

Proponente: 33.B
Proposta: 2025/1968
del 10/10/2025



**COMUNE DI
REGGIO NELL'EMILIA**

R.U.D. 1212
del 13/10/2025

SISTEMI INFORMATIVI E TRANSIZIONE DIGITALE

Dirigente: BERTANI Ing. Andrea

DETERMINAZIONE DIRIGENZIALE

OGGETTO: ADESIONE ALLA CONVENZIONE INTERCENT-ER "SERVIZI DI TRASMISSIONE DATI E VOCE SU RETI FISSE E MOBILI – LOTTO 1 E 2" PER FORNITURA DI SERVIZI NELL'AMBITO DELLA SICUREZZA E PROTEZIONE DEI DATI - SERVIZIO CERTEGO DEI SERVIZI MDR (MANAGED DETECTION & RESPONSE IN MODALITÀ 24X365) PER 24 MESI DALLA DATA DEL COLLAUDO DELLA NUOVA CONFIGURAZIONE A VALERE SU PNRR M1C1, FINANZIATO DALL'UNIONE EUROPEA ALL'INTERNO DELL'INIZIATIVA NEXGENERATIONEU – INVESTIMENTO M1C1 I1.5" – CUP J81B24000320001

IL DIRIGENTE DEL SERVIZIO SISTEMI INFORMATIVI E TRANSIZIONE DIGITALE

Richiamati:

- la deliberazione di Consiglio Comunale n. 13 del 21/01/2025 con cui è stata approvata la nota di aggiornamento al D.U.P. (Documento Unico di Programmazione) 2025-2029;
- la deliberazione di Consiglio Comunale n. 14 del 21/01/2025 con cui sono stati approvati il Bilancio di Previsione 2025 – 2027 ed i relativi allegati;
- la deliberazione di Giunta Comunale n.12 adottata nella seduta del 30/01/2025, esecutiva ai sensi di legge, con la quale è stato approvato il Piano Esecutivo di Gestione 2025-2027 - assegnazione risorse finanziarie per macro obiettivi, ai sensi dell'art. 169 co 1 e 2;
- la deliberazione di Giunta Comunale n. 8 del 23/01/2025 e successiva determinazione dirigenziale R.U.A.D. n. 152 del 29/01/2025, con la quale è stata approvata la nuova Struttura organizzativa dell'Ente;
- la delibera di Giunta Comunale n.63 del 31/3/2025 dichiarata immediatamente esecutiva, con cui è stato approvato il Piano Integrato di Attività e Organizzazione (PIAO) 2025/2027 e contestuale aggiornamento del Piano Esecutivo di Gestione e relativi allegati, approvato con GC 12 del 30/1/2025 e successivi aggiornamenti;
- la delibera di Consiglio Comunale n.123/2025 del 26/05/2025 con cui è stata deliberata la 3^a variazione al Bilancio di previsione finanziario 2025-2027 e relativi allegati;
- la deliberazione di Giunta Comunale n. 133 del 26/06/2025 con cui si è provveduto ad approvare il 1^a aggiornamento del Piano Esecutivo di Gestione 2025 e Piano Integrato Attività e Organizzazione (PIAO) 2025-2027 alle sezioni 2.2 "Performance" e 2.3 "Anticorruzione";
- il provvedimento P.G. n. 2025/27629 del 30/01/2025 con il quale il Sindaco ha attribuito incarico dirigenziale all'ing. Andrea Bertani, incarico conferito ai sensi dell'articolo 13 – sezione A del vigente Regolamento sull'Ordinamento Generale degli Uffici e dei Servizi;

Visti:

- il Regolamento (UE) 2021/241, che istituisce il dispositivo per la ripresa e la resilienza, così come integrato dal Regolamento delegato (UE) 2021/2106 della Commissione europea del 28 settembre 2021;
- Il Piano Nazionale di Ripresa e Resilienza (PNRR) valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio, notificata all'Italia dal Segretariato generale del Consiglio con nota LT 161/21, del 14 luglio 2021;

- il Decreto Legge 6 maggio 2021, n. 59, convertito con modificazioni dalla Legge 1° luglio 2021, n. 101, recante “Misure urgenti relative al Fondo complementare al Piano nazionale di ripresa e resilienza e altre misure urgenti per gli investimenti”;
- Il Decreto-legge del 31 maggio 2021, n. 77, coordinato con la legge di conversione 29 luglio 2021, n. 108;
- il Decreto-legge 9 giugno 2021, n. 80, coordinato con la legge di conversione 6 agosto 2021, n. 113;
- il Decreto del Ministero 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” e successive modificazioni;
- il Decreto del Ministero dell'Economia e delle Finanze dell'11 ottobre 2021, “Procedure relative alla gestione finanziaria delle risorse previste nell'ambito del PNRR di cui all'art.1, comma 1042, della Legge 30 dicembre 2020, n.178;
- il Decreto Legge 6 novembre 2021, n.152, convertito con modificazioni dalla Legge 29 dicembre 2021, n. 233, recante “Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose”;
- il Decreto del Presidente del Consiglio dei Ministri del 15 settembre 2021, che definisce le modalità, le tempistiche e gli strumenti per la rilevazione dei dati di attuazione finanziaria, fisica e procedurale relativa a ciascun progetto finanziato nell'ambito del Piano Nazionale di Ripresa e Resilienza, nonché dei milestone e target degli investimenti e delle riforme e di tutti gli ulteriori elementi informativi previsti nel Piano necessari per la rendicontazione alla Commissione europea;
- il DPCM 07/12/2021;
- il Decreto Legge 30 aprile 2022, n. 36, convertito con modificazioni dalla Legge 29 giugno;
- il D.lgs 2022, n. 79, recante “Ulteriori misure urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)”;
- la Delibera ANAC n. 122/2022;
- le circolari del Ministero dell'Economia e delle Finanze nn. 31, 32, 33 del 2021 e nn. 4, 6, 27, 29, 30, 31, 34, 37 del 2022 e ss.mm.ii.;

Visti inoltre:

- il Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026 dell'Agenzia per l'Italia Digitale (AGID);
- il “Testo unico delle leggi sull'ordinamento degli enti locali” approvato con D.Lgs. n. 267/2000, ed in particolare gli articoli 107 e 192;
- il D.Lgs. n. 81/2008 ed in particolare l'art. 26, comma 6;
- il D.lgs n. 36/2023;
- il decreto-legge 16 luglio 2020 n. 77, convertito, con modificazioni, dalla legge 11 settembre 2020 n. 120;
- il decreto-legge 31 maggio 2021 n. 77, convertito, con modificazioni, dalla legge 29 luglio 2021 n. 108;
- il D.P.R. n. 207/2010, regolamento attuativo del Codice dei contratti, per le parti ancora in vigore;
- l'art. 26 della legge n. 488/1999;
- l'art. 328 del D.P.R. 207/2010 e l'art. 7 del d.l. 52/2012, convertito in legge 94/2012;

- l'art. 1 comma 512 della legge 208/2015, (Legge di stabilità 2016), il quale prevede che le amministrazioni pubbliche provvedano ai propri approvvigionamenti di beni e servizi informatici e di connettività esclusivamente tramite Consip spa o i soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e servizi disponibili presso gli stessi soggetti;

Premesso che:

- ▣ con determinazione dirigenziale RUD 24 del 20/01/2022 in adesione alla Convenzione Intercenter – servizi di trasmissione dati e voce su reti fisse (lotto 1) si è provveduto al rinnovo del servizio di Network Incident e Breach Detection tramite tecnologia CERTEGO;
- ▣ con determina dirigenziale RUD n.1372 del 04/12/2023 è stato affidato a TELECOM ITALIA S.P.A. il servizio di sicurezza e protezione dei dati Network Incident Breach Detection, in adesione alla convenzione INTERCENT-ER “Servizi di trasmissione dati e voce su reti fisse” per la durata di 12 mesi dal 01/12/2023 – 30/11/2024;
- ▣ per consentire l’attivazione del servizio è stato necessario installare e configurare una componente hardware, il fornitore ha quindi completato l’attivazione e la configurazione delle componenti solo nel 2024 e redatto il verbale di collaudo nel luglio 2024, è stato quindi necessario ridefinire il periodo di erogazione del servizio con decorrenza dal 01/07/2024 fino al 30/06/2025;
- ▣ l’erogazione del servizio è quindi terminata il 30/06/2025;

Considerato che:

- ▣ gli adempimenti in materia di sicurezza previsti dalla normativa in vigore (GDPR, Misure minime AGID) impongono sempre una maggior attenzione alle azioni volte a prevenire il furto di dati personali. Il furto dei dati personali può avvenire in molteplici modi che vanno dalla violazione dei sistemi perimetrali di sicurezza, all’installazione di “agenti malevoli” (malware, pyware, trojan, virus, ecc.) sugli endpoint, a comportamenti errati da parte degli utenti;
- ▣ al di là dei diversi sistemi di sicurezza che si possono attivare (firewall, antispam, protezione da ransomware, antivirus, antim malware, ecc) esiste un approccio diverso che lavora parallelamente a tali sistemi; questo consiste in sistemi di raccolta di eventi provenienti da fonti dati diverse (es: sistema operativo, application server, web server, apparati di rete, ecc) che vengono poi messi in correlazione per capire se sono in atto attività “sospette”;

- tali attività devono essere indagate per verificare se possono portare ad una compromissione/furto di dati e l'appliance Certego installata all'interno della rete raccoglie ed analizza il traffico da/verso internet;
- Certego si basa sulla piattaforma proprietaria di Unified Security Operations "Certego PanOptikon" e prevede la predisposizione di un servizio di Managed Detection & Response

in modalità 24x365. E' una tecnologia che tramite un'appliance installata all'interno rete ed un pool di persone specializzate in sicurezza IT permette di intercettare comportamenti anomali, introdurre rapidamente misure correttive per evitarne la diffusione o limitarne il danno, attivare soluzioni di più ampio respiro per impedire il ripetersi dell'evento. Inoltre, sempre in collaborazione con l'ente, provvede a progettare soluzioni idonee ad impedire il ripetersi dell'evento. Provvede inoltre in caso di perdita di dati a fornire le informazioni necessarie per le segnalazioni agli organi competenti come previsto dal GDPR;

Presto inoltre atto che:

- il Comune di Reggio Emilia in data 22/03/2024 ha presentato propria candidatura all'Avviso Pubblico n. 08/2024, Investimento 1.5 "Cybersecurity", per la presentazione di proposte di interventi di potenziamento della resilienza Cyber dei grandi Comuni, richiedendo il finanziamento per una somma complessiva **di € 478.240,00**;
- il Dipartimento per la Trasformazione Digitale ha comunicato l'ammissione della candidatura del Comune di Reggio Emilia per l'avviso n. 08/2024, Investimento 1.5 "Cybersecurity", nome progetto: "Piano di potenziamento della sicurezza informatica", acquisita agli atti del settore al PG N. 191902 del 16/07/2024 ed è stato assunto il Codice Unico di Progetto **CUP J81B24000320001**;
- tra gli obiettivi del progetto vi è anche l'adozione di un servizio di monitoraggio degli eventi di sicurezza teso alla tempestiva rilevazione tecnologica di anomalie sul sistema informatico dell'Ente.

Dato atto che:

- tutti i servizi Certego MDR comprendono, di base, una serie di attività e funzionalità che sono le seguenti:
 - INCIDENT RESPONSE: L'attività del team di Security Operation comprende la completa gestione degli incident anche di severity elevata, in particolare l'analisi degli asset che sono stati coinvolti allo scopo di individuare i movimenti dell'attaccante;
 - SERVICE REVIEW: sono previste delle Service Review periodiche del servizio nel quale analizzare le prestazioni e il livello di servizio;

-EARLY WARNING: un servizio aggiuntivo di monitoraggio continuativo ed automatizzato dei database pubblici di vulnerabilità exploit. Tramite la definizione di specifiche keyword di ricerca è possibile analizzare questi dati e segnalare eventuali corrispondenze rilevate che indichino la possibile presenza di vulnerabilità sui sistemi utilizzati all'interno o all'esterno dell'infrastruttura;

- DNS SECURE;

- ripetto al servizio utilizzato in precedenza, a seguito di interlocuzione tecnica con il fornitore si ritiene opportuno attivare un nuovo modulo di Endpoint Detection, in precedenza non disponibile, integrato con il software Trend Micro di recente acquisizione da parte dell'Ente,

nonché un modulo che consenta l'integrazione degli IOC Feed di Certego direttamente nel firewall principale dell'Ente;

- MODULI DI THREAT DETECTION: Il modulo Endpoint Detection è previsto per 1500 endpoint TrendMicro. L'abilitazione di questo modulo permette identificare ed analizzare potenziali minacce in esecuzione sui sistemi del Comune di Reggio Emilia attraverso la raccolta di dati telemetrici a basso livello. Per ottenere un livello di visibilità massima sugli endpoint, il monitoraggio avviene attraverso un agente software installato sulle macchine del cliente (Client e Server, Windows, Linux e macOS).

- MODULI DI THREAT INTELLIGENCE: Threat Intelligence IOC Feeds. È previsto l'inserimento degli IOC feed di Certego per un perimetro di 1 Firewall. L'abilitazione di questo modulo prevede l'attivazione di un flusso costante di condivisione di indicatori di compromissione (Indicator of Compromise - IOC) prodotti dalla piattaforma proprietaria di Threat Intelligence di Certego. Questi indicatori (IP e domini verificati malevoli) verranno importati nei sistemi di difesa perimetrale per potenziarne le capacità preventive.

Tali nuove funzionalità aggiuntive consentiranno di migliorare la postura di sicurezza dell'ente a fronte di potenziali minacce cyber.

Oltre le funzionalità suindicate sono previste attività sistemistiche relative al supporto e setup tenant Trend Vision One (V1) ed alla configurazione dell'integrazione con Certego PanOptikon per erogazione servizio ETDM, configurazione degli accessi alla console V1 e dei ruoli degli utenti/gruppi in base alle attività che dovranno svolgere;

Per l'erogazione del servizio è stata effettuata richiesta di progetto esecutivo a TIM (azienda aggiudicataria della "CONVENZIONE PER L'AFFIDAMENTO DI SERVIZI DI TRASMISSIONE DATI E VOCE SU RETI FISSE E MOBILI – LOTTI 1 e 2", stipulata in data 06/07/2022 dall'Agenzia Regionale Intercent-ER) per i seguenti Servizi aggiuntivi - servizi di sicurezza:

- n° 2050 - PanOptikon SOAR Platform - Standard Service - 2000-2499 Assets
- n° 1500 - Endpoint Detection - 1000-1500 Agents
- n° 1 - Vision One Data Pipeline
- n° 1 - Threat Intelligence IOC Feeds - S

- Attività sistemistiche configurazione Trend Micro e servizio supporto Net&Sys (24 mesi)

Preso atto che:

- il servizio Certego Breach Detection & Incident Response è scaduto e risulta opportuno, per le motivazioni sopra indicate, provvedere a riattivarlo, stante il ruolo che riveste nell'ambito della sicurezza e protezione dei dati;
- alla data odierna risulta attiva la convenzione Intercent-ER denominata "CONVENZIONE PER L'AFFIDAMENTO DI SERVIZI DI TRASMISSIONE DATI E VOCE SU RETI FISSE E MOBILI – LOTTI 1 e 2", dove all'interno del LOTTO 1, è prevista l'erogazione di servizi di sicurezza analoghi alle necessità dell'Ente;
- come previsto dalla convenzione, il Servizio Sistemi Informativi e Transizione Digitale ha richiesto alla ditta Telecom Italia Spa, aggiudicataria della convenzione anzidetta, il progetto

esecutivo per l'erogazione del servizio di sicurezza e protezione dei dati per la durata di 24 mesi;

- Telecom Italia SpA ha trasmesso il progetto esecutivo Codice Progetto n.TLC25J0Q ed il prospetto economico (PG N.2025/0241667) allegati A) e B) del presente atto quali parti integranti;

Considerato che:

- Certego aiuta l'Ente a rilevare, analizzare e neutralizzare le minacce informatiche in tempo reale. Combinando tecnologie avanzate con analisti esperti, offre quindi una protezione proattiva e monitoraggio continuo per garantire la sicurezza delle infrastrutture digitali;
- L'adozione di tale sistema consente pertanto di perseguire gli obiettivi del Piano di Potenziamento della sicurezza Informatica dell'Ente;

Presa visione dei già citati documenti "progetto esecutivo cod. TLC25J0Q", contenente le condizioni contrattuali e le caratteristiche tecniche del servizio in oggetto, che sono ritenute idonee per le esigenze di questo ente, e "prospetto economico" da cui risulta una spesa complessiva di € **€ 103.795,20 (IVA esclusa)** si ritiene opportuno aderire alla convenzione suddetta per la fornitura del Servizio Certego dei servizi MDR (Managed Detection & Response in modalità 24x365) per 24 mesi dalla data del collaudo della nuova configurazione;

Posto che:

- l'art. 1 comma 512 della legge 208/2015, (Legge di stabilità 2016), prevede che le amministrazioni pubbliche provvedano ai propri approvvigionamenti di beni e servizi informatici e di connettività esclusivamente tramite CONSIP spa o i soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e servizi disponibili presso gli stessi soggetti.

- l'art. 50, comma 1, lett. b) D Lgs 36/2023 stabilisce che le stazioni appaltanti procedono all'affidamento dei contratti, tramite "affidamento diretto dei servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo inferiore a 140.000 euro, anche senza consultazione di più operatori economici, assicurando che siano scelti soggetti in possesso di documentate esperienze pregresse idonee all'esecuzione delle prestazioni contrattuali, anche individuati tra gli iscritti in elenchi o albi istituiti dalla stazione appaltante;
- ai sensi dell'art.17 del D.lgs 36/2023 comma 1 e 2 " in caso di affidamento diretto, l'atto adottato dall'ente individua l'oggetto, l'importo e il contraente, unitamente alle ragioni della sua scelta, ai requisiti di carattere generale e, se necessari, a quelli inerenti alla capacità economico-finanziaria e tecnico-professionale".

Considerato quanto sopra esposto, la fornitura del servizio in adesione alla convenzione Intercenter-ER, da effettuarsi mediante emissione di ordinativo di fornitura sul portale <https://intercenter.regione.emiliaromagna>, si configura come segue:

Convenzione Intercenter denominata "servizi di trasmissione dati e voce su reti fisse (lotto 1) e mobili (lotto 2) " CIG CONVENZIONE LOTTO 1 9016294130 Ditta Telecom SpA, P.I. 00488410010

Descrizione	UT unitaria	CM unitaria	OdF unitaria per 10 mesi	OdF totale per 10 mesi
Servizi base	390,00	0,00	390,00	39.780,00
Servizi aggiuntivi	313,80	26,15	575,30	58.680,60
TOTALE	€ 703,80	€ 26,15	€ 965,30	€ 98.460,60

	Mesi	UT unitario	canone mese unitario	Quantità	tot UT	Tot. Canone per 24 mesi di servizio	Totale prezzo al cliente, per 24 mesi di servizio
Giornata figura professionale armonizzazione soluzioni IP nativo (attivazione)	24	390,00	0,00 €	102	39.000,00 €	0,00 €	39.780,00 €
Pacchetto sicurezza advanced IPS, codice regionale BS0004013	24	313,80 €	26,15 €	102	32.007,60 €	32.007,60 €	64.015,20 €

Totale 103.795,20 €

Dato atto che:

- sono stati condotti accertamenti volti ad appurare l'esistenza di rischi da interferenza e che, in conformità a quanto previsto dall'art. 26 comma 3 del D.Lgs. 81/2008 e dalla determinazione AVCP n. 3/2008 del 5.3.2008 per le modalità di svolgimento dell'appalto, non sussistono rischi di interferenza con il personale comunale in quanto trattasi di servizio di natura intellettuale; non è pertanto necessario redigere il DUVRI e, conseguentemente, i costi per la sicurezza per rischi da interferenze sono pari a 0 (zero);
- il documento DURC risulta regolare e in corso di validità fino al 05/01/2026 e sarà recepito in atti e verificato durante tutte le fasi di vigenza contrattuale, ai sensi dell'art. 2 della legge n. 266/2002;
- Il contratto verrà stipulato ai sensi dell'art.18 comma 1 del D.lgs 36/2023 e del vigente "Regolamento comunale per la disciplina dei contratti" del Comune di Reggio Emilia, mediante corrispondenza secondo l'uso commerciale;

Dato atto inoltre che:

- le verifiche previste dalla vigente normativa, nei confronti dell'aggiudicatario suindicato, afferenti al possesso dei requisiti generali e morali di cui agli artt. 94, 95 D.Lgs. 36/2023, sono state effettuate da Intercent-ER/SATER in sede di aggiudicazione della convenzione;
- il responsabile del procedimento (RUP) è l'Ing. Andrea Bertani, dirigente del Servizio Sistemi Informativi e Transizione Digitale;

Atteso che sul presente provvedimento si esprime, con la sottoscrizione dello stesso, parere favorevole in ordine alla regolarità e correttezza dell'azione amministrativa come prescritto dall'art. 147 bis del D. Lgs. 267/2000.

DETERMINA

1. di richiamare la premessa a costituire parte integrante del presente dispositivo;
2. di aderire, per le motivazioni in premessa esposte alla convenzione **“Servizi di trasmissione dati e voce su reti fisse ”** stipulata fra la centrale di committenza Intercent-ER e la Ditta TELECOM ITALIA SpA con sede legale in Milano – P.I. 00488410010, per la fornitura del servizio di Network incident e Breach Detection come dettagliato nel progetto esecutivo cod. TLC25J0Q, contenente le condizioni contrattuali e le caratteristiche tecniche del servizio in oggetto e nel “prospetto economico”, **allegati A) e B) del presente atto quali parti integranti**, una spesa complessiva di € 103.795,20 (iva esclusa) pari a € 126.630,14 iva 22% compresa;

3. di dare atto che l'ordinativo di fornitura verrà effettuato secondo le modalità disposte da Intercent-er attraverso la propria piattaforma e darà origine al contratto con il fornitore aggiudicatario così come disposto dal capitolato tecnico visibile sul sito Intercent-er;
4. di dare atto che le verifiche previste dalla vigente normativa, nei confronti dell'aggiudicatario suindicato, afferenti al possesso dei requisiti generali e morali di cui agli artt. 94, 95 D.Lgs. 36/2023, sono state effettuate da Intercent-ER/SATER in sede di aggiudicazione della convenzione e che pertanto la ditta affidataria è in possesso dei requisiti previsti dalla vigente normativa;
5. di accertare l'entrata complessiva di € 126.630,14 (iva compresa) quale finanziamento del progetto PNRR M1C1 I1.5 "DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA - CYBERSECURITY", - Codice del piano dei conti integrato: 4.02.01.01.003 - al capitolo **9923/10** denominato "PNRR-M1C1-INVESTIMENTO 1.5_ CYBERSECURITY DIGITALIZZAZIONE INNOVAZIONE E SICUREZZA NELLA PA OBIETTIVO 2024_PG_3341 - CUP J81B24000320001 == VEGG. CAP. U 40823/10 del bilancio pluriennale 2025/2027, esercizio 2025 - Centro di Costo 0107 , si conferma che il contributo, accertato in quanto sussistono tutti i requisiti di legge, per quanto di conoscenza, è tuttora esigibile e conseguentemente liquidabile. Si precisa che si stanno attivando tutte le procedure necessarie alla riscossione e si proseguirà su tale linea in base alla normativa in materia
6. di impegnare la spesa complessiva di € 126.630,14 (iva compresa) in favore della ditta TELECOM ITALIA SPA con imputazione alla Missione: 01; Programma: 08; Titolo: 1 codice del piano dei conti integrato: 2.02.01.07.999, del Bilancio 2025-2027 al capitolo n.**40823/10** denominato PNRR-M1C1-INVESTIMENTO 1.5_ CYBERSECURITY DIGITALIZZAZIONE INNOVAZIONE E SICUREZZA NELLA PA OBIETTIVO 2024_PG_3341 - CUP J81B24000320001 ==VEGG CAP. E 9923/10 , centro di costo 0107; codice Modalità di gestione Conto annuale 002;
7. che sarà cura del RUP, ad avvenuta attribuzione del Codice Identificativo di Gara (CIG), pubblicarlo nella sezione - "AVCP/ANAC - L. 190/2012 - della sezione Trasparenza di J-ente Atti e comunicarlo al fornitore affidatario tramite procedura jente nell'emissione del buono d'ordine;
8. di disporre l'invio alla Ragioneria per le procedure di cui all'art. 183, 7° comma, del T.U. D. Leg.vo n. 267 del 18/8/2000;
9. di adempiere agli obblighi di pubblicità di cui agli art. 23 e 37 di cui al D.Lgs. 33/2013 (Decreto trasparenza), all'art. 1 co. 32 della L. 190/2012, all'art. 20 del D.Lgs. 36/2023.

Si attesta che non sussistono situazioni di conflitto d'interesse in capo al Dirigente firmatario.

IL DIRIGENTE DEL SERVIZIO
(Ing. Andrea Bertani)

