CITTA' DI TORINO

DIPARTIMENTO SERVIZI INTERNI
DIVISIONE SISTEMI INFORMATIVI
S. INFRASTRUTTURE E CYBERSECURITY

ATTO N. DD 5832 **Torino, 13/10/2023**

DETERMINAZIONE DIRIGENZIALE

OGGETTO: PNRR – MISURA M1C1 - DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA - INVESTIMENTO 1.5 "CYBERSECURITY" - DETERMINA A CONTRARRE PER NUOVA ADESIONE ALL'ACCORDO QUADRO CONSIP AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI - ID 2296 LOTTO 1 - SERVIZI DI FORMAZIONE E SECURITY AWARENESS - CUP C17H22002840006 CIG PADRE 88846293CA CIG DERIVATO A01A10FBBA - FINANZIATO DALL'UNIONE EUROPEA - NEXTGENERATIONEU, INDIZIONE E PRENOTAZIONE IMPEGNO DI SPESA EURO 182.996,48 IVA 22% COMPRESA.

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.

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.

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 prende 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.

Lo scenario normativo in cui il Comune opera prevede la Normativa Europea, la Direttiva NIS, il Cyber Security Act ed il DL 105/2019 “Perimetro di sicurezza cibernetica” che sottolineano l’importanza dell’attenzione al fenomeno del cybercrime, il quale è in costante aumento anche nell’ambito PA. Il fenomeno è evidenziato come in crescita (Rapporto Clusit 2021) anche in relazione alle mutate condizioni lavorative dovute alla pandemia Covid.

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 di 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 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;

Considerato che nel Piano Triennale per l'Informatica della PA, aggiornato al triennio 2022-2024, la sicurezza assume un ruolo strategico e trasversale, comprendendo tutte le attività per la regolazione e regolamentazione della sicurezza nella Pubblica Amministrazione che sono state assegnate ad AgID;

Considerato che viene raccomandata l'adozione in tutti i progetti di un approccio "security by default", imponendo alle Pubbliche Amministrazioni di rendersi conformi alle Misure minime di sicurezza ICT;

Considerato che il Piano delle Gare Strategiche ICT, concordato tra Consip e AgID, ha l'obiettivo, tra le altre cose, di mettere a disposizione delle PP.AA. delle specifiche iniziative finalizzate all'acquisizione di prodotti e di servizi nell'ambito della sicurezza informatica, facilitando l'attuazione del Piano Triennale e degli obiettivi del PNRR in ambito, restando in linea con le disposizioni normative relative al settore della cybersicurezza;

Dato atto che AgID ha concordato l'indirizzo strategico per la progettazione della presente iniziativa con particolare riferimento sui contenuti tecnici e sui meccanismi di coordinamento e controllo dell'utilizzo dello strumento di acquisizione, Consip S.p.A., in qualità di soggetto Stazione Appaltante, ha aggregato i fabbisogni e predisposto la procedura di gara e gestirà la stipula dei contratti per le amministrazioni centrali e locali e le PA devono intraprendere misure ed azioni per l'avvio di progetti finalizzati alla trasformazione digitale dei propri servizi in base al Modello strategico evolutivo dell'informatica della PA e ai principi definiti nel Piano Triennale;

In particolare visto l'Accordo Quadro stipulato da Consip avente ad oggetto "L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296" suddiviso in 2 lotti: Lotto 1 "Servizi di sicurezza da remoto" e Lotto 2 "Servizi di compliance e controllo";

Considerato che:

- il Lotto 1 "Servizi di Sicurezza da remoto" ha l'obiettivo di mettere a disposizione delle Amministrazioni un insieme di servizi di sicurezza - erogati da remoto e in logica continuativa - per la protezione delle infrastrutture, delle applicazioni e dei dati;
- il Lotto 2 "Servizi di Compliance e controllo" ha l'obiettivo di mettere a disposizione delle Amministrazioni servizi - erogati "on-site" in logica di progetto – finalizzati alla elaborazione di un "progetto di sicurezza" che identifica lo stato di salute della sicurezza del sistema informativo

dell'Amministrazione e nel controllo imparziale sulla corretta esecuzione dei servizi di sicurezza del Lotto 1 nonchè sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

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 proposta per questa Amministrazione è il nr. 1 per i servizi di Sicurezza da Remoto con durata di 24 (ventiquattro) mesi con decorrenza dal 26/09/2022 e scadenza il 26/09/2024, termine ultimo entro il quale si potrà affidare il Contrattio Attuativo;

Considerato che il Lotto 1 prevede il seguente servizio:

- Servizio L1.S9 – Formazione e Security Awareness

Considerato che la Città di Torino necessita di specifici servizi di formazione al fine sensibilizzare i propri dipendenti e collaboratori sui vari aspetti della sicurezza delle informazioni, aumentando il livello di consapevolezza dei dipendenti e quindi elevando il livello di sicurezza dell'Organizzazione. L'obiettivo ultimo è sviluppare negli utenti le competenze, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e per reagire al meglio a fronte di eventuali problemi.

In particolare, con il Piano dei Fabbisogni si richiede l'erogazione, con il supporto della piattaforma Cyberguru, di un servizio di formazione per 7500 utenti, al fine di accrescere la consapevolezza di dipendenti e collaboratori su vari aspetti della sicurezza delle informazioni e sviluppare in tali utenti le competenze, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e per reagire al meglio a fronte di eventuali problemi.

Preso atto dell'aggiudicazione da parte di CONSIP del Lotto 1 per le Amministrazioni Locali alla RTI costituendo Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A. e Difesa e Analisi Sistemi S.p.A., (mandataria Accenture S.p.A. Partita IVA 13454210157; in qualità di mandanti : Fastweb S.p.A. Partita I.V.A. 12878470157, Fincantieri NexTech S.p.A Partita I.V.A.: 00890740111 e Difesa e Analisi Sistemi S.p.A. Partita IVA 14961281004);

Preso atto che le modalità di adesione al Contratto Quadro di cui trattasi prevedono la stipula di un Contratto Esecutivo con il RTI aggiudicatario previo espletamento di una serie di fasi procedurali quali:

- la redazione, anche con il supporto del Fornitore, di un "Piano dei Fabbisogni" contenente le indicazioni relative ai servizi che si intende realizzare;
- la predisposizione da parte del Fornitore di un "Piano Operativo" che raccolga e dettagli le richieste dell'Amministrazione contenute nel "Piano di Fabbisogni" formulando una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nel Contratto Quadro citato;
- la stipula del "Contratto Esecutivo" che definisce i termini e le condizioni che, unitamente alle disposizioni contenute nel Contratto Quadro e suoi allegati, regolano l'erogazione in favore della Amministrazione da parte del Fornitore dei servizi che saranno forniti con il Progetto Esecutivo;

Considerato il Piano dei Fabbisogni (all. 1) prevede attività, relative al progetto C17H22002840006, da realizzarsi entro 12 mesi dalla data di attivazione, compatibilmente con il vincolo definito dall'Accordo quadro, rispetto alla sua durata residua;

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;
Considerato che la stipula del Contratto Esecutivo sarà sottoscritta da questa Amministrazione dopo l'adesione mediante Ordine Diretto di Acquisto all'unico fornitore aggiucatario, alle condizioni ed ai termini fissati dall'Accordo Quadro, per un massimale economico stimato in € 182.996,48 (IVA 22% inclusa), relativamente al progetto:

- progetto "Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino" - CUP C17H22002840006: euro 149.997,12 oltre IVA al 22% per un totale complessivo di euro 182.996,48 per la fornitura del servizio L1.S9 Formazione e Security Awareness, così come meglio dettagliato nel Piano dei Fabbisogni;

Considerate le previsioni di avanzamento del progetto si provvede a prenotare le somme come da dettaglio economico;

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;

Dato atto che l'intervento è stato inserito nella programmazione biennale 2023/2024 con il codice S00514490010202300298;

Dato atto che non sussistono, nè in capo all'Istruttore, nè in capo al DEC, nè in capo al RUP, cause di conflitto di interesse, anche potenziale, ex art 6-bis della L. 241/1990 e ss.mm.ii. e art. 1, comma 9, lettera e) della L. 190/2012, nonchè condizioni di incompatibilitàndi cui all'art. 35-bis del D. Lgs. 165/2001 e che risultano rispettate le disposizioni di cui al vigente Piano Integrato di Attività e Organizzazione;

Valutata l'esigenza di aderire all'Accordo Quadro (AQ) avente ad oggetto "L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 - Lotto 1 Servizi di Sicurezza da Remoto" per acquisire e rendere disponibili alle Amministrazioni servizi con carattere di innovazione tecnologica per l'attuazione del Codice dell'Amministrazione Digitale, nonché del Piano Triennale ICT della PA.

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 individuare nel Dott. Massimo Massimino del Servizio INFRASTRUTTURE E CYBERSECURITY della Divisione Sistemi Informativi il Responsabile Unico del Procedimento;

2) di autorizzare, per i motivi esposti in premessa, l’espletamento delle fasi procedurali propedeutiche alla nuova adesione del Comune di Torino all'Accordo Quadro per i servizi di "Servizi di Sicurezza da Remoto" Lotto 1 dell'Accordo Quadro stipulato da Consip avente ad oggetto "L’AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296" CIG PADRE 88846293CA CIG DERIVATO A01A10FBBA stipulato da CONSIP con il costituendo Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A. e Difesa e Analisi Sistemi S.p.A., (mandataria Accenture S.p.A. Partita IVA 13454210157; in qualità di mandanti : Fastweb S.p.A. Partita I.V.A. 12878470157, Fincantieri NexTech S.p.A Partita I.V.A.: 00890740111 e Difesa e Analisi Sistemi S.p.A. Partita IVA 14961281004); per l'affidamento di Servizi di Formazione e Security Awareness;

3) dato atto che l'operatore economico si impegna a orientare il proprio futuro operato in conformità con le disposizioni dell’attuale Piano Triennale ICT e con le normative in materia di Cybersecurity di riferimento ed adeguarsi alle dinamiche evolutive, utilizzando la tecnologia per accompagnare il processo di trasformazione digitale della PA;

4) di disporre di avviare l’iter procedurale di cui sopra attraverso la redazione e l’invio al R.T.I., secondo le modalità previste dal Contratto Quadro, del “Piano dei Fabbisogni” (All. 1);

5) di rimandare a successivi provvedimenti l’approvazione del “Piano Operativo” e la conseguente autorizzazione alla stipula del relativo “Contratto Esecutivo”;

6) di prenotare l'importo di € 182.996,48 (IVA 22% inclusa) come da dettaglio economico finanziario;

7) 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, 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;

8) 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;
- il presente provvedimento non è pertinente alle disposizioni in materia di valutazione dell'impatto economico (VIE);
- che il presente provvedimento è rilevante ai fini della pubblicazione nella sezione "Amministrazione Trasparente";
- che la presente determinazione è stata sottoposta al controllo di regolarità amministrativa ai sensi dell'art. 147-bis TUEL e con la sottoscrizione si rilascia parere di regolarità tecnica favorevole;
- 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;
- l'esigibilità della spesa avverrà entro il 31/12 di ogni anno, come da dettaglio economico.

Dettaglio economico-finanziario

Si prenota la spesa di Euro 182.996,48 relativamente al progetto "Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino" - CUPC17H22002840006, con la seguente imputazione:

Importo	Anno Bilancio	Missione	Programma	Titolo	Macro Aggregato	Capitolo Articolo	Servizio Responsabile	Scadenza obbligazione
30.499,41	2023	01	08	1	03	088160002001	027	31/12/2023
152.497,07	2024	01	08	1	03	088160002001	027	31/12/2024
Descrizione capitolo e articolo		PNRR-M1 C1 I1.5 CYBERSECURITY INCR. DELLA CONS. DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZ. DEL RISCHIO NELLA CITTA' DI TORINO - SERVIZI FORMAZIONE- CUP C17H2200284006 VED 6800026 E 27						
Conto Finanziario n°		Descrizione Conto Finanziario						
U.1.03.02.04.999		Acquisto di servizi per altre spese per formazione e addestramento n.a.c.						

La spesa è finanziata da fondi accertati con D.D 5584 del 05/10/2023 (ACCERTAMENTO 4433/2023, ACCERTAMENTO 2377/2024) come segue:

Importo	Anno Bilancio	Titolo	Tipologia	Categoria	Capitolo Articolo	Servizio Responsabile	Scadenza obbligazione
30.499,41	2023	2	0101	01	006800026001	068	31/12/2023
152.497,07	2024	2	0101	01	006800026001	068	31/12/2024
Descrizione capitolo e articolo		*PNRR-M1 C1 I1.5 CYBERSECURITY INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SIST PER LA MITIGAZ. DEL RISCHIO NELLA CITTA' DI TORINO CUP C17H22002840006 VEDASI 088160002 SP set 068*					
Conto Finanziario n°		Descrizione Conto Finanziario					
E.2.01.01.01.001		Trasferimenti correnti da Ministeri					

IL DIRIGENTE
Firmato digitalmente
Massimo Massimino

ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 – **LOTTO 1**

PIANO DEI FABBISOGNI

INDICE

1. DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione:	COMUNE DI TORINO
Indirizzo	Piazza Palazzo di Città 1
CAP	10122
Comune	Torino
Provincia	TO
Regione	Piemonte
Codice Fiscale	00514490010
Codice IPA	C_L219
Indirizzo mail	-
PEC	protocolloGenerale@cert.comune.torino.it

Referente Amministrazione	Massimo Massimino
Ruolo	Dirigente Servizio Infrastrutture e Cybersecurity
Telefono	011 011 30501
Indirizzo mail	massimo.massimino@comune.torino.it
PEC	innovazione@cert.comune.torino.it

2. CONTESTO

- ***DESCRIZIONE DELL'AMMINISTRAZIONE CONTRAENTE***

Il Comune di Torino è una realtà complessa, in costante innovazione. Ha circa 7500 dipendenti, collocati su circa 200 sedi.

- ***DESCRIZIONE DEL CONTESTO TECNOLOGICO, APPLICATIVO E PROCEDURALE***

Il Sistema Informativo (SI) del Comune di Torino è un sistema complesso ed articolato che integra la gestione dei procedimenti amministrativi interni all'ente con l'offerta di servizi on line verso cittadini, professionisti ed imprese.
L'innovazione tecnologica è stata intesa con una doppia valenza: da un lato come strumento abilitante per ottenere trasparenza, efficienza ed efficacia dai processi amministrativi interni, dall'altro per promuovere e offrire ai cittadini servizi disponibili in rete.
Lo scenario normativo in cui il Comune opera prevede la Normativa Europea, la Direttiva NIS, il Cyber Security Act ed il DL 105/2019 "Perimetro di sicurezza cibernetica" che sottolineano l'importanza dell'attenzione al fenomeno del cybercrime, il quale è in costante aumento anche nell'ambito PA; fenomeno che è evidenziato come in crescita (Rapporto Clusit 2021) anche in relazione alle mutate condizioni lavorative dovute alla pandemia Covid.
In tale contesto l'Ente si propone di attuare vari 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.
Una delle attività principali da mettere in atto è quello dell'aumento della consapevolezza del rischio cyber da parte di tutti i dipendenti

▪ DESCRIZIONE DELL'ESIGENZA

Il presente capitolo ha lo scopo di descrivere le esigenze di Comune di Torino nell'ambito dei servizi offerti dall'Accordo quadro AQ 2296 – Lotto 1 per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, stipulato da Consip S.p.A. (Consip) e dal Raggruppamento Temporaneo di Imprese (RTI) composto da:

- Accenture S.p.A.
- Fastweb S.p.A.
- Fincantieri NexTech S.p.A.
- Difesa e Analisi Sistemi S.p.A..

Il Comune di Torino necessita dei servizi di seguito indicati, al fine sensibilizzare i propri dipendenti e collaboratori sui vari aspetti della sicurezza delle informazioni, aumentando il livello di consapevolezza dei dipendenti e quindi elevando il livello di sicurezza dell'Organizzazione. L'obiettivo è sviluppare negli utenti le competenze, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e per reagire al meglio a fronte di eventuali problemi.

Il Comune di Torino si impegna ad effettuare l'opportuna segnalazione al Centro di Valutazione e Certificazione Nazionale (CVCN) qualora i servizi richiesti siano inseriti nel Perimetro di sicurezza nazionale cibernetica.

- ***SINTESI DEI SERVIZI RICHIESTI***

Le richieste del presente Piano dei Fabbisogni riguardano l'erogazione dei seguenti servizi:

Servizio L1.S9 – Formazione e Security Awareness

Si richiede l'erogazione, con il supporto della piattaforma Cyberguru, di un servizio di formazione per 7500 utenti, al di accrescere la consapevolezza di dipendenti e collaboratori su vari aspetti della sicurezza delle informazioni e sviluppare in tali utenti le competenze, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e per reagire al meglio a fronte di eventuali problemi.

Tali servizi sono riassunti nella seguente tabella che descrive le numerosità richieste per la loro erogazione. Si richiede, altresì che il piano di lavoro abbia una durata complessiva di 12 mesi.

L1.S9 – FORMAZIONE E SECURITY AWARENESS								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S9	Formazione e Security Awareness	A task	A corpo	gg/p Team ottimale	606			

Nell'ambito dei servizi richiesti, si elencano di seguito i servizi per i quali è richiesto il collaudo:

- N.A.

- ***LUOGO DI EROGAZIONE***

In base alla modalità di esecuzione dei servizi le prestazioni contrattuali dovranno essere svolte come di seguito indicato:

- per i servizi erogati *da remoto*: presso i Centri Servizi del Fornitore;
- per i servizi on-site: presso le sedi dell'Amministrazione ove specificato dall'Amministrazione stessa.

INDICATORE DI PROGRESSO

Per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID, ove successivamente modificate ed integrate, sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di servizi previsti nell'Ordinativo), che sarà determinato come da schema seguente:

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	**Fonte dati**	Piano dei Fabbisogni o Piano di lavoro Generale
Periodo di riferimento	Momento di Pianificazione dell'intervento	**Frequenza di misurazione**	Per ogni intervento pianificato
Dati da rilevare	*N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento* *NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID*		
Regole di campionamento	Nessuna		
Formula	$Ip = (N_1 - N_0)/N_T$		
Regole di arrotondamento	Nessuna		
Valore di soglia	*N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;*		
Applicazione	Amministrazione Contraente		

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. Avviso_Pubblico.pdf 

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