DETERMINAZIONE DEL DIRETTORE GENRALE

N. DG/209/2025 del registro delle determinazioni

OGGETTO: Adesione all'Accordo Quadro CONSIP "Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni ID2296 – Lotto 1" per la realizzazione di un Security Operations Center (SOC) Regionale.

Il giorno 22 (ventidue) del mese di settembre 2025, nella sede degli uffici di InnovaPuglia S.p.A. (nel seguito InnovaPuglia) sita in Valenzano (BA) alla Str. Prov. Casamassima Km 3,

il Direttore Generale

Visti

- il D. Lgs. n. 36/2023;
- il D. Lgs. n. 50/2016 (nel seguito Codice);
- la Legge 24 Dicembre 2006 n.296 (Finanziaria 2007);
- la Legge n.90 del 28 Giugno 2024 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici";
- il Decreto Legislativo n.138 del 4 settembre 2024 "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;
- le linee guida, emanate dall'Agenzia per la Cybersicurezza Nazionale;
- il D. Lgs. 7 marzo 2005 n.82 e smi Codice Amministrazione digitale;
- l'art. 226, co. 2, lett. a), del d.lgs. n. 36/2023 il quale dispone che a decorrere dal 1° luglio 2023 le disposizioni di cui al d.lgs. n. 50/2016 continuano ad applicarsi esclusivamente ai procedimenti in corso, intendendo per tali: le procedure e i contratti per i quali i bandi o avvisi con cui si indice la procedura di scelta del contraente siano stati pubblicati prima della data in cui il codice acquista efficacia;
- l'esito della seduta del Consiglio di amministrazione del 19/09/2025, di cui al verbale n. 35, con il quale si approva il progetto di acquisto in argomento e si autorizza l'emissione dell'ordinativo d'acquisto diretto attraverso adesione all'Accordo Quadro CONSIP Lotto 1 ID 2296, nominando all'uopo RUP della procedura l'Ing. Massimiliano Serafino e delegando il Direttore Generale all'adozione dei provvedimenti conseguenti.

Premesso che:

- la Legge n.90 del 28 Giugno 2024 "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*" impone all'articolo 8, ai soggetti indicati, tra i quali le società in house che forniscono servizi informatici e le aziende sanitarie locali, di provvedere:

  a) allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;

  b) alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;

  c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;

  d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;

  e) alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d);

  f) alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la Cybersicurezza Nazionale;

  g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza;

- il Decreto Legislativo n.138 del 4 settembre 2024 "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*" definisce l'ambito di applicazione del decreto, individuando nell'Allegato III e IV le categorie di pubbliche amministrazioni, ed in particolare, nel nostro ambito di interesse, "*le Regioni e le Province autonome, le Aziende sanitarie locali, gli Enti e le Istituzioni di ricerca, le Società in house, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175*", soggette al decreto e agli obblighi della direttiva NIS (*Network Information Security*) riguardo l'attuazione di misure nel campo della cybersecurity;
- le linee guida, emanate dall'Agenzia per la Cybersicurezza Nazionale, indirizzano i soggetti individuati dall'articolo 1, comma 1, della legge 28 giugno 2024, n. 90 verso il rafforzamento della propria resilienza in coerenza con quanto disposto dall'articolo 8 della legge, individuano le misure di sicurezza da adottare per il rafforzamento della resilienza, supportano ed indirizzano i soggetti nella implementazione delle misure di sicurezza mediante la definizione di modalità di implementazione raccomandate;
- con la D.G.R. 16 maggio 2023, n. 663 la Giunta Regionale ha indicato come vincolante l'indirizzo all'utilizzo del Data Center di Regione Puglia presso InnovaPuglia S.p.A per tutti i servizi regionali, di qualsiasi tipologia e ambito, compresi tutti i servizi dei Data Center delle Aziende Sanitarie Locali, delle Aziende Ospedaliere e degli IRCCS pubblici della Regione Puglia;
- la determinazione n. 164179 del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale (ACN) stabilisce le modalità e le specifiche di base per l'adempimento degli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto legislativo 4 settembre 2024, n.138;
- con la D.G.R del 16 dicembre 2024, n. 1793 la Giunta Regionale ha deliberato di affidare al Responsabile della Transizione al Digitale di Regione Puglia, in coerenza con la complessiva strategia regionale sull'ICT, il coordinamento, la governance e la definizione di tutti gli indirizzi strategici in ambito di cybersecurity;

- la Regione Puglia ha avviato da tempo un processo di trasformazione digitale investendo contestualmente nella cybersecurity, riconoscendone il valore determinante al fine di rilanciare competitività e produttività della Regione e per il raggiungimento dei propri obiettivi nell'ambito del percorso verso l'innovazione e la trasformazione digitale, riconoscendone il valore determinante al fine di rilanciare competitività e produttività della Regione e per il raggiungimento dei propri obiettivi nell'ambito del percorso verso l'innovazione e la trasformazione digitale;
- in tale contesto, il rafforzamento delle capacità cyber del sistema regionale è, inoltre, una priorità per la Regione Puglia quale strumento decisivo per rispondere efficacemente alle crescenti sfide nel mondo digitale e dare esecuzione, al contempo, alle strategie nazionali ed europee;
- l'intervento indicato prevede la realizzazione di un Piano Strategico della Cybersecurity, finalizzato alla definizione delle linee di indirizzo regionali in ambito cybersecurity, e ad individuare una serie di iniziative, da attuare nel medio-lungo termine, per rafforzare in modo significativo le capacità della Regione e degli Enti coinvolti, contribuendo così a garantire un ambiente digitale più sicuro e resiliente.

Considerato che:

- con atto dirigenziale N. 00007 del 07/12/2023 del Registro delle Determinazioni della AOO 202, Codice CIFRA: Codice CIFRA: 202/DIR/2023/00009, Il Dirigente del Servizio Tecnico e Transizione Digitale ha approvato il "Piano di Potenziamento della Cybersecurity della Regione Puglia" ed ha affidato ad InnovaPuglia S.p.A. l'esecuzione delle attività afferenti al Piano (cod. progetto RP2405), nel rispetto degli obiettivi generali di ciascuno e degli obiettivi realizzativi;
- la Direzione Generale di InnovaPuglia S.p.A. ha inviato via PEC al Dirigente del Servizio Tecnico e Transizione Digitale con protocollo in uscita numero: inpu/AOO_1/PROT/27/03/2024/0002415 la comunicazione di presa in carico del Piano di Potenziamento della Cybersecurity della Regione Puglia;
- in data 10/07/2024 con numero di protocollo inpu/AOO_1/PROT/10/07/2024/0005099 è stata inviata una richiesta di rimodulazione del Quadro Economico del "Piano di Potenziamento della Cybersecurity della Regione Puglia" al Responsabile della Transizione Digitale della Regione Puglia;
- in data 05/12/2024 con numero di protocollo n: inpu/AOO_1/PROT/05/12/2024/0008518 del 05/12/2024 è stata approvata la richiesta di rimodulazione del Quadro Economico del "Piano di Potenziamento della Cybersecurity della Regione Puglia";
- la legislazione vigente (legge n.90/2024, Decreto Legislativo n. 134 del 4 settembre 2024) in ambito cybersecurity pone obblighi in carico alla Pubblica Amministrazione riguardanti l'innalzamento della postura di sicurezza al fine di garantire la resilienza dei sistemi ed in particolare i requisiti di integrità, confidenzialità e disponibilità dei dati, mediante anche la definizione di politiche e processi e la implementazione di sistemi di difesa dagli attacchi cibernetici;
- il Piano Strategico di Cybersecurity intende:

  - potenziare e ottimizzare le capacità di monitoraggio continuo e rilevazione degli eventi di sicurezza;
  - migliorare i processi e i meccanismi di risposta e contenimento degli incidenti di sicurezza;
  - assicurare una gestione efficace delle crisi e salvaguardare la continuità dei processi a supporto dei servizi erogati;
  - incrementare la visibilità sugli asset, identificando e prioritizzando quelli critici secondo una logica risk-based e garantirne una corretta gestione e protezione;
  - assicurare che minacce, rischi e vulnerabilità siano tempestivamente identificati, valutati e mitigati su base continuativa;

- adottare soluzioni che consentano la protezione della rete da accessi non autorizzati verso tutti quei dispositivi non gestiti direttamente (ad esempio, i laptop personali di utenti che lavorano da remoto o di personale sanitario/farmaceutico che opera sui sistemi software regionali);
- creare un Cybersecurity Defense Center unico regionale, nel quale confluiranno le attuali funzioni del CSIRT e del SOC, con l'obiettivo di creare una struttura in grado di erogare molteplici servizi di sicurezza verso gli enti regionali, con particolare riferimento ai servizi di monitoraggio continuo, rilevazione e risposta agli eventi/incidenti di sicurezza;
- ampliare e consolidare le competenze individuali in ambito cybersecurity per le figure professionali della sicurezza informatica;
- aumentare la consapevolezza del personale sui rischi cyber, promuovendo l'adozione di buone pratiche per contrastare le minacce cyber;

- in considerazione del panorama delle minacce emergenti e dei più recenti attacchi informatici rivolti alla Pubblica Amministrazione, si rende necessario adottare un rinnovato approccio alla cybersecurity, capace di rafforzare il coordinamento e l'armonizzazione nella gestione delle tematiche di sicurezza e di potenziare la postura complessiva del sistema regionale. In quest'ottica la creazione di SOC regionale rappresenta lo strumento centrale per garantire monitoraggio, rilevamento, analisi e risposta agli incidenti di sicurezza informatica in un ambito territoriale complesso e distribuito;
- il SOC regionale svolge la funzione tecnica e di monitoraggio continuo h24, supportata da piattaforme per la raccolta, correlazione e analisi centralizzata dei log di sicurezza, sistemi di rilevamento della rete, strumenti di analisi forense e tecniche di individuazione basate anche su intelligenza artificiale;
- il SOC regionale ha molteplici vantaggi: concentra risorse e competenze, ottimizzando costi e tempi mediante l'utilizzo di tecnologie già implementate ed in uso; promuove la condivisione di informazioni di threat intelligence tra amministrazioni e organismi strategici; migliora la capacità di prevenzione e risposta coordinata; supporta la conformità normativa (NIS2, GDPR, disposizioni nazionali) e contribuisce a garantire la continuità operativa anche in caso di incidenti;
- alla luce di quanto su esposto si rende quindi necessaria la implementazione e la conduzione operativa di un SOC regionale, che si integri con il Computer Security Incident Response Team (CSIRT) della Regione Puglia, ovvero di una struttura centralizzata in grado di monitorare, rilevare, analizzare e gestire eventi di sicurezza al fine della prevenzione di incidenti informatici per la protezione degli Enti della Pubblica Amministrazione Regionale, del Data Center Regionale e della Regione Puglia;

Rilevato che:

- è necessario procedere alla acquisizione di servizi per il raggiungimento degli obiettivi indicati e per il rispetto degli obblighi normativi a carico della Pubblica Amministrazione;
- si è proceduto alla preliminare verifica di ricorrere alle Convenzioni/Accordi Quadro/Contratti Quadro Consip e agli strumenti del portale del MePA, all'esito della quale è stato individuato l'Accordo Quadro (AQ) definito ai sensi del D.lgs. 50/2016 e ss.mm e ii., per l'affidamento di Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni - Lotto 1 (ID 2296), CIG 88846293CA;
- si può ricorrere, per l'acquisizione dei servizi necessari, al succitato Accordo Quadro (AQ) che risulta particolarmente idoneo alle esigenze operative di cui sopra.

Atteso altresì che:

- aggiudicatario dell'Accordo Quadro CONSIP "Servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni Lotto 1 – Servizi di sicurezza da remoto" è il RTI

costituito da Accenture S.p.A., Fincantieri Nextech S.p.A., Fasteweb S.p.A., Deas, Difesa e Analisi Sistemi S.p.A.;

- l'art. 54, comma 3, del Codice prevede che nell'ambito di un Accordo Quadro concluso con un solo operatore economico, gli appalti sono aggiudicati entro i limiti delle condizioni fissate nell'accordo quadro stesso.

Rilevato che:

- la disciplina dell'Accordo Quadro prevede che l'adesione di ciascuna Amministrazione al Lotto di interesse avvenga a condizioni tutte fissate secondo i termini e le condizioni dell'Accordo medesimo con l'unico operatore aggiudicatario, attraverso l'inoltro di un Ordine Diretto di Acquisto (OdA);
- in particolare, l'adesione deve avvenire in base al seguente iter:

  ➢ l'Amministrazione interessata trasmette all'operatore selezionato, il proprio "Piano dei fabbisogni" in cui espone le proprie esigenze e gli obiettivi che intende conseguire;
  ➢ l'operatore riscontra la richiesta dell'Amministrazione trasmettendo il "Piano operativo" in cui espone la propria soluzione tecnica rispetto al fabbisogno rappresentato;
  ➢ l'Amministrazione procede alla valutazione del "Piano operativo", in esito alla quale potrà procedere alla relativa accettazione, al rifiuto o alla richiesta di modifica;
  ➢ ove accetti il Piano operativo, l'Amministrazione procede alla stipula del Contratto esecutivo.

Dato atto che:

- l'oggetto della presente acquisizione è l'affidamento dei seguenti servizi:

  - *L1.S1 – Security Operation Center;*
  - *L1.S7 – Protezione degli endpoint;*
  - *L1.S15 – Servizi Specialistici.*

  per la realizzazione delle seguenti attività:

  - Servizio 24x7 di monitoraggio e alerting degli eventi/minacce di sicurezza;
  - Gestione della piattaforma SIEM;
  - Supporto alla gestione degli incidenti di sicurezza;
  - Protezione dei dispositivi;
  - Servizi avanzati effettuati da personale specializzato per la realizzazione e conduzione operativa 24x7 del SOC regionale.

  L'obiettivo finale di questo intervento consiste nell'assicurare un presidio costante e continuativo, attivo 24 ore su 24 e 7 giorni su 7, volto al controllo, al monitoraggio, alla gestione proattiva, alla gestione e risoluzione di eventi di sicurezza e/o di incidenti dell'intero perimetro tecnologico di riferimento, al fine di garantire la massima sicurezza, affidabilità e continuità operativa dei servizi digitali regionali.

  Il perimetro tecnologico di applicazione dei servizi indicati in precedenza è costituito dai seguenti membri della Constituency Regionali (Agenzie, Società in house, Enti Sanitari e Consiglio Regionale): InnovaPuglia S.p.A - Data Center Regionale; Regione Puglia; ASL Bari; ASL BAT; ASL Taranto; ASL Lecce; ASL Brindisi; ASL Foggia; Policlinico di Bari; Policlinico Riuniti di Foggia; IRCCS "De Bellis" di Castellana Grotte (BA); IRCCS "Giovanni Paolo II" di Bari; Consiglio Regionale della Puglia; ADISU Puglia; ARPAL; ARPA Puglia; ARIF Puglia; ARESS; ARTI; Puglia Promozione; ASSET; Puglia Sviluppo.

- è stato redatto il "Piano dei Fabbisogni" che descrive i requisiti dei servizi richiesti ed è stato trasmesso in data 02/09/2025, con protocollo n. inpu/AOO_1/PROT/02/09/2025/0007954, tramite PEC, all'operatore economico sopraindicato;
- in data 15/09/2025 l'operatore economico ha trasmesso il Piano Operativo, acquisito agli atti con prot. n. inpu/AOO_1/PROT/0008711 che, sebbene non allegato, costituisce parte integrante della presente determinazione, contenente la proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro e nei relativi allegati;

Atteso che:

- l'erogazione dei servizi avrà durata 24 mesi per i servizi L1.S1 – Security Operation Center e L1.S7 – Protezione degli Endpoint e 27 mesi per il servizio L1.S15 – Servizi Specialistici;
- l'importo del contratto esecutivo è pari ad € 5.200.182,00 (Cinquemilioniduecentomilacentottantadue/00 Euro) IVA esclusa;
- trattandosi di servizi di natura intellettuale, con attività accessorie inferiori alle 5 giornate persona presso la/le sede/i di esecuzione della fornitura, sono pari a zero e non vi è pertanto l'obbligo di predisporre i documenti di cui all'art. 26, commi 3, 3 bis e 3 ter del d.lgs. n. 81/2008;
- come previsto dall'art. 29 del Accordo Quadro, ai sensi dell'art. 4, comma 3-quater, del D.L. 6 luglio 2012, n. 95, convertito con modificazioni in legge 7 agosto 2012, n. 135, si applica il contributo di cui all'art. 18, comma 3, D.Lgs. 177/2009, come disciplinato dal D.P.C.M. 23 giugno 2010 che le Amministrazioni Beneficiarie sono tenute a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla data di perfezionamento del Contratto esecutivo;
- il predetto contributo nella misura prevista dall'art. 2, lettera b) "Contributo dovuto con riferimento ad accordi o contratti quadro" del Dpcm 23 giugno 2010 (5 per mille del valore del contratto esecutivo sottoscritto se superiore ad € 1.000.000,00) è pari ad € 26.000,91 (Ventiseimila/91 Euro);
- l'importo complessivo dell'acquisizione in oggetto è pertanto pari ad € **5.226.182,91 (Cinquemilioniduecentoventiseimilacentottantadue/91 euro)** dei quali € 26.000,91 (Ventiseimila/91 Euro) come contributo Consip;
- la copertura dei costi di acquisizione è prevista dalla voce "*Attività commissionate all'esterno*" del Quadro Economico del Piano di Potenziamento della Cybersecurity della Regione Puglia" (CUP: B31C23000820006 – Codice: RP2405_OR1).
- le fatturazioni per le prestazioni oggetto del contratto esecutivo avverranno con cadenza bimestrale sulla base dei prezzi unitari stabiliti nell'Allegato "C" all'Accordo Quadro Consip "Corrispettivi e Tariffe".

Visti pertanto:

- il Piano Operativo, trasmesso tramite PEC in data 15 settembre 2025 e acquisito agli atti con prot. prot. n. inpu/AOO_1/PROT/0008711 nella medesima data;
- lo Schema di Contratto che, ancorché non allegato, è parte integrante della presente determinazione

Preso atto:

- che il CIG originale dell'Accordo Quadro è 88846293CA e che, attraverso la Piattaforma Contratti Pubblici (PCP) di ANAC è stato assegnato alla presente procedura il CIG derivato B8524F5D81;

- del chiarimento giuridico del Servizio Supporto Giuridico del MIT n. 2507 del 17/04/2024 in merito ai contratti attuativi stipulati dopo il 01 luglio 2023 a valere su un Accordo Quadro disciplinato dal d.lgs. n. 50/2016

Visti gli atti contenenti l'istruttoria;

Visti i pareri di regolarità procedurale, contabile e amministrativa

Tutto ciò ***premesso, considerato e ritenuto,***

DETERMINA

1. **di aderire** all'Accordo Quadro CONSIP "Servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni ID2296 – Lotto1" per la realizzazione di un Security Operations Center (SOC) Regionale, stipulato ai sensi dell'art. art. 54, comma 3, del D.lgs. n. 50/2016 da Consip S.p.A. con il RTI aggiudicatario composto Accenture S.p.A., Fincantieri Nextech S.p.A., Fasteweb S.p.A., Deas, Difesa e Analisi Sistemi S.p.A., attraverso la stipula di un contratto esecutivo per un importo pari a **€ 5.200.182,00 (Cinquemilioniduecentomilacentottantadue/00 Euro)** IVA esclusa e contributo a Consip pari ad € 26.000,91 (Ventiseimila/91 Euro);
2. **di approvare** il Piano Operativo, trasmesso tramite PEC in data 15 settembre 2025 e acquisito agli atti con prot. prot. n. inpu/AOO_1/PROT/0008711 nella medesima;
3. **di approvare** lo schema di contratto, parte integrante della presente determinazione, per l'affidamento del servizio in oggetto;
4. **di prendere atto** che InnovaPuglia, secondo le regole definite per l'AQ cui si intende aderire, è tenuta a versare a Consip S.p.A., entro il termine di trenta giorni solari dalla data di perfezionamento del Contratto Esecutivo, un contributo pari a € 26.000,91 nel rispetto di quanto previsto dall'art. 2, lettera b), del D.P.C.M. 23 giugno 2010;
5. **di dare atto** che la copertura dei costi di acquisizione è prevista dalla voce "Attività commissionate all'esterno" del Quadro Economico del Piano di Potenziamento della Cybersecurity della Regione Puglia" (CUP: B31C23000820006 – Codice: RP2405_OR1);
6. **di dare atto** che è stato nominato Responsabile Unico del Procedimento, ai sensi dell'articolo 31 del D.lgs. 50/2016 l'Ing. Massimiliano Serafino

Il presente provvedimento, redatto in un unico originale e composto da n. 7 facciate sarà:

- acquisito agli atti dell'Ufficio della Segreteria di Direzione Generale per la raccolta, la pubblicazione e la notifica agli Uffici competenti per i successivi adempimenti;

- pubblicato nella sezione "Società-Trasparente" del sito di InnovaPuglia S.p.A. nei termini di legge salve le garanzie previste dalla legge 241/1990 e dal D. Lgs. n. 33/2013 s.m.i. e D. Lgs. 50/16 s.m.i. in tema di accesso ai documenti amministrativi, nel rispetto della tutela della riservatezza dei cittadini secondo quanto disposto dal Regolamento UE n. 2016 /679 in materia di protezione dei dati personali, nonché dal d.lgs. 196/2003 e dal D.lgs. n. 101/2018 e ss.mm.ii., ed ai sensi del vigente Modello Organizzativo Operativo sul trattamento dei dati di InnovaPuglia.

Il Direttore Generale
Ing. Francesco Surico

Francesco
Surico
22.09.2025
15:50:46
GMT+01:00