



SETTORE INNOVAZIONE DIGITALE COMUNICAZIONE PATRIMONIO E PROVVEDITORATO
SERVIZIO SISTEMI INFORMATIVI

Fasc. 02.11.02.02/29/2025

I.P. 2820/2025

DETERMINAZIONE DIRIGENZIALE CON IMPEGNO DI SPESA

N. 1198 DEL 29/05/2025

SETTORE INNOVAZIONE DIGITALE COMUNICAZIONE PATRIMONIO E
PROVVEDITORATO
SERVIZIO SISTEMI INFORMATIVI

OGGETTO: PNRR, MISSIONE 1, COMPONENTE 1, INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5. DENOMINATO CYBER_IN_BO (ID: 24_WP9_A8_CITTÀ METROPOLITANA DI BOLOGNA) CUP: C36G24000020006 - ENGINEERING D.HUB SPA - ACQUISIZIONE E IMPLEMENTAZIONE SERVIZIO SOC PER LA PREVENZIONE DA ATTACCHI CYBER. CIG MASTER: 97219284C8; CIG DERIVATO: B6F6C7A62E.

Il Dirigente/Funziario delegato

DECISIONE

1) **Dispone:**

- a) per le ragioni esposte in motivazione, ai sensi dell'art. 50, comma 1, lett. b) 1 e del combinato disposto degli artt. 225, co. 8 e 226, co. 1 del D.lgs. 36/2023, l'affidamento in

¹ Ai sensi dell'art. 225, comma 8, D.lgs. 36/2023 che prevede "In relazione alle procedure di affidamento e ai contratti riguardanti investimenti pubblici, anche suddivisi in lotti, finanziati in tutto o in parte con le risorse previste dal PNRR e dal PNC, nonché dai programmi cofinanziati dai fondi strutturali dell'Unione Europea, ivi comprese le infrastrutture di supporto ad essi connesse, anche se non finanziate con dette risorse, si applicano, anche dopo il 1° luglio 2023, le disposizioni di cui al decreto-legge n. 77 del 2021, convertito, con modificazioni, dalla legge n. 108 del 2021, al decreto-legge 24 febbraio 2023, n. 13, nonché le specifiche disposizioni legislative finalizzate a semplificare e agevolare la realizzazione degli obiettivi stabiliti dal PNRR, dal PNC nonché dal Piano nazionale integrato per l'energia e il clima 2030 di cui al regolamento (UE) 2018/1999 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018" e dell'art. 226, co. 1, D.lgs. 36/2023 che prevede "Il decreto legislativo 18 aprile 2016, n. 50 del 2016, è abrogato dal 1° luglio 2023."

convenzione Intercent-ER denominata SERVIZI DI IT SYSTEM MANAGEMENT 2 – LOTTO 1, ad Engineering D.Hub SpA, avente sede legale in Viale Carlo Viola 76, 11026 Pont-Saint-Martin (Valle d'Aosta/Vallée d'Aoste) e P.Iva 12622480155, per l'acquisizione di un servizio SOC per la prevenzione di attacchi cyber nell'ambito del progetto PNRR, Missione 1, Componente 1, Investimento .5 “Cybersecurity” M1C1I1.5. denominato Cyber_In_BO (ID: 24_WP9_A8_Città Metropolitana di Bologna) del Piano Nazionale di Ripresa e Resilienza (PNRR);

- b) l'Accertamento ai sensi dell'art. 179 del D. Lgs. n. 267/2000, della somma di € 61.872,30 sul Cap. E 201951/0 - PNRR_M1C1 INV 1.5_Cybersecurity_CUP_C36G24000020006_Trasferimeti correnti da Amministrazioni pubbliche - Cdc 012 (Cod. SIOPE 2010101999) da parte di: AGENZIA PER LA CYBERSICUREZZA NAZIONALE (codice: 94350) (tipologia entrata: contributi a rendicontazione) per acquisizione di un servizio SOC per la prevenzione di attacchi cyber nell'ambito del progetto pnrr, missione 1, componente 1, investimento 1.5 "cybersecurity" m1c1i1.5. denominato cyber_in_bo (id: 24_wp9_a8_città metropolitana di bologna) cup c36g24000020006. CIG: B6F6C7A62E;
- c) l'Impegno ai sensi dell'art. 191 del D. Lgs. n. 267/2000, della somma di € 61.872,30 (di cui euro 50.715,00 netti più iva al 22% pari ad euro 11.157,3) sul Cap. S 102307/0 - PNRR_M1C1 INV 1.5_Cybersecurity_CUP_C36G24000020006_Servizi informatici e di telecomunicazioni - Cdc 012 (Cod. SIOPE 1030219001) in favore di ENGINEERING D. HUB S.P.A. (codice: 93146) per fornitura di un servizio SOC per la protezione Cyber nell'ambito del progetto PNRR, missione 1, componente 1, investimento 1.5 "Cybersecurity" MLCLI 1.5. denominato Cyber_in_Bo (id: 24_wp9_a8_Città Metropolitana di Bologna). CIG: B6F6C7A62E;
- d) che alla stipula del contratto si provvederà secondo quanto previsto dall'art. 18, comma 1 del Codice, mediante l'utilizzo della piattaforma Intercent-ER, tramite ordinativo di fornitura (num. Registro PI223921-25) con adesione alla convenzione Intercent-ER denominata SERVIZI DI IT SYSTEM MANAGEMENT 2 – LOTTO 1;
- e) di provvedere al pagamento della somma di cui sopra, subordinatamente al corretto adempimento delle fasi contabili successive alla presente determinazione.

2) **Dà atto:**

- a) del rispetto delle misure di prevenzione della corruzione indicate all'interno della sezione "Rischi corruttivi e trasparenza" del PIAO 2025-2027 e in particolare nel documento

“Dettaglio dei rischi e delle misure correlate, responsabile, tempistica e report facenti capo al rischio n. B.

- b) che il RUP del presente provvedimento è il sottoscritto in qualità di Dirigente del Settore Innovazione digitale, comunicazione, patrimonio e provveditorato, che dichiara l'assenza di conflitti di interessi nel merito;
- c) che in relazione alla fornitura in oggetto non è stato predisposto il documento unico di valutazione dei rischi da interferenza (DUVRI) ai sensi dell'art. 26, comma 3 del D.Lgs. n. 81/2008, in quanto non si ravvedono rischi da interferenza e, pertanto, i costi relativi alla sicurezza sono pari a zero.
- d) del rispetto del principio di rotazione di cui all'art. 49 del D.lgs. 36/2023;
- e) che per la verifica della regolarità contributiva e del possesso dei requisiti di ordine generale, Intercent-ER ha già provveduto ad effettuare i relativi controlli in materia, sia al momento dell'aggiudicazione della gara dalla stessa esperita, sia in sede di stipula della convenzione;
- f) che il RUP ha provveduto a tutti gli adempimenti in materia di comunicazioni e trasparenza di cui agli artt. 20 e 23 del Dlgs n.36/2023.

MOTIVAZIONE

L'Agenzia per la Cybersicurezza Nazionale (di seguito anche "ACN" o "Agenzia") è Soggetto Attuatore dell'Investimento 1.5, Missione 1, Componente 1 del PNRR come individuata dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri (DTD) – Amministrazione Centrale Titolare – con nota prot. DTD n. 2982 del 22 ottobre 2021 e successivo Accordo tra le citate Amministrazioni del 14 dicembre 2021, registrato dalla Corte dei conti il 18 gennaio 2022 al n. 95, e ss.mm.ii.

Nell'ambito del Piano Operativo per l'attuazione del citato investimento, e ai fini del raggiungimento di milestone e target (M&T) assegnati, l'ACN ha previsto la selezione di progetti a titolarità di altri soggetti sub-attuatori, tra i quali la Città Metropolitana di Bologna.

All'interno del progetto presentato dalla Città Metropolitana di Bologna sono state definite delle aree di intervento e le relative attività necessarie a migliorare la postura di sicurezza dell'Ente.

Obiettivo di questo intervento è dare risposta all'esigenza dell'Ente di attivare un servizio SOC per la protezione da attacchi Cyber e di acquisire servizi sistemistici necessari per la continuità delle attività per la gestione e lo sviluppo in sicurezza delle infrastrutture tecnologiche on-site. Sono pertanto richiesti i servizi operativi ed evolutivi al fine di garantire la protezione Cyber, la gestione, la manutenzione e lo sviluppo delle architetture informatiche, oltre che il supporto specialistico per la gestione delle infrastrutture hardware e software di base, utilizzati dall'Amministrazione.

La soluzione richiesta è un servizio di assistenza sistemistica e SOC, operativo 7X24 che, avvalendosi anche di prodotti dotati di tecnologie con intelligenza artificiale, siano in grado di prevenire attacchi informatici e, se necessario, intervenire a difesa della rete cliente. I servizi di Managed Detection and Response (MDR) disponibili saranno d'ausilio al fine della segnalazione di attacchi ed eventi sospetti.

Il servizio di assistenza sistemistica e SOC sarà strutturato nell'analisi dei seguenti perimetri:

- Network
- Mail
- Server
- Endpoint
- Dati e applicazioni On-premise ed in cloud

Il sistemista si avvarrà di servizi di Managed Detection and Response (MDR) per:

- intercettare e confermare proattivamente la presenza di eventuali minacce ed incidenti;
- determinare il raggio di azione delle minacce;
- avviare azioni volte a fermare, contenere e neutralizzare le minacce;
- supportare il personale tecnico dell'Ente nella scelta di soluzioni tecniche finalizzate alla risoluzione definitiva dei problemi di sicurezza.

Il servizio di assistenza è rivolto alla manutenzione preventiva, adattativa e correttiva di una infrastruttura di rete di base composta da: server fisici e virtualizzati in ambiente VMware, Microsoft e Commvault, Citrix e Sophos. Il servizio comprende una serie di interventi, atti a monitorare le condizioni di buon funzionamento della infrastruttura inserita in manutenzione. Tali controlli saranno mirati al monitoraggio dei Servizi fondamentali in carico ad ogni Server. La soluzione di network e management, che sarà implementata come prerequisito alla erogazione del servizio di assistenza proposto, è una applicazione basata su Web, completa e integrata ed installata presso il datacenter del cliente. L'applicazione che sarà fornita è costituita da una suite di moduli complementari che permettono di automatizzare le seguenti funzionalità:

- Network Monitoring/Alerts Modulo che fornisce servizi di monitoraggio proattivo di server o di workstation con notifica immediata di problemi o variazioni. Sfruttando questo modulo i servizi offerti dalla azienda permettono di effettuare un monitoraggio proattivo della rete del Cliente con notifica immediata di problemi o variazioni. Un alert di sistema segnala la disattivazione dei server critici, un'alterazione della configurazione da parte degli utenti oppure una possibile minaccia alla sicurezza;
- Event Monitoring/Alerts Modulo per monitorare i sistemi. Sfruttando questo modulo i servizi offerti dalla azienda effettuano un monitoraggio proattivo degli event log.

Per la fornitura di questi servizi si utilizzerà la Convenzione Intercent-ER denominata SERVIZI DI IT SYSTEM MANAGEMENT 2 – LOTTO 1, il cui aggiudicatario è il Raggruppamento Temporaneo di Imprese (RTI) composto dalle società Engineering D.Hub, Engineering Ingegneria Informatica, TIM, S3K, Laboratori Guglielmo Marconi e DGS, in quanto è in grado di fornire una soluzione che soddisfa alle richieste descritte. Inoltre, l'ordinamento 8 stabilisce che le amministrazioni pubbliche siano tenute ad approvvigionarsi di beni e servizi utilizzando gli strumenti di acquisto messi a disposizione da Consip S.p.A. o dalle centrali di committenza regionali costituite ai sensi dell'articolo 1, comma 455, della legge 27 dicembre 2006, n. 296, per gli acquisti di beni e servizi per la pubblica amministrazione. Con la presente, pertanto, si determina l'adesione alla Convenzione in oggetto e contestualmente si dà corso alle procedure per la formalizzazione dell'adesione per la fornitura dei servizi descritti.

Si procede, pertanto, all'affidamento del servizio in oggetto il cui onere finanziario, indicato nel dispositivo del presente provvedimento, trova copertura finanziaria sul Cap. 122307 - PNRR_M1C1 INV 1.5_Cybersecurity_CUP_C36G24000020006_Servizi Informatici e di Telecomunicazione - Cdc 012 del Bilancio di Previsione 2025/2027, annualità 2025.

L'aggiudicatario dovrà assumere gli obblighi di tracciabilità dei flussi finanziari previsti dall'art. 3 della legge 13/8/2010, n. 136 e successive modifiche, ed in particolare dovrà utilizzare uno o più conti correnti, accessi presso banche o presso la società Poste italiane Spa, dedicati alla commessa di cui si tratta, effettuando tutti i movimenti finanziari relativi all'appalto su detti conti correnti mediante bonifico bancario o postale (o mediante strumenti di pagamento diversi dal bonifico bancario o postale, purché idonei ad assicurare la piena tracciabilità), riportanti, per la specifica procedura i codici identificativi gara.

Per quanto riguarda i termini di fatturazione, si rimanda al testo della convenzione Intercent-ER denominata SERVIZI DI IT SYSTEM MANAGEMENT 2 - LOTTO 1- CIG 97219284C8.

Avverso il presente provvedimento è esperibile ricorso al TAR di Bologna nel termine di 30 gg. decorrente dalla data di notifica o comunicazione dell'atto o dalla piena conoscenza di esso.

Il presente atto è adottato in conformità all'art. 107 del D.Lgs. n° 267/2000 “Testo unico delle leggi sull'ordinamento degli enti locali” all'art. 23 del vigente regolamento di organizzazione degli uffici e dei servizi.

L'imputazione del presente impegno avviene nell'esercizio 2025 in cui è prevista la scadenza dell'obbligazione, ai sensi del D. Lgs. n. 118/2011 - Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli Enti Locali e dei loro organismi, a norma degli artt. 1 e 2 della Legge n. 42/2009 integrata dal D. Lgs n. 126/2014.

Si richiamano:

- la delibera del Consiglio metropolitano n. 66 della seduta del 23/12/2024 - Approvazione del Bilancio di Previsione 2025-2027 e dei relativi allegati;
- l'atto del Sindaco metropolitano n. 294 del 23/12/2024 - Approvazione del Piano Esecutivo di Gestione per il triennio 2025-2027.

Bologna, 29/05/2025

Firmato digitalmente
Dott. BOCCOLA FABRIZIO²

² Documento prodotto e conservato in originale informatico e firmato digitalmente ai sensi dell'art. 20 del 'Codice dell'Amministrazione Digitale' nella data risultante dai dati della sottoscrizione digitale. L'eventuale stampa del documento costituisce copia analogica sottoscritta con firma a mezzo stampa predisposta secondo l'articolo 3 del D.lgs 12 febbraio 1993, n. 39 e l'articolo 3bis, comma 4bis del Codice dell'amministrazione digitale.