CITTA' DI TORINO

DIPARTIMENTO SERVIZI INTERNI
DIVISIONE SISTEMI INFORMATIVI
S. INFRASTRUTTURE E CYBERSECURITY

ATTO N. DD 1009 **Torino, 19/02/2025**

DETERMINAZIONE DIRIGENZIALE

OGGETTO: DETERMINA A CONTRARRE PER L'ADESIONE ALL'ACCORDO QUADRO CONSIP AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI. CIG PADRE 8884642E81 CIG DERIVATO B5A827C520 - INDIZIONE E PRENOTAZIONE IMPEGNO DI SPESA PRESUNTO EURO 295.337,60 € IVA 22% INCLUSA.

Il Piano delle Gare Strategiche ICT previste nell'ambito del Piano Triennale per l'informatica della Pubblica Amministrazione pone tra i suoi obiettivi quello di mettere a disposizione delle PA specifiche iniziative finalizzate all'acquisizione di prodotti e di servizi nell'ambito della sicurezza informatica per l'attuazione del Piano stesso e degli obiettivi del PNRR in quest'ambito, restando in linea con le disposizioni normative relative al settore della cybersicurezza.
Nella logica di continuità di servizio con il Contratto Quadro SPC Cloud - Lotto 2, l'iniziativa Sicurezza da remoto è stata bandita ai sensi dell'art. 4, comma 3 quater del d.l. 95/2012, in base al quale Consip Spa svolge le attività di centrale di committenza relative alle Reti telematiche delle pubbliche amministrazioni, al Sistema pubblico di connettività ai sensi del decreto legislativo 7 marzo 2005, n. 82, e alla Rete internazionale delle pubbliche amministrazioni ai sensi del decreto medesimo nonché ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311.
Tale iniziativa si affianca alle gare strategiche ai fini dell'attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione nelle versioni 2018-2020 e successive, nell'attuazione del processo di trasformazione digitale del Paese.

L'Accordo Quadro ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni, prevede una modalità di affidamento dei Contratti Esecutivi, tramite ordinativo di fornitura a condizioni tutte fissate e si compone di due Lotti: Lotto 1 dedicato ai servizi di sicurezza e Lotto 2 a quello di compliance e controllo.

Preso atto che nella PA ci sono frequenti attacchi a portali che bloccano i servizi erogati e

costituiscono danno di immagine e che è in crescita anche il fenomeno denominato data breach (violazione dei dati) che rappresenta anche una grave violazione del GDPR;
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;

Tenuto conto che tale Accordo è stato stipulato da Consip con vari Raggruppamenti aggiudicatari della procedura aperta medesima e che il Lotto di interesse è il nr. 2 per i servizi di Compliance e controllo;

Dato atto che il Lotto 2 comprende i seguentì servizi di fornitura:
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

Preso atto dell'aggiudicazione da parte di CONSIP del Lotto 2 per le Amministrazioni Locali alla RTI: - 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);

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 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 €. 295.337,60 (IVA 22% inclusa);

Valutato comunque che la chiusura del contratto esecutivo avverrà entro il 31/12/2025, pertanto prima della scadenza temporale dell'AQ, all'esaurirsi del massimale economico previsto;

Dato atto che l'acquisizione oggetto del presente atto è inserita nella programmazione 2025-2027

degli acquisti di beni e servizi con il CUI S00514490010202400252;

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;

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 2 Servizi di Compliance e Controllo" per acquisire servizi in conformità con le disposizioni dell'attuale Piano Triennale ICT e con le normative in materia di Cyber security di riferimento ed adeguarsi alle dinamiche evolutive, utilizzando la tecnologia per accompagnare il processo di trasformazione digitale della PA;

Dato atto che con Deliberazione della Giunta Comunale D.G.C. n. 487 del 6 agosto 2024 si approvava la Strategia Digitale 2024/2028 della Città, che definisce un modello di trasformazione digitale "Citizen-Centric", all'interno del quale vengono declinati quattro obiettivi strategici: la centralità della persona e relazione con il territorio, il valore dei dati per la Città, la sicurezza e resilienza dei servizi digitali e l'Amministrazione digitale;

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 Progetto;

2) di autorizzare, per i motivi esposti in premessa, l'espletamento delle fasi procedurali propedeutiche all'adesione del Comune di Torino all'Accordo Quadro per i servizi di "Servizi di compliance e controllo" Lotto 2 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 8884642E81 CIG DERIVATO B5A827C520 stipulato da CONSIP con il 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 per l'acquisto con Ordine Diretto di SERVIZI DI COMPLIANCE E CONTROLLO;

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 € 295.337,60 (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 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.

9) di dare atto:

- 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;
- l'esigibilità della spesa avverrà entro il 31/12/2025.

Dettaglio economico-finanziario

Si prenota la spesa di Euro 295.337,60 IVA 22% INCLUSA, con la seguente imputazione:

CUI S00514490010202400252

Importo	Anno Bilancio	Missione	Programma	Titolo	Macro Aggregato	Capitolo Articolo	Servizio Responsabile	Scadenza obbligazione
€ 295.337,60	2025	01	08	1	03	026900003003	027	31/12/2025
Descrizione capitolo e articolo		SISTEMI INFORMATIVI - ACQUISTO DI SERVIZI - SERVIZI DI SUPPORTO SPECIALISTICO PER LA TRASFORMAZIONE DIGITALE - settore 027						
Conto Finanziario n°		Descrizione Conto Finanziario						
U.1.03.02.19.011		Processi trasversali alle classi di servizio						

IL DIRIGENTE
Firmato digitalmente
Massimo Massimino

Identificativo: Piano dei Fabbisogni V01

Data: 03/02/2025

ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

LOTTO 2 – SERVIZI DI COMPLIANCE E CONTROLLO

PUBBLICHE AMMINISTRAZIONI LOCALI

DOCPROPERTY Title * MERGEFORMAT Piano dei fabbisogni

Comune di Torino

Deloitte. EY teleco

Firma

1 INTRODUZIONE

1.1 Ambito

Nel settembre 2021 CONSIP ha bandito una procedura aperta, suddivisa in due lotti, per "l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296". Il Lotto 2, inerente ai servizi di compliance e controllo, è stato assegnato come primo aggiudicatario al Raggruppamento Temporaneo di Imprese (RTI), la cui mandataria è Deloitte Consulting S.r.l. SB e le società mandanti sono EY Advisory S.p.A. e Teleco S.r.l., per la stipula di contratti esecutivi con le Pubbliche Amministrazioni Locali (PAL).

La durata dell'Accordo Quadro, originariamente di 24 mesi, è stata estesa a 35 mesi, decorrenti dalla data di attivazione. Per durata dell'Accordo Quadro si intende il periodo entro il quale le Amministrazioni potranno affidare, a seguito della approvazione del Piano Operativo, contratti esecutivi agli operatori economici aggiudicatari parti dell'Accordo Quadro per l'approvvigionamento dei servizi oggetto dell'Accordo Quadro. Ciascun Contratto esecutivo avrà una durata massima di 48 mesi decorrenti dalla relativa data di conclusione delle attività di presa in carico.

Il presente documento costituisce il "Piano dei fabbisogni" (o "Ordinativo di fornitura"), contenente i) i requisiti, i servizi, le caratteristiche qualitative, i dimensionamenti; ii) la descrizione del contesto tecnologico ed applicativo e la descrizione delle attività dimensionate, al fine di permettere la identificazione e contestualizzazione dei servizi nonché la eventuale declinazione delle figure professionali e degli strumenti a supporto.

1.2 Richieste dell'Amministrazione contraente

Il Comune di Torino è l'istituzione pubblica che gestisce l'omonima città. Gli obiettivi strategici che il Comune di Torino si pone mirano a rafforzare il sistema metropolitano in modo tale che accresca la propria intelligenza ed efficienza; lo scopo principale è, infatti, quello di migliorare la qualità della vita dei cittadini.

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.

A partire dal 2022, Il Comune di Torino ha avviato una serie di interventi finalizzati al miglioramento della propria postura di sicurezza. Tali iniziative si inseriscono nel contesto dell'adesione all' "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". In occasione di tale bando finalizzato alla concessione di Fondi PNRR, il Comune di Torino ha aderito all'iniziativa e presentato due progettualità per le quali è stato ottenuto il finanziamento.

Nel corso del 2022 e 2023, sono stati eseguiti due assessment in ambito Cybersecurity volti alla valutazione dello stato di maturità della sicurezza delle informazioni nell'Ente. Tali assessment si sono concentrati principalmente sui processi trasversali del Comune, con un approfondimento su 10 Ambiti di Servizi, principalmente rivolti al cittadino.

Da tali analisi sono quindi emerse una serie di azioni prioritarie al fine di definire un programma sulla sicurezza delle informazioni ed innalzare il livello di maturità in ambito Cyber dell'Ente.

Le azioni, in parte già indirizzate e completate tramite i progetti svolti, riguardavano 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.

In aggiunta alle esigenze in ambito sicurezza delle informazioni, parzialmente indirizzate con gli interventi sopra menzionati, il contesto normativo attuale (vedi Legge Cybersicurezza n.90/2024 e D.lgs. 138/2024 – Direttiva NIS2) richiede un'attenzione ancora maggiore alle tematiche legate alla cybersecurity.

Il Comune è pertanto determinato a implementare azioni concrete per adeguarsi ai requisiti normativi, sviluppando e adeguando processi, politiche e procedure che rafforzino la sicurezza complessiva dell'Ente e tutelino i dati e le informazioni dei cittadini, contribuendo così a un ambiente digitale più sicuro e resiliente. 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 per mitigare i rischi e per contrastare eventi di cybercrime.

Nell'ambito del presente Piano dei Fabbisogni si richiede pertanto un'attività di supporto nell'adeguamento delle iniziative strategiche, individuate a seguito degli assessment effettuati per il rafforzamento della propria Cybersecurity Posture, ai requisiti minimi stabiliti dalla Legge 90 e dalla Direttiva NIS2.

L'intervento mira a proseguire il lavoro di rafforzamento della relazione tra il Comune di Torino e i propri cittadini, aumentando la sicurezza e la resilienza del Sistema Informativo della Città e iniziato con il primo Piano dei Fabbisogni in ambito (2022).

1.3 Riferimenti

IDENTIFICATIVO	TITOLO/DESCRIZIONE
ID 2296 - Gara Sicurezza da remoto - Allegato 1 - Capitolato Tecnico Generale	Capitolato Tecnico Generale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Allegato 2B - Capitolato Tecnico Speciale Lotto 2	Capitolato Tecnico Speciale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Capitolato Oneri	Capitolato d'Oneri della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Bando GURI	Bando GURI della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI

	SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

1.4 Acronimi e glossario

DEFINIZIONE/ACRONNIMO	DESCRIZIONE
RTI	Raggruppamento Temporaneo di Impresa
AQ	Accordo Quadro
CE	Contratto Esecutivo
PAL	Pubblica Amministrazione Locale
PA	Pubblica Amministrazione
PAC	Pubblica Amministrazione Centrale
S.I.	Sistema Informativo
DLT R.A.	Deloitte Risk Advisory Srl
EY	EY Advisory SpA
Teleco	Teleco Srl

2 Anagrafica dell'amministrazione

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
Indirizzo mail	_
PEC	ProtocolloGenerale@cert.comune.torino.it
Codice PA	c_l219
Comparto di Appartenenza (PAL/PAC)	PAL

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	Massimo
Cognome	Massimino
Telefono	01101130501
Indirizzo mail	massimo.massimino@comune.torino.it
PEC	innovazione@cert.comune.torino.it

3 Contesto di riferimento

3.1 Contesto dei servizi

Il Sistema Informativo (SI) della Città di Torino è un sistema complesso ed articolato che integra la gestione dei procedimenti amministrativi interni all'Ente con l'offerta di servizi online 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.

Il Sistema Informativo della Città di Torino si è storicamente modellato sulle competenze dell'Ente, in un primo periodo con risorse ICT interne all'Ente e, successivamente, con l'adesione al CSI Piemonte, con infrastrutture poste nel data center del Consorzio. L'evoluzione tecnologica e il progressivo sviluppo dei servizi digitali hanno determinato uno sviluppo basato su due modelli architetturali, all'interno dei quali sono operativamente attive diverse filiere tecnologiche. La configurazione attuale del S.I. si è accresciuta nel tempo e, ad oggi, risulta composta sia da tecnologie di ultima generazione che da sistemi più datati con una situazione di sovrapposizione, nel parco applicativo, di diverse generazioni tecnologiche. Nel corso degli anni gli interventi hanno privilegiato principalmente lo sviluppo di nuovi servizi a discapito dell'evoluzione tecnologica dei servizi esistenti, aumentando di conseguenza il grado di obsolescenza tecnologica che, ad oggi, costituisce un vincolo rispetto al programma di abilitazione al cloud come previsto dal Piano Triennale AgID.

Lo scenario normativo attuale in cui il Comune opera comprende la Normativa Europea, la Legge sulla Cybersicurezza n.90/2024, il D.lgs. 138/2024 (recepimento della Direttiva (UE) 2022/2555 NIS 2) e il Cyber Security Act. Tali normative evidenziano l'importanza di prestare attenzione al fenomeno del cybercrime, il quale è in costante aumento anche nell'ambito PA. Tale incremento è ulteriormente sottolineato dal Rapporto Clusit 2024, che mette in luce come le mutate condizioni lavorative a seguito della pandemia da Covid-19 abbiano contribuito a questa tendenza.

In particolare, il Decreto 138/2024 e la Legge Cybersicurezza n.90/2024 prevedono obblighi specifici per i soggetti in perimetro, tra cui il Comune di Torino, individuando specifici ambiti, requisiti e misure di sicurezza che ciascun soggetto deve adottare per il rafforzamento della propria resilienza.

AgID ha inoltre individuato nel proprio piano triennale alcune azioni strategiche che saranno attuate anche attraverso la realizzazione dei Computer Emergency Response Team (Cert) regionali, cioè di un tipo specifico di Cert di prossimità, ora denominato CSIRT.

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

3.2 Contesto tecnico ed operativo

Una parte delle componenti "trasversali" del S.I. è gestita in maniera condivisa con le altre PA piemontesi consorziate nel CSI-Piemonte, con obiettivi di razionalizzazione e di economie di scala. La gestione dei servizi digitali erogati dal Comune è quindi prevalentemente affidata al CSI; tuttavia, vi è una parte dei servizi acquisiti dal mercato o erogati da ulteriori terze parti.

3.3 Contesto Economico – Finanziario

Per l'attuazione delle attività di cui al presente Piano dei Fabbisogni l'Amministrazione fa ricorso a fondi dell'Ente.

4 Ambiti funzionali oggetto di intervento

Il significativo processo di trasformazione digitale intrapreso dal Comune di Torino, finalizzato a innovare i servizi offerti ai cittadini, insieme alla necessità di rispondere in modo rapido ed efficace ai cambiamenti provenienti dall'ambiente esterno, evidenziano l'urgenza di prestare sempre più attenzione alle questioni relative alla sicurezza delle informazioni e alla protezione dei dati.

Emergono di fatto nuove esigenze in materia di sicurezza delle Informazioni e delle Infrastrutture, in parte dovute alle recenti normative entrate in vigore per il rafforzamento della cybersicurezza. Tali esigenze sono inoltre dovute al mutamento degli scenari di rischio, dalle nuove minacce e all'ampliamento delle superfici di attacco esposte, da un punto di vista sia interno (es. performance della modalità di lavoro remoto, gestione della sicurezza degli endpoint, miglioramento delle modalità di accesso da remoto ai sistemi) che esterno (es. evoluzioni di modalità e target degli attacchi).

Il Comune, pertanto, è impegnato a rispondere a queste nuove necessità di conformità in ambito di sicurezza informatica, prestando particolare attenzione alle più recenti normative europee e nazionali, tra cui la Legge sulla Cybersicurezza n. 90/2024 e il D.lgs. 138/24, che recepiscono la Direttiva (UE) 2022/2555 NIS 2.

4.1 Obiettivi e benefici da perseguire

L'obiettivo principale del Comune di Torino consiste nell'attuazione delle azioni strategiche delineate in conformità ai requisiti e degli ambiti previsti dalle recenti normative, quali la Legge 90 e la Direttiva NIS 2, e in accordo con i Piani di Progetto approvati dall'Agenzia Nazionale per la Cybersicurezza e finanziati con fondi PNRR.

Le azioni identificate riguardano principalmente la revisione e integrazione del corpo documentale, comprendente metodologie, regolamenti, politiche e procedure precedentemente redatti a seguito degli assessment condotti, con l'obiettivo di adeguare tali documenti alle disposizioni previste dalle nuove normative vigenti (L2.S16 – Security Strategy).

In aggiunta a quanto precedentemente esposto, è inoltre importante proseguire con l'esecuzione delle attività di Business Impact Analysis e Risk Analysis, revisionando ed estendendo il perimetro delle analisi, al fine di includere tutti i servizi e applicativi critici.

In questo contesto, si inquadra anche la necessità dell'esecuzione di un'ulteriore simulazione di Crisi (Table Top), con la finalità di valutare i processi di escalation, i ruoli definiti e il grado di preparazione dell'organizzazione a seguito dei differenti Scenari di incidenti e Crisi (L2.S21 - Supporto all'analisi e alla gestione incidenti).

Tali iniziative consentiranno di potenziare ulteriormente la capacità di gestione dei processi che influenzano la sicurezza delle informazioni dell'Ente, contribuendo così a una significativa riduzione dei rischi cyber inerenti alla propria organizzazione e derivanti dagli attacchi informatici, nonché al conseguente aumento del livello di resilienza alle minacce.

Al fine, inoltre, di elevare il livello di sicurezza dei servizi dell'Ente, in ottemperanza agli obiettivi strategici definiti nel Piano Triennale AgID, ed attraverso l'analisi effettuata in precedenza circa lo stato dei servizi e delle infrastrutture dell'Ente, compreso il loro grado di obsolescenza, e del rischio cyber correlato, l'iniziativa prevede l'esecuzione di ulteriori Test tecnici sui servizi critici identificati dall'organizzazione (L2.S22 - Penetration testing).

4.2 Categorizzazione dell'intervento

4.2.1 Categorizzazione di I livello

	AMBITO I LIVELLO (LAYER)	OBIETTIVI PIANO TRIENNALE
	SERVIZI	Servizi al cittadino
		Servizi a imprese e professionisti
		Servizi interni alla propria PA
		Servizi verso altre PA
	DATI	Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
		Aumentare la qualità dei dati e dei metadati
		Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
	PIATTAFORME	Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
		Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
		Incrementare e razionalizzare il numero di piattaforme per le amministrazioni al fine di semplificare i servizi ai cittadini
		Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
		Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud)
		Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA
	INTEROPERABILITÀ	Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
		Adottare API conformi al Modello di Interoperabilità
x	**SICUREZZA INFORMATICA**	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
		Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

4.2.2 Categorizzazione di II livello

I LIVELLO (LAYER)		II LIVELLO
SERVIZI		Servizi al cittadino
		Servizi a imprese e professionisti
		Servizi interni alla propria PA
		Servizi verso altre PA

PIATTAFORME		Sanità digitale (FSE e CUP)
		Identità Digitale
		Pagamenti digitali
		App IO
		ANPR
		NoiPA
		INAD
		Musei
		Siope+
DATI		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INTEROPERABILITA		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INFRASTRUTTURE		Data center e Cloud
		Connettività
SICUREZZA INFORMATICA	*x*	Portali istituzionali e CMS
	x	Sensibilizzazione del rischio cyber

5 Servizi richiesti

Di seguito si riporta una sintesi dei servizi e relativa quantificazione:

SERVIZI RICHIESTI				
ID	NOME SERVIZIO	VOCE DI COSTO	QUANTITA'	IMPORTO
L2.S16	Security Strategy	L2.S16 — gg/p Team ottimale	**508**	**127.000,00 €**
L2.S21	Supporto all'analisi e alla gestione incidenti	L2.S21 – gg/p Team Ottimale	**147**	**24.990,00 €**
L2.S22	Penetration testing	L2.S22 – gg/p Team ottimale	**546**	**90.090,00 €**
			TOTALE	**242.080,00 €**

5.1 Dettaglio dei servizi richiesti

5.1.1 L2.S16 - Security Strategy

5.1.1.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
Revisione e integrazione del corpo documentale e dei processi in ambito cybersecurity	Revisione e integrazione dei principali processi in ambito Cybersecurity del Comune e formalizzazione di relativi manuali, politiche e procedure.	Manuali, politiche e procedure Report BIA Report Analisi del Rischio Cyber
Misurazione indicatori in ambito sicurezza delle informazioni	Monitoraggio periodico dei KPI per verificare lo stato di maturità in ambito Cybersecurity.	Dashboard di misurazione performance del programma di sicurezza

5.1.1.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Security Solution Architect
- Senior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.1.3 Attivazione e durata

Si prevede l'avvio del servizio entro il 1° marzo 2025 per una durata di 10 mesi (entro il 31 dicembre 2025).

5.1.2 L2.S21 - Supporto all'analisi e gestione degli incidenti

5.1.2.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
Simulazione Table Top	Esecuzione di una simulazione di incident in modalità Table-top	Report della Simulazione

5.1.2.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Security Analyst
- Junior Security Analyst
- Forensic Expert

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.2.3 Attivazione e durata

Si prevede l'avvio del servizio entro il 1° marzo 2025 per una durata di 10 mesi (entro il 31 dicembre 2025).

5.1.3 L2.S22 - Penetration testing

5.1.3.1 Descrizione e caratteristiche del servizio

Macro-attività	Attività	Deliverable
Esecuzione Penetration test	Esecuzione del Penetration test sui servizi applicativi dell'Ente fino ad un massimo di 5 Target	PT Executive Summary PT Technical Report PT Remediation Plan

5.1.3.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Penetration tester
- Junior Penetration tester
- Forensic Expert

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.3.3 Attivazione e durata

Si prevede l'avvio del servizio entro il 1° marzo 2025 per una durata di 10 mesi (entro il 31 dicembre 2025).

5.2 Organizzazione e figure di riferimento dell'amministrazione

Il principale punto di contatto dell'amministrazione è Massimo Massimino, direttore del Servizio Infrastrutture e Cybersecurity.

L'amministrazione si riserva di poter identificare durante l'esecuzione del contratto ulteriori figure di riferimento con le quali il fornitore potrà interfacciarsi.

5.3 Organizzazione e figure di riferimento del fornitore

Si richiede di indicare nel Piano Operativo le persone incaricate dal Fornitore per la conduzione del progetto e i relativi ruoli/responsabilità.

6 Elementi quantitativi e qualitativi per il dimensionamento servizi

6.1 Elementi quantitativi dei servizi

Si riporta di seguito una caratterizzazione quantitativa di riferimento data dalla complessità dei processi individuati:

ID	NOME SERVIZIO	Gg/p Team ottimale	Uffici interessati	Ambiti di servizio	Numero Key user coinvolti	Numero Volumi
L2.S16	Security Strategy	508	**c.a.10**	**c.a.15**	**c.a.20**	**N/A**
L2.S21	Supporto all'analisi e alla gestione incidenti	147	**c.a.10**	**c.a.15**	**c.a.20**	**N/A**
L2.S22	Penetration testing	546	**c.a.10**	**c.a.15**	**c.a.20**	**5 Target**

6.2 Elementi qualitativi dei servizi

I servizi dovranno essere svolti tenendo conto delle linee guida tecniche e la normativa vigente o le successive modifiche che verranno individuate.

6.3 Pianificazione dei servizi

La durata ipotizzata per la fornitura è di 10 mesi dalla data di attivazione, compatibilmente con il vincolo definito dall'Accordo quadro, ovvero che i Contratti Esecutivi hanno una durata massima pari alla durata residua, al momento della sua stipula, dell'Accordo Quadro.

Di seguito si riporta la pianificazione di massima del programma con indicazione degli obiettivi in ambito del presente piano dei fabbisogni.

	Mese1	Mese2	Mese3	Mese4	Mese5	Mese6	Mese7	Mese8	Mese9	Mese10
L2.S16										
L2.S21										
L2.S22										