# CITTÀ METROPOLITANA DI GENOVA

Direzione Sviluppo economico e provveditorato
Servizio Sviluppo economico e sistemi informativi

## Attestazione documenti allegati

Atto N. 3011/2024

**OGGETTO: ID.2024_169 PNRR M1C1I1.5 - "CYBERSECURITY" - FINANZIATO DALL'UNIONE EUROPEA, NEXTGENERATIONEU. SERVIZIO DI CONSULENZA E ACQUISTO FORNITURE PER L'ATTUAZIONE DEL PROGETTO "CYBER CMGE"- AFFIDAMENTO IN HOUSE AI SENSI DELL'ART. 7 DEL D.LGS. N. 36/2023 A LIGURIA DIGITALE S.P.A. - CUP D41B20001480006 - CIG B451B6CDF8 - IMPORTO DI EURO 1.257.713,37 ONERI FISCALI INCLUSI.**

Si dichiara che all'atto in oggetto sono allegati i seguenti documenti, per i quali si riportano il titolo e l'hash code calcolato prima della firma dell'atto stesso (se l'allegato è firmato digitalmente)

### Allegati:

Nome file allegato: PR_DET_PROP_3307_2024.docx
Hash:
0C9D3A637AFBC98FC599B85C495D0DE72D5D15651D7430D1CE7D65B9D7FE58D58F61D42C5C394DA0D0840AC0D1F6E645F6FD9AA8188EB1FB46842CA2BCD996F8

Nome file allegato: Congruità LD per il progetto Cyber-CMGE_signed.pdf
Hash:
37B6D942E63594CD59677A34CD125A001EBD3544D7929BCC185CDA61FB2DF496B8D0ED7E6665DBF27CF3ABE1E46C620B87A2A992CAC90C584F375813B65F8C62

Nome file allegato: Capitolato per fornitura di un servizio di consulenza per attuazione progetto CYBER CMGE.pdf
Hash:
B986C1141B53CCC7DD744CD9C9D295166F5542ED20865626E05FC3D57729731F6C8346DBB5C9FFA60320DBACF69BE69F66EB91C0DC95003CF0C0BF580EAF4DD0

**Sottoscritta da**
**(MAURIZIO TORRE)**
**con firma digitale**

# CITTÀ METROPOLITANA DI GENOVA

***Atto dirigenziale***

Direzione Sviluppo economico e provveditorato
Servizio Sviluppo economico e sistemi informativi

Atto N. 3011/2024

Finanziato dall'Unione europea NextGenerationEU

**PIANO NAZIONALE DI RIPRESA E RESILIENZA**

**Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"**

**M1C1I1.5**

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Città Metropolitana di Genova

**Oggetto: ID.2024_169 PNRR M1C1I1.5 - "CYBERSECURITY" - FINANZIATO DALL'UNIONE EUROPEA, NEXTGENERATIONEU. SERVIZIO DI CONSULENZA E ACQUISTO FORNITURE PER L'ATTUAZIONE DEL PROGETTO "CYBER CMGE"- AFFIDAMENTO IN HOUSE AI SENSI DELL'ART. 7 DEL D.LGS. N. 36/2023 A LIGURIA DIGITALE S.P.A. - CUP D41B20001480006 - CIG B451B6CDF8 - IMPORTO DI EURO 1.257.713,37 ONERI FISCALI INCLUSI.**

In data 22/11/2024 il dirigente MAURIZIO TORRE, nella sua qualità di responsabile, adotta il seguente Atto dirigenziale;

Vista la Legge 7 aprile 2014 n. 56, "Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni";

Richiamato lo Statuto della Città Metropolitana di Genova;

Visto l'art. 107, commi 1, 2 e 3, del Decreto Legislativo 18 agosto 2000, n. 267, "Testo unico delle leggi sull'ordinamento degli enti locali".

Premesso che

- la Missione 1 "*Digitalizzazione, Innovazione, Competitività, Cultura e Turismo*", Componente 1 "*Digitalizzazione, Innovazione e Sicurezza della P.A.*", Investimento 1.5 "*Cybersecurity*" del PNRR prevede interventi per la digitalizzazione delle infrastrutture tecnologiche e dei servizi della P.A., rafforzando le difese cyber nazionali, mediante lo stanziamento complessivo di € 623.000.000,00 (seicentoventitremilioni/00);

- 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"*, individua il Dipartimento per la Trasformazione Digitale

(DTD) della Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante *"Cybersecurity"*;

- in data 14 dicembre 2021, è stato sottoscritto un accordo stipulato, tra il Dipartimento per la trasformazione digitale e l'Agenzia per la Cybersicurezza Nazionale (di seguito denominata anche ACN), ai sensi dell'articolo 5, comma 6, del n. Decreto Legislativo 18 aprile 2016, n. 50, di cui al prot. ACN n. 896 del 15 dicembre 2021, per disciplinare lo svolgimento in collaborazione delle attività di realizzazione dell'"*Investimento 1.5*", registrato dalla Corte dei Conti il 18 gennaio 2022 al n. 95, e modificato dall'atto aggiuntivo del 14 luglio 2023, registrato dalla Corte dei Conti il 5 settembre 2023 al n. 2425;

Dato atto che:

- in data 26/02/2024 è stato pubblicato l'avviso pubblico n. 08/2024 "*per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5*";

- l'avviso era volto alla selezione di proposte progettuali riguardanti la realizzazione di interventi di potenziamento della *resilienza cyber* delle Pubbliche Amministrazioni, finalizzati ad irrobustire le infrastrutture e i servizi digitali del Sistema Paese nonché migliorare le competenze specialistiche necessarie e a garantire adeguati livelli di cyber resilienza, realizzando un percorso virtuoso di gestione del rischio cyber che prevede:

    - il finanziamento per la realizzazione di un censimento dei livelli di maturità della postura di sicurezza delle PA;

    - il finanziamento per la realizzazione di interventi di potenziamento dell'organizzazione, dei processi e delle procedure per la gestione del rischio cyber nella PA;

    - il finanziamento per la realizzazione di un piano programmatico di potenziamento delle capacità cyber a favore del personale in modo da rafforzare il percorso di trasformazione digitale sicura della PA

Preso atto che

- con nota prot. n. 22766 del 05/04/2024 e successiva nota di integrazione n. 24174 del 11/04/2024, Città Metropolitana di Genova ha manifestato all'Agenzia per la Cybersicurezza Nazionale l'interesse a partecipare, presentando il progetto denominato "Cyber-CMGE" per un importo complessivo pari a euro 1.345.753,31 (CUP D41B20001480006), coinvolgendo i seguenti comuni del territorio: Borzonasca, Camogli , Campomorone, Carasco, Casarza Ligure, Casella, Chiavari, Cicagna, Cogoleto, Cogorno, Crocefieschi, Gorreto, Lavagna, Lorsica, Mele, Montoggio, Ne, Orero, Pieve Ligure,

Portofino, Rapallo, Recco, Ronco Scrivia, Rovegno, Santa Margherita Ligure, Santo Stefano d'Aveto, Savignone, Sestri Levante, Vobbia;

- ACN ha trasmesso, con PEC acquisita al Protocollo Generale n. 44690 del 12/07/2024, la determina di ammissione di Città Metropolitana di Genova alle successive fasi della procedura di aggiudicazione;

- ACN ha comunicato, con PEC acquisita al Protocollo Generale n. 57411 del 25/09/2024, che Città Metropolitana di Genova è stata ammessa al finanziamento, essendo il suo progetto classificato 8° su 79 proposte (escludendo le proposte parzialmente finanziate e le proposte non ammesse alla selezione), e contestualmente ha trasmesso la determina di concessione del finanziamento di euro 1.345.753,31 per la realizzazione del progetto presentato "Cyber-CMGE", richiedendo la sottoscrizione dell'Atto d'Obbligo per dare seguito all'attuazione del progetto;

Considerato il Decreto del Sindaco metropolitano n. 71 dell'11 ottobre 2024 con cui ha autorizzato il Responsabile per la Transizione Digitale alla sottoscrizione dell'Atto d'Obbligo tra Città Metropolitana di Genova e l'Agenzia per la Cybersicurezza Nazionale;

Richiamato l'atto dirigenziale della Direzione Sviluppo economico e provveditorato di Città Metropolitana n. 2822 del 05/11/2024 con cui è stato nominato Responsabile Unico del Progetto (RUP) Flavio Rossi, responsabile dell'Ufficio Sistemi Informativi, demandando allo stesso la definizione di tutti gli atti successivi necessari alla corretta realizzazione del progetto.

Considerato che il progetto "CYBER-CMGE" prevede il miglioramento delle capacità di governo e gestione del rischio cyber, per contrastare uno scenario di minaccia in continua evoluzione, e contestualmente consentire una risposta tempestiva a potenziali attacchi informatici, intervenendo nelle seguenti linee d'azione:

1. Governance e programmazione cyber: coordinamento, supervisione e gestione olistica e integrata della cybersecurity attraverso la programmazione strategica di investimenti e iniziative;

2. Gestione del rischio cyber e della continuità operativa: individuazione, valutazione e trattamento sistematico dei rischi associati all'ambito cyber, e implementazione di un piano volto a garantire la resilienza di funzioni e servizi critici in caso di eventi avversi;

3. Gestione e risposta agli incidenti di sicurezza: monitoraggio, identificazione e gestione degli incidenti cyber, e ripristino dei sistemi impattati;

4. Gestione delle identità digitali e degli accessi logici: governo delle identità e definizione dei permessi di accesso alle risorse al fine di autenticare e autorizzare correttamente persone, gruppi e servizi in base agli attributi specifici e ai principi di "*need to know*", "*least privilege*" e "*segregation of duties*";

5. Sicurezza delle applicazioni, dei dati e delle reti: protezione dell'infrastruttura applicativa e di rete, e regolamentazione dei processi di protezione dei dati riservati, al fine di prevenire l'occorrenza di potenziali incidenti cyber e ridurne gli impatti.

Rilevato che le fasi per la conduzione del progetto sono molteplici e complesse, coinvolgono la programmazione e la gestione del finanziamento, il rispetto della normativa comunitaria e nazionale di settore, il monitoraggio della realizzazione degli interventi, il controllo dello stato di avanzamento fisico, procedurale e finanziario e la rendicontazione secondo le regole dell'amministrazione centrale e del PNRR.

Ritenuto opportuno avvalersi del supporto di un soggetto esterno, qualificato e idoneo a fornire i servizi tecnico al RUP e i contributi specialistici nelle attività di governance del progetto.

Considerato che i servizi richiesti possono essere affidati a Liguria Digitale S.p.A., società ICT della Regione Liguria e partecipata da Città Metropolitana di Genova e da altri enti, per operare secondo il modello dell'in house providing, stabilito dall'ordinamento dell'Unione Europea e dall'ordinamento interno a norma degli articoli 16 del Decreto Legislativo 19 agosto 2016, n. 175, "Testo unico in materia di società a partecipazione pubblica" e dal Decreto Legislativo 18 aprile 2016, n. 50, come riportato nell'art. 4 dello statuto societario, soggetta al controllo analogo congiunto da parte di tutti i soci, anche perché Liguria Digitale risulta anche affidataria in house da parte di Città Metropolitana di altri servizi su cui impatta pesantemente il progetto in questione.

Considerato che Liguria Digitale è individuata quale centrale di committenza prevalentemente per l'acquisto di beni e servizi informatici (ICT) come articolazione funzionale della Stazione Unica Appaltante Regionale (SUAR), Soggetto Aggregatore qualificato di diritto, ed opera pertanto quale Stazione Appaltante e Centrale di Committenza qualificata, in favore sia degli Enti aderenti sia della stessa società, in piena ottemperanza alle disposizioni normative di cui al decreto legislativo 31 marzo 2023 n. 36 recante "Codice dei Contratti Pubblici", iscritta nell'elenco ANAC, con il massimo livello di qualificazione per gli acquisti di servizi e forniture senza limiti di importo (SF1).

Ritenuto pertanto di avvalersi di Liguria Digitale anche come stazione appaltante per gli affidamenti previsti a progetto, con particolare riguardo all'acquisto di materiale informatico da destinare a dotazione degli uffici di Città Metropolitana per un importo pari a Euro 607.110,00 oneri fiscali inclusi, per ragioni di unitarietà del progetto e di economie dei processi.

Vista la relazione in atti sulla congruità economica dell'offerta di Liguria Digitale, predisposta ai sensi dell'art. 7 del Decreto Legislativo 31 marzo 2023, n. 36, dall'Ufficio Sistemi Informativi, nella quale viene evidenziata la convenienza di tale soluzione attraverso una valutazione della congruità dei costi, reputando l'offerta dei costi interni di commessa formulata da Liguria Digitale S.p.a. ragionevolmente congrua ed in linea con i servizi richiesti, come si evince dal benchmarking effettuato dalla Società Ernst & Young sui profili professionali e sul costo medio delle relative prestazioni con riferimento al mercato dei servizi ICT inserito nella Relazione Previsionale e Programmatica 2024 della società.

Rilevato che:

# CITTÀ METROPOLITANA DI GENOVA

***Atto dirigenziale***

Direzione Sviluppo economico e provveditorato
Servizio Sviluppo economico e sistemi informativi

- con delibera del Consiglio Metropolitano n. 11 del 22/05/2019 la Città Metropolitana di Genova, confermando la volontà espressa con la delibera del Consiglio Metropolitano n. 52 del 28 dicembre 2018, ha approvato la partecipazione alla società Liguria Digitale S.p.A. secondo i contenuti dello statuto e dei patti parasociali;

- la società Liguria Digitale S.p.A. è vincolata a realizzare oltre l'80% del proprio fatturato nei confronti e nell'interesse della Regione Liguria, degli Enti soci e dei loro organismi ausiliari per i quali opera al costo (art. 4 dello statuto);

- nei patti parasociali è garantito che gli Enti Soci esercitano su Liguria Digitale S.p.A. il controllo analogo a quello esercitato sulle proprie strutture e in relazione ai servizi dalla stessa prestati nei loro confronti: i Soci, in particolare, esercitano il controllo analogo congiunto mediante la partecipazione diretta al Comitato di Coordinamento dei Soci di cui all'art. 25 dello statuto;

- con nota prot. PG/2020/108486 del 25 marzo 2020, in ottemperanza all'art.192 del Decreto Legislativo 18 aprile 2016, n. 50, Codice dei Contratti Pubblici, la Regione Liguria ha comunicato all'ANAC l'iscrizione della società Liguria Digitale S.p.A., nell'elenco delle amministrazioni aggiudicatrici che operano mediante affidamenti diretti in house da part degli Enti soci;

- con nota prot. n. 6829/2021 del 10 febbraio 2021, Città Metropolitana chiedeva a Regione Liguria di fornire evidenza all'A.N.A.C. "dell'avvenuta comunicazione di variazione della compagine sociale o, in alternativa, di procedervi quanto prima inserendo la scrivente Amministrazione tra i soci che esercitano il controllo analogo congiunto, come previsto dal punto 7 delle Linee Guida A.N.A.C. n. 7";

- con nota prot. n. 8644/2021 del 19 febbraio 2021, Regione Liguria chiedeva ad A.N.A.C. l'aggiornamento dell'elenco di cui all'art. 192 del Decreto Legislativo 50/2016 "inserendo la Città Metropolitana di Genova tra gli enti che hanno acquisito una partecipazione societaria in Liguria Digitale S.p.A.";

- con nota prot. n. 37867/2021 del 30 luglio 2021 Città Metropolitana richiedeva ad A.N.A.C. "l'aggiornamento dell'Elenco delle Amministrazioni aggiudicatrici e degli enti aggiudicatori che operano mediante affidamenti diretti nei confronti di proprie società in house ex art. 192 del Decreto Legislativo 18 aprile 2016, n. 50".

Atteso che, con nota interna n. 68061 del 15/11/2024, nell'ambito della Direzione Sviluppo Economico e Provveditorato, l'Ufficio Sistemi Informativi ha richiesto all'Ufficio Centrale Acquisti, a ciò preposto ai sensi delle vigenti "Istruzioni operative acquisti", le attività propedeutiche all'affidamento in house a Liguria Digitale del servizio in oggetto.

Preso atto che la funzione di Responsabile di Procedimento per la fase di affidamento, ai sensi dell'art. 15, comma 4, del Decreto Legislativo 31 marzo 2023, n. 36, è stata svolta dalla Dott.ssa Francesca Damonte, responsabile dell'Ufficio Centrale Acquisti, che ha acquisito sulla piattaforma

# CITTÀ METROPOLITANA DI GENOVA

***Atto dirigenziale***

Direzione Sviluppo economico e provveditorato
Servizio Sviluppo economico e sistemi informativi

telematica MEPA, mediante interoperabilità con la Piattaforma dei Contratti Pubblici (PCP) di ANAC, il CIG n. B451B6CDF8, ai sensi della Legge del 13 agosto 2010, n. 136.

Dato atto che la procedura di acquisto è stata svolta tenendo conto delle seguenti disposizioni:

- Decreto Legislativo 31 marzo 2023, n. 36, Codice dei Contratti Pubblici, ed in particolare:

  art. 17, comma 2, decisione di contrarre;

  art. 23, comma 5, obblighi informativi verso la Banca dati nazionale dei contratti pubblici attraverso le piattaforme telematiche;

  art. 25, piattaforme di approvvigionamento digitale;

- il Decreto Legge 31 maggio 2021, n. 77 convertito con modificazioni dalla legge 29 luglio 2021, n. 108, ed in particolare l'art. 51;

- Istruzioni operative verifiche contraente, stipula e conservazione del contratto adottate con atto dirigenziale della Segreteria e Direzione Generale n. 1715 del 28 luglio 2023.

Dato atto che l'Ufficio Centrale Acquisti:

- ha acquisito sulla piattaforma telematica MEPA (procedura n. NG4833600) il preventivo di Liguria Digitale per un importo contrattuale così determinato:

| | |
|---|---|
| Importo complessivo | 1.030.912,61 € |
| IVA al 22% | 226.800,77 € |
| **TOTALE** (oneri fiscali inclusi) | **1.257.713,38 €** |

  comprensivi di Euro 607.110,00 oneri fiscali inclusi, destinati all'acquisto di attrezzature informatiche.

- al termine della fase istruttoria, ha trasmesso all'Ufficio Sistemi Informativi con nota interna n. 68395 del 18/11/2024 la documentazione relativa all'offerta pervenuta;

Dato atto che il responsabile di procedimento per la fase di affidamento attesta la regolarità e correttezza dell'azione amministrativa per quanto di competenza, ai sensi dell'articolo 147-bis del Decreto Legislativo 18 agosto 2000, n. 267;

Atteso che Città Metropolitana si riserva di definire in accordo con ACN la destinazione ad altri utilizzi, nell'ambito del progetto, delle economie generate dai ribassi d'asta o dai prezzi di acquisto in convenzione Consip e/o sulla base di accordi quadro stipulati da altri soggetti aggregatori.

Visto il Bilancio di previsione 2024 - 2026 approvato in via definitiva dal Consiglio Metropolitano

# CITTÀ METROPOLITANA DI GENOVA

## *Atto dirigenziale*

Direzione Sviluppo economico e provveditorato
Servizio Sviluppo economico e sistemi informativi

con la propria Deliberazione n. 34 del 15 dicembre 2023;

Visto il Decreto del Sindaco metropolitano n. 11 dell'8 febbraio 2024 con cui sono stati approvati il Piano Integrato di Attività e Organizzazione (PIAO) e relativi allegati, il Piano Esecutivo di Gestione 2024-2026 e il Gender Equality Plan 2024-2026;

Dato atto che:

- alla spesa derivante dal presente provvedimento si farà fronte con le risorse disponibili sugli stanziamenti di bilancio indicati nel prospetto contabile;
- il presente provvedimento diventa efficace con l'apposizione del visto attestante la copertura finanziaria espresso ai sensi dell'articolo 147-bis del Decreto Legislativo 18 agosto 2000, n. 267, come da allegato;

Vista la Determinazione del Sindaco Metropolitano n.1/2022 del 13/01/2022 "Approvazione definitiva del nuovo Codice di Comportamento dei dipendenti di Città Metropolitana di Genova";

Preso atto che:

- l'istruttoria del presente atto è stata svolta da Claudio Chiesa che attesta la regolarità e correttezza dell'azione amministrativa per quanto di competenza, ai sensi dell'articolo 147-bis del Decreto Legislativo 18 agosto 2000, n. 267, e che provvederà a tutti gli atti necessari all'esecuzione del provvedimento, fatta salva l'esecuzione di ulteriori adempimenti posti a carico di altri soggetti;
- non sono stati segnalati casi di conflitto d'interessi, anche potenziale, che comportino l'obbligo di astensione da parte del responsabile dell'istruttoria e dei dipendenti che partecipano alla presente procedura, ai sensi dell'art. 16 del D. Lgs. 36/2023, e ai sensi dell'art. 6-bis della Legge 7 agosto 1990, n. 241;
- nel presente procedimento si è operato nel rispetto della normativa sulla privacy, con particolare riferimento ai principi di necessità, di pertinenza e non eccedenza;

Considerato che con la sottoscrizione del presente atto il dirigente attesta:

- la regolarità e correttezza dell'azione amministrativa, ai sensi dell'articolo 147-bis del Decreto Legislativo 18 agosto 2000, n. 267;
- in attuazione del piano anticorruzione della Città Metropolitana di Genova, ai sensi dell'art. 16 del Decreto Legislativo 31 marzo 2023, n. 36, e ai sensi dell'art. 6-bis della Legge 7 agosto 1990, n. 241, di non trovarsi in una situazione di conflitto di interessi, anche potenziale, rispetto al presente procedimento;

Ritenuto opportuno pubblicare il presente provvedimento sul sito informatico della Stazione Unica Appaltante della Città Metropolitana di Genova e assolvere gli obblighi di pubblicità legale secondo le modalità contenute nel provvedimento ANAC n. 264 del 20/06/2023

# CITTÀ METROPOLITANA DI GENOVA

## *Atto dirigenziale*

Direzione Sviluppo economico e provveditorato
Servizio Sviluppo economico e sistemi informativi

**DISPONE**

Per i motivi specificati in premessa:

1. di affidare in house, ai sensi dell'art. 7, comma 2, del Decreto Legislativo 21 marzo 2023, n. 36, a Liguria Digitale S.p.A., i servizi di supporto alla gestione del progetto "CYBER-CMGE" per un importo contrattuale complessivo di Euro 1.257.713,37 (oneri fiscali inclusi), a seguito di arrotondamento, da eseguirsi nel pieno rispetto del capitolato speciale d'oneri di cui all'Allegato "A", che forma parte integrante del presente atto;

2. di formalizzare l'affidamento in house di cui al punto 1 mediante contratto da stipularsi in forma di scrittura privata;

3. di assumere a favore della società Liguria Digitale S.p.A. l'impegno di spesa di € 1.257.713,37 (oneri fiscali inclusi), secondo il prospetto contabile riportato in calce al presente provvedimento;

4. di autorizzare il pagamento di € 660,00 a titolo di contributo ANAC mediante impegno n. 377/2024, sul codice di bilancio 0102104 azione 1000481, con denominazione "Pagamento contributo ANAC per l'esercizio 2024", assunto con Atto dirigenziale del Responsabile del Servizio Stazione Unica Appaltante n. 20 del 9 gennaio 2024;

5. di pubblicare il presente provvedimento sul sito informatico della Stazione Unica Appaltante della Città Metropolitana di Genova e assolvere agli obblighi di pubblicità legale secondo le modalità contenute nel provvedimento ANAC n. 264 del 20/06/2023.

6. di pubblicare il presente provvedimento nella sezione Amministrazione Trasparente della Città Metropolitana di Genova.

**Sottoscritta dal Dirigente**
**(MAURIZIO TORRE)**
**con firma digitale**

**Modalità e termini di impugnazione:**

La presente determinazione dirigenziale può essere impugnata, ai sensi degli artt. 119 e 120 del Decreto Legislativo 2 luglio 2010 n. 104, con ricorso giurisdizionale al Tribunale Amministrativo Regionale (T.A.R.) Liguria, entro 30 giorni dalla data di pubblicazione all'albo pretorio on-line.

# CITTÀ METROPOLITANA DI GENOVA

***Atto dirigenziale***

Direzione Sviluppo economico e provveditorato

Servizio Sviluppo economico e sistemi informativi

Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Città Metropolitana di Genova

# PNRR – Missione 1 – Componente 1 – Asse 1
# Investimento 1.5 “Cybersecurity”

# AFFIDAMENTO A LIGURIA DIGITALE S.P.A. DI UN SERVIZIO DI CONSULENZA PER ATTUAZIONE PROGETTO “CYBER-CMGE”

## CUP D41B20001480006

**Relazione sulla valutazione della congruità economica dell’offerta ai sensi dell’art. 7 del Decreto legislativo 31 marzo 2023 n.36 “Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici”**

# Relazione sulla valutazione della congruità economica dell’offerta

# Sommario

# Introduzione

Città Metropolitana di Genova aderisce alla misura 1.5 che ha come obiettivo il rafforzamento dell'ecosistema digitale nazionale, potenziando i servizi di gestione della minaccia cyber.

La misura 1.5 ha come obiettivo il rafforzamento l'ecosistema digitale nazionale, potenziando i servizi di gestione della minaccia cyber. Il tutto grazie ad una rinnovata capacità di monitoraggio, prevenzione e scrutinio tecnologico a supporto della transizione digitale del Paese.

Le attività progettuali sono mirate al miglioramento delle capacità di governo e gestione del rischio cyber, per contrastare uno scenario di minaccia in continua evoluzione, e contestualmente consentire una risposta tempestiva a potenziali attacchi informatici. Gli interventi previsti sono:

1. Governance e programmazione cyber: coordinamento, supervisione e gestione olistica e integrata della cybersecurity attraverso la programmazione strategica di investimenti e iniziative;
2. Gestione del rischio cyber e della continuità operativa: individuazione, valutazione e trattamento sistematico dei rischi associati all'ambito cyber, e implementazione di un piano volto a garantire la resilienza di funzioni e servizi critici in caso di eventi avversi;
3. Gestione e risposta agli incidenti di sicurezza: monitoraggio, identificazione e gestione degli incidenti cyber, e ripristino dei sistemi impattati;
4. Gestione delle identità digitali e degli accessi logici: governo delle identità e definizione dei permessi di accesso alle risorse al fine di autenticare e autorizzare correttamente persone, gruppi e servizi in base agli attributi specifici e ai principi di "*need to know*", "*least privilege*" e "*segregation of duties*";
5. Sicurezza delle applicazioni, dei dati e delle reti: protezione dell'infrastruttura applicativa e di rete, e regolamentazione dei processi di protezione dei dati riservati, al fine di prevenire l'occorrenza di potenziali incidenti cyber e ridurne gli impatti.

Inoltre, al fine di promuovere l'adozione di un approccio sistemico allo sviluppo di ciascuno degli interventi citati, ciascuno degli stessi può essere riconducibile a una o più delle seguenti tipologie di intervento:

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento: insieme di attività mirate all'identificazione e all'analisi della postura di sicurezza del Soggetto proponente e alla definizione conseguente di un piano strategico di potenziamento, al fine di supportare il processo di evoluzione del livello di maturità riscontrato verso il livello target auspicato dall'Agenzia e ridurre la superficie d'attacco;
B. Miglioramento dei processi e dell'organizzazione: attività volte all'analisi e al potenziamento del framework documentale di cybersecurity – tramite la revisione dei processi esistenti o la definizione di nuovi – al fine di standardizzarne e ottimizzarne l'esecuzione;
C. Formazione e miglioramento della consapevolezza delle persone: attività formative su tematiche di cybersecurity a favore del personale dei Soggetti proponenti, per sviluppare una cultura cyber, incrementare la consapevolezza e le competenze specialistiche e divulgare buone pratiche per la prevenzione e la gestione di potenziali attacchi;
D. Progettazione e sviluppo di nuovi sistemi e tecnologie: attività volte all'acquisizione e al potenziamento di sistemi e tecnologie cyber a supporto dei processi e abilitanti per incrementarne il livello di maturità. Pertanto, ciascuna delle attività che si intende realizzare dovrà dunque essere

incasellata all'interno di un'iniziativa organica più articolata con il coinvolgimento potenziale anche di ulteriori tipologie di intervento che concorrono al perseguimento del medesimo obiettivo.

Con deliberazione del Consiglio Metropolitano n.11/2019, la Città Metropolitana di Genova ha approvato la partecipazione alla società Liguria Digitale S.p.A. secondo i contenuti dello Statuto e dei Patti parasociali, confermando la volontà espressa con la deliberazione del Consiglio della Città Metropolitana n. 52 del 28 dicembre 2018.

Nei Patti parasociali è garantito che gli Enti Soci esercitano su Liguria Digitale il controllo analogo a quello esercitato sulle proprie strutture e in relazione ai servizi dalla stessa prestati nei loro confronti. I Soci, in particolare, esercitano il controllo analogo congiunto mediante la partecipazione diretta al Comitato di Coordinamento dei Soci di Liguria Digitale di cui all'art. 25 dello Statuto sociale.

Con nota protocollo PG/2020/108486 del 25/03/2020, in ottemperanza all'art. 192 del D.L.vo 50/2016 (Codice dei Contratti Pubblici), la Regione Liguria ha comunicato l'iscrizione della società Liguria Digitale S.p.A. quale organismo in house dell'elenco delle amministrazioni aggiudicatrici che operano mediante affidamenti diretti nei confronti delle "proprie "società in house.

Con nota n. 6829/2021 del 10 febbraio 2021, Città metropolitana chiedeva a Regione Liguria di fornire evidenza all'A.N.A.C. "dell'avvenuta comunicazione di variazione della compagine sociale o, in alternativa, di procedervi quanto prima inserendo la scrivente Amministrazione tra i soci che esercitano il controllo analogo congiunto, come previsto dal punto 7 delle Linee Guida A.N.A.C. n. 7".

Con nota n. 8644/2021 del 19 febbraio 2021, Regione Liguria chiedeva ad A.N.A.C. l'aggiornamento dell'elenco di cui all'art. 192 del D. lgs 50/2016 e ss.mm.ii. "inserendo la CM di Genova tra gli enti che hanno acquisito una partecipazione societaria in Liguria Digitale S.p.A.".

Con nota n. 37867/2021 del 30/07/2021 Città Metropolitana richiedeva ad A.N.A.C. "l'aggiornamento dell'Elenco delle Amministrazioni aggiudicatrici e degli enti aggiudicatori che operano mediante affidamenti diretti nei confronti di proprie società in house ex art. 192 del D. Lgs 50 2016".

Con nota n. 37867/2021 del 30/07/2021 Città Metropolitana richiedeva ad A.N.A.C. "l'aggiornamento dell'Elenco delle Amministrazioni aggiudicatrici e degli enti aggiudicatori che operano mediante affidamenti diretti nei confronti di proprie società in house ex art. 192 del D. Lgs 50 2016".

Dato atto che Città Metropolitana di Genova, ha richiesto a **Liguria Digitale S.p.A.** la presentazione di un preventivo per il servizio in oggetto attraverso la piattaforma telematica Mepa (procedura numero NG4833600).

Liguria Digitale S.p.A. ha presentato a questa amministrazione la documentazione relativa alla procedura di cui sopra, tra cui la proposta tecnico economica.

Sulla base di tale proposta tecnico economica per poter procedere all'affidamento *in house*, trattandosi di servizi disponibili sul mercato in regime di concorrenza, la *Direzione Sviluppo economico e provveditorato* ha effettuato una valutazione di congruità economica dell'offerta della stessa, ai sensi dell'articolo 7 comma 2 del nuovo Codice degli Appalti, di cui la presente relazione rappresenta l'esito.

## Oggetto della valutazione

La proposta è relativa al servizio di consulenza per attuazione progetto "CYBER-CMGE" e risponde a quanto richiesto dal capitolato. In particolare la fornitura dei servizi relativi a:

- **Intervento 1: Governance e programmazione cyber**
  - **Attività:** Analisi dei report, vulnerability assessment e campagne di phishing
  - **Attività:** Consolidamento dei documenti relativi alla descrizione dell'organizzazione dei processi
- **Intervento 2: Gestione del rischio cyber e della continuità operativa**
  - **Attività:** Test di vulnerability assessment della infrastruttura di rete
- **Intervento 3: Gestione e risposta agli incidenti di sicurezza**
  - **Attività:** Acquisto e messa in esercizio servizio SIEM e acquisto/integrazione servizio XDR (per Città Metropolitana di Genova e per i Comuni aderenti al progetto)
- **Intervento 5: Sicurezza delle applicazioni, dei dati e delle reti**
  - **Attività:** Acquisto e messa in esercizio servizio di Lan Monitoring and Management

E l'acquisto di beni e servizi relativi a:

- **Apparati di rete centrali e periferici della rete informatica di CMGE**
- **Sistema wifi centralizzato interconnesso alla rete informatica di CMGE**
- **Piattaforma asset inventory**
- **Acquisto e messa in esercizio piattaforma MTM (Mobile threat management)**
- **Corsi di formazione specifica**

Il preventivo per l'intera fornitura è pari a **Euro 1.030.912,61 (IVA esclusa)** pari a **Euro 1.257.713,38 (IVA inclusa).**

# Valutazione della congruità dei costi

## Parte A - Costi interni di commessa

La prima parte della proposta fa riferimento ai componenti relativi ai cinque interventi sopra descritti sono così strutturate (i costi sono da intendersi IVA esclusa):

| Attività | Profilo professionale | Numero giornate previste | Costo giornaliero medio per fascia | Costo totale |
|---|---|---|---|---|
| Analisi dei report, vulnerability assessment e campagne di phishing | Account manager | 4 | Euro 570,57 | Euro 2.282,28 |
| | Administration | 10 | Euro 368,68 | Euro 3.686,76 |
| | ICT security specialist | 70 | Euro 408,80 | Euro 28.616,28 |
| | Project manager | 20 | Euro 511,63 | Euro 10.232,64 |
| | | | | **Euro 44.817,96** |
| Consolidamento dei documenti relativi alla descrizione dell'organizzazione dei processi | Account manager | 7 | Euro 570,57 | Euro 3.993,99 |
| | Administration | 3,5 | Euro 368,68 | Euro 1.290,37 |
| | Business analyst | 170 | Euro 415,07 | Euro 70.562,58 |
| | Project manager | 27 | Euro 511,63 | Euro 13.814,06 |
| | | | | **Euro 89.661,00** |
| Test di vulnerability assessment della infrastruttura di rete | ICT security specialist | 51 | Euro 408,80 | Euro 20.849,00 |
| | | | | **Euro 20.849,00** |
| Acquisto/integrazione servizio XDR (per Città Metropolitana di Genova e per i Comuni aderenti al progetto) | ICT security specialist | 89 | Euro 408,80 | Euro 36.383,56 |
| | | | | **Euro 36.383,56** |
| Acquisto e messa in esercizio servizio SIEM | ICT security specialist | 140 | Euro 408,80 | Euro 57.232,56 |
| | | | | **Euro 57.232,56** |
| Acquisto e messa in esercizio servizio di Lan Monitoring and Management | Account manager | 3 | Euro 570,57 | Euro 1.711,71 |
| | Administration | 2 | Euro 368,68 | Euro 737,35 |
| | Network and system specialist | 54 | Euro 416,33 | Euro 22.481,71 |
| | Service manager | 54 | Euro 517,90 | Euro 27.966,71 |
| | Project manager | 20 | Euro 511,63 | Euro 10.232,64 |
| | | | | **Euro 63.130,12** |
| | | | | |
| Straordinari/Reperibilità/Diarie/Trasferte | | | | **Euro 92,67** |

| | |
|---|---|
| **TOTALE Costi interni di Commessa** | **Euro 312.166,87** |
| Costi generali (pari al 25,40% dei costi interni di commessa già inglobati nei costi giornalieri medi) | |
| | |
| | **Euro 312.166,87** |

Le spese attribuite alle voci di Straordinari, Reperibilità, Diarie e Trasferte, a causa del loro importo marginale, non saranno conteggiate ai fini della valutazione di congruità.

## Parte B – Servizi di commessa

La seconda parte della proposta prevede l'acquisto delle forniture di beni e servizi sotto elencati. Liguria Digitale ha proposto un acquisto allineato ai valori dichiarati nel capitolato:

| ID ITEM | Descrizione | Importo (IVA esclusa) |
|---|---|---|
| **ITEM_A** | Apparati di rete centrali e periferici della rete informatica di CMGE | **408.500,00 €** |
| **ITEM_B** | Sistema wifi centralizzato interconnesso alla rete informatica di CMGE | **89.131,15 €** |
| **ITEM_C** | Piattaforma asset inventory | **45.409,84 €** |
| **ITEM_D** | Acquisto e messa in esercizio piattaforma MTM (Mobile threat management) | **23.114,75 €** |
| **ITEM_E** | Corsi di formazione specifica | **152.590,00 €** |

## Esiti valutazione

Si dettagliano gli esiti della valutazione di congruità dei costi offerti da Liguria Digitale S.p.A., in qualità di società *in house* della Città Metropolitana di Genova, per le attività di supporto sopra dettagliate.

La valutazione è effettuata ai sensi del comma 2 dell'articolo 7 del Decreto Legislativo n. 36 del 31/03/2023 "Codice degli Appalti" secondo il quale "*Le stazioni appaltanti e gli enti concedenti possono affidare direttamente a società in house lavori, servizi o forniture, nel rispetto dei principi di cui agli articoli 1, 2 e 3. Le stazioni appaltanti e gli enti concedenti adottano per ciascun affidamento un provvedimento motivato in cui danno conto dei vantaggi per la collettività, delle connesse esternalità e della congruità economica della prestazione, anche in relazione al perseguimento di obiettivi di universalità, socialità, efficienza, economicità, qualità della prestazione, celerità del procedimento e razionale impiego di risorse pubbliche. In caso di prestazioni strumentali, il provvedimento si intende sufficientemente motivato qualora dia conto dei vantaggi in termini di economicità, di celerità o di perseguimento di interessi strategici. I vantaggi di economicità possono emergere anche mediante la comparazione con gli standard di riferimento della società Consip S.p.a. e delle altre centrali di committenza, con i parametri ufficiali elaborati da altri enti regionali nazionali o esteri oppure, in mancanza, con gli standard di mercato.*"

La società Liguria Digitale S.p.A., come previsto all'art. 4 comma 1 dello Statuto, "*è strutturata al servizio della Regione Liguria e degli Enti soci, opera secondo il modello dell'"in house providing" stabilito dall'ordinamento*

*dell'Unione Europea e dall'ordinamento interno a norma degli articoli 16 del D.Lgs.175/2016 e del D.Lgs.50/2016*".

La Città Metropolitana di Genova esercita nei confronti di Liguria Digitale S.p.A. un "*controllo analogo a quello esercitato sulle proprie strutture organizzative e in relazione ai servizi dalla stessa prestati*" nei suoi confronti, come previsto all'artico 25 dello Statuto e dall'articolo 2 e seguenti dei Patti Parasociali.

## Valutazione parte A – Costi interni di commessa

Le giornate richieste per Intervento *1 "Governance e programmazione cyber"* sono le seguenti:

Attività: Analisi dei report, vulnerability assessment e campagne di phishing

| | |
|---|---|
| Account Manager | 4 |
| Administration | 10 |
| ICT Security Specialist | 70 |
| Project Manager | 20 |

Attività: Consolidamento dei documenti relativi alla descrizione dell'organizzazione dei processi

| | |
|---|---|
| Account Manager | 7 |
| Administration | 3,5 |
| Business Analyst | 170 |
| Project Manager | 27 |

Visto che le giornate offerte da Liguria digitale per le attività sopra indicate sono esattamente quelle richieste, si ritiene che il numero di giornate previste per l'Intervento 1 siano congrue per le attività in esame.

Le giornate richieste per *Intervento 2 "Gestione del rischio cyber e della continuità operativa"* sono le seguenti:

Attività: Test di vulnerability assessment della infrastruttura di rete

| | |
|---|---|
| ICT Security Specialist | 51 |

Visto che le giornate offerte da Liguria digitale per le attività sopra indicate sono esattamente quelle richieste, si ritiene che il numero di giornate previste per l'Intervento 2 siano congrue per le attività in esame.

Le giornate richieste per *Intervento 3 "Gestione e risposta agli incidenti di sicurezza"* sono le seguenti:

Attività: Acquisto e messa in esercizio servizio SIEM e acquisto/integrazione servizio XDR (per Città Metropolitana di Genova e per i Comuni aderenti al progetto)

| | |
|---|---|
| ICT Security Specialist | 229 |

Visto che le giornate offerte da Liguria digitale per le attività sopra indicate sono esattamente quelle richieste, si ritiene che il numero di giornate previste per l'Intervento 3 siano congrue per le attività in esame.

Le giornate richieste per *Intervento 5 "Sicurezza delle applicazioni, dei dati e delle reti"* sono le seguenti:

Attività: Acquisto e messa in esercizio servizio di Lan Monitoring and Management

| | |
|---|---|
| Account Manager | 3 |
| Administration | 2 |
| Network and system specialist | 54 |
| Project manager | 20 |
| Service Manager | 54 |

Visto che le giornate offerte da Liguria digitale per le attività sopra indicate sono esattamente quelle richieste, si ritiene che il numero di giornate previste per l'Intervento 5 siano congrue per le attività in esame.

Nella proposta tecnico – economica di Liguria Digitale S.p.A, i costi giornalieri, comprensivi della quota costi generali (pari al 25,40%), al netto dell'IVA, delle suddette figure sono i seguenti:

| | |
|---|---|
| **Account manager** | Euro 570,57 |
| **Administation** | Euro 368,68 |
| **Business analyst** | Euro 415,07 |
| **ICT security specialist** | Euro 408,80 |
| **Network and system specialist** | Euro 416,33 |
| **Project manager** | Euro 511,63 |
| **Service Manager** | Euro 517,90 |

Nel Comitato di Coordinamento dei Soci di Liguria Digitale S.p.A. del 27/05/2021 al punto 1 dell'ordine del giorno risultava:

1. Approvazione Relazione Previsionale e Programmatica 2021-2023 e presentazione del benchmarking effettuato dalla Società Ernst & Young sui profili professionali e sul costo medio delle relative prestazioni con riferimento al mercato dei servizi ICT, come deliberato dal Comitato di Coordinamento Soci del 16.11.2020.

Durante il Comitato è stato precisato che si sta lavorando, nell'ottica di un percorso di miglioramento costante del processo, ad un modello di riferimento che, partendo dalla attestata congruità dei profili tariffari, porti a formulare un regolamento generale di valutazione della congruità, basato anche su un Catalogo dei Servizi, in fase di completamento da parte di Liguria Digitale.

Con riferimento a quanto deliberato dal Comitato di Coordinamento dei Soci del 16 novembre 2020, al fine di continuare a garantire il pieno allineamento del modello gestionale al costo in uso in Liguria Digitale ai requisiti di congruità degli affidamenti, è stato ricordato che i Soci avevano approvato all'unanimità quanto segue:

1) *"dare mandato a Liguria Digitale di sottoporre alla verifica del Comitato di Coordinamento dei Soci, a norma dell'art. 7 del Disciplinare Quadro ed entro il 31/01/2021, un idoneo confronto dei suoi costi medi giornalieri (comprensivi dei costi indiretti) con altri soggetti operanti nel medesimo mercato per servizi equivalenti e tenendo anche conto di eventuali Certificazioni di Qualità possedute. A tal fine Liguria Digitale è tenuta a:*

*a) procedere alla conversione delle sue attuali tariffe/fasce professionali in un numero adeguato e definito di profili professionali che renda maggiormente diretto e semplificato il raffronto con il mercato; l'elenco delle tariffe sarà presentato contestualmente alla Relazione Previsionale e Programmatica 2021-2023;*

*b) affidare a una primaria Società, individuata a norma del D.lgs. n. 50/2016 e previa valutazione da affidarsi ad una Commissione giudicatrice composta almeno per 2/3 da rappresentanti degli Enti Soci, il benchmarking delle tariffe per ciascun profilo professionale;*

*2) assegnare al Settore Informatica della Regione Liguria il coordinamento delle attività affidate a Liguria Digitale come da punto che precede e la gestione del flusso informativo tra la Società e i Soci e tra i Soci stessi."*

Durante il coordinamento i soci sono stati informati che lo studio in oggetto è stato svolto dalla Società Ernst & Young, individuata a norma del D. Lgs n. 50/2016, con l'ausilio di un gruppo di lavoro appositamente costituito, coordinato dal Settore Informatica della Regione Liguria e da A.Li.Sa., che ha fornito il proprio contributo in tutte le fasi del progetto manifestando le esigenze dei Soci in merito alla valutazione di congruità delle tariffe per i profili professionali individuati.

Sono quindi state illustrate le risultanze dello studio di benchmarking, che confronta come richiesto le tariffe giornaliere per profilo professionale di Liguria Digitale con i range tariffari di altri soggetti operanti nel medesimo mercato per servizi equivalenti.

Al termine della presentazione, è stato evidenziato come **l'esito del confronto effettuato confermi la congruità delle tariffe giornaliere per profilo professionale di Liguria Digitale con i range tariffari di altri soggetti operanti nel medesimo mercato per servizi equivalenti** e si è ribadita l'adozione del modello al costo nella determinazione del valore delle forniture.

Nella proposta tecnico economica presentata da Liguria Digitale S.p.A. sono state utilizzate le tariffe giornaliere per profilo professionale di Liguria Digitale calcolate per l'anno 2024.

Le tariffe giornaliere per profilo professionale di Liguria Digitale calcolate per l'anno 2024 sono riportate nella Relazione Previsionale e Programmatica 2024 approvata e trasmessa ai Soci da Regione Liguria con PROTOCOLLO. U.0006391.30-11-2023.

Come dichiarato nella succitata Relazione Previsionale e Programmatica 2024, le tariffe giornaliere per profilo professionale, per l'anno 2024, risultano ampiamente all'interno dei range tariffari di mercato rilevati nel 2021 attraverso lo studio di benchmarking predisposto dalla Società Ernst & Young.

### Valutazione parte B – Servizi di commessa

Per la seconda parte della proposta, l'attività richiesta a Liguria Digitale è quella di configurarsi come stazione appaltante per l'acquisto dei beni/servizi sopra elencati, considerando che Liguria Digitale è specializzata negli acquisti informatici e che gestirà anche l'intero project management in-house.

Città Metropolitana di Genova ha chiesto, a capitolato, la verifica di eventuali convenzioni attive su CONSIP per l'acquisto dei beni/servizi in oggetto o, se non presenti, l'utilizzo del Mercato Elettronico della Pubblica Amministrazione al fine di poter individuare il miglior prodotto come rapporto qualità/prezzo.

Liguria Digitale si è dichiarata disponibile ad esplorare i sopra citati canali d'acquisto, al fine di individuare quanto richiesto, nel rispetto del nuovo Codice degli Appalti e a comunicare eventuali economie di spesa al fine di consentire a Città Metropolitana di Genova una rimodulazione degli investimenti per il progetto.

Vista la dichiarazione di Liguria Digitale in merito alle modalità operative con cui opererà come stazione appaltante per Città Metropolitana di Genova, riteniamo congruo il servizio di acquisto dei beni/servizi in oggetto.

## Valutazione della congruità degli ammortamenti di Commessa

Nella proposta tecnico – economica di Liguria Digitale S.p.A. è inserita la voce relativa agli ammortamenti su beni di proprietà della società stessa, ma tale voce non è valorizzata.

## Valutazione della congruità dei Beni di Commessa

Nella proposta tecnico – economica di Liguria Digitale S.p.A. è inserita la voce relativa ai Beni di Commessa, ma tale voce non è valorizzata.

## Conclusioni

La presente relazione ha valutato la congruità economica della proposta tecnico economica presentata da Liguria Digitale S.p.A. relativamente alla "*Fornitura di un servizio di consulenza per attuazione progetto "CYBER-CMGE""* secondo le disposizioni dettate dal comma 2 dell'articolo 7 del D.lgs 36/2023 per ogni singola attività prevista.

Sulla base dell'analisi svolta si ritiene che l'offerta economica sia ragionevolmente congrua ed in linea con i servizi richiesti avendo verificato, per la parte A - Costi interni di commessa, che i costi del personale sono in linea a quelli di mercato e che il numero di giornate previste sono ragionevoli per le singole attività.

Per quanto riguarda la parte B - Servizi di commessa, si ritiene congruo il servizio offerto da Liguria Digitale come stazione appaltante per la Città Metropolitana di Genova.

# PNRR – Missione 1 – Componente 1 – Asse 1
# Investimento 1.5 “Cybersecurity”

# CAPITOLATO SPECIALE DI APPALTO

# FORNITURA DI UN SERVIZIO DI CONSULENZA PER ATTUAZIONE PROGETTO “CYBER-CMGE”

## CUP D41B20001480006

**13 novembre 2024**

# INDICE

# ART. 1 OGGETTO DELL'APPALTO

La misura 1.5 ha come obiettivo il **rafforzamento l'ecosistema digitale nazionale,** potenziando i servizi di gestione della minaccia cyber. Il tutto grazie ad una **rinnovata capacità di monitoraggio, prevenzione e scrutinio** tecnologico a supporto della **transizione digitale del Paese**.

Le attività progettuali sono mirate al miglioramento delle capacità di governo e gestione del rischio cyber, per contrastare uno scenario di minaccia in continua evoluzione, e contestualmente consentire una risposta tempestiva a potenziali attacchi informatici. Gli interventi previsti sono:

1. Governance e programmazione cyber: coordinamento, supervisione e gestione olistica e integrata della cybersecurity attraverso la programmazione strategica di investimenti e iniziative;
2. Gestione del rischio cyber e della continuità operativa: individuazione, valutazione e trattamento sistematico dei rischi associati all'ambito cyber, e implementazione di un piano volto a garantire la resilienza di funzioni e servizi critici in caso di eventi avversi;
3. Gestione e risposta agli incidenti di sicurezza: monitoraggio, identificazione e gestione degli incidenti cyber, e ripristino dei sistemi impattati;
4. Gestione delle identità digitali e degli accessi logici: governo delle identità e definizione dei permessi di accesso alle risorse al fine di autenticare e autorizzare correttamente persone, gruppi e servizi in base agli attributi specifici e ai principi di "*need to know*", "*least privilege*" e "*segregation of duties*";
5. Sicurezza delle applicazioni, dei dati e delle reti: protezione dell'infrastruttura applicativa e di rete, e regolamentazione dei processi di protezione dei dati riservati, al fine di prevenire l'occorrenza di potenziali incidenti cyber e ridurne gli impatti.

Inoltre, al fine di promuovere l'adozione di un approccio sistemico allo sviluppo di ciascuno degli interventi citati, ciascuno degli stessi può essere riconducibile a una o più delle seguenti tipologie di intervento:

A. Analisi della postura di sicurezza e definizione di un piano di potenziamento: insieme di attività mirate all'identificazione e all'analisi della postura di sicurezza del Soggetto proponente e alla definizione conseguente di un piano strategico di potenziamento, al fine di supportare il processo di evoluzione del livello di maturità riscontrato verso il livello target auspicato dall'Agenzia e ridurre la superficie d'attacco;
B. Miglioramento dei processi e dell'organizzazione: attività volte all'analisi e al potenziamento del framework documentale di cybersecurity – tramite la revisione dei processi esistenti o la definizione di nuovi – al fine di standardizzarne e ottimizzarne l'esecuzione;
C. Formazione e miglioramento della consapevolezza delle persone: attività formative su tematiche di cybersecurity a favore del personale dei Soggetti proponenti, per sviluppare una cultura cyber, incrementare la consapevolezza e le competenze specialistiche e divulgare buone pratiche per la prevenzione e la gestione di potenziali attacchi;
D. Progettazione e sviluppo di nuovi sistemi e tecnologie: attività volte all'acquisizione e al potenziamento di sistemi e tecnologie cyber a supporto dei processi e abilitanti per incrementarne il livello di maturità. Pertanto, ciascuna delle attività che si intende

realizzare dovrà dunque essere incasellata all'interno di un'iniziativa organica più articolata con il coinvolgimento potenziale anche di ulteriori tipologie di intervento che concorrono al perseguimento del medesimo obiettivo.

| TIPOLOGIE DI INTERVENTI / INTERVENTI | A. Analisi della postura di sicurezza e definizione di un piano di potenziamento | B. Miglioramento dei processi e dell'organizzazione | C. Formazione e miglioramento della consapevolezza delle persone | D. Progettazione e sviluppo di nuovi sistemi e tecnologie |
|---|---|---|---|---|
| 1. Governance e programmazione cyber | • Analisi di dettaglio e definizione di un programma evolutivo in termini di processi, organizzazione e tecnologie *cyber* | • Definizione modello organizzativo struttura *cyber* | • Formazione e certificazioni specialistiche<br>• Promozione ed esecuzione di iniziative di *cyber culture*<br>• Svolgimento di simulazioni e campagne di *awareness* a tema *cyber* (es. simulazione attacco di *phishing*) | • Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. *GRC, asset inventory*, piattaforma *e-learning*) |
| 2. Gestione del rischio cyber e della continuità operativa | • Valutazione del rischio su *asset* in perimetro<br>• *Business Impact Analysis* su servizi in perimetro | • Definizione metodologia di valutazione del rischio<br>• Definizione processo *backup & restore* | • Formazione e certificazioni specialistiche e di prodotto | • Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. strumenti di *backup, security ratings, cyber threat intelligence*) |
| 3. Gestione e risposta agli incidenti di sicurezza | • *Red Teaming* | • Definizione processo di gestione degli incidenti *cyber*<br>• Definizione processo di gestione dei log<br>• Definizione di *playbook* per la risposta a incidenti *cyber* noti | • *Table Top Exercise*<br>• Formazione e certificazioni specialistiche e di prodotto | • Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. *SIEM, SOAR, Case Management*) |
| 4. Gestione delle identità digitali e degli accessi logici | • Valutazione e *hardening* della postura di sicurezza di *Active Directory* | • Definizione processo di gestione delle identità e degli accessi ai sistemi informativi | • Formazione e certificazioni specialistiche e di prodotto | • Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. *IAM, PAM, IGA, MFA*) |
| 5. Sicurezza delle applicazioni, dei dati e delle reti | • *VA/PT*<br>• Verifica e rafforzamento delle configurazioni di sicurezza perimetrale e monitoraggio | • Analisi e reingegnerizzazione di reti e architetture<br>• Definizione processo di *security by design*<br>• Definizione processo di sviluppo sicuro codice<br>• Definizione processo di gestione delle vulnerabilità | • Formazione e certificazioni specialistiche e di prodotto | • Acquisizione e implementazione/sviluppo tecnologie abilitanti (es. *firewall, WAF, anti-DDoS, DLP*) |

Il presente capitolato disciplina la fornitura di un servizio di consulenza specialistica e affiancamento tecnico per la realizzazione delle **attività 1.A, 1.B, 2.A, 3.D, 5.D** sopra elencate e della fornitura degli ITEM citati in ART. 3 relativi alle **attività 1.D, 2.C, 2.D, 3.C, 4.C, 5.A, 5.C** descritte in dettaglio nell'ART. 3.

# ART. 2 CARATTERISTICHE DEL SERVIZIO

Il servizio richiesto comprende la fornitura di personale di adeguato livello professionale per la realizzazione delle seguenti attività.

## Intervento 1: Governance e programmazione cyber

### Tipologia di intervento A: Analisi della postura di sicurezza e definizione di un piano di potenziamento

| **Attività:** Analisi dei report, vulnerability assessment e campagne di phishing | **N.GIORNI** |
|---|---|
| Account Manager | 4 |
| Administration | 10 |
| ICT Security Specialist | 70 |
| Project Manager | 20 |
| **TOT** | **104** |

### Tipologia di intervento B: Miglioramento dei processi e dell'organizzazione

| **Attività:** Consolidamento dei documenti relativi alla descrizione dell'organizzazione dei processi | **N.GIORNI** |
|---|---|
| Account Manager | 7 |
| Administration | 3,5 |
| Business Analyst | 170 |
| Project Manager | 27 |
| **TOT** | **207,5** |

## Intervento 2: Gestione del rischio cyber e della continuità operativa

### Tipologia di intervento A: Analisi della postura di sicurezza e definizione di un piano di potenziamento

| **Attività:** Test di vulnerability assessment della infrastruttura di rete | **N.GIORNI** |
|---|---|
| ICT Security Specialist | 51 |
| **TOT** | **51** |

### Intervento 3: Gestione e risposta agli incidenti di sicurezza

**Tipologia di intervento D: Progettazione e sviluppo di nuovi sistemi e tecnologie**

| **Attività:** Acquisto e messa in esercizio servizio SIEM e acquisto/integrazione servizio XDR (per Città Metropolitana di Genova e per i Comuni aderenti al progetto) | **N.GIORNI** |
|---|---|
| ICT Security Specialist | 229 |
| **TOT** | **229** |

### Intervento 5: Sicurezza delle applicazioni, dei dati e delle reti

**Tipologia di intervento D: Progettazione e sviluppo di nuovi sistemi e tecnologie**

| **Attività:** Acquisto e messa in esercizio servizio di Lan Monitoring and Management | **N.GIORNI** |
|---|---|
| Account Manager | 3 |
| Administration | 2 |
| Network and System Specialist | 54 |
| Service Manager | 54 |
| Project Manager | 20 |
| **TOT** | **133** |

## ART. 3 FORNITURE DA ACQUISTARE

L'affidamento in oggetto prevede l'acquisto delle forniture di beni e servizi sotto elencati. Le forniture di beni devono essere acquistate utilizzando eventuali convenzioni CONSIP attive o, se non presenti, utilizzando il Mercato Elettronico della Pubblica Amministrazione.

Per ciascuna fornitura è richiesto di specificare il dettaglio dei costi.

| **ID ITEM** | **Descrizione** | **Totale a disposizione (IVA esclusa)** |
|---|---|---|
| **ITEM_A** | Apparati di rete centrali e periferici della rete informatica di CMGE | **408.500,00 €** |

| | | |
|---|---|---|
| **ITEM_B** | Sistema wifi centralizzato interconnesso alla rete informatica di CMGE | **89.131,15 €** |
| **ITEM_C** | Piattaforma asset inventory | **45.409,84 €** |
| **ITEM_D** | Acquisto e messa in esercizio piattaforma MTM (Mobile threat management) | **23.114,75 €** |
| **ITEM_E** | Corsi di formazione specifica | **152.590,00 €** |

### ITEM_A - Apparati di rete centrali e periferici

Si considera per questo item l'acquisto per la sostituzione di tutti gli apparati di rete dell'Ente, così suddiviso:

- **n. 2 switch 24 porte in fibra ottica layer 3**
- **n. 50 switch 48 porte PoE layer 3**
- **n. 36 gruppi di continuità da rack dimensionati per switch sopra indicati**
- **Patch cord e accessori armadi rack necessari all'installazione**
- **Software di gestione centralizzato**

All'interno della cifra indicata sono considerati anche i costi per attività di acquisto, sopralluogo tecnico iniziale, lavori di posa in opera, configurazione degli apparati e collaudo finale.

### ITEM_B - Sistema wifi centralizzato

Si considera per questo item, l'acquisto dei dispositivi wifi per l'intera copertura wireless della sede distaccata di Quarto (Largo Cattanei 3 – Genova). Nello specifico sono richiesti:

- **n. 60 Access Point con le seguenti caratteristiche minimali:**
  - IEEE 802.11ax (Wifi6 certified)
  - possibilità di realizzare un sistema di distribuzione wireless WDS ovvero possibilità di utilizzare il mezzo radio Wi-fi per la distribuzione della connettività "backhaul" verso Access Point non direttamente connessi alla rete cablata contemporaneamente alla funzione di AP. I dispositivi offerti dovranno pertanto garantire contemporaneamente la funzione di AP e di WDS.
  - almeno una interfaccia base T con supporto del protocollo IEEE 802.3bz
  - Client Authentication alle WLAN tramite captive portal con repository utenze interno ed esterno
  - capacità di localizzazione e gestione dei rogue access point
- **Cablaggio dei relativi punti rete necessari**

- **Patch cord e accessori armadi rack necessari all'installazione**
- **Software di gestione centralizzato**

**Il Brand per gli Access Point forniti deve essere lo stesso del Brand degli Switch**

All'interno della cifra indicata sono considerati anche i costi per attività di acquisto, sopralluogo tecnico iniziale, lavori di posa in opera, configurazione degli apparati e collaudo finale.

### ITEM_C - Piattaforma asset inventory

Si considera per questo item, l'acquisto e l'attività di configurazione iniziale (set up) di un sistema di asset inventory per l'Ente, avente le seguenti caratteristiche minimali:

open source, interfaccia web based, storia completa delle modifiche effettuate su qualunque scheda dati (versioning), funzioni di ricerca avanzata, definizione di filtri e viste per un accesso personalizzato ai dati, associazione di documenti alla singola scheda, motore di workflow integrato per gestione flussi ticket, reportistica integrata, profilazione utenti/gruppi di utenti con modalità multitenant, interoperabilità con altre applicazioni tramite webservice in particolare con l'infrastruttura Active Directory e con il sistema OCS Inventory presenti nell'Ente , funzioni di import / export CSV, possibilità di configurare e gestire operazioni automatiche (compreso invio mail), fornitura di un Portale Self-Service per gli utenti non tecnici, fornitura di APP mobile per gestione ticket.

### ITEM_D – Piattaforma MTM

Si considera per questo item, l'acquisto e l'attività di configurazione iniziale (set up) del sistema di Mobile threat management per l'Ente, avente le seguenti caratteristiche minimali:

gestione centralizzata dei dispositivi mobili, monitoraggio dei dispositivi mobili in ottemperanza alle normative sulla privacy, protezione della connettività internet dei dispositivi mobili con particolare attenzione ai casi di contatti o connessioni con reti di tipo wifi esterne all'Ente, protezione nell'utilizzo di applicazioni di posta elettronica, messaggistica e navigazione web contro malware, phishing e smishing, protezione di dati e documenti che si trovano sui dispositivi mobili, report di sicurezza degli eventi potenzialmente pericolosi e degli attacchi verificatisi, assistenza per il mantenimento aggiornato delle APP presenti sui dispositivi e l'individuazione di possibili di loro vulnerabilità legate a versioni superate.

### ITEM_E – Formazione

Si considera per questo item, l'acquisto e l'attività organizzazione dei corsi di formazione specifica per il personale tecnico dell'ente e per il personale dei Comuni aderenti al progetto. Nello specifico:

- Corsi base a tema Cyber Security Awareness per fornire ai dipendenti dell'Ente e dei Comuni del Territorio aderenti al progetto, le conoscenze necessarie a fronteggiare il costante evolversi degli attacchi cyber;
- Corsi specialistici propedeutici alle certificazioni COMPTIA (Security+ e Network+) per il personale tecnico IT degli dell'Ente e dei Comuni del Territorio aderenti al progetto;
- Corsi specialistici in ambito Windows Server relativi al miglioramento delle competenze riguardanti la progettazione, l'implementazione, la configurazione e la gestione di un ambiente Microsoft Active Directory.
- Corsi di formazione specialistica e certificazione sui prodotti di rete acquistati per il rafforzamento della infrastruttura di rete dell'ente.

# ART. 4 GANTT DI PROGETTO

| Intervento | Tipologia di intervento | Attività | Inizio | Fine |
|---|---|---|---|---|
| *1. Governance e programmazione cyber* | A. Analisi della postura di sicurezza e definizione di un piano di potenziamento | Analisi dei report, ad esempio, vulnerability assessment (4) campagne di phishing (3) | 01/11/2024 | 28/11/2025 |
| *1. Governance e programmazione cyber* | B. Miglioramento dei processi e dell'organizzazione | Consolidamento dei documenti relativi alla descrizione dell'organizzazione dei processi | 01/11/2024 | 31/07/2025 |
| *1. Governance e programmazione cyber* | C. Formazione e miglioramento della consapevolezza delle persone | Campagne di phishing (n. 3) | 01/11/2024 | 30/09/2025 |
| *1. Governance e programmazione cyber* | D. Progettazione e sviluppo di nuovi sistemi e tecnologie | Acquisto e messa in esercizio piattaforma di asset inventory | 01/11/2024 | 30/06/2025 |
| *2. Gestione del rischio cyber e della continuità operativa* | A. Analisi della postura di sicurezza e definizione di un piano di potenziamento | Test di vulnerability assessment della infrastruttura di rete | 01/11/2024 | 31/10/2025 |
| *2. Gestione del rischio cyber e della continuità operativa* | B. Miglioramento dei processi e dell'organizzazione | Completamento e consolidamento delle valutazioni del rischio | 01/11/2024 | 28/11/2025 |
| *2. Gestione del rischio cyber e della continuità operativa* | C. Formazione e miglioramento della consapevolezza delle persone | Acquisizione della piattaforma per diffusione della conoscenza di base della cyber security awareness | 01/11/2024 | 28/11/2025 |
| *2. Gestione del rischio cyber e della continuità operativa* | D. Progettazione e sviluppo di nuovi sistemi e tecnologie | Acquisto e messa in esercizio piattaforma MTM (Mobile threat management) | 01/11/2024 | 02/05/2025 |
| *3. Gestione e risposta agli incidenti di sicurezza* | A. Analisi della postura di sicurezza e definizione di un piano di potenziamento | Red Teaming | 01/11/2024 | 31/10/2025 |

| | | | | |
|---|---|---|---|---|
| *3. Gestione e risposta agli incidenti di sicurezza* | B. Miglioramento dei processi e dell'organizzazione | Attività erogata dal personale specialistico della società In House | 01/11/2024 | 28/03/2025 |
| *3. Gestione e risposta agli incidenti di sicurezza* | C. Formazione e miglioramento della consapevolezza delle persone | Consolidamento conoscenza specialistica e conseguimento certificazioni COMPTIA | 01/11/2024 | 31/10/2025 |
| *3. Gestione e risposta agli incidenti di sicurezza* | D. Progettazione e sviluppo di nuovi sistemi e tecnologie | Acquisto e messa in esercizio servizio SIEM | 01/11/2024 | 30/04/2025 |
| *3. Gestione e risposta agli incidenti di sicurezza* | D. Progettazione e sviluppo di nuovi sistemi e tecnologie | Acquisto (Comuni del territorio) e integrazione (CMGE) servizio XDR | 01/11/2024 | 31/10/2025 |
| *4. Gestione delle identità digitali e degli accessi logici* | C. Formazione e miglioramento della consapevolezza delle persone | Consolidamento conoscenza specialistica in ambito Windows Server e Active Directory | 01/11/2024 | 31/10/2025 |
| *5. Sicurezza delle applicazioni, dei dati e delle reti* | A. Analisi della postura di sicurezza e definizione di un piano di potenziamento | Acquisto e messa in opera di apparati attivi necessari alla segmentazione della rete (layer 3) | 01/11/2024 | 30/06/2025 |
| *5. Sicurezza delle applicazioni, dei dati e delle reti* | A. Analisi della postura di sicurezza e definizione di un piano di potenziamento | Acquisto e messa in opera sistema wifi centralizzato interconnesso alla rete di CMGE | 01/11/2024 | 30/06/2025 |
| *5. Sicurezza delle applicazioni, dei dati e delle reti* | C. Formazione e miglioramento della consapevolezza delle persone | Consolidamento conoscenza specialistica in ambito Microsoft Windows client (Win11) | 01/11/2024 | 31/10/2025 |
| *5. Sicurezza delle applicazioni, dei dati e delle reti* | D. Progettazione e sviluppo di nuovi sistemi e tecnologie | Acquisto e messa in esercizio servizio di Lan Monitoring and Management | 01/11/2024 | 30/09/2025 |
| *5. Sicurezza delle applicazioni, dei dati e delle reti* | C. Formazione e miglioramento della consapevolezza delle persone | Consolidamento conoscenza specialistica e certificazione in ambito infrastruttura e gestione apparati attivi | 01/11/2024 | 31/10/2025 |

## ART. 5 DURATA / TERMINI CONTRATTUALI

Il servizio richiesto dovrà essere svolto all'interno del periodo di durata del progetto, che si concluderà il **30 novembre 2025** (Salvo diversa indicazione dall'Agenzia per la Cybersicurezza Nazionale). I rilasci devono rispettare il GANTT di progetto secondo quanto riportato all'ART. 4.

## ART. 6 CORRISPETTIVO E MODALITÀ DI PAGAMENTO

L'importo complessivo stimato per il servizio è pari a **€. 1.030.912,61**. = (unmilionetrentamilanovecentododici/61) oneri fiscali e previdenziali esclusi.

Il corrispettivo contrattuale verrà determinato applicando su tale importo il ribasso proposto dall'Appaltatore per il servizio in oggetto.

Il corrispettivo s'intende comprensivo di ogni onere relativo al servizio reso a regola d'arte ed è fisso ed invariabile per tutta la durata del contratto, fatte salve eventuali modalità di revisione prezzi.

L'Appaltatore riconosce che il prezzo è rimunerativo e di non avere, quindi, alcun diritto a chiedere ulteriori patti, condizioni, prezzi e/o compensi diversi, maggiori o comunque più favorevoli di quelli fissati.

Le somme saranno pagate a presentazione della relativa fattura emessa dall'Appaltatore secondo una logica bimestralmente a seconda delle ore lavorate a SAL e per beni acquistati, secondo la seguente tempistica:

| **EMISSIONE FATTURA** | **PERIODO DI RIFERIMENTO** |
|---|---|
| Gennaio 2025 | 1 novembre 2024 – 31 dicembre 2024 |
| Marzo 2025 | 1 gennaio 2025 – 28 febbraio 2025 |
| Maggio 2025 | 1 marzo 2025 – 30 aprile 2025 |
| Luglio 2025 | 1 maggio 2025 – 30 giugno 2025 |
| Settembre 2025 | 1 luglio 2025 – 31 agosto 2025 |
| Novembre 2025 | 1 settembre 2025 – 31 ottobre 2025 |
| Dicembre 2025 | 1 novembre 2025 – 30 novembre 2025 |

Le liquidazioni avverranno all'atto dell'approvazione, da parte della Città Metropolitana di Genova, del rendiconto dell'attività svolta.

Il rendiconto dovrà descrivere dettagliatamente l'attività realizzata e mettere in relazione gli obiettivi fissati a inizio contratto e i risultati raggiunti e rilevare in maniera chiara e puntuale gli eventuali scostamenti registrati rispetto agli obiettivi iniziali anche in riferimento alla tempistica prevista.

Le fatture devono essere obbligatoriamente redatte in modalità elettronica mediante l'utilizzo del sistema informatico messo a disposizione sul sito www.fatturapa.gov.it.

Al fine di consentire il corretto indirizzamento delle fatture elettroniche, si riporta di seguito il codice ufficio, consultabile anche all'interno dell'Indice delle Pubbliche Amministrazioni (www.indicepa.gov.it): Codice Univoco Ufficio: UFGE40 Città Metropolitana di Genova.

La data di ricevimento della fattura corrisponde a quella in cui la stessa è stata correttamente caricata sul Sistema di interscambio per le fatture elettroniche.

La dicitura da inserire in oggetto della fattura dovrà essere la seguente:

- Documento contabile finanziario a valere su *Progetto PNRR [M1.C1.A1 – INVESTIMENTO 1.5] finanziato dall'Unione Europea – Next GenerationEU*;
- Titolo del Progetto: "Cyber-CMGE";
- CUP D41B20001480006;
- CIG XXXXXXXXXXXXX;

La fattura deve altresì, riportare l'annotazione "scissione dei pagamenti" al fine di consentire alla Città Metropolitana di Genova di adempiere a quanto disposto dall'art. 17-ter del D.P.R. 26 ottobre 1972, n. 633, introdotto dall'art. 1, comma 629, lettera b), della legge 23 dicembre 2014, n. 190 (split payment). Saranno pertanto liquidati all'Appaltatore i soli importi riferiti all'imponibile, mentre verranno trattenute le somme relative all'IVA per il successivo riversamento all'erario.

La data di ricevimento della fattura corrisponde a quella in cui la stessa è stata correttamente caricata sul Sistema di interscambio per le fatture elettroniche.

Il pagamento delle fatture è effettuato, ai sensi del Decreto Legislativo 9 ottobre 2002, n. 231, "Attuazione della direttiva 2000/35/CE relativa alla lotta contro i ritardi di pagamento nelle transazioni commerciali" e ss.mm.ii., entro 30 (trenta) giorni dal ricevimento delle stesse.

I termini di pagamento si intendono rispettati con la trasmissione del mandato alla Tesoreria.

In caso di crediti indebitamente maturati dall'Amministrazione a seguito di errori di fatturazione, omissione di servizi, pretesi danni o risarcimenti, o per effetto dell'applicazione di sanzioni amministrative e contestazioni, gli stessi saranno portati in deduzione del corrispettivo dovuto mediante emissione di specifica nota di credito da parte dell'Appaltatore in occasione del primo pagamento utile.

L'Appaltatore non è esonerato dagli obblighi e dagli oneri derivanti dal contratto in tutti i casi di ritardo nel pagamento da parte dell'Amministrazione, dovuto a cause di forza maggiore.

Le disposizioni del presente articolo trovano applicazione in tutti i casi di pagamento diretto da parte dell'Amministrazione dei subappaltatori.

## ART. 7 TRACCIABILITÀ DEI FLUSSI FINANZIARI

I pagamenti verranno effettuati dalla Città Metropolitana di Genova esclusivamente mediante bonifico su conto corrente bancario o postale dedicato, ai sensi di quanto previsto dall'articolo 3 della Legge 13 agosto 2010, n. 136.

L'Appaltatore s'impegna a comunicare gli estremi identificativi del conto dedicato entro 7 giorni dalla stipula del contratto unitamente alle generalità e al codice fiscale delle persone delegate ad operare su di esso, fermo restando che in assenza di dette comunicazioni l'Amministrazione non esegue i pagamenti senza che l'Appaltatore possa avere nulla a pretendere per il ritardo.

Non è consentito all'Appaltatore di segnalare più di un conto dedicato alle transazioni economiche con l'Amministrazione. La segnalazione di un nuovo conto dedicato comporta automaticamente la cessazione dell'operatività da parte della Città Metropolitana di Genova sul conto precedentemente indicato.

L'Appaltatore si impegna a rispettare tutti gli obblighi e gli adempimenti previsti dall'articolo 3 della Legge 13 agosto 2010, n. 136, sulla tracciabilità dei flussi finanziari.

La violazione degli obblighi di tracciabilità previsti dalla Legge 13 agosto 2010, n. 136 e dal presente contratto comporta la risoluzione dello stesso.

L'Appaltatore s'impegna a comunicare ai sub-appaltatori, sub-contraenti e sub-fornitori il codice unico di progetto (CUP) e il codice identificativo gara (CIG) relativi all'appalto.

L'Appaltatore inoltre deve prevedere nei contratti sottoscritti con i sub-appaltatori, i sub-fornitori e i sub-contraenti, apposite clausole con cui gli stessi s'impegnano al rispetto dei suddetti obblighi, ed è tenuto a risolvere tali contratti in caso di violazione della controparte degli obblighi di tracciabilità finanziaria, dandone immediata comunicazione all'Amministrazione e alla Prefettura - Ufficio Territoriale del Governo.

## ART. 8 SUBAPPALTO

Si stabilisce che debbano essere direttamente eseguite dall'Appaltatore le attività di consulenza e che pertanto NON possono essere subappaltate.

## ART. 9 VARIANTI INTRODOTTE DAL COMMITTENTE

La Stazione Appaltante, nei casi previsti dalla normativa vigente, potrà richiedere variazione al contratto stipulato.

In tali casi, l'Appaltatore è obbligato ad assoggettarsi alla variazione richiesta alle stesse condizioni previste dal contratto.

## ART. 10 RESPONSABILE DEL SERVIZIO

All'atto della stipula del contratto, l'Appaltatore, dovrà comunicare alla Stazione Appaltante, il Responsabile del servizio, che fungerà da unica interfaccia con i responsabili coinvolti della Stazione Appaltante.

## ART. 11 OBBLIGHI DERIVANTI DAI RAPPORTI DI LAVORO

L'Appaltatore si obbliga ad ottemperare a tutti gli obblighi verso i propri dipendenti e/o collaboratori derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro, ivi compresi quelli in tema di igiene e sicurezza, nonché previdenza e disciplina infortunistica, assumendo a proprio carico tutti i relativi oneri.

L'assunzione e il trattamento economico del personale devono avvenire nel rispetto della normativa vigente e il rapporto di lavoro deve essere regolato dai contratti collettivi di categoria, nonché da quelli integrativi e territoriali.

Gli oneri retributivi, previdenziali, assistenziali e assicurativi sono a carico dell'Appaltatore, senza che possa essere avanzata nei confronti della Città Metropolitana di Genova alcuna rivendicazione da parte del personale dell'Appaltatore.

L'Appaltatore si impegna ad applicare i contratti collettivi anche dopo la loro scadenza fino alla conclusione delle procedure di rinnovo previste dalla contrattazione collettiva di settore.

L'Amministrazione si riserva la facoltà di effettuare verifiche sulla regolarità dei rapporti di lavoro, anche per gli effetti contributivi ed assicurativi. L'Appaltatore si impegna ad esibire la documentazione contabile e amministrativa necessaria per l'esecuzione dei controlli.

## ART. 12 ADEMPIMENTI IN MATERIA DI PARI OPPORTUNITÀ E INCLUSIONE LAVORATIVA

Per perseguire le finalità relative alle pari opportunità, generazionali e di genere e per promuovere l'inclusione lavorativa delle persone disabili, in relazione alle procedure afferenti agli investimenti

pubblici finanziati, in tutto o in parte, con le risorse previste dal PNRR e dal PNC, si applicano le disposizioni seguenti, di cui al D.L. 77/2021:

**Art. 47, comma 2**: *nel caso in occupi un numero di dipendenti superiore a 50*, l'Appaltatore allega alla documentazione amministrativa copia dell'ultimo rapporto sulla situazione del personale redatto ai sensi dell'art. 46 del Decreto Legislativo 11 aprile 2006 n. 198, con attestazione della sua conformità a quello eventualmente trasmesso alle rappresentanze sindacali aziendali e alla Consigliera e al Consigliere Regionale di Parità. In caso di inosservanza dei termini previsti dal comma 1 del medesimo articolo 46, produce attestazione della contestuale trasmissione del rapporto sulla situazione del personale redatto ai sensi dell'art- 46 del Decreto Legislativo 11 aprile 2006 n. 198, alle rappresentanze sindacali aziendali e alla Consigliera e al Consigliere Regionale di Parità;

**Art. 47, comma 3**: *nel caso in cui occupi un numero di dipendenti pari o superiore a 15*, l'Appaltatore, si impegna a consegnare alla Stazione Appaltante, entro sei mesi dalla stipula del contratto, una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni e in relazione allo stato di assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità, dell'intervento della Cassa integrazione guadagni, dei licenziamenti, dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta. La relazione di cui al primo periodo è trasmessa alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità.

La violazione degli obblighi di cui all'art. 47, comma 3 del D.L. 77/2021 determina l'impossibilità per l'operatore economico di partecipare, in forma singola ovvero in raggruppamento temporaneo, per un periodo di dodici mesi, ad ulteriori procedure di affidamento afferenti agli investimenti pubblici finanziati, in tutto o in parte, con le risorse del PNRR e PNC.

**Art. 47, comma 3bis***: sempre nel caso in cui occupi un numero di dipendenti pari o superiore a 15,* l'Appaltatore è tenuto a consegnare alla Stazione Appaltante, nel termine di sei mesi dalla stipula del contratto, la certificazione di cui all'articolo 17 della legge 12 marzo 1999, n. 68, e una relazione relativa all'assolvimento degli obblighi di cui alla medesima legge e alle eventuali sanzioni e provvedimenti disposti a suo carico nel triennio antecedente la data di scadenza di presentazione del preventivo. La relazione di cui al presente periodo è trasmessa alle rappresentanze sindacali aziendali.

**Art. 47, comma 4**: l'Appaltatore si impegna a riservare, in caso di necessità di effettuare nuove assunzioni per l'esecuzione del presente contratto o per la realizzazione di attività ad esso connesse o strumentali, almeno la quota del 30% delle stesse sia all'occupazione giovanile (persone di età inferiore ai 36 anni) sia all'occupazione femminile;

## ART. 13 TRATTAMENTO DEI DATI PERSONALI

Le parti si obbligano ad effettuare i trattamenti di dati personali acquisiti e trattati in connessione con l'esecuzione del contratto in conformità alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 sulla protezione dei dati personali ("GDPR") ed alla normativa nazionale applicabile in materia di protezione dei dati personali, in particolare del Decreto legislativo 30 giugno 2003 n. 196 e del Decreto legislativo 10 agosto 2018 n. 101.

La Città Metropolitana di Genova, a sensi della normativa sopra citata, informa l'Appaltatore che tratterà i dati contenuti nel contratto esclusivamente per lo svolgimento delle attività e per l'assolvimento degli obblighi previsti dalla normativa vigente in relazione ad adempimenti connessi con il contratto, e si impegna a trattarli secondo quanto previsto dal citato Regolamento UE e in base all'"informativa resa ai sensi dell'articolo 13 del citato Regolamento" contenuta nei documenti di gara.

Considerato che in conseguenza dell'affidamento del servizio in oggetto l'Appaltatore si troverà ad effettuare il trattamento di dati personali per conto dell'Ente (Titolare del trattamento), assumendo la qualifica di Responsabile del trattamento ai sensi e per gli effetti di cui all'articolo 28 del Regolamento (UE) 2016/679 ("GDPR"), contestualmente alla stipula del contratto verrà sottoscritto l'Allegato 7 - appendice contrattuale relativa all'incarico del Responsabile del trattamento dei dati personali.

La Città Metropolitana di Genova informa fin d'ora l'Appaltatore che il contratto concluso tra le parti per il servizio/fornitura in oggetto verrà pubblicato nella "Sezione Trasparenza" del sito internet istituzionale, ai sensi della delibera ANAC n. 7 del 17 gennaio 2023 di aggiornamento del Piano Nazionale Anticorruzione (Allegato 9)

## ART. 14 CLAUSOLE DI LEGALITÀ

L'Appaltatore si impegna:

- ad accettare e rispettare la policy anticorruzione, allegata al Piano Integrato di Attività e Organizzazione della Città Metropolitana di Genova approvato con Decreto del Sindaco Metropolitano e disponibile nella Sezione Amministrazione trasparente del sito Istituzionale della Città Metropolitana di Genova, di impegnarsi ad osservare e a far osservare ai propri dipendenti, collaboratori e sub contraenti la suddetta policy, pena la risoluzione del contratto;
- a segnalare alla Stazione Appaltante qualsiasi tentativo di turbativa, irregolarità o distorsione nelle fasi di svolgimento della procedura e/o durante l'esecuzione del contratto, da parte di ogni interessato o addetto o di chiunque possa influenzare le decisioni relative alla procedura

in oggetto, nonché a collaborare con le forze di polizia, denunciando ogni tentativo di estorsione, intimidazione o condizionamento di natura criminale;

- a verificare l'insussistenza a proprio carico dell'obbligo di astensione e a mantenere nel corso di tutta la sua esecuzione una posizione che non lo ponga in conflitto d'interesse con la Stazione Appaltante ai sensi degli articoli 16 e 95, comma 1, lett. b) del D. Lgs. 36/2023;
- a riferire tempestivamente alla Prefettura ogni illecita richiesta di denaro, prestazione o altra utilità, offerta di protezione, nonché ogni illecita interferenza avanzata prima della procedura e/o dell'affidamento ovvero nel corso dell'esecuzione del contratto, nei confronti di un proprio rappresentante, agente o dipendente e di ogni altro soggetto che intervenga a qualsiasi titolo nell'esecuzione contrattuale e di cui lo stesso venga a conoscenza. L'omissione di tale adempimento consente alla Città Metropolitana di Genova di chiedere la risoluzione del contratto;
- nell'esecuzione dell'appalto, a rispettare e far rispettare dai propri dipendenti, collaboratori e subcontraenti il "Codice di comportamento" dei dipendenti pubblici adottato con D.P.R. n. 62/2013, nonché il "Codice di comportamento" della Città Metropolitana, approvato con determinazione del Sindaco Metropolitano n.1/2022 del 13 gennaio 2022, pubblicato sul sito della Città Metropolitana di Genova nella sezione "Amministrazione trasparente – Atti generali", di cui dichiara di aver preso visione. La violazione degli obblighi di comportamento comporta per l'Amministrazione la facoltà di risolvere il contratto, qualora, in ragione della gravità o della reiterazione, la stessa sia ritenuta grave;

In ottemperanza al disposto di cui all'art. 53, comma 16 ter, del Decreto Legislativo 30 marzo 2001, n.165, l'Appaltatore dichiara che non sono stati affidati incarichi o lavori retribuiti, di natura autonoma o subordinata, a ex dipendenti delle pubbliche amministrazioni di cui all'art.1, comma 2, del medesimo decreto, che siano cessati dal servizio da meno di tre anni, se questi avevano esercitato, nei confronti dell'Appaltatore medesimo, poteri autoritativi o negoziali in nome e per conto dell'Amministrazione di appartenenza.

Attraverso il seguente link: https://whistleblowing.cittametropolitana.genova.it/ è possibile accedere alla piattaforma informatica di Città Metropolitana di Genova che consente di segnalare, in ottemperanza alla delibera ANAC n.469 del 9 giugno 2021 'Linee guida Whistleblowing', eventuali irregolarità, illeciti e condotte illegali che riguardino codesta Amministrazione.

## ART. 15 SPESE CONTRATTUALI

Sono a carico dell'Appaltatore le spese di stipulazione del contratto, pari ad euro 250,00 ai sensi dell'Allegato I.4 al D. Lgs. 36/2023, nonché qualsiasi atto inerente e conseguente alla stipula dello stesso.

## ART. 16 CONTROVERSIE

Per qualsiasi controversia che dovesse sorgere tra le parti in ordine all'interpretazione del presente capitolato speciale e la corretta esecuzione delle disposizioni contrattuali in esso contenute sarà competente il Foro di Genova. È esclusa qualsiasi forma di arbitrato.

## ART. 17 DISPOSIZIONI IN MATERIA DI PRINCIPIO DNSH

Il Dispositivo per la ripresa e la resilienza (Regolamento UE 241/2021) stabilisce che tutte le misure dei Piani Nazionali per la Ripresa e Resilienza (PNRR) debbano soddisfare il principio di "non arrecare danno significativo agli obiettivi ambientali". Tale vincolo si traduce in una valutazione di conformità degli interventi al principio del "Do No Significant Harm" (DNSH), che è stato declinato nei seguenti sei obiettivi ambientali:

1. *Mitigazione dei cambiamenti climatici*

   Un'attività economica non deve portare a significative emissioni di gas serra (GHG).

2. *Adattamento ai cambiamenti climatici*

   Un'attività economica non deve determinare un maggiore impatto negativo sul clima attuale e futuro, sull'attività stessa o sulle persone, sulla natura o sui beni.

3. *Uso sostenibile e protezione delle risorse idriche e marine*

   Un'attività economica non deve essere dannosa per il buono stato dei corpi idrici (superficiali, sotterranei o marini) e determinare il deterioramento qualitativo o la riduzione del potenziale ecologico.

4. *Transizione verso l'economia circolare, con riferimento anche a riduzione e riciclo dei rifiuti*

   Un'attività economica non deve portare a significative inefficienze nell'utilizzo di materiali recuperati o riciclati, ad incrementi nell'uso diretto o indiretto di risorse naturali, all'incremento significativo di rifiuti, al loro incenerimento o smaltimento, causando danni ambientali significativi a lungo termine.

5. *Prevenzione e riduzione dell'inquinamento dell'aria, dell'acqua o del suolo*

   Un'attività economica non deve determinare un aumento delle emissioni di inquinanti nell'aria, nell'acqua o nel suolo.

6. *Protezione e ripristino della biodiversità e della salute degli ecosistemi*

   Un'attività economica non deve essere dannosa per le buone condizioni e la resilienza degli ecosistemi o per lo stato di conservazione degli habitat e delle specie, comprese quelle di interesse per l'Unione.

Al fine assistere le Amministrazioni titolari di misure e i Soggetti attuatori degli interventi nel processo di indirizzo e nella raccolta di informazioni e verifica per assicurare il rispetto del principio DNSH, è stata pubblicata dalla Ragioneria Generale dello Stato una Guida Operativa, corredata di relative check list, che fornisce indicazioni sui requisiti tassonomici, sulla normativa corrispondente e sugli elementi utili per documentare il rispetto di tali requisiti (ultima versione della Guida Operativa pubblicata nella Circolare n.33[1], del 13 ottobre 2022).

## DOCUMENTAZIONE DA PRESENTARE

Il presente capitolato prevede la fornitura di servizi cloud, per cui è necessario applicare la Scheda n. 6 "***Servizi informatici di hosting e cloud***" prevista dalla Guida Operativa.

Il fornitore, dovrà quindi, dimostrare di avere la certificazione di sistema di gestione ambientale di tipo ISO 14001 o EMAS rilasciata sotto accreditamento.

[1] Circolare del 13 ottobre 2022, n. 33

Proposta n. 3307/2024

# CITTÀ METROPOLITANA DI GENOVA

## VISTO ATTESTANTE LA COPERTURA FINANZIARIA

Ai sensi degli artt. 147Bis 1° comma, 153 e 183 del decreto legislativo 18 agosto 2000, n.267

**Proponente: Ufficio Reti informatiche**

**Oggetto: ID.2024_169 PNRR M1C1I1.5 - "CYBERSECURITY" - FINANZIATO DALL'UNIONE EUROPEA, NEXTGENERATIONEU. SERVIZIO DI CONSULENZA E ACQUISTO FORNITURE PER L'ATTUAZIONE DEL PROGETTO "CYBER CMGE"- AFFIDAMENTO IN HOUSE AI SENSI DELL'ART. 7 DEL D.LGS. N. 36/2023 A LIGURIA DIGITALE S.P.A. - CUP D41B20001480006 - CIG B451B6CDF8 - IMPORTO DI EURO 1.257.713,37 ONERI FISCALI INCLUSI.**

Il presente atto produce effetti diretti o indiretti sulla situazione economico-finanziaria e/o sul patrimonio dell'ente, evidenziate nelle imputazioni contabili di seguito indicate, per cui si esprime parere: FAVOREVOLE

Annotazioni o motivazioni del parere contrario:

## VISTO ATTESTANTE LA COPERTURA FINANZIARIA

| S/E | Codice | Cap. | Azione | | Importo | Prenotazione | | Impegno | | Accertamento | | CUP | CIG |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Euro | N. | Anno | N. | Anno | N. | Anno | | |
| USCITA | 0102104 | 0 | 1000481 | + | 660,00 | | | 377 | 2024 | | | D41B20001480006 | B451B6CDF8 |
| Note: Contributo ANAC | | | | | | | | | | | | | |
| USCITA | 0108202 | 0 | 2003740 | + | 607.110,00 | 241 | 2025 | 248 | 2025 | | | D41B20001480006 | B451B6CDF8 |
| Note: PNRR M1C1I1.5 - "CYBERSECURITY" – PROGETTO "CYBER-CMGE" – LAVORO 142 | | | | | | | | | | | | | |
| USCITA | 0108103 | 0 | 1003934 | + | 650.603,37 | 239 | 2025 | 249 | 2025 | | | D41B20001480006 | B451B6CDF8 |
| Note: PNRR M1C1I1.5 - "CYBERSECURITY" – PROGETTO "CYBER-CMGE" – LAVORO 142 | | | | | | | | | | | | | |

| | | | |
|---|---|---|---|
| **TOTALE ENTRATE:** | + | | |
| **TOTALE SPESE:** | + | 1.258.373,37 | |

Genova li, 22/11/2024

**Sottoscritto dal responsabile**
**della Direzione Risorse**
**(SILVIA FABRIS)**
**con firma digitale**