



CITTA' DI TORINO

**DIPARTIMENTO SERVIZI INTERNI
DIVISIONE SISTEMI INFORMATIVI
S. INFRASTRUTTURE E CYBERSECURITY**

ATTO N. DD 5727

Torino, 01/10/2024

DETERMINAZIONE DIRIGENZIALE

OGGETTO: PNRR – MISURA M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" - "CYBERSECURITY: INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZIONE DEL RISCHIO NELLA CITTA' DI TORINO - AMPLIAMENTO DEL SISTEMA DI CONTROLLO E MONITORAGGIO" - AFFIDAMENTO AL CSI PIEMONTE E IMPEGNO DI SPESA DI €. 28.500,00 (IVA ESENTE) CIG B32E46D74B- CUP C17H22002840006- FINANZIATO DALL'UNIONE EUROPEA - NEXT GENERATION EU.

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 stata 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.

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;

Premesso che con deliberazione dell'11 gennaio 2021 n. 2/2021 (mecc. 2020 02603/027) il Consiglio Comunale ha approvato lo schema di convenzione con il CSI Piemonte per l'outsourcing del sistema informativo della Città che rappresenta il quadro normativo di riferimento per regolare i rapporti tra CSI e Città in tema di affidamenti diretti in house, nonché per definire il dettaglio dei servizi, le procedure operative e le modalità di controllo. La Convenzione è stata sottoscritta in data 14 gennaio 2021 (Rep. n. 1/2021) con scadenza il 31/12/2025. Sulla base della Convenzione sottoscritta si può procedere all'approvazione delle singole PTE relative ai servizi ad hoc di cui la Città necessita.

Dato atto che in data 25/09/2024 è pervenuta la PTE "Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino - Ampliamento del sistema di controllo e monitoraggio" - PNRR – Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" -CUP C17H22002840006 (All.1), prot. CSI n. 00016956/2024 del 25/09/2024, Ns. prot. n. 784 del 25/09/2023 di Euro 28.500,00 =(IVA esente ai sensi dell'art.10, comma 2 del DPR 633/72 e smi);

Considerato che la proposta concorre all'attuazione degli interventi definiti dalla Città di Torino nell'ambito del Piano Nazionale di Ripresa e Resilienza e in particolare nella Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity". Inserendosi in questo quadro, la proposta ha contenuti coerenti con gli obiettivi generali dell'investimento ovvero la realizzazione di un percorso virtuoso di gestione del rischio cyber che possa dotare la Città dei necessari strumenti e processi per una gestione del rischio cyber in linea con le migliori prassi nazionali e internazionali. E' in particolare prevista la realizzazione di una serie di interventi di potenziamento a mediobreve termine dei servizi e delle infrastrutture in essere della Città. La proposta è inoltre coerente con i principi del Regolamento (UE) 2021/241, che istituisce il dispositivo per la ripresa e la resilienza e del Piano Nazionale di Ripresa e Resilienza (PNRR) valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio, notificata all'Italia dal Segretariato generale del Consiglio con nota LT 161/21, del 14 luglio 2021.

La gestione della sicurezza informatica pone particolare attenzione al miglioramento costante del livello di sicurezza delle infrastrutture e delle diverse componenti applicative dei servizi IT. Oltre all'utilizzo di apparecchiature hardware e di software specifici, è fondamentale poter disporre sia di competenze professionali sia di servizi di monitoraggio della sicurezza applicativa ed infrastrutturale che possano intervenire non solo in fase di effettivo attacco informatico, ma anche in fase di prevenzione, con azioni di supporto nel continuo miglioramento delle difese, attraverso l'individuazione delle vulnerabilità potenzialmente sfruttabili dagli attacchi esterni, a completamento delle informazioni ricavabili dalla analisi dei log dei sistemi, al fine di un'identificazione sempre più rapida di problemi presenti sui sistemi che garantiscono l'erogazione dei servizi.

A tale scopo, i servizi di "security reputation" o "security scoring" forniscono un indicatore di rischio cyber calcolato utilizzando fonti aperte e, conseguentemente, utilizzando dati oggettivi e

misurabili (es. vulnerabilità note, servizi esposti che potrebbero essere utilizzati come vettore di accesso, etc..). Questi servizi consentono di valutare la postura di sicurezza e di effettuare una valutazione quantitativa e oggettiva del livello di rischio informatico legato ai servizi esposti e quindi potenzialmente oggetto di attacchi cyber. Il valore della reputation peggiora ogni qualvolta vengono individuate delle vulnerabilità e migliora ogni qualvolta vengono sanate, offrendo così uno stato sempre aggiornato della sicurezza del sistema complessivo.

In particolare la Città di Torino ha richiesto, nell'ambito del complesso delle attività relative alla Cybersecurity inerenti il presente progetto PNRR, di poter disporre del servizio "Security reputation (Security Scoring)" utilizzato dal CSI, con una personalizzazione che non può essere attuata se non "estendendo" il servizio in essere; nello specifico la Città ha necessità di avere una vista dedicata sullo strumento di monitoraggio, escludendo la possibilità che possa visionare vulnerabilità o situazioni di anomalia su servizi o sistemi di altri Enti gestiti dal CSI, e necessita di espandere il perimetro di analisi a sistemi che non rientrano nel perimetro di gestione del Consorzio in quanto gestiti da fornitori terzi.

Il servizio, attraverso attività di analisi dei servizi e sistemi esposti su internet e senza installazione di strumenti all'interno della rete dell'Ente, fornisce un punteggio (scoring) indicativo del livello di sicurezza dell'Ente; in particolare vengono forniti:

- Valutazione e analisi puntuale del proprio rischio cyber
- Mappatura dettagliata delle vulnerabilità riscontrate ed azioni correttive suggerite
- Analisi di conformità dei propri controlli di sicurezza rispetto allo standard CIS
- Gestione delle criticità con assegnazione del livello di priorità e visualizzazione attraverso dashboards e reports;

Si riporta nel seguito il prospetto relativo al preventivo per i servizi preposti, dettagliatamente descritti al punto 4) "Descrizione delle attività previste" della PTE:

Fornitura	Servizio	Importo preventivato (€)
N.1 Servizio Security Scoring Bitsight	Servizi di Rete e Sicurezza – fornitura di servizio di Security Scoring	28.500,00

Tenuto conto che il CUI per il progetto CUP C17H22002840006 "Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio" è il seguente: S00514490010202300298 programma 2023/2024;

Visto che con deliberazione della Giunta Comunale n. mecc 2017-2219/27 del 13/06/2017 la Città ha approvato i criteri e le check list per la valutazione di congruità delle CTE e delle PTE di servizi IT in affidamento in house al CSI Piemonte (All.2);

Visto il nuovo "Catalogo e Listino dei servizi del CSI", a valere dal 1 gennaio 2024, documento approvato dal Consiglio di Amministrazione nella seduta del 22 settembre 2023;

Visto che nella medesima convenzione tra Città e CSI, all'art. 6, comma 2, il Consorzio s'impegna a fornire stime economiche a preventivo non superiori, a parità di servizi proposti, a quelle indicate

nelle convenzioni o accordi quadro messi a disposizione da Consip S.p.A. o da Centrali di Committenza Regionali o disponibili sul MEPA per servizi analoghi e le medesime stime devono essere, comunque, allineate ai prezzi di mercato;

Considerato che acquisita la PTE si è dunque proceduto ad applicare i criteri stabiliti dalla deliberazione richiamata ed a norma dell'art. 192 del D.Lgs. 50/2016, che trova una continuità applicativa nel combinato disposto degli articoli 1, 2 3 e 7 del D. Lgs. 36/2023, si è attestata la congruità come da relazione sottoscritta e allegata dal Funzionario in EQ. Mauro Correndo (All.3);

Considerato che il CSI Piemonte rientra nella fattispecie per cui non sussiste l'obbligo di richiedere il codice CIG (Codice Identificativo di gara) ai fini della tracciabilità dei flussi finanziari (affidamenti diretti a società in house), come chiarito dalla determinazione dell'AVCP n. 4 del 7 luglio 2011 "Linee guida sulla tracciabilità dei flussi finanziari ai sensi dell'art. 3 della Legge 13 agosto 2010, n. 136", aggiornata da ultimo con delibera n. 585 del 19 dicembre 2023. Dato atto che si è provveduto ad acquisire comunque il CIG, tenuto conto della FAQ Anac sulla digitalizzazione dei contratti pubblici D7 che prescrivono la richiesta del CIG per consentire:

- l'identificazione univoca di una procedura di affidamento ed il suo monitoraggio, garantendo pubblicità e trasparenza;
- l'adempimento degli obblighi contributivi.

Richiamati i principi contabili in materia di imputazione delle spese, di cui al D.Lgs 118/2011, come integrati e corretti con D.Lgs 126/2014.

Occorre ora procedere occorre ora procedere, ai sensi della Convenzione vigente, all'impegno di Euro 28.500,00= (IVA esente ai sensi dell'art. 10 comma 2 DPR 633/1972 e smi) per l'affidamento del servizio "CYBERSECURITY: Ampliamento del sistema di controllo e monitoraggio", a favore del CSI Piemonte - C.so Unione Sovietica, 216 – 10134 Torino – P. IVA 01995120019, in qualità di soggetto in house della Città. In ottemperanza a quanto disposto dal vigente Regolamento per la Disciplina dei Contratti della Città di Torino, dopo l'avvenuta esecutività del presente provvedimento, si procederà alla regolare stipulazione del contratto.

Dato atto che l'esigibilità dell'obbligazione avverrà entro il 31/12/2024

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, l'affidamento diretto a favore del CSI Piemonte C.so Unione Sovietica, 216 – 10134 Torino – P. IVA 01995120019, in attuazione della Convenzione approvata con deliberazione del Consiglio Comunale dell'11 gennaio 2021 n. 2/2021 (mecc. 2020 02603/027) e sottoscritta in data 14/01/2021 (Rep.1/2021), ai sensi dell'art. 7, comma 2, del D.lvo 36/2023, per il servizio "Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino - Ampliamento del sistema di controllo e monitoraggio" - nell'ambito del progetto PNRR – Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" -CUP C17H22002840006;
2. di specificare che la spesa complessiva di Euro 28.500,00=(IVA esente ai sensi dell'art. 10 del D.P.R. 633/1972 e s.m.i.), come da PTE allegata (All.1);
3. di dare atto che si è proceduto ad applicare i criteri stabiliti dalla deliberazione n.mecc. 2017-2219/27 nella check list allegata, redatta dal Funzionario in E.Q. Mauro Correndo (All. 2) e che, a norma dell'art. 192 del D.Lgs. 50/2016, che trova una continuità applicativa nel combinato disposto degli articoli 1, 2 3 e 7 del D. Lgs. 36/2023, si attesta la congruità come da relazione sottoscritta (All.3);
4. di dare atto che il Responsabile Unico del Procedimento è il Dott. Massimo MASSIMINO, Dirigente della Divisione Infrastrutture e Cybersecurity;
5. di dichiarare ai sensi dell'art. 6 bis della L. n. 241/1990 e delle disposizioni del Codice di Comportamento della Città l'insussistenza di cause di conflitto di interesse, anche potenziale in capo al sottoscritto.
6. di dare atto:
 - 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".
 - il presente provvedimento non è pertinente alle disposizioni in materia di valutazione dell'impatto economico (VIE);
 - che l'esigibilità dell'obbligazione avverrà entro il 31/12/2024.

Dettaglio economico-finanziario

Si impegna la spesa di Euro 28.500,00 con la seguente imputazione:

Importo	Anno Bilancio	Mis-sio-ne	Pro-gram-ma	Ti-to-lo	Ma-cro Ag-gre-gato	Capitolo Articolo	Servi-zio Res-ponsa-bile	Scadenza obbliga-zione
28.500,00	2024	01	08	2	02	118660004003	027	31/12/2024
<i>Descrizione capitolo e articolo</i>		PNRR-M1 C1 I1.5 CYBERSEC. INCREM. DELLA CONSAP. DEL RISCHIO CYBER E SVIL. N. SIST. PER LA MITIGAZ. DEL RISC. NELLA CITTA' DI TO.C17H22002840006 AMPL. DEL SIST. DI CONTR. E MONIT. VED 046500056 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 2203/2024:

Importo	Anno Bilancio	Titolo	Tipologia	Categoria	Capitolo e articolo	Responsabile Servizio	Scadenza Obbligazione
28.500,00	2024	4	0200	01	046500056	068	31/12/2024
<i>Descrizione capitolo e articolo</i>		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

Check list per la valutazione di congruità delle PTE

Indicatore di congruità: **81,54**

Check list Efficienza e qualità del servizio			Settore Responsabile valutazione	Valori pesati	Valori PTE	Punti PTE	Applicabile?	Basso	Medio	Alto	Molto Alto
								10 punti	40 punti	70 punti	100 punti
Efficienza e qualità del servizio	Vincoli temporali	Vi sono esigenze temporali derivanti da obblighi normativi o da obiettivi dell'Amministrazione che possono condizionare i tempi di disponibilità dei risultati del progetto o le modalità di realizzazione?	Settore Sistemi Informativi	8	8	100	SI	I tempi richiesti sono tali da rendere attuabile una acquisizione dei servizi dal mercato, con successivo apprendimento del contesto da parte dell'affidatario	I tempi richiesti non condizionano i processi produttivi o di approvvigionamento, a meno di ritardi dovuti a fattori esterni (dilazione dell'avvio attività, interventi normativi...). In caso di acquisizione dal mercato, i tempi necessari all'espletamento della procedura di gara sarebbero compatibili con gli obiettivi dell'Amministrazione	I tempi richiesti possono condizionare l'approvvigionamento di risorse produttive apposite per il progetto. Il processo produttivo generalmente non necessita di iterazioni rilevanti. I tempi di una procedura di gara sarebbero compatibili con gli obiettivi dell'Amministrazione se ridotti al minimo e senza fattori negativi esterni (ricorsi)	I tempi richiesti per la messa a disposizione dei risultati del progetto vincolano esplicitamente le possibilità di acquisizione di risorse produttive all'esterno o i processi di realizzazione. E' possibile che alcune fasi progettuali debbano essere iterate in funzione della parziale revisione dei requisiti. I tempi di una procedura di gara sarebbero incompatibili con gli obiettivi dell'Amministrazione
	Competenze richieste	Il progetto richiesto necessita di un elevato livello di conoscenza dell'organizzazione dell'Amministrazione e del sistema informativo? I tempi di apprendimento delle competenze non ancora possedute avrebbero un impatto significativo su tempi e costi del progetto?	Settore Sistemi Informativi	10	10	100	SI	La proposta progettuale può essere definita "a scaffale", ovvero i risultati prescindono dal contesto organizzativo e tecnologico dell'Amministrazione. Non sono presenti necessità di integrazione con altre componenti del sistema informativo	La proposta progettuale prescinde da aspetti organizzativi interni all'Ente. Per eventuali integrazioni con il sistema informativo dell'Ente è sufficiente una conoscenza documentale delle modalità di integrazione applicativa	La proposta progettuale presuppone la conoscenza degli aspetti organizzativi dell'Ente o delle integrazioni necessarie con il sistema informativo. Un team progettuale non in possesso delle conoscenze necessiterebbe di approfondimenti in tal senso con il committente in fase di analisi	La proposta progettuale caratterizza il progetto come fortemente personalizzato sulla specifica situazione dell'Ente, per gli aspetti organizzativi o per dipendenze con altre componenti del sistema informativo dell'Ente. Un team progettuale non a conoscenza dell'uno o dell'altro degli elementi necessiterebbe di un tempo significativo di apprendimento del contesto
	Continuità di gestione	I servizi di gestione successiva del sistema informativo proposto necessitano delle competenze acquisite o in possesso del team di sviluppo, sia dal punto di vista tecnologico (manutenzione correttiva e servizi sistemistici o di sicurezza), sia dal punto di vista del supporto all'utente (assistenza applicativa, supporto specialistico, elaborazione dati)? La proposta evidenzia tra i deliverables la redazione di documenti atti a facilitare la gestione successiva (manuale del servizio, manuale utente...)	Settore Sistemi Informativi	10	0	0	NO	La gestione sia informatica che verso l'utente non necessita di particolari conoscenze in possesso del team di sviluppo. La proposta non evidenzia la redazione di documentazione utile alla gestione del sistema e all'erogazione di servizi all'utente	La gestione del sistema, sia informatica che per i servizi all'utente, è facilitata dalle competenze richieste al team di sviluppo ma è affidata alla disponibilità della documentazione utile	Le conoscenze necessarie all'erogazione dei servizi corrispondono almeno in parte alle competenze richieste al team di sviluppo. La proposta progettuale garantisce la documentazione utile alla gestione informatica e sistemistica del sistema	E' auspicabile che la gestione venga effettuata da figure professionali che hanno collaborato al progetto di sviluppo (i servizi verso l'utente). La proposta progettuale evidenzia i documenti utili ai servizi di gestione
	Integrazione nel sistema informativo	Il sistema informativo risultante dal progetto presenta una elevata necessità di integrazione applicativa con altre componenti del sistema informativo dell'Amministrazione? Necessita ad esempio di integrazione con componenti "core" del sistema informativo (economico, del personale, archivistico...)?	Settore Sistemi Informativi	11	0	0	NO	Il progetto non richiede particolari integrazioni con altre componenti del sistema informativo (eccetto integrazioni con il sistema di identità digitale)	Il progetto non richiede integrazioni con componenti "core" del sistema informativo dell'Amministrazione, ma richiede integrazioni con componenti trasversali come ad esempio l'identità digitale o anagrafiche gestite dall'Amministrazione	Il progetto richiede alcune integrazioni (oltre all'identità digitale) con altre componenti del sistema informativo dell'Amministrazione o con sistemi informativi di altre Amministrazioni.	Il progetto richiede numerose integrazioni con altre componenti "core" del sistema informativo (archivio, bilancio, personale...) o con anagrafiche proprie dell'Amministrazione o con sistemi informativi di altre Amministrazioni.
	Monitoraggio/grado di misurabilità impatto sul tessuto socio-economico e sulla cittadinanza	Impatto sui cittadini e sulle imprese del territorio	Settore Sistemi Informativi	8	0,8	10	SI	Il progetto ha una valenza interna, quindi incide solo indirettamente al cittadino	Il progetto ha una valenza interna e parzialmente verso il cittadino	Il progetto fornisce alcune utility al cittadino	Il progetto ha una valenza rilevante per il cittadino, fornendo servizi fruibili on-line, in mobilità per interagire con l'Ente.

Check list Efficienza e qualità del servizio			Settore Responsabile valutazione	Valori pesati	Valori PTE	Punti PTE	Applicabile?	Basso	Medio	Alto	Molto Alto
								10 punti	40 punti	70 punti	100 punti
Universalità e socialità	Multi-canalità e utilizzo in mobilità	Multi-canalità ed utilizzo in mobilità (automazione dei procedimenti di back office, dematerializzazione, centralizzazione e integrazione banche dati, Internet of Things, etc.)	Settore Sistemi Informativi	5	5	100	SI	Il progetto non implementa soluzioni multi-canale e un uso in mobilità.	Il progetto implementa soluzioni multi-canale ma non un uso in mobilità.	Il progetto implementa soluzioni per un uso in mobilità ma non multi-canale.	Il progetto implementa soluzioni multi-canale e un uso in mobilità.
	Livello di riusabilità e capacità di diffusione su scala metropolitana	Il sistema viene realizzato nell'ottica di un suo potenziale riutilizzo verso altri Enti.	Settore Sistemi Informativi	5	0	0	NO	Il sistema non è riusabile, perché personalizzato su tipicità dell'Ente.	Il sistema non è facilmente riusabile, necessita di significativi adeguamenti.	Il sistema può essere oggetto di riutilizzo con alcuni adeguamenti.	Il sistema è facilmente installabile e configurabile in modalità scalare da un Ente riutilizzatore.
	Estensione del sistema informativo	Nel caso di sviluppo evolutivo di un sistema informativo gestionale esistente, è prevalente la dimensione dello stesso rispetto all'entità dell'evolutiva? Sarebbe altrimenti ipotizzabile lo sviluppo o acquisizione di figure professionali per le evoluzioni necessarie? Sarebbe ipotizzabile affidare il singolo intervento evolutivo al team progettuale diverso da quello che lo gestisce	Settore Sistemi Informativi	13	0	0	NO	Per dimensioni, l'intervento evolutivo potrebbe essere affidato ad altro fornitore o potrebbe giustificare una sostituzione del sistema informativo gestionale. Tuttavia la proposta progettuale non esamina queste possibilità	L'intervento evolutivo interviene su una dimensione percentuale significativa del sistema informativo gestionale esistente e la proposta progettuale non offre informazioni sull'opportunità di una eventuale sostituzione del sistema	L'intervento evolutivo interviene su una dimensione non superiore al 20% del sistema informativo gestionale esistente	L'intervento evolutivo interviene su una dimensione non superiore al 10% del sistema informativo gestionale esistente e la proposta progettuale motiva la scelta di non acquisire il sistema ex-novo
Check list economica			Settore Responsabile valutazione	Valore pesato				Basso	Medio	Alto	Molto Alto
								10 punti	40 punti	70 punti	100 punti
Economicità	La PTE comprende forniture CONSIP	Il CSI acquisisce, mediante convenzioni, accordi e contratti quadro, servizi di sviluppo software (figure professionali e function point) da CONSIP, SCR o gara. Il peso economico è rapportato alla % dell'importo della fornitura CONSIP, SCR o gara della PTE.	Settore Sistemi Informativi	5	5	100	SI	L'importo della fornitura CONSIP deve essere <= 30% del totale della PTE	L'importo della fornitura CONSIP deve essere superiore al 30% e <= 40% del totale della PTE	L'importo della fornitura CONSIP deve essere superiore al 40% e <= 50% del totale della PTE	L'importo della fornitura CONSIP deve essere superiore al 50% del totale della PTE
	Economicità dei servizi professionali	Rispetto alle attività erogate tramite giornate professionali, è possibile fare riferimento a tariffari o benchmark di riferimento per attività analoghe (principalmente strumenti CONSIP)? La proposta progettuale risulta vantaggiosa dal punto di vista dei costi?	Settore Sistemi Informativi	13	0	0	NO	I costi delle attività risultano svantaggiosi rispetto a quanto calcolabile con tariffari di riferimento in misura pari o superiore al 10%	I costi delle attività risultano svantaggiosi rispetto a quanto calcolabile con tariffari di riferimento in misura compresa tra il 9,99% e il 5,00%	I costi delle attività risultano svantaggiosi rispetto a quanto calcolabile con tariffari di riferimento in misura compresa tra il 4,99% e lo 0,01% .	I costi delle attività risultano vantaggiosi rispetto a quanto calcolabile con tariffari di riferimento in misura pari o inferiore.
	Economicità della produzione del software misurata in function point	Rispetto al software prodotto e misurabile in FP con misurazione IFPUG il costo del singolo Function Point, con riferimenti rilevati nell'AQ Consip Sviluppo Applicativi (classe di progetto gestionale: ciclo completo) nel benchmark 2016, risulta vantaggioso dal punto di vista economico? Il costo medio del FP AQ Consip è di 210,69 Euro. Il costo massimo del FP per la PA rilevato in sede di benchmark è quotato in 375,51 Euro. Oltre il valore massimo del benchmark la PTE viene dichiarata non congrua.	Settore Sistemi Informativi	9	0	0	NO	Il costo medio del FP è compreso tra 300,01 e 375,51 Euro.	Il costo medio del FP è compreso tra 300,00 e 260,01 Euro.	Il costo medio del FP è compreso tra 260,00 e 210,70 Euro.	Il costo medio del FP è pari o inferiore a Euro 210,69
	Rilevanza attività non acquisibili dal mercato	Il costo delle attività non acquisibili sul mercato sommato ai costi stimabili per la gestione della procedura di gara e di gestione del contratto sarebbe prevalente rispetto al costo delle attività acquisibili sul mercato?	Settore Sistemi Informativi	3	3	100	SI	La proposta progettuale non permette di individuare le attività non acquisibili dal mercato o comunque il loro costo, sommato ai costi stimabili per la gestione del contratto non sono significativi	La proposta progettuale evidenzia le attività non acquisibili dal mercato. Il costo di queste attività sommato ai costi stimabili per la gestione del contratto sono vantaggiosi rispetto al costo delle attività disponibili e non acquisite sul mercato in misura non superiore al 10%	La proposta progettuale evidenzia le attività non acquisibili dal mercato. Il costo di queste attività sommato ai costi stimabili per la gestione del contratto sono equivalenti al costo delle attività disponibili e non acquisite sul mercato	La proposta progettuale evidenzia le attività non acquisibili dal mercato. Il solo costo di queste attività è prevalente rispetto al costo delle attività disponibili e non acquisite sul mercato
TOTALE PUNTI CUMULABILI NELLA CHECKLIST				100	81,538						
SOMMA DEI PUNTEGGI MASSIMI APPLICABILI				39							



CITTA' DI TORINO

DIPARTIMENTO SERVIZI INTERNI
DIVISIONE SISTEMI INFORMATIVI
SERVIZIO INFRASTRUTTURE E CYBERSECURITY

Nota congruità PTE “CSI “Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino - Ampliamento del sistema di controllo e monitoraggio” - PNRR – Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” -CUP C17H22002840006” - IMPEGNO DI SPESA DI EURO € 28.500,00= (IVA ESENTE AI SENSI DELL'ART. 10 D.P.R. 633/1972 E S.M.I.)”

L'attuale normativa (articolo 192 del D.Lgs. n. 50/2016), che trova una continuità applicativa nel combinato disposto degli articoli 1,2,3 e 7 del D.Lgs 36/2023, ovvero del nuovo codice dei contratti pubblici, prevede espressamente che le amministrazioni effettuino “la valutazione sulla congruità economica dell’offerta dei soggetti in house, avuto riguardo all’oggetto e al valore della prestazione, dando conto nella motivazione del provvedimento di affidamento delle ragioni del mancato ricorso al mercato”.

Pertanto, come previsto nella Convenzione con il CSI Piemonte sono stati stabiliti e approvati il 13/6/17 con deliberazione della Giunta Comunale n. 2017 2219 i criteri per la valutazione di congruità delle CTE e delle PTE dei servizi IT.

Le attività qui finanziate fanno riferimento alla PTE ““Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino - Ampliamento del sistema di controllo e monitoraggio” - PNRR – Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” -CUP C17H22002840006” alla quale il collega in E.Q. Mauro CORRENDO ha applicato la check-list stabilita dalla deliberazione per l’indicazione di giudizio qualitativo e quantitativo dell’intera proposta.

Poiché l’indicatore di congruità ha valore 81,54 la PTE risulta congrua in quanto superiore a 80.

Dirigente
Servizio Infrastrutture e Cybersecurity
Dott. Massimo MASSIMINO
(firmato digitalmente)



All.

**AUTODICHIARAZIONE DI ASSENZA DI CONFLITTO DI INTERESSI PER IL
PERSONALE COINVOLTO NELLE PROCEDURE DI AGGIUDICAZIONE / ESECUZIONE
DELL'APPALTO:**

PROCEDURA DI GARA PNRR – MISURA M1C1 INVESTIMENTO 1.5 "CYBERSECURITY" -
"CYBERSECURITY: INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO
NUOVI SISTEMI PER LA MITIGAZIONE DEL RISCHIO NELLA CITTA' DI TORINO - AMPLIAMENTO DEL
SISTEMA DI CONTROLLO E MONITORAGGIO" - AFFIDAMENTO AL CSI PIEMONTE E IMPEGNO DI
SPESA DI €. 28.500,00 (IVA ESENTE) CIG B32E46D74B - CUP C17H22002840006- FINANZIATO
DALL'UNIONE EUROPEA - NEXTGENERATIONEU. del 25/09/2024

CUP C17H22002840006 CIG B32E46D74B

Il sottoscritto Massimo Massimino

coinvolto in qualità di RUP

nella procedura di gara in oggetto, vista la normativa vigente relativa alle situazioni, anche potenziali, di
conflitto di interessi

DICHIARA

sotto la propria responsabilità e in piena conoscenza della responsabilità penale prevista per le false
dichiarazioni ex art. 76 del D.P.R. n. 445/2000, dalle disposizioni del Codice penale e dalle leggi speciali in
materia, ai sensi degli articoli 46 e 47 del D.P.R. 445/2000:

- di non trovarsi in situazioni di conflitto di interessi di qualsiasi natura, anche potenziale, e di non avere
direttamente o indirettamente un interesse finanziario, economico o altro interesse personale che
potrebbe rappresentare ed essere percepito come una minaccia all'imparzialità e indipendenza nel
contesto della presente procedura di selezione. In particolare, dichiara di non trovarsi in una delle
seguenti circostanze in cui si presume un conflitto di interessi, anche potenziale:
 - partecipazione diretta o indiretta all'interno del capitale sociale dei soggetti partecipanti, di soggetti
o organizzazioni di cui sia tutore, curatore, procuratore o agente, ovvero di società, enti o associazioni, anche
non riconosciute, direttamente controllate dallo stesso;

- aver lavorato o aver rivestito cariche di amministratore all'interno del soggetto partecipante, ovvero di società, enti o associazioni, anche non riconosciute, direttamente controllate dallo stesso nei 24 mesi antecedenti all'avvio della procedura di selezione pubblica;
 - esercizio da parte di parenti o affini entro il secondo grado, coniuge o convivente di attività politiche, professionali, economiche o finanziarie che li pongano in contatti frequenti con il soggetto partecipante o coinvolgimento degli stessi nelle decisioni o nelle attività ad esso inerenti;
 - essere titolare di diritti aventi natura patrimoniale o di sfruttamento economico (diritti d'autore/brevetti, partecipazioni, titolarità di quote, etc.) su prodotti o quote del soggetto partecipante
o affini che operino nel settore merceologico di interesse della procedura di selezione;
 - esistenza di cause pendenti o grave inimicizia o rapporti di credito o debito significativi tra il soggetto partecipante e soggetti o organizzazioni di cui sia tutore, curatore, procuratore o agente, ovvero di società, enti o associazioni, anche non riconosciute, direttamente controllate dallo stesso;
 - ricezione di omaggi dal soggetto partecipante di importo ritenuto non modico, superiore a 100 (cento) euro, nei 12 mesi antecedenti all'avvio della procedura di selezione.
- Di non essere a conoscenza di aver procedimenti penali pendenti e di non aver riportato condanne anche con sentenza non passata in giudicato, per i reati previsti nel Capo I, Titolo II del libro II del codice penale;
 - di impegnarsi a non utilizzare a fini privati le informazioni di cui dispone per ragioni di ufficio, a non divulgarle al di fuori dei casi consentiti e ad evitare situazioni e comportamenti che possano ostacolare il corretto adempimento dei compiti o nuocere agli interessi e all'immagine dell'Amministrazione di appartenenza;
 - di impegnarsi a comunicare tempestivamente eventuali variazioni del contenuto della presente dichiarazione e a rendere, se del caso, una nuova dichiarazione sostitutiva;
 - di autorizzare la pubblicazione dei presenti dati personali sul sito istituzionale dell'Amministrazione di appartenenza;
 - che la presente dichiarazione è resa ai sensi e per gli effetti dell'art. 6-bis L. 241/90, degli artt. 6-7 del D.P.R. 62/2013, dell'art. 53, comma 14, del D.lgs 165/2001 e dell'art. 15, comma 1, lettera c) del D.lgs. 33/2013.

Dichiara, infine, di avere preso visione dell'informativa sul trattamento dei dati personali nel rispetto del Regolamento (UE) 679/2016, del decreto legislativo 30 giugno 2003, n. 196, così come novellato dal decreto legislativo 10 agosto 2018, n. 101, nonché secondo le disposizioni contenute nell'art. 22 del Regolamento (UE) 2021/241.

TORINO

FIRMA IN DIGITALE

Si dichiara che sono parte integrante del presente provvedimento gli allegati riportati a seguire ¹, archiviati come file separati dal testo del provvedimento sopra riportato:

1. COTO_DSI_PNRR_PTE_ACN_Cybersecurity_Security_Scoring.pdf.p7m
2. All._-Autodichiarazione_assenza_Conflitto_di_Interessi__Donzella_signed.pdf
3. All._-Autodichiarazione_assenza_Conflitto_di_Interessi__Correndo.pdf.p7m



¹ L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento