizi Essenziali (OSE) e di Fornitori di Servizi Digitali (FSD), il legislatore nazionale è di recente intervenuto, con il Decreto Legge n. 105/2019, per definire il perimetro di sicurezza nazionale cibernetica.

Visto il D.L. 77/2021 che considera la cyber security delle PP.AA.un asset fondamentale a servizio della digitalizzazione del Paese;

Visto l'Accordo Quadro art. 54, comma 3, del d. lgs. n. 50/2016 e s.m.i., stipulato da Consip avente ad oggetto "L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - ID Sigef 2296 - Lotto 2 Servizi di Compliance e Controllo" - rientrante nel Piano delle Gare Strategiche ICT, e previsto da AgID per l'acquisizione di servizi in conformità con le disposizioni dell'attuale Piano Triennale ICT e con le normative in materia di Cybersecurity di riferimento e l'adeguamento alle dinamiche evolutive, utilizzando la tecnologia per accompagnare il processo di trasformazione digitale della PA. Nello specifico l'Accordo Quadro prevede per il Lotto 2 i seguenti servizi:

- L2.S16 Security Strategy
- L2.S17 Vulnerability Assessment
- L2.S18 Testing del codice – Statico
- L2.S19 Testing del codice – Dinamico
- L2.S20 Testing del codice – Mobile
- L2.S21 Supporto all'analisi e gestione degli incidenti
- L2.S22 Penetration Testing
- L2.S23 Compliance normativa

Tenuto conto che, tale Accordo è stato stipulato da Consip con vari Raggruppamenti aggiudicatari della procedura aperta medesima e che il Lotto di interesse per questa Amministrazione è il nr. 2 per i servizi di Compliance e controllo con durata di 24 (ventiquattro) mesi con decorrenza 01 settembre 2022 e scadenza il 31 agosto 2024, termine ultimo entro il quale si potrà affidare il Contrattio Attuativo;

Preso atto dell'aggiudicazione da parte di CONSIP del Lotto 2 per le Amministrazioni Locali alla RTI costituendo Deloitte Risk Advisory S.r.l. - EY Advisory S.p.A. - Tele-co S.r.l. (mandataria Deloitte Risk Advisory S.p.A. Partita IVA: 05059250158; in qualità di mandanti EY Advisory S.p.A.: Partita I.V.A.: 13221390159 e TELECO S.R.L.: Partita I.V.A.: 02856220922);

Premesso che:
- Con determinazione a contrarre n. DD 2988 del 06/06/2023 veniva autorizzato l'espletamento delle fasi procedurali propedeutiche alla nuova adesione del Comune di Torino all' Accordo Quadro avente ad oggetto "L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI– ID 2296" - CIG PADRE 8884642E81 CIG DERIVATO 9816963E22, stipulato da CONSIP con il Raggruppamento Temporaneo di Imprese (di seguito "R.T.I." o "Fornitore") costituito da Deloitte Risk Advisory S.r.l. in qualità di mandataria, EY ADVISORY S.p.A. e Teleco S.r.l., in qualità di mandanti, Partita IVA: 05059250158, per l'acquisto con Ordine Diretto di SERVIZI DI COMPLIANCE E CONTROLLO;
- Con la suddetta determinazione dirigenziale n. DD 2988/23 si è proceduto all'indizione e alla prenotazione di impegno di spesa presunto, per l'affidamento, di Euro 893.534,10 (IVA 22% COMPRESA) che provvedeva, inoltre, a imputare la somma sui capitoli di spesa rispettivamente per ciascuno dei 2 CUP così come segue:
- CUP C17H22002830006 capitolo rubricato "PNRR-M1 C1 I1.5 CYBERSECURITY ANALISI DELLA POSTURA DI SICUREZZA E MIGLIORAM. NELLA GESTIONE DEI PROCESSI LEGATI ALLA CIBERSECURITY DELLA CITTA' DI TORINO C17H22002830006 VEDASI 046500057 E set. 027";
- CUP C17H22002840006 capitolo di spesa rubricato "PNRR-M1 C1 I1.5 CYBERSECURITY INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZ. DEL RISCHIO NELLA CITTA' DI TORINO C17H22002840006 VEDASI 046500056 E set. 027";

Considerato inoltre che i servizi che verranno attivati - e che verranno remunerati a corpo - dettagliatamente indicati al punto 4.3) "Dettaglio dei servizi richiesti" del Piano Operativo (All.1) sono i seguenti:

- Security Strategy - codice servizio: L2.S16 e nello specificio prevede:
  - Integrazione del Piano strategico e Roadmap iniziative evolutive Cyber, con l'obiettivo di fornire alla Città un Piano Strategico in ambito Cybersecurity, che, a partire dagli obiettivi definiti nella propria strategia digitale, descriva le linee evolutive previste per la Sicurezza Informatica dell'Ente. L'acquisizione del servizio prevede l'esecuzione delle attività di un assessment verticale su altri ambiti verticali (fino a 6) finalizzato all'identificazione delle ulteriori iniziative da integrare nel piano strategico dell'Ente in ambito sicurezza delle informazioni.
  - Definizione e redazione corpo documentale, con l'obiettivo di fornire alla Città un framework documentale coerente con i gap identificati durante l'assessment svolto. In particolare, si prevede di definire e revisionare i principali processi in ambito Cybersecurity del Comune con formalizzazione di relativi manuali, politiche e procedure;
  - Definizione e misurazione indicatori in ambito sicurezza delle informazioni, con l'obiettivo di

munire la Città di Torino di un framework di KPI fruibili per il monitoraggio delle performance e per il raggiungimento degli obiettivi rispetto al piano definito.

- Supporto all'analisi e gestione degli incidenti - codice servizio: L2.S21 e nello specifico prevede:
  - Modello e processi di gestione della crisi ICT, attraverso attività di aggiornamento delle procedure di escalation e del modello organizzativo di gestione delle crisi con riferimento ad ulteriori scenari;
  - Simulazione Table Top, attraverso l'esecuzione di una simulazione di incident in modalità table-top;
  - Revisione del processo di Rilevazione e risposta agli incidenti, attraverso la revisione del modello di gestione e risposta agli incidenti.

- Penetration Testing - codice servizio: L2.S22 e nello specificio prevede:
  - Esecuzione del Penetration test sull'infrastruttura e sui servizi dell'Ente fino ad un massimo di 6 Target, con l'obiettivo di verificare concretamente la possibilità di sfruttare le eventuali vulnerabilità identificate su sistemi/reti/applicazioni/dispositivi dell'Amministrazione

Considerato che i servizi sopracitati vengono dettagliatamente quantificati al punto 4.2) del Piano Operativo così come segue:
- Progetto "Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino" - CUP C17H22002830006: euro 660.326,00 oltre IVA al 22% per un totale complessivo di euro 805.597,72 per le forniture di servizi L2.S16 Security Strategy, L2.S21 Supporto all'analisi e gestione degli incidenti ed L2.S22 Penetration Testing;

- Progetto "Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino" - CUP C17H22002840006: euro 72.079,00 oltre IVA al 22% per un totale complessivo di euro 87.936,38 per le forniture di servizi L2.S16 Security Strategy ed L2.S22 Penetration Testing;

Tenuto conto che i CUI per i 2 progetti sono rispettivamente:
- CUP C17H22002830006 "Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino" CUI S00514490010202300297;
- CUP C17H22002840006 "Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio" CUI S00514490010202300298;

Considerato che al punto 4. dell'Allegato B - Piano di Progetto - dell'Avviso viene fornito il dettaglio delle tipologie di spese ammissibili, tra le quali sono previste spese generali e altri costi di esercizio direttamente imputabili all'attività progettuale nella misura pari al 7% di costi diretti ammissibili ai sensi dell'art. 54 lett. a del Reg. (UE) 2021/1060;

Considerato che si rispetta il dettato di cui all'art. 183 comma 6 del D.Lgs.267/2000 TUEL. Nello specifico, le funzioni del suddetto servizio sono da considerarsi fondamentali, ai sensi dell'art. 14 comma 27 del D.L. 78/2010. Tale norma individua, tra le principali funzioni, alla lettera a) "organizzazione generale dell'amministrazione.." all'interno della quale il suddetto servizio è da considerarsi necessario per il funzionamento delle iniziative che consentiranno di aumentare la capacità di gestione dei processi aventi impatto sulla sicurezza delle informazioni dell'Ente, con conseguente riduzione dei rischi cyber inerenti alla propria organizzazione e derivanti dagli attacchi informatici, nonché aumentare di conseguenza il livello di resilienza alle minacce e si sottoscriverà pertanto contratto pluriennale;

Tenuto conto della Deliberazione della Corte dei Conti – Sezione Regionale di Controllo per il Piemonte - prot. 54/2021/SRCPIE/INPR del 10/03/2021, si attesta che l'affidamento previsto dal presente provvedimento non è assimilabile alla fattispecie dell'incarico esterno di studio, ricerca e consulenza come indicata dall'art. 1 commi 9, 56, 57 e 173 della Legge 266/2005 e dall'articolo 7 comma 6 del D. Lgs n. 165/2001, bensì a quella della prestazione di servizi, in quanto non è destinato a fornire supporto conoscitivo-esperienziale all'amministrazione conferente, in vista di decisioni da assumere o di progetti da realizzare, bensì a coprire necessità di prestazioni autosufficienti nell'iter procedimentale, che non possono essere svolte da personale interno;

Occorre ora procedere all'approvazione del Piano Operativo e contestuale autorizzazione alla stipula del Contratto Esecutivo con il Fornitore.

Tutto ciò premesso,

IL DIRIGENTE

- Visto l'art. 107 del Testo Unico delle leggi sull'Ordinamento degli Enti Locali, approvato con D.Lgs 18 agosto 2000 n. 267
- Visto l'art. 74 dello Statuto della Città;
- Visti gli artt. 182, 183 e 191 del D.Lgs. 267/2000 e s.m.i.;
- Visto l'art. 3 del D. Lgs 118/2011 e s.m.i.;
- Richiamato il principio contabile della gestione finanziaria di cui all'allegato 4/2 del D.Lgs. 118/2011 e s.m.i.;
- Visto il vigente Regolamento comunale di contabilità armonizzata;
- Nell'ambito delle risorse finanziarie assegnate;

DETERMINA

1. di approvare, per i motivi indicati in premessa, il Piano Operativo (n. ns prot. 505 del 16/06/2023), allegato al presente provvedimento di cui forma parte integrante (All. 1), presentato dal Raggruppamento Temporaneo di Imprese composto dalle aziende Deloitte Risk Advisory S.r.l. (mandataria capo-gruppo), EY ADVISORY S.p.A. e Teleco S.r.l., sulla base del Piano dei Fabbisogni a suo tempo inviato relativo al Lotto 2 dell'Accordo Quadro stipulato tra CONSIP S.p.A. e lo stesso RTI , per l'acquisto con Ordine Diretto di SERVIZI DI COMPLIANCE E CONTROLLO - CIG primario: 8884642E81 – CIG derivato: 9816963E22;
2. di dare atto che il Responsabile Unico del Procedimento è il Dott. Massimo MASSIMINO, Dirigente della Divisione Infrastrutture e Cybersecurity;
3. di procedere conseguentemente alla stipula del relativo Contratto Esecutivo, per un importo complessivo della fornitura di servizi di Euro 732.405,00 (= IVA ESCLUSA), per un importo complessivo di Spesa di Euro 893.534,10 (= IVA 22% COMPRESA) che trova copertura nella somma prenotata con la DD 2988/2023;
4. si dà atto che si rispetta il dettato di cui all'art. 183 comma 6 del D.Lgs.267/2000 TUEL. Nello specifico, le funzioni del suddetto servizio sono da considerarsi fondamentali, ai sensi dell'art. 14 comma 27 del D.L. 78/2010. Tale norma individua, tra le principali funzioni, alla lettera a)

"organizzazione generale dell'amministrazione.." all'interno della quale il suddetto servizio è da considerarsi necessario per il funzionamento delle iniziative che consentiranno di aumentare la capacità di gestione dei processi aventi impatto sulla sicurezza delle informazioni dell'Ente, con conseguente riduzione dei rischi cyber inerenti alla propria organizzazione e derivanti dagli attacchi informatici, nonché aumentare di conseguenza il livello di resilienza alle minacce e si sottoscriverà pertanto contratto pluriennale;

5. di attestare, tenuto conto della Deliberazione della Corte dei Conti – Sezione Regionale di Controllo per il Piemonte - prot. 54/2021/SRCPIE/INPR del 10/03/2021, che l'affidamento previsto dal presente provvedimento non è assimilabile alla fattispecie dell'incarico esterno di studio, ricercae consulenza come indicata dall'art. 1 commi 9, 56, 57 e 173 della Legge 266/2005 e dall'articolo 7 comma 6 del D. Lgs n. 165/2001, bensì a quella della prestazione di servizi, in quanto non è destinato a fornire supporto conoscitivo-esperienziale all'amministrazione conferente, in vista di decisioni da assumere o di progetti da realizzare, bensì a coprire necessità di prestazioni autosufficienti nell'iter procedimentale, che non possono essere svolte da personale interno;
6. di dare atto:

- dell'avvenuto accertamento dell'insussistenza di situazioni di conflitto di interessi inerenti il presente procedimento, in attuazione dell'art. 6bis della L. 241/1990 e s.m.i. nonché ai sensi dell'art. 42 del D.Lgs. 50/2016;
- che il seguente provvedimento non è soggetto alla validazione della Divisione Economato come da circolare n. 4650 del 20 ottobre 2011;
- che ai sensi della circolare prot. n. 9649 del 26/11/2012 il presente provvedimento non comporta oneri di utenza;
- che la presente determinazione è stata sottoposta al controllo di regolarità amministrativa ai sensi dell'art. 147-bis TUEL e che con la sottoscrizione si rilascia parere di regolarità tecnica favorevole;
- che il presente provvedimento è rilevante ai fini della pubblicazione nella sezione "Amministrazione Trasparente";
- ai sensi della circolare prot. n.16298 del 19/12/2012 il presente provvedimento non è pertinente alle disposizioni in materia di valutazione dell'impatto economico (VIE);
- che l'esigibilità dell'obbligazione avverrà entro il 31/12 di ogni esercizio finanziario interessato.

Dettaglio economico-finanziario

La spesa di Euro 893.534,10 trova capienza nelle somme prenotate con n. DD 2988/2023 con le seguenti imputazioni:
- di cui euro 805.597,72 per progetto "Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino" - CUP C17H22002830006 - :

Importo	Anno Bilancio	Missione	Programma	Titolo	Macro Aggregato	Capitolo Articolo	Servizio Responsabile	Scadenza obbligazione
245.773,80 559.823,92	2023 2024	01 01	08 08	2 2	02 02	118660005001 118660005001	027 027	31/12/2023 31/12/2024

Descrizione capitolo e articolo	PNRR-M1 C1 I1.5 CYBERSECURITY ANALISI DELLA POSTURA DI SICUREZZA E MIGLIORAM. NELLA GESTIONE DEI PROCESSI LEGATI ALLA CIBERSECURITY DELLA CITTA' DI TORINO C17H22002830006 VEDASI 046500057 E set. 027
Conto Finanziario n°	Descrizione Conto Finanziario
U.2.02.03.02.001	Sviluppo software e manutenzione evolutiva

- di cui euro 87.936,38 per progetto “Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino” - CUP C17H22002840006:

Importo	Anno Bilancio	Missione	Programma	Titolo	Macro Aggregato	Capitolo Articolo	Servizio Responsabile	Scadenza obbligazione
26.380,91 61.555,47	2023 2024	01 01	08 08	2 2	02 02	118660004001 118660004001	027 027	31/12/2023 31/12/2024
Descrizione capitolo e articolo		PNRR-M1 C1 I1.5 CYBERSECURITY INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZ. DEL RISCHIO NELLA CITTA' DI TORINO C17H22002840006 VEDASI 046500056 E set. 027						
Conto Finanziario n°		Descrizione Conto Finanziario						
U.2.02.03.02.001		Sviluppo software e manutenzione evolutiva						

Tali spese trovano capienza nei fondi accertati con D.D. 1585 del 03/04/2023:

ACCERTAMENTO 3410/2023:

Importo	Anno Bilancio	Titolo	Tipologia	Categoria	Capitolo e articolo	Responsabile Servizio	Scadenza Obbligazione
245.773,80	2023	4	0200	01	046500057001	068	31/12/2023
Descrizione capitolo e articolo		PNRR-M1 C1 I1.5 CYBERSECURITY ANALISI DELLA POSTURA DI SICUREZZA E MIGLIORAM. NELLA GESTIONE DEI PROCESSI LEGATI ALLA CYBERSECURITY DELLA CITTA' DI TORINO C17H22002830006 VEDASI CAP. 118660005 SPESA - Resp. E SETT, 068					
Conto Finanziario n°		Descrizione Conto Finanziario					
E.4.02.01.01.001		Contributi agli investimenti da Ministeri					

ACCERTAMENTO 2202/2024:

Importo	Anno Bilancio	Titolo	Tipologia	Categoria	Capitolo e articolo	Responsabile Servizio	Scadenza Obbligazione
559.823,92	2024	4	0200	01	046500057001	068	31/12/2024
Descrizione capitolo e articolo	PNRR-M1 C1 I1.5 CYBERSECURITY ANALISI DELLA POSTURA DI SICUREZZA E MIGLIORAM. NELLA GESTIONE DEI PROCESSI LEGATI ALLA CYBERSECURITY DELLA CITTA' DI TORINO C17H22002830006 VEDASI CAP. 118660005 SPESA - Resp. E SETT. 068						
Conto Finanziario n°	Descrizione Conto Finanziario						
E.4.02.01.01.001	Contributi agli investimenti da Ministeri						

ACCERTAMENTO 3411/2023:

Importo	Anno Bilancio	Titolo	Tipologia	Categoria	Capitolo e articolo	Responsabile Servizio	Scadenza Obbligazione
26.380,91	2023	4	0200	01	046500056001	068	31/12/2023
Descrizione capitolo e articolo	PNRR-M1 C1 I1.5 CYBERSECURITY INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZ. DEL RISCHIO NELLA CITTA' DI TORINO C17H22002840006 VEDASI CAP. 118660004 SPESA - Resp. E SETT. 068						
Conto Finanziario n°	Descrizione Conto Finanziario						
E.4.02.01.01.001	Contributi agli investimenti da Ministeri						

ACCERTAMENTO 2203/2024:

Importo	Anno Bilancio	Titolo	Tipologia	Categoria	Capitolo e articolo	Responsabile Servizio	Scadenza Obbligazione
61.555,47	2024	4	0200	01	046500056001	068	31/12/2024
Descrizione capitolo e articolo	PNRR-M1 C1 I1.5 CYBERSECURITY INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZ. DEL RISCHIO NELLA CITTA' DI TORINO C17H22002840006 VEDASI CAP. 118660004 SPESA - Resp. E SETT. 068						
Conto Finanziario n°	Descrizione Conto Finanziario						

E.4.02.01.01.001	Contributi agli investimenti da Ministeri

IL DIRIGENTE
Firmato digitalmente
Massimo Massimino