CITTA' DI TORINO

DIPARTIMENTO SERVIZI INTERNI
DIVISIONE SISTEMI INFORMATIVI
S. INFRASTRUTTURE E CYBERSECURITY

ATTO N. DD 2988 **Torino, 06/06/2023**

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 2 - CUP C17H22002830006 E CUP C17H22002840006 CIG PADRE 8884642E81 CIG DERIVATO 9816963E22 - FINANZIATO DALL'UNIONE EUROPA - NEXTGENERATIONEU, INDIZIONE E PRENOTAZIONE IMPEGNO DI SPESA EURO 893.534,10 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.

Nel corso del 2022, Il Comune di Torino ha avviato una serie di interventi finalizzati al miglioramento della postura di sicurezza. Tali iniziative si inseriscono nel contesto dell’adesione al sopracitato Avviso pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” M1C1I1.5 WP-9”.

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.

Tali iniziative 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.

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 2020-2022, 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;

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;

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 Amministrazione è il nr. 2 per i servizi di Compliance e controllo con durata di 24 (ventiquattro) mesi con decorrenza 01 settembre 2022 e scadenza il 31 agosto 2024, termine ultimo entro il quale si potrà affidare il Contrattio Attuativo;

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

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 € 893.534,10 (IVA 22% inclusa), così suddiviso:

- progetto "Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino" - CUP C17H22002830006: euro 660.326,00 oltre IVA al 22% per un totale complessivo di euro 805.597,72 per le forniture di servizi L2.S16 Security Strategy, L2.S21 Supporto all'analisi e gestione degli incidenti ed L2.S22 Penetration Testing, così come meglio dettagliate nel Piano dei Fabbisogni;
- progetto "Cybersecurity: incremento della consapevolezza del rischio cyber e sviluppo nuovi sistemi per la mitigazione del rischio nella Città di Torino" - CUP C17H22002840006: euro 72.079,00 oltre IVA al 22% per un totale complessivo di euro 87.936,38 per le forniture di servizi L2.S16 Security Strategy ed L2.S22 Penetration Testing, così come meglio dettagliate nel Piano dei Fabbisogni;

Tenuto conto che i rispettivi CUI sono attualmente in fase di richiesta;

Considerato l'ipotetico avanzamento del progetto si provvede a prenotare le somme come da dettaglio economico;

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

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;

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 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 9816963E22 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'affidamento 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 Cyber security 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 € 893.534,10 (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;
- ai sensi della circolare prot. n.16298 del 19/12/2012 il presente provvedimento non è pertinente alle disposizioni in materia di valutazione dell'impatto economico (VIE);
- che 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 di ogni anno, come da dettaglio economico.

Dettaglio economico-finanziario

Si prenota la spesa di 893.534,10 Euro con le seguenti imputazioni:
- di cui euro 805.597,72 per progetto "Analisi della postura di sicurezza e miglioramento nella gestione dei processi legati alla cybersecurity della Città di Torino" - CUP C17H22002830006 - :

Importo	Anno Bilancio	Missione	Programma	Titolo	Macro aggregato	Capitolo e articolo	Responsabile	Scadenza Obbligazione
245.773,80 559.823,92	2023 2024	01 01	08 08	2 2	02 02	118660005001 118660005001	027 027	31/12/2023 31/12/2024
Descrizione capitolo e articolo	PNRR-M1 C1 I1.5 CYBERSECURITY ANALISI DELLA POSTURA DI SICUREZZA E MIGLIORAM. NELLA GESTIONE DEI PROCESSI LEGATI ALLA CIBERSECURITY DELLA CITTA' DI TORINO C17H22002830006 VEDASI 046500057 E set. 027							
Conto Finanziario n°	Descrizione Conto Finanziario							
U.2.02.03.02.001	Sviluppo software e manutenzione evolutiva							

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

Importo	Anno Bilancio	Missione	Programma	Titolo	Macro aggregato	Capitolo e articolo	Responsabile	Scadenza Obbligazione
26.380,91 61.555,47	2023 2024	01 01	08 08	2 2	02 02	11866000 4001 11866000 4001	027 027	31/12/2023 31/12/2024
Descrizione capitolo e articolo		PNRR-M1 C1 I1.5 CYBERSECURITY INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZ. DEL RISCHIO NELLA CITTA' DI TORINO C17H22002840006 VEDASI 046500056 E set. 027						
Conto Finanziario n°		Descrizione Conto Finanziario						
U.2.02.03.02.001		Sviluppo software e manutenzione evolutiva						

Tali spese trovano capienza nei fondi accertati con D.D. 1585 del 03/04/2023:
ACCERTAMENTO 3410/2023

Importo	Anno Bilancio	Titolo	Tipologia	Categoria	Capitolo e articolo	Responsabile Servizio	Scadenza Obbligazione
245.773,80	2023	4	0200	01	046500057001	068	31/12/2023
Descrizione capitolo e articolo		PNRR-M1 C1 I1.5 CYBERSECURITY ANALISI DELLA POSTURA DI SICUREZZA E MIGLIORAM. NELLA GESTIONE DEI PROCESSI LEGATI ALLA CYBERSECURITY DELLA CITTA' DI TORINO C17H22002830006 VEDASI CAP. 118660005 SPESA - Resp. E SETT, 068					
Conto Finanziario n°		Descrizione Conto Finanziario					
E.2.01.01.01.001		Trasferimenti correnti da Ministeri					

ACCERTAMENTO 2202/2024

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

ACCERTAMENTO 3411/2023

Importo	Anno Bilancio	Titolo	Tipologia	Categoria	Capitolo e articolo	Responsabile Servizio	Scadenza Obbligazione
61.555,47	2024	4	0200	01	046500056001	068	31/12/2024
Descrizione capitolo e articolo	PNRR-M1 C1 I1.5 CYBERSECURITY INCREMENTO DELLA CONSAPEVOLEZZA DEL RISCHIO CYBER E SVILUPPO NUOVI SISTEMI PER LA MITIGAZ. DEL RISCHIO NELLA CITTA' DI TORINO C17H22002840006 VEDASI CAP. 118660004 SPESA - Resp. E SETT. 068						
Conto Finanziario n°	Descrizione Conto Finanziario						
E.4.02.01.01.001	Contributi agli investimenti da Ministeri						

IL DIRIGENTE

Firmato digitalmente
Massimo Massimino

Identificativo: Piano dei Fabbisogni V03

Data: 22/03/2023

Firma

Deloitte. EY teleco

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 Risk Advisory S.r.l. 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 è di 24 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.

Nel corso del 2022, Il Comune di Torino ha avviato una serie di interventi finalizzati al miglioramento della postura di sicurezza. Tali iniziative si inseriscono nel contesto dell'adesione 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.

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

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

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

Nell'ambito del presente Piano dei Fabbisogni si richiede un'attività di supporto nell'implementazione delle iniziative strategiche di breve-medio e lungo periodo, individuate a seguito dell'assessment effettuato come prioritarie per il rafforzamento della propria Cybersecurity Posture. 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

Indicare gli elementi contrattuali di riferimento

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

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 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.
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 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.

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 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.

3.2 Contesto tecnico ed operativo

Una parte delle componenti "trasversali" al 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 è possibile da parte dell'Amministrazione il ricorso, in tutto o in parte, all'utilizzo dei fondi economici ai sensi del D.L.

77/2021. Inoltre l'Amministrazione ricorrerà ai fondi PNRR relativi 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".

4 Ambiti funzionali oggetto di intervento

Il profondo processo di trasformazione digitale avviato dal Comune di Torino, avente la finalità di portare innovazione nei servizi forniti ai cittadini, e la capacità di dover rispondere in maniera rapida ed efficace ai cambiamenti imposti anche dall'ambiente esterno pongono la necessità di una maggior attenzione alle tematiche che riguardano la sicurezza delle informazioni e la protezione dei dati.

Emergono di fatto nuove esigenze di sicurezza delle Informazioni e delle Infrastrutture dovute al mutamento degli scenari di rischio, dalle nuove minacce e dall'estensione 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). Inoltre, il Comune intende far fronte alle nuove esigenze di conformità in ambito privacy e sicurezza con particolare riferimento alle più recenti normative in ambito Europeo e Nazionale.

4.1 Obiettivi e benefici da perseguire

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 azioni identificate riguardano in larga parte la definizione, revisione e relativa formalizzazione in un corpo documentale (manuali, regolamenti, politiche e procedure) dei processi fondamentali inerenti all'ambito della sicurezza delle informazioni, che risultano definiti in modo lasco lato Ente e la cui gestione attuale si affida in larga parte ai processi in essere propri di CSI Piemonte (L2.S16 – Security Strategy).

In aggiunta a quanto sopra indicato, e con l'obiettivo di proseguire nella verifica del livello di maturità Cybersecurity - con riferimento ai processi e servizi posti in essere dai differenti ambiti di servizi al cittadino erogati dal Comune di Torino (che, tenuto conto della loro natura intrinsecamente variegata, potrebbero riportare difformità e specificità rispetto a quanto rilevato mediante l'assessment trasversale), si pone l'obiettivo di integrare il Piano strategico e la Roadmap evolutiva delle iniziative in ambito Cybersecurity con eventuali ulteriori azioni che dovessero emergere a seguito dell'esecuzione di assessment della Cyber Posture verticali su ulteriori ambiti di servizi (L2.S16 – Security Strategy).

In questo contesto, si inquadra anche la necessità di proseguire con i lavori di ridefinizione del Piano di risposta agli incidenti e il modello per la ripartenza dei servizi in caso di attacco/incidente informatico in accordo con quanto definito all'interno del Piano triennale ICT della Città di Torino 2022-2024 (L2.S21 - Supporto all'analisi e alla gestione incidenti).

Tali iniziative 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.

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 dello 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 Test tecnici su ulteriori 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

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

4.3 Indicatori di digitalizzazione

4.3.1 Indicatori generali di digitalizzazione

Di seguito si riportano gli indicatori Generali di digitalizzazione previsti per la presente fornitura:

INDICATORI DI COLLABORAZIONE E		VALORE EX ANTE	VALORE EX POST
	Riuso di processi per erogazione servizi digitali	*Nessuna*	*Gestione Uniforme della Sicurezza delle informazioni per i servizi erogati dall'Ente*

Per ciascuno dei soprariportati indicatori, verrà effettuata una valutazione in fase di avvio dei singoli interventi progettuali e a valle, così da misurare il livello di digitalizzazione raggiunto per ciascuno di essi.

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	**2277**	**569.250,00 €**
L2.S21	Supporto all'analisi e alla gestione incidenti	L2.S22 – gg/p Team Ottimale	**324**	**55.080,00 €**
L2.S22	Penetration testing	L2.S22 – gg/p Team ottimale	**655**	**108.075, 00 €**
			TOTALE	**732.405,00 €**

Sulla base di quanto previso dai progetti ACN, i servizi di sopra indicati verranno rendicontati con riferimento a questi CUP:

SERVIZI RICHIESTI

ID	NOME SERVIZIO	Macro - Attività	CUP	IMPORTO
L2.S16	Security Strategy	Integrazione al Piano strategico e Roadmap iniziative evolutive Cyber Definizione e redazione corpo documentale	**C17H22002830006**	**528.267,00 €**
L2.S16	Security Strategy	Definizione e misurazione indicatori in ambito sicurezza delle informazioni	**C17H22002840006**	**40.983,00 €**
L2.S21	Supporto all'analisi e alla	Modello e processi di	**C17H22002830006**	**55.080,00 €**

	gestione incidenti	gestione della crisi ICT Revisione del processo di Rilevazione e risposta agli incidenti Simulazione Table Top		
L2.S22	Penetration testing	Esecuzione Penetration test (4 TARGET)	**C17H22002830006**	**76.979,00 €**
L2.S22	Penetration testing	Esecuzione Penetration test (2 TARGET)	**C17H22002840006**	**31.096,00 €**
			TOTALE	**732.405,00 €**

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
Integrazione al Piano strategico e Roadmap iniziative evolutive Cyber	Esecuzione di un assessment verticale su altri ambiti verticali (fino a 6) finalizzato all'identificazione delle ulteriori iniziative da integrare nel piano strategico dell'Ente in ambito sicurezza delle informazioni.	Piano Strategico Cybersecurity
Definizione e redazione corpo documentale	Definizione e revisione dei principali processi in ambito Cybersecurity del Comune e formalizzazione di relativi manuali, politiche e procedure.	Manuali, politiche e procedure
Definizione e misurazione indicatori in ambito sicurezza delle informazioni	Identificazione dei KPI per verificare lo stato di maturità in ambito Cybersecurity e definizione del processo di monitoraggio.	Elenco indicatori 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 in concerto con l'Amministrazione i task e i rispettivi 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 Aprile 2023 per una durata di un anno.

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
Modello e processi di gestione della crisi ICT	Aggiornamento delle procedure di escalation e del modello organizzativo di gestione delle crisi con riferimento ad ulteriori scenari	Procedura di Crisis Management.
Simulazione Table Top	Esecuzione di una simulazione di incident in modalità table-top	Report della Simulazione
Revisione del processo di Rilevazione e risposta agli incidenti	Revisione del modello di gestione e risposta agli incidenti	Playbook di risposta agli incidenti aggiornati

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 Aprile 2023 per una durata di un anno.

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 6 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 Aprile 2023 per una durata di un anno.

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	2277	**c.a.10**	**c.a.15**	**c.a.20**	**N/A**
L2.S21	Supporto all'analisi e alla gestione incidenti	324	**c.a.10**	**c.a.15**	**c.a.20**	**N/A**
L2.S22	Penetration testing	655	**c.a.10**	**c.a.15**	**c.a.20**	**6 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 12 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.

	Mese 1	Mese 2	Mese 3	Mese 4	Mese 5	Mese 6	Mese 7	Mese 8	Mese 9	Mese 10	Mese 11	Mese 12
L2.S16												
L2.S21												
L2.S22												

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