Bur n. 48 del 16/04/2024

(Codice interno: 527480)

DECRETO DEL DIRETTORE DELLA DIREZIONE ICT E AGENDA DIGITALE n. 21 del 11 marzo 2024

Attuazione della D.G.R. n. 1027 del 22/08/2023. Accertamento dell'entrata relativa all'assegnazione statale di risorse del Piano Nazionale di Ripresa e Resilienza (PNRR), Missione 1 Componente 1 Investimento 1.5 "Cybersecurity" M1C1I1.5 di cui alla Determina prot. n. 30697 del 30/11/2023 del Direttore generale dell'agenzia per la cybersicurezza nazionale, recante determina di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse a valere sull'Avviso n. 6/2023, e contestuale copertura dell'obbligazione passiva giuridicamente perfezionata a seguito dell'adesione all'Accordo Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni ai sensi dell'art. ex art. 54, co. 4 lett. a) d.lgs. n. 50/2016, Lotto 1 CIG n. 88846293CA, ID SIGEF 2296, ai fini dell'acquisto di servizi specialistici e di formazione e security awareness al fine di erogare un tutoraggio in tutte le fasi di set-up, implementazione e manutenzione del CERT Regionale e di monitorare l'efficacia della formazione erogata, per la durata di dodici (11) mesi dalla data di conclusione delle attività di presa in carico e non oltre il 31 dicembre 2024. CIG derivato B079874EAF, CUP H19B23000100006, CUI S80007580279202200155.

[Informatica]

Note per la trasparenza:
Con il presente provvedimento, in attuazione della D.G.R. n. 1027 del 22/08/2023, si autorizza l'adesione all'Accordo Quadro per l'affidamento servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni ai sensi dell'art. ex art. 54, co. 4 lett. a) d.lgs. n. 50/2016, Lotto 1 CIG n. 88846293C, CIG derivato B079874EAF, CUP H19B23000100006, mediante sottoscrizione di contratto esecutivo, ai fini dell'acquisto di servizi specialistici e di formazione e security awareness al fine di erogare un tutoraggio in tutte le fasi di set-up, implementazione e manutenzione del CERT Regionale e di monitorare l'efficacia della formazione erogata, in attuazione della Missione 1 Componente 1 Investimento 1.5 "Cybersecurity" M1C1I1.5, di cui alla Determina prot. n. 30697 del 30/11/2023 del Direttore generale dell'agenzia per la cybersicurezza nazionale, per la durata di undici (11) mesi dalla data di conclusione delle attività di presa in carico e non oltre il 31 dicembre 2024, per l'importo complessivo di Euro 1.500.000,00 iva inclusa. Si procede alla copertura dell'obbligazione giuridicamente vincolante e all'assunzione di impegno pluriennale di spesa. L'acquisto dà attuazione alla Programmazione triennale degli acquisti di forniture e servizi 2024/2026, approvata dalla Giunta regionale con Deliberazione n. 82 del 12 febbraio 2024. Codice CUI S80007580279202200155.

Il Direttore

Premesso che

Negli ultimi venti anni, la diffusione delle nuove tecnologie dell'informazione e delle comunicazioni ha progressivamente focalizzato il centro delle attività umane di carattere sociale, politico ed economico all'interno di una nuova dimensione, denominata cibernetica. Lo straordinario aumento dell'utilizzo di internet ha contribuito allo sviluppo del settore ICT, con un notevole impatto su tutte le funzioni della società moderna. Lo spazio cibernetico ha permesso immense opportunità di sviluppo economico, grazie alle quali le economie dei paesi più avanzati hanno subito una forte accelerazione. Tuttavia, l'incremento delle opportunità è stato accompagnato da un parallelo incremento delle vulnerabilità. Infatti, la digitalizzazione dei servizi e delle informazioni ha inevitabilmente accresciuto l'esposizione al rischio: il pericolo di furto, manomissione e compromissione dei dati nello spazio cibernetico ha evidenziato la necessità di mettere in sicurezza le attività in esso condotte. Il crimine informatico costituisce la piaga maggiore della sicurezza delle reti e delle informazioni, a livello di portata e di danni economici. Il costo del cybercrime è in continua crescita, provocando un ingente trasferimento di risorse al di fuori delle economie nazionali. Inoltre, strutture pubbliche che gestiscono quotidianamente dati ed informazioni digitali riguardanti cittadini si trovano a doverne garantire non solo la disponibilità e l'integrità, ma anche la riservatezza. Nel febbraio 2013 l'Unione europea ha adottato la propria strategia di cybersicurezza, invitando tutti gli Stati membri a fare altrettanto. Il Decreto del Presidente del Consiglio dei Ministri (DPCM) del 24 gennaio 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica, ha quindi definito l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche informatizzate. A dicembre 2013, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico ed il relativo Piano nazionale per la protezione cibernetica e la sicurezza informatica hanno stabilito gli indirizzi strategici e quelli operativi per la messa in sicurezza delle attività condotte nel cyber spazio.

In data 02/08/2022 è stato pubblicato l'avviso pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul

PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5.

L'avviso aveva lo scopo di individuare, mediante procedura valutativa selettiva con graduatoria, proposte progettuali finalizzate al potenziamento del livello di maturità delle capacità cyber dei sistemi informativi delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome.

Con Deliberazione n. 1174 del 27/09/2022 la Giunta Regionale, nell'approvare il "Progetto CERT Regionale (Computer Emergency Response Team)" di Regione del Veneto, autorizzava la Direzione ICT e Agenda Digitale a partecipare al suindicato avviso pubblico mediante la presentazione di due proposte di interventi di potenziamento della resilienza cyber di Regione del Veneto.

In data 14/10/2022 la Direzione ICT e Agenda Digitale, in risposta al suindicato Avviso pubblico trasmetteva all'agenzia per la Cybersicurezza Nazionale, con nota prot. n. 0480126 il progetto denominato "Realizzazione sistemi propedeutici per la costituzione del CERT della Regione Veneto" e con nota prot. n. 0480134 il progetto denominato "Assessment della postura Cyber".

Entrambi i progetti sono stati ammessi a finanziamento per un importo di Euro 1.000.000,00 ciascuno.

Con Deliberazione n. 1024 del 22/08/2023, la Giunta Regionale ha approvato il Progetto esecutivo del CERT (Computer Emergency Response Team) Regionale, che sarà organizzato presso la Direzione ICT e Agenda Digitale, individuando nel suo Direttore il Presidente del Comitato Strategico del CERT Regionale.

In data 11/08/2023 è stato pubblicato l'avviso pubblico a sportello n. 6/2023 per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici rivolto a Regioni e alle Province autonome di Trento e Bolzano a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity"M1C1I1.5.

L'Avviso aveva lo scopo di individuare, mediante procedura a sportello, proposte progettuali finalizzate all'attivazione o al potenziamento di Computer Security Incident Response Team (CSIRT), da costituirsi o già costituiti presso le Regioni, deputati alla prevenzione e alla mitigazione del rischio cyber mediante attività di supporto alla gestione delle vulnerabilità, alla condivisione di informazioni e della situational awareness, al monitoraggio del livello di protezione e al rilevamento, analisi e risposta degli incidenti di sicurezza informatica.

I CSIRT Regionali potranno operare, mediante opportuni Accordi di collaborazione, in stretta sinergia con l'Agenzia e con il CSIRT Italia, attraverso la condivisione di metodologie e strumenti per la gestione delle informazioni e degli incidenti di cybersecurity, delle vulnerabilità, delle crisi e degli attacchi informatici ai sistemi informativi delle Regioni.

La dotazione finanziaria dell'Avviso ammonta complessivamente ad Euro 28.000.000,00. L'importo massimo ammissibile a finanziamento è pari ad Euro 1.000.000,00 per progetto. Nell'ipotesi di iniziative progettuali il cui ambito di intervento intercetti l'ambito sanitario e/o di efficientamento energetico e/o di tutela del territorio e delle risorse idriche, è prevista una dotazione premiale aggiuntiva di Euro 500.000,00.

In tali casi, l'importo massimo ammissibile a finanziamento è pari ad Euro 1.500.000,00 per progetto.

Ciascun Soggetto partecipante potrà presentare una sola progettualità.

L'avviso a sportello è stato aperto il giorno 11/08/2023 sino al 25/09/2023 ore 18:00.

In data 15/09/2023, in attuazione della D.G.R. n. 1027 del 22/08/2023, la Direzione ICT e Agenda Digitale, in risposta all'avviso pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PNRR, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity", trasmetteva all'agenzia per la Cybersicurezza Nazionale, con nota prot. n. 0504839 il piano di progetto denominato "Attivazione CERT-CSIRT regionale".

Il suindicato progetto si pone il fine di:

- definire un modello di governance del CSIRT Regionale e un modello operativo attraverso il disegno e la implementazione dei processi core e l'attribuzione chiara di ruoli e responsabilità;
- progettare ed erogare percorsi formativi per l'upskilling del personale che opera per il raggiungimento degli obiettivi del mandato.

Il modello organizzativo del CSIRT di Regione del Veneto sarà organizzato su tre livelli di Governo (strategico, direttivo e operativo) che identificheranno gli attori principali ed i relativi ruoli per lo sviluppo e l'operatività del CSIRT stesso. Tale modello definirà le relazioni tra il CSIRT di Regione del Veneto, gli Enti aderenti, le Istituzioni nazionali (CSIRT Italiano e altri CSIRT di settore) e le istituzioni internazionali.

Il livello strategico fornirà l'indirizzo sulle politiche di conduzione del CSIRT Regionale e costituirà un punto decisionale per l'escalation di incidenti gravi verso le autorità competenti.

Il livello direttivo sarà responsabile di indirizzare la strategia, definendo processi e procedure che garantiscano il raggiungimento degli obiettivi prefissati, avvalendosi di esperti di Cybersecurity ed interloquendo con le istituzioni /organizzazioni nazionali.

Il livello operativo sarà responsabile dell'implementazione e della manutenzione dei processi e delle procedure definite a livello direttivo.

I tre livelli saranno declinati con riferimento al CSIRT Regionale e agli Enti locali aderenti che concorreranno con ruolo attivo alla gestione

Sarà definito il modello operativo con cui il CSIRT effettuerà l'erogazione dei servizi inclusi nel perimetro (i.e. gestione del rischio, business continuity, sensibilizzazione e formazione, SOC/incident management, vulnerability management, threat intelligence, sviluppo sicuro/analisi del codice), attraverso la definizione di tutti i processi coinvolti, l'attribuzione delle responsabilità in una logica RACI, l'identificazione di potenziali strumenti/fonti dati a supporto. I processi saranno strutturati nel rispetto del Ciclo di Deming (PLAN-DO-CHECK-ACT) con l'obiettivo di implementare una strategia di miglioramento continuo attuata attraverso l'esercizio stesso dei processi nel tempo.

Il CSIRT Regionale identificherà poi gli obiettivi formativi e definirà un programma di formazione specifico per gli attori coinvolti nella gestione della sicurezza. In particolare:

- identificherà le necessità - in termini di conoscenze, competenze e abilità - del personale impegnato nel funzionamento del CSIRT, al fine di poter sviluppare percorsi di training appropriati ed in linea con i loro bisogni;
- definirà il format più opportuno per la formazione dei soggetti identificati (online, in aula) e predisporrà il materiale didattico inclusivo di test finali di apprendimento;
- svilupperà un programma di tutoraggio che consenta al personale del CSIRT di apprendere da personale esperto.

In coerenza con le linee guida di ACN sulle figure professionali che compongono il modello organizzativo di un CSIRT a supporto dell'erogazione dei servizi, sono stati identificati a livello macro gli ambiti formativi che si intendono attivare in relazione alle 5 aree di operatività dei profili professionali (Info sec event management, info sec incident management, vulnerability management, situational awareness, knowledge transfer). Si riportano di seguito un elenco non esaustivo dei possibili ambiti formativi da attivare:

- minacce e vulnerabilità informatiche
- fasi di un attacco informatico
- tecniche e procedure di attacco
- identificazione e classificazione incidenti
- risposta e gestione degli incidenti
- tecnologie di protezione e rilevamento delle intrusioni

vettori di attacco informatico

- tecniche di Social Engineering
- identificazione intrusioni su host e reti
- Vulnerability Assessment & Penetration Test
- gestione del rischio

Saranno, inoltre, progettati ed erogati interventi formativi specifici relativi alla gestione della crisi come:

- gestione e mitigazione del rischio
- processi decisionali e di escalation
- comunicazioni interne ed esterne in caso di incidenti

attraverso format che consentano di rendere quanto più efficace l'apprendimento e favorire l'interazione con i soggetti coinvolti (es. esercizi di simulazione di incidenti).

Il progetto prevede per il settore sanitario le medesime attività e i medesimi approcci descritti ai punti precedenti.

Il modello di governance e operativo precedentemente illustrato sarà applicato anche agli Enti Sanitari che saranno assegnati al cluster con massima criticità. Pertanto, anche il personale tecnico locale sarà fortemente coinvolto nelle attività di gestione della sicurezza e le figure del top management parteciperanno a livello direttivo e strategico al funzionamento/potenziamento del CSIRT. Nell'ambito del percorso formativo che sarà progettato ed erogato per il personale impegnato nel funzionamento del CSIRT (descritto ai punti precedenti nel dettaglio) saranno previsti interventi specifici per accrescere la conoscenza / competenza sugli aspetti cyber peculiari del mondo health (es. discovery degli asset medicali connessi in rete, analisi e monitoraggio del rischio con particolare riferimento alle principali minacce cyber a cui il settore health è esposto, nuovi vettori di attacco per le tecnologie IoMT).

Dato atto che:

- l'esigenza sopra citata è emersa dalle verifiche tecniche interne effettuate dal titolare della P.O. Convergenza e Modelli Architetturali per i sistemi ICT; tale esigenza è stata quindi rappresentata al Direttore della U.O. Sistemi Informativi, servizi e tecnologie digitali, che l'ha riferita al Direttore della Direzione;
- il Responsabile del Procedimento, ai sensi dell'art. 5 della Legge n. 241 del 1990, è il Direttore della Direzione ICT e Agenda Digitale, dott. Idelfo Borgo.

Atteso che:

- Con Determina n. 30697 del 30/11/2023, recante concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse a valere sull'Avviso n. 6/2023, il Direttore generale dell'agenzia per la cybersicurezza nazionale ha rifinanziato con ulteriori euro 490.306,51 (quattrocento novanta mila trecento sei/51) la dotazione finanziaria iniziale complessiva dell'Avviso 06/2023, di cui alla determina ACN prot. n. 21472 dell'8 agosto 2023, al fine dello scorrimento della graduatoria dei progetti ammissibili ma parzialmente finanziabili per esaurimento delle risorse disponibili, coerentemente con la previsione di cui al par. 4.3 "L'importo massimo ammissibile a finanziamento è pari a 1.000.000,00 € per progetto. Nell'ipotesi di iniziative progettuali il cui ambito di intervento intercetti l'ambito sanitario e/o di efficientamento energetico e/o di tutela del territorio e delle risorse idriche, è prevista una dotazione premiale aggiuntiva di 500.000,00 €. In tali casi, l'importo massimo ammissibile a finanziamento è pari a 1.500.000,00 € per progetto"; ha quindi approvato la graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziate a valere sull'Avviso 6/2023 "a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici" PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5". A Regione del Veneto per il progetto "Attivazione CERT-CSIRT regionale" è riconosciuto un contributo pari ad Euro 1.500.000,00 iva inclusa; CUP H19B23000100006. Il finanziamento è stato comunicato con nota agli atti al prot. n. 647495 in data 05/12/2023.
- Con nota in data 29/12/2023, prot. n. 0688927 l'amministrazione regionale trasmetteva all'Agenzia per la cybersicurezza nazionale l'atto d'obbligo, ai sensi di quanto previsto dal paragrafo 7.2 dell'Avviso M1C1I1.5.
- L'avviso ha ad oggetto la selezione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici. Nell'ipotesi di proposta di un intervento da realizzare ex novo, il Soggetto attuatore dell'intervento dovrà avviare le attività connesse al progetto ammesso a finanziamento entro 10 giorni lavorativi a partire dalla data di trasmissione dell'Atto d'obbligo da parte del Soggetto attuatore dell'intervento all'Agenzia, ferma restando la possibilità di avvio anticipato nel rispetto del cronoprogramma approvato. Nel caso in cui il progetto presentato preveda lo svolgimento di una o più delle attività di cui ai punti 1), 2) e 3) del paragrafo 4.1, pena la revoca del contributo e il recupero da parte dell'Agenzia delle somme eventualmente anticipate, i progetti ammessi a finanziamento dovranno concludersi entro il 31 dicembre 2024. Nel caso in cui il progetto presentato preveda anche lo svolgimento di attività di cui al punto 4) del precedente paragrafo 4.1, limitatamente a quest'ultime, i progetti ammessi a finanziamento potranno concludersi entro e non oltre la data del 31 dicembre 2025.

Considerato che:

- è disponibile dal 26/09/2022 l'Accordo Quadro CIG 88846293CA stipulato in data 04/08/2022, per la durata di 24 mesi, nell'ambito delle iniziative per l'attuazione del Piano Triennale per l'informatica della Pubblica Amministrazione, tra Consip S.p.a., per conto del Ministero dell'Economia e delle Finanze la società Accenture S.p.A., sede legale in Milano, Via Privata Nino Bonnet n. 10, P. IVA 13454210157, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti Fastweb S.p.A. con sede legale in Milano, Piazza Adriano Olivetti n.1, P. IVA 12878470157, Fincantieri NextTech S.p.A., con sede legale in Milano, Via Carlo Ottavio Cornaggia n. 10, P. IVA 00890740111 e DEAS- Difesa e Analisi Sistemi S.p.A., con sede legale in Roma Via della Colonna Antonina n. 46, P. IVA 14961281004, con l'obiettivo di mettere a disposizione

delle Amministrazioni un insieme di servizi di sicurezza - erogati da remoto e in logica continuativa - per la protezione delle infrastrutture, delle applicazioni e dei dati. Tale contratto mette a disposizione i seguenti servizi di sicurezza: Security Operation Center (SOC), Next Generation Firewall, Web Application Firewall, Gestione continua delle vulnerabilita di sicurezza, Threat Intelligence & Vulnerability Data Feed, Protezione navigazione Internet e Posta elettronica, Protezione degli end-point, Certificati SSL, Servizio di Formazione e Security awareness, Gestione dell'identita e l'accesso utente, Firma digitale remota, Sigillo elettronico, Timbro elettronico, Validazione temporale elettronica qualificata, Servizi Specialistici e Indicatori di digitalizzazione.

- tale Contratto Quadro prevede che l'adesione allo stesso delle Pubbliche Amministrazioni avvenga mediante la sottoscrizione di un Contratto esecutivo messo a disposizione da Consip S.p.a.;
- la Direzione ICT e Agenda Digitale ha verificato, a seguito dell'invio del Piano dei Fabbisogni in data 03/01/2024 prot. n. 0003189 e del ricevimento in data 15/02/2024 del Piano Operativo "AQSEC-2296L1-PO", agli atti al prot. agli atti al prot. n. 79950 in data 15/02/2024, la possibilità di acquisto di servizi al fine di erogare un tutoraggio in tutte le fasi di set-up, implementazione e manutenzione del CERT Regionale e di monitorare l'efficacia della formazione erogata. Tale servizio ha lo scopo di fornire:
    - ♦ L1S9 Formazione e Security Awareness: formazione specialistica per i soggetti coinvolti nella gestione della sicurezza, al fine di garantire la conoscenza dei principi di funzionamento e monitoraggio del CERT Regionale e degli aspetti tecnici necessari per l'espletamento dei diversi ruoli. I volumi previsti sono 925 gg/p Team Ottimale.
    - ♦ L1S15 Servizi specialistici: supporto alle attività di governance in tutte le fasi di set-up, implementazione e manutenzione del CERT Regionale. I volumi previsti sono 4.098 gg/p Team Ottimale.

Il servizio "Formazione e Security Awarness" è mirato a sensibilizzare il personale dell'Amministrazione su svariati aspetti sicurezza delle informazioni, incrementando il loro livello di consapevolezza così da innalzare il livello di sicurezza dell'organizzazione stessa e l'efficacia in termini di protezione dei dati aziendali critici e dei dati personali. Lo scopo è quello di sviluppare nel personale le competenze essenziali, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e reagire al meglio a fronte di eventuali problemi.

L'attività di formazione prevede l'erogazione di formazione specialistica per gli attori coinvolti nel raggiungimento degli obiettivi e mandato del CERT Regionale e dei servizi erogati. Tale formazione indirizzerà, tra l'altro, il potenziamento delle competenze cyber del personale tecnico impiegato nel funzionamento del CSIRT, tramite:

- Identificazione delle necessità - in termini di conoscenze, competenze e abilità - del personale tecnico impegnato nel funzionamento del CSIRT, al fine di poter sviluppare percorsi di training appropriati ed in linea con i loro bisogni;
- Definizione del format più opportuno per la formazione dei soggetti identificati (online, in aula) e predisposizione del materiale didattico.
- Sviluppo di un programma di tutoraggio che consenta al personale del CSIRT e ai membri della Constituency di apprendere da personale esperto.

In coerenza con le linee guida di ACN sulle figure professionali che compongono il modello organizzativo di un CSIRT a supporto dell'erogazione dei servizi, sono stati identificati a livello macro gli ambiti formativi che si intendono attivare in relazione alle 5 aree di operatività dei profili professionali: Info sec event management, info sec Incident management, Vulnerability Management, Situational Awareness, knowledge transfer.

Per espletare le attività di formazione, a seguito di una prima fase di definizione del programma e di pianificazione delle singole iniziative, saranno quindi erogate specifiche sessioni di formazione, quali a titolo esemplificativo: sessioni in aula di corsi base relativi alle 5 aree sopra riportate, supporto per il conseguimento di specifiche certificazioni da parte dei principali profili del CSIRT regionale, simulazioni table-top (e.g.: attività a tavolino che simulano gravi incidenti di sicurezza informatica) al fine di verificare le procedure di risposta agli incidenti implementate ed accrescere la consapevolezza del personale incaricato della gestione di tali incidenti.

Il servizio specialistico è volto a supportare l'Amministrazione in tutte le fasi di set-up, implementazione e manutenzione del CERT Regionale.

In particolare, attraverso un'attività di affiancamento, sarà guidato e supervisionato l'operato dell'organizzazione con il fine di definire e attuare un modello di governance del CSIRT Regionale e un modello operativo che indirizzi i processi di funzionamento core e l'attribuzione chiara di ruoli e responsabilità.

Nello specifico nella fase di set-up del CERT Regionale il supporto prevede le seguenti attività:

- Inventory dei processi che sottendono i servizi offerti dal CSIRT,
- Definizione del Catalogo dei servizi,
- Definizione di Processi e Workflows,

- Definizione del Modello organizzativo, delle competenze e dei programmi di formazione in linea con i bisogni,
- Piano di gestione della sicurezza delle informazioni,
- Identificazione ed allestimento ambienti,
- Piano di automazione dei processi e definizione KPI,
- Requisiti di dettaglio per la fase implementativa,
- Piano di cooperazione con altri CERT.

Nella fase di implementazione del CERT Regionale il supporto prevede le seguenti attività:

- Documentazione di processi e procedure di dettaglio,
- Sottoscrizione degli accordi con la constituency ed eventuali partner,
- Piano di comunicazione dedicato per il lancio del CERT,
- Allestimento degli ambienti,
- Implementazione delle tecnologie per l'automazione dei processi,
- Esecuzione dei test dei servizi e fine tuning,
- Costituzione del team CERT,
- Implementazione delle policy e procedure di sicurezza delle informazioni,

Una volta implementato il CERT, sono infine previste le seguenti attività:

- Revisione annuale delle performance del CERT,
- Revisione annuale dei bisogni degli stakeholder,
- Approvazione annuale del budget,
- Raccolta dei requisiti per il miglioramento del CERT,
- Definizione requisiti di dettaglio degli interventi di miglioramento per l'avvio della fase di design,
- Definizione preliminare del budget per gli interventi di miglioramento.

I servizi saranno erogati per una durata di 11 mesi dalla data di conclusione delle attività di presa in carico, che si prevede entro un mese dalla stipula del contratto, per l'importo complessivo massimo di Euro 1.228.868,00 iva esclusa ed in particolare Euro 228.956,00 per il servizio L1S9 (Formazione e Security Awareness) ed Euro 999.912,00 per il servizio L1S15 (Servizi specialistici).

- Così come previsto dall'art. 29 dell'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, al contratto esecutivo si applica il contributo di cui all'art. 18, comma 3, D.Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010. Pertanto, 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 presente Contratto esecutivo, il predetto contributo nella misura prevista dall'art. 2, lettera a) (8 per mille del valore del contratto esecutivo sottoscritto se non superiore ad € 1.000.000,00) o lettera b) (5 per mille del valore del contratto esecutivo sottoscritto se superiore ad € 1.000.000,00), del D.P.C.M. 23 giugno 2010, in ragione del valore complessivo del presente Contratto Esecutivo. I contributi sono considerati fuori campo dell'applicazione dell'IVA, ai sensi dell'art.2, comma 3, lettera a) del D.P.R. del 1972. In caso di specie essendo l'importo del contatto esecutivo pari ad Euro 1.229.508,20 iva esclusa l'ammontare del contributo dovuto a Consip è pari ad Euro 6.147,54.
- Con l'approvazione del Progetto dei Fabbisogni, il Contratto Esecutivo con il Fornitore sarà stipulato sulla base dell'apposito schema di contratto esecutivo disponibile sul sito di Consip.

Verificata la correttezza tecnica ed economica del Piano Operativo "AQSEC-2296L1-PO", agli atti al prot. n. 79950 in data 15/02/2024, trasmesso dal Raggruppamento temporaneo costituito tra le società Accenture S.p.A., mandataria, Fastweb S.p.A., mandante, Fincantieri NextTech S.p.A., mandante e DEAS- Difesa e Analisi Sistemi S.p.A., mandante.

Visto l'art. 1, comma 512 della legge 28 dicembre 2015, n. 208 che stabilisce che "al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, fermi restando gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente, le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 196, provvedono ai propri approvvigionamenti esclusivamente tramite Consip SpA o i soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti".

Ritenuto:

- che l'Accordo Quadro per l'affidamento servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni ai sensi dell'art. ex art. 54, co. 4 lett. a) d.lgs. n. 50/2016, Lotto 1 CIG n. 88846293CA, sia idoneo a

soddisfare le esigenze esposte in premessa e pertanto di ricorrere alla stessa per l'acquisto, per 11 mesi a decorrere dalla data di conclusione delle attività di presa in carico, di servizi di Formazione e Security Awareness e Servizi Specialistici al fine di erogare un tutoraggio in tutte le fasi di set-up, implementazione e manutenzione del CERT Regionale e di monitorare l'efficacia della formazione erogata;
- di autorizzare la sottoscrizione del Contratto esecutivo CIG derivato B079874EAF, CUP H19B23000100006, secondo lo schema messo a disposizione da Consip S.p.a sul portale dedicato all'iniziativa, dando atto che lo stesso sarà sottoscritto dal Direttore della Direzione ICT e Agenda Digitale;
- di nominare, ai sensi dell'art. 101 del D.Lgs n. 50/2016, il Direttore dell'Esecuzione del contratto nel Direttore della U.O. Sistemi Informativi, servizi e tecnologie digitali, ing. Paolo Barichello.

Dato atto che:

- la tipologia della prestazione, servizi intellettuali e di servizi svolti da remoto, senza accesso ai locali regionali, non comporta la presenza di rischi da interferenza nella sua esecuzione tali da richiedere la redazione del Documento Unico Valutazione Rischi Interferenti (DUVRI) di cui al decreto legislativo 9 aprile 2008, n. 81 e che pertanto gli oneri per la sicurezza di natura interferenziale sono pari a zero.
- il contratto esecutivo CIG derivato B079874EAF, CUP H19B23000100006 è stato, in data odierna, sottoscritto dall'amministrazione e trasmesso al fornitore;

Visti:

- il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" che prevede l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (di seguito "ACN" o "Agenzia") e, in particolare, gli articoli 5 e 7;
- l'articolo 7, comma 1, lettere m) e n), del suddetto decreto-legge n. 82/2021 che ha attribuito all'Agenzia tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale e i compiti di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, nonché la responsabilità di sviluppare "capacità nazionali di prevenzione, monitoraggio, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici [...]";
- l'articolo 7, comma 1, lettera t), del citato decreto-legge n. 82/2021 che individua l'Agenzia quale autorità che "promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione Europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza nazionale e dei correlati servizi applicativi [...]";
- il 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";
- il decreto legislativo 18 maggio 2018, n. 65, recante "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione";
- il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica";
- il decreto del Presidente del Consiglio dei ministri del 10 marzo 2023, con cui è stato conferito al Prefetto Bruno Frattasi l'incarico di Direttore generale dell'Agenzia;
- il decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, recante "Regolamento di organizzazione e funzionamento dell'Agenzia per la Cybersicurezza Nazionale" e, in particolare, l'articolo 5;
- il Piano Nazionale di Ripresa e Resilienza (PNRR) - presentato alla Commissione in data 30 giugno 2021 e valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021, notificata all'Italia dal Segretariato generale del Consiglio con nota LT161/21, del 14 luglio 2021 - e, in particolare, le indicazioni contenute relativamente al raggiungimento di Milestone e Target;
- 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", che individua la Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante "Cybersicurezza";
- l'Accordo stipulato, in data 14 dicembre 2021, tra l'Agenzia e il Dipartimento per la Trasformazione digitale, ai sensi dell'articolo 5, comma 6, del d.lgs. n. 50/2016, di cui al prot. ACN. n. 896 de 15 dicembre 2021, disciplinante lo svolgimento in collaborazione delle attività di realizzazione dell'"Investimento 1.5", registrato dalla Corte dei Conti il 18 gennaio 2022 al n. 95, così come modificato dall'atto aggiuntivo approvato con decreto del Capo del DTD n. 126/2023-PNRR del 3 agosto 2023, registrato dalla Corte dei Conti il 5 settembre 2023 al n. 2425;
- l'atto di organizzazione prot. ACN n. 1776 del 1° marzo 2022, avente per oggetto "Adozione del modello organizzativo dell'Agenzia per la Cybersicurezza Nazionale per l'attuazione dell'Investimento 1.5 recante "Cybersicurezza" Missione 1, Componente 1, del PNRR e individuazione del personale incaricato a svolgere le funzioni e i compiti delegati all'Agenzia, in qualità di Soggetto Attuatore dell'investimento, dal Dipartimento per la

Trasformazione Digitale", così come modificata dalla determina ACN prot. n. 12011 del 16 settembre 2022;

- la determina ACN prot. n. 21472 dell' 8 agosto 2023 con la quale è stato approvato l'Avviso pubblico n. 06/2023 avente ad oggetto la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici" a valere sul "PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" - Codice d'Investimento M1C1I1.5 (di seguito "Avviso") e i relativi allegati ed è stato individuato, quale Responsabile del procedimento, il Dott. Luca Nicoletti;

Visto l'Avviso pubblico 6/2023 a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento della capacità di prevenzione, gestione e risposta degli incidenti informatici a favore di Regioni e le province autonome di Trento e Bolzano a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5 con dotazione finanziaria complessiva pari ad euro 28.000.000,00 (ventottomilioni//00). L'importo massimo ammissibile a finanziamento è pari a 1.000.000,00 € per progetto. Nell'ipotesi di iniziative progettuali il cui ambito di intervento intercetti l'ambito sanitario e/o di efficientamento energetico e/o di tutela del territorio e delle risorse idriche, è prevista una dotazione premiale aggiuntiva di 500.000,00 €. In tali casi, l'importo massimo ammissibile a finanziamento è pari a 1.500.000,00 € per progetto. Gli interventi ammessi a finanziamento debbano concludersi entro il 31/12/2024; nel caso in cui il progetto intercetti l'ambito sanitario e/o di efficientamento energetico e/o di tutela del territorio e delle risorse idriche, limitatamente a quest'ultime, i progetti ammessi a finanziamento potranno concludersi entro e non oltre la data del 31 dicembre 2025.

Vista la Determina n. 30697 del 30/11/2023, recante concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse a valere sull'Avviso n. 6/2023, il Direttore generale dell'agenzia per la cybersicurezza nazionale ha rifinanziato con ulteriori euro 490.306,51 (quattrocentonovantamilatrecentosei/51) la dotazione finanziaria iniziale complessiva dell'Avviso 06/2023, di cui alla determina ACN prot. n. 21472 dell'8 agosto 2023, al fine dello scorrimento della graduatoria dei progetti ammissibili ma parzialmente finanziabili per esaurimento delle risorse disponibili, coerentemente con la previsione di cui al par. 4.3 "L'importo massimo ammissibile a finanziamento è pari a 1.000.000,00 € per progetto. Nell'ipotesi di iniziative progettuali il cui ambito di intervento intercetti l'ambito sanitario e/o di efficientamento energetico e/o di tutela del territorio e delle risorse idriche, è prevista una dotazione premiale aggiuntiva di 500.000,00 €. In tali casi, l'importo massimo ammissibile a finanziamento è pari a 1.500.000,00 € per progetto"; ha quindi approvato la graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziate a valere sull'Avviso 6/2023 "a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici" PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5". A Regione del Veneto per il progetto "Attivazione CERT-CSIRT regionale" è riconosciuto un contributo pari ad Euro 1.500.000,00 iva inclusa; CUP H19B23000100006. Il finanziamento è stato comunicato con nota agli atti al prot. n. 647495 in data 05/12/2023.

Visto l'art. 53 del D.Lgs. n. 118/2011 ed in particolare il punto 3.6 dell'allegato 4/2;

Visto l'art.15, comma 4 del DL 77 del 31/05/2021che consente agli enti di accertare le entrate derivanti dal trasferimento delle risorse del PNRR e del PNC sulla base della formale deliberazione di riparto o assegnazione del contributo a proprio favore, senza dover attendere l'impegno dell'amministrazione erogante, con imputazione agli esercizi di esigibilità ivi previsti;

Vista la Faq n. 48 del 15.12.2021 della Commissione Arconet che fornisce ulteriori chiarimenti sugli interventi di semplificazione e flessibilità riguardanti la contabilità degli enti territoriali diretti a favorire l'attuazione del PNRR e del Piano Nazionale Complementare (PNC);

Attestato che sono presenti i seguenti elementi costitutivi dell'accertamento:

- le ragioni del credito, la Determina n. 30697 del 30/11/2023, recante concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse a valere sull'Avviso n. 6/2023, il Direttore generale dell'agenzia per la cybersicurezza nazionale ha rifinanziato con ulteriori euro 490.306,51 (quattrocentonovantamilatrecentosei/51) la dotazione finanziaria iniziale complessiva dell'Avviso 06/2023, di cui alla determina ACN prot. n. 21472 dell'8 agosto 2023, al fine dello scorrimento della graduatoria dei progetti ammissibili ma parzialmente finanziabili per esaurimento delle risorse disponibili, coerentemente con la previsione di cui al par. 4.3 "L'importo massimo ammissibile a finanziamento è pari a 1.000.000,00 € per progetto. Nell'ipotesi di iniziative progettuali il cui ambito di intervento intercetti l'ambito sanitario e/o di efficientamento energetico e/o di tutela del territorio e delle risorse idriche, è prevista una dotazione premiale aggiuntiva di 500.000,00 €. In tali casi, l'importo massimo ammissibile a finanziamento è pari a 1.500.000,00 € per progetto"; ha quindi approvato la graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziate a valere sull'Avviso 6/2023 "a sportello per la presentazione di proposte di interventi volti all'attivazione e al potenziamento di CSIRT Regionali per il

rafforzamento delle capacità di prevenzione, gestione e risposta degli incidenti informatici" PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5". A Regione del Veneto per il progetto "Attivazione CERT-CSIRT regionale" è riconosciuto un contributo pari ad Euro 1.500.000,00 iva inclusa; CUP H19B23000100006. Il finanziamento è stato comunicato con nota agli atti al prot. n. 647495 in data 05/12/2023 e l'idoneo titolo giuridico a supporto del credito costituito dal D.L. 31/05/2021, N.77 - DECRETO DEL DIRETTORE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE 30/11/2023, N.30697);

- capitolo, piano dei conti, soggetto debitore, importi ed esigibilità dell'entrata come indicati **nell'Allegato Contabile A**, parte integrante e sostanziale del presente provvedimento;

Attestato che le attività si concluderanno nel 2024 e che il cronoprogramma della spesa, secondo le specifiche e l'esigibilità contenute nell'Allegato **A** contabile del presente atto, parte integrante e sostanziale del presente provvedimento, è così di seguito sinteticamente rappresentato:

TABELLA: CRONOPROGRAMMA DI SPESA

ANNO	CAPITOLI	PIANO DEI CONTI	DESCRIZIONE	IMPORTO
2024	105203	U.1.03.00.00.000	PNRR - M1.C1.1.5 - REALIZZAZIONE DEL PROGETTO "ATTIVAZIONE DEL CERT- CSIRT REGIONALE" - ACQUISTO DI BENI E SERVZI (D.L. 31/05/2021, N.77 - DECRETO DEL DIRETTORE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE 30/11/2023, N.30697)	279.326,32
2024	105203	U.1.03.02.19.000	PNRR - M1.C1.1.5 - REALIZZAZIONE DEL PROGETTO "ATTIVAZIONE DEL CERT- CSIRT REGIONALE" - ACQUISTO DI BENI E SERVZI (D.L. 31/05/2021, N.77 - DECRETO DEL DIRETTORE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE 30/11/2023, N.30697)	1.220.673,68
			TOTALE	1.500.000,00

Atteso che nell'ambito del contratto CIG derivato B079874EAF le attività saranno svolte dalle aziende secondo la ripartizione indicata nel Piano Operativo, agli atti al prot. n. 50356 in data 30/01/2024 e precisamente: Accenture S.p.a. 90,00%, Fastweb S.p.a. 10,00%, Fincantieri NextTech S.p.A. 0,00% e DEAS- Difesa e Analisi Sistemi S.p.A. 0,00%. In particolare il servizio di Formazione e Security Awareness sarà eseguito integralmente dalla società Accenture S.p.a. e i Servizi specialistici saranno svolti pro quota dalle società Accenture S.p.a. e Fastweb S.p.a.

Ritenuto necessario provvedere alla copertura dell'obbligazione giuridica passiva perfezionata e, quindi di provvedere alla copertura dell'obbligazione giuridica passiva perfezionata e di impegnare a favore della società Accenture S.p.A., sede legale in Milano, Via Privata Nino Bonnet n. 10, P. IVA 13454210157, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti Fastweb S.p.A. con sede legale in Milano, Piazza Adriano Olivetti n.1, P. IVA 12878470157, Fincantieri NextTech S.p.A., con sede legale in Milano, Via Carlo Ottavio Cornaggia n. 10, P. IVA 00890740111 e DEAS- Difesa e Analisi Sistemi S.p.A., con sede legale in Roma Via della Colonna Antonina n. 46, P. IVA 14961281004, la somma di Euro 1.500.000,00 iva al 22% inclusa (Iva pari ad Euro 270.491,80), che si configura debito commerciale, il tutto secondo le specifiche e l'esigibilità contenute nell'**Allegato A contabile** del presente atto, del quale costituisce parte integrante e sostanziale, per le motivazioni di cui alla premessa.

Precisato che:

- Coerentemente a quanto previsto nel "Capitolato tecnico speciale per servizi di sicurezza da remoto" la modalità di remunerazione del servizio di Formazione e Security Awarness e del servizio specialistico è "progettuale (a corpo)" e la metrica di misurazione è "Giorni/Persona del team ottimale".

La consuntivazione avrà una cadenza mensile; mensilmente verrà prodotto un report di sintesi che sarà discusso Amministrazione. Il report riporterà, a livello di progetto e a livello di obiettivo: i) avanzamento e scostamenti rispetto al piano di lavoro; ii) attività svolte e attività previste; iii) rischi e problematiche operative; iv) punti aperti; v) azioni da intraprendere per il corretto svolgimento delle attività. alla consegna dei deliverable previsti.

La fatturazione avrà una cadenza bimestrale posticipata. Il pagamento del corrispettivo sarà effettuato dalla Stazione Appaltante, a mezzo mandato a 30 gg dalla data di ricevimento della fattura, che dovrà essere emessa dall'aggiudicatario successivamente all'adozione della verifica funzionale sulla quantità e qualità del servizio erogato ed è in ogni caso subordinato all'esaurimento delle procedure amministrative/contabili proprie dell'Amministrazione regionale. Eventuali contestazioni interromperanno detti termini;

- l'Amministrazione regionale dovrà operare sull'importo netto progressivo delle prestazioni una ritenuta annua dello 0,50% (zero virgola cinque per cento, come previsto dall'art. 10.4 del Contratto Quadro) per l'anno 2024 che verrà liquidata complessivamente dalla stessa solo al termine del Contratto Esecutivo e previa acquisizione del documento unico di regolarità contributiva.

Dato atto che:

- la presente procedura di gara dà attuazione al Programma triennale degli acquisti di forniture e servizi 2024/2026 approvato dalla Giunta regionale con Deliberazione n. 82 del 12 febbraio 2024, Codice CUI S80007580279202200155;
- il contratto genererà spesa corrente e si riferisce a contratto necessario a garantire la continuità dei servizi connessi con le funzioni fondamentali dell'Amministrazione (art 10, comma 3, lett. a) del D.lgs 118/2011);

Atteso, altresì, che si provvederà a comunicare al destinatario della spesa le informazioni relative all'impegno assunte col presente provvedimento.

Dato atto che è necessario disporre la copertura dell'obbligazione giuridica passiva perfezionata della spesa relativa al contributo Consip, che deve essere corrisposto a norma dell'art. 18, co. 3 del D.Lgs. n. 177 del 01/12/2009 attuato dal DPCM del 23/06/2010, pari ad Euro 6.147,54= (fuori campo dell'applicazione dell'IVA, ai sensi dell'art. 2, comma 3, lettera a) del D.P.R. del 1972), che si configura debito non commerciale, a carico del capitolo di spesa. 103653 "Spese per lo sviluppo del Sistema Informativo Regionale" art 15 P.d.c. 1.02.01.99.99 "IMPOSTE, TASSE E PROVENTI ASSIMILATI A CARICO DELL'ENTE N.A.C." del Bilancio regionale 2024 - 2026. Esercizio finanziario 2024, avente l'occorrente disponibilità secondo le specifiche e l'esigibilità contenute **nell'Allegato A** contabile del presente atto;

Visto:

- l'articolo 13 della legge regionale 31 dicembre 2012, n. 54 che definisce i compiti dei Direttori di Direzione;
- la D.G.R. n. 1823 del 6 dicembre 2019 di approvazione delle nuove linee guida sugli acquisti sotto soglia;
- l'art. 29 del D.Lgs n. 50/2016 che stabilisce gli atti relativi alle procedure per l'affidamento di appalti pubblici di servizi, forniture, opere devono essere pubblicati sul profilo del committente, nella sezione "Amministrazione trasparente", nonché sul sito del Ministero delle infrastrutture e dei trasporti;

TUTTO CIO' PREMESSO

- VISTI il D.Lgs. n. 50 del 18/04/2016 e succ.mod.e int.;
- RICHIAMATO l'art. 1, comma 512 della legge 28 dicembre 2015, n. 208
- VISTO il D.Lgs. n. 126/2014 integrativo e correttivo del D.Lgs. n. 118/2011;
- VISTA la Legge Regionale n. 39 del 29/11/2001 e ss.mm. ii. nonchè la Legge Regionale n. 1/2011;
- VISTO il DPR n. 101 del 04/04/2002 *"Regolamento recante criteri e modalità per l'espletamento da parte delle amministrazioni pubbliche di procedure telematiche di acquisto per l'approvvigionamento di beni e servizi";*
- VISTA la L.R. n. 32 del 22/12/2023 "Bilancio di previsione 2024-2026";
- VISTA la D.G.R. n. 1615 del 22/12/2023 che approva il documento tecnico di accompagnamento del Bilancio di previsione 2024-2026 e successive variazioni;
- VISTO il Decreto n. 25 del 29/12/2023 del Segretario Generale della Programmazione che approva il Bilancio Finanziario Gestionale 2024-2026 e successive variazioni;
- VISTA la D.G.R. n. 36 del 23/01/2024 "Direttive per la gestione del Bilancio di Previsione 2024 - 2026;
- VISTO l'art. 23 del D.Lgs. del 14/03/2013, n. 33 in tema di "Amministrazione Trasparente";
- VISTA la D.G.R. n. 1027 del 22/08/2023.

decreta

1. che le premesse costituiscono parte integrante e sostanziale del presente atto;
2. di dare atto che il Responsabile del procedimento è il Direttore della Direzione ICT e Agenda Digitale, Dott. Idelfo Borgo che ricopre anche il Ruolo di Direttore dell'Esecuzione;
3. di nominare, ai sensi dell'art. 101 del D.Lgs n. 50/2016, il Direttore dell'Esecuzione del contratto nel Direttore della U.O. Sistemi Informativi, servizi e tecnologie digitali, ing. Paolo Barichello;
4. di dare atto che, in data 04/08/2022, è stato sottoscritto il Contratto Quadro nell'ambito delle iniziative per l'attuazione del Piano Triennale per l'informatica della Pubblica Amministrazione tra Consip S.p.a., per conto del Ministero dell'Economia e delle Finanze e la società Accenture S.p.A., sede legale in Milano, Via Privata Nino Bonnet n. 10, P. IVA 13454210157, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti Fastweb S.p.A. con sede legale in Milano, Piazza Adriano Olivetti n.1, P. IVA 12878470157, Fincantieri NextTech S.p.A., con sede legale in Milano, Via Carlo Ottavio Cornaggia n. 10, P. IVA 00890740111 e

DEAS- Difesa e Analisi Sistemi S.p.A., con sede legale in Roma Via della Colonna Antonina n. 46, P. IVA 14961281004, per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni ai sensi dell'art. ex art. 54, co. 4 lett. a) d.lgs. n. 50/2016, Lotto 1 CIG n. 88846293CA, per la durata di 24 mesi;

5. di procedere all'appalto per l'acquisto di servizi al fine di erogare un tutoraggio in tutte le fasi di set-up, implementazione e manutenzione del CERT Regionale e di monitorare l'efficacia della formazione erogata, mediante adesione al Contratto Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le pubbliche amministrazioni ai sensi dell'art. ex art. 54, co. 4 lett. a) d.lgs. n. 50/2016, Lotto 1 CIG n. 88846293CA, ai sensi dell'art. 1, comma 512 della legge 28 dicembre 2015, n. 208, e in attuazione della D.G.R. n. 1174 del 27/09/2022, per l'importo di Euro 1.229.508,20 iva esclusa, per la durata di undici (11) mesi dalla data di conclusione delle attività di presa in carico e non oltre il 31 dicembre 2024, con ciò approvando il Piano Operativo "AQSEC-2296L1-PO", agli atti al prot. n. 79950 in data 15/02/2024, trasmesso dal Raggruppamento temporaneo costituito tra le società Accenture S.p.A., mandataria, Fastweb S.p.A., mandante, Fincantieri NextTech S.p.A., mandante e DEAS- Difesa e Analisi Sistemi S.p.A., mandante;
6. di autorizzare pertanto la sottoscrizione del Contratto esecutivo CIG derivato B079874EAF, CUP H79B22000180001, secondo lo schema messo a disposizione da Consip S.p.a nel portale dedicato all'iniziativa, dando atto che lo stesso sarà sottoscritto dal Direttore della Direzione ICT e Agenda Digitale;
6. di dare atto di dare atto in data odierna il contratto esecutivo CIG derivato B079874EAF, CUP H79B22000180001 è stato sottoscritto dall'amministrazione e trasmesso al fornitore;
7. di dare atto che la tipologia della prestazione, servizi intellettuali e di servizi svolti da remoto, senza accesso ai locali regionali, non comporta la presenza di rischi da interferenza nella sua esecuzione tali da richiedere la redazione del Documento Unico Valutazione Rischi Interferenti (DUVRI) di cui al decreto legislativo 9 aprile 2008, n. 81 e che pertanto gli oneri per la sicurezza di natura interferenziale sono pari a zero;
8. di autorizzare la spesa complessiva pari ad Euro 1.500.000,00 iva al 22% inclusa (Iva pari ad Euro 270.491,80), riferita all'incarico per servizi informatici, dando atto che trattasi di debito commerciale;
9. di dare atto che nell'ambito del contratto CIG derivato 98567195D5 le attività saranno svolte dalle aziende secondo la ripartizione indicata nel Piano Operativo, agli atti al prot. n. 79950 in data 15/02/2024 e precisamente: Accenture S.p.a. 90,00%, Fastweb S.p.a. 10,00%; in particolare il servizio di Formazione e Security Awareness sarà eseguito integralmente dalla società Accenture S.p.a. e i Servizi specialistici saranno svolti pro quota dalle società Accenture S.p.a. e Fastweb S.p.a.
10. di associare quindi agli impegni i seguenti beneficiari ed importi:

Beneficiari	Importo compresa iva
società Accenture S.p.a. S.r.l. S.B.., mandataria, con sede legale in Milano, Via Privata Nino Bonnet n. 10, P. IVA 13454210157	€ 1.500.000,00
Fastweb S.p.A., mandante, con sede legale in Milano, Piazza Adriano Olivetti n.1, P. IVA 12878470157	€ 0
Fincantieri NextTech S.p.A., con sede legale in Milano, Via Carlo Ottavio Cornaggia n. 10, P. IVA 00890740111	€ 0
DEAS- Difesa e Analisi Sistemi S.p.A., con sede legale in Roma Via della Colonna Antonina n. 46, P. IVA 14961281004	€ 0

11. di corrispondere a favore della società Accenture S.p.A., sede legale in Milano, Via Privata Nino Bonnet n. 10, P. IVA 13454210157, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti Fastweb S.p.A. con sede legale in Milano, Piazza Adriano Olivetti n.1, P. IVA 12878470157, Fincantieri NextTech S.p.A., con sede legale in Milano, Via Carlo Ottavio Cornaggia n. 10, P. IVA 00890740111 e DEAS-Difesa e Analisi Sistemi S.p.A., con sede legale in Roma Via della Colonna Antonina n. 46, P. IVA 14961281004, la somma pari ad Euro 1.500.000,00 iva al 22% inclusa (Iva pari ad Euro 270.491,80) con periodicità bimestrale, in ragione dei servizi effettivamente prestati nel rispetto del Piano Operativo. Il pagamento del corrispettivo sarà effettuato dalla Stazione Appaltante, a mezzo mandato a 30 gg dalla data di ricevimento della fattura, che dovrà essere emessa dall'aggiudicatario successivamente all'adozione della verifica funzionale sulla quantità e qualità del servizio erogato ed è in ogni caso subordinato all'esaurimento delle procedure amministrative/contabili proprie dell'Amministrazione regionale. Eventuali contestazioni interromperanno detti termini;
12. di dare atto che il Codice Unico Ufficio della Direzione ICT e Agenda Digitale ai fini della fatturazione elettronica è il seguente: 350 EDA;
13. di accertare l'entrata, ai sensi del punto 3.6 del D.Lgs. 118/2011e smi, secondo le specifiche e l'esigibilità contenute nell'**Allegato A contabile** del presente atto, del quale costituisce parte integrante e sostanziale, per le motivazioni di cui in premessa come da tabella:

capito di entrata/siope/debitore	anno 2024
Capitolo 105203 NRR - M1.C1.1.5 - REALIZZAZIONE DEL PROGETTO "ATTIVAZIONE DEL CERT- CSIRT REGIONALE" - ACQUISTO DI BENI E SERVZI (D.L. 31/05/2021, N.77 - DECRETO DEL DIRETTORE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE 30/11/2023, N.30697) Anagrafe n. 00183745 AGENZIA PER LA CYBER SICUREZZA NAZIONALE - A.C.N. Codice Siope TRASFERIMENTI CORRENTI DA PRESIDENZA DEL CONSIGLIO DEI MINISTRI E.2.01.01.01.003	Euro 1.500.000,00

14. di dare atto che il crono programma della spesa, secondo le specifiche e l'esigibilità contenute **nell'Allegato A** contabile del presente atto, parte integrante e sostanziale del presente provvedimento, è così di seguito sinteticamente rappresentato:

TABELLA: CRONOPROGRAMMA DI SPESA				
ANNO	CAPITOLI	PIANO DEI CONTI	DESCRIZIONE	IMPORTO
2024	105203	U.1.03.00.00.000	PNRR - M1.C1.1.5 - REALIZZAZIONE DEL PROGETTO "ATTIVAZIONE DEL CERT- CSIRT REGIONALE" - ACQUISTO DI BENI E SERVZI (D.L. 31/05/2021, N.77 - DECRETO DEL DIRETTORE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE 30/11/2023, N.30697)	279.326,32
2024	105203	U.1.03.02.19.000	PNRR - M1.C1.1.5 - REALIZZAZIONE DEL PROGETTO "ATTIVAZIONE DEL CERT- CSIRT REGIONALE" - ACQUISTO DI BENI E SERVZI (D.L. 31/05/2021, N.77 - DECRETO DEL DIRETTORE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE 30/11/2023, N.30697)	1.220.673,68
			TOTALE	1.500.000,00

15. di disporre la copertura dell'obbligazione giuridica passiva perfezionata e di impegnare a favore della società della società Accenture S.p.A., sede legale in Milano, Via Privata Nino Bonnet n. 10, P. IVA 13454210157, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti Fastweb S.p.A. con sede legale in Milano, Piazza Adriano Olivetti n.1, P. IVA 12878470157, Fincantieri NextTech S.p.A., con sede legale in Milano, Via Carlo Ottavio Cornaggia n. 10, P. IVA 00890740111 e DEAS- Difesa e Analisi Sistemi S.p.A., con sede legale in Roma Via della Colonna Antonina n. 46, P. IVA 14961281004, la somma pari ad Euro 1.500.000,00 iva al 22% inclusa (Iva pari ad Euro 270.491,80), che si configura debito commerciale, il tutto secondo le specifiche e l'esigibilità contenute nell'**Allegato A contabile** del presente atto, del quale costituisce parte integrante e sostanziale, per le motivazioni di cui alla premessa;
16. di attestare che l'obbligazione di cui si dispone l'impegno è perfezionata ed è esigibile secondo la scadenza della spesa per la quale viene stabilito il relativo vincolo;
17. di dare atto che l'Amministrazione regionale dovrà operare sull'importo netto progressivo delle prestazioni una ritenuta annua dello 0,50% (zero virgola cinque per cento, come previsto dall'art. 10.4 del Contratto Quadro) per l'anno 2024 che verrà liquidata complessivamente dalla stessa solo al termine del Contratto Esecutivo e previa acquisizione del documento unico di regolarità contributiva, importo impegnato nel 2024;
18. di dare atto che la presente procedura di gara dà attuazione al Programma triennale degli acquisti di forniture e servizi 20242026 approvato dalla Giunta regionale con Deliberazione n. 82 del 12 febbraio 2024. Codice CUI S80007580279202200155;
19. di autorizzare la spesa pari ad Euro 6.147,54= (fuori campo dell'applicazione dell'IVA, ai sensi dell'art. 2, comma 3, lettera a) del D.P.R. del 1972), che si configura debito non commerciale,
20. di disporre la copertura dell'obbligazione giuridica passiva perfezionata della spesa relativa al contributo Consip, a norma dell'art. 18, co. 3 del D.Lgs. n. 177 del 01/12/2009 attuato dal DPCM del 23/06/2010, pari ad Euro 6.147,54= (fuori campo dell'applicazione dell'IVA, ai sensi dell'art. 2, comma 3, lettera a) del D.P.R. del 1972), che si configura debito non commerciale, a carico del capitolo di spesa. 103653 "Spese per lo sviluppo del Sistema Informativo Regionale" art 15 P.d.c. 1.02.01.99.99 "IMPOSTE, TASSE E PROVENTI ASSIMILATI A CARICO DELL'ENTE N.A.C." del Bilancio regionale 2024 - 2026. Esercizio finanziario 2024, avente l'occorrente disponibilità secondo le specifiche e l'esigibilità contenute nell'Allegato **A** contabile del presente atto;
21. di corrispondere la somma complessiva di Euro 6.147,54 (fuori campo dell'applicazione dell'IVA, ai sensi dell'art.2, comma 3, lettera a) del D.P.R. del 1972) a Consip S.p.a., sede legale e operativa in Via Isonzo 19/d, 00198 - Roma,

Codice Fiscale e Partita Iva n. 05359681003 non appena esecutivo il provvedimento, precisato che la liquidazione avverrà in assenza di nota di debito o di fatturazione, mediante liquidazione che non necessità di fattura o nota di debito;

22. di attestare che la copertura dell'obbligazione assunta per una spesa pari ad Euro 1.500.000,00 IVA al 22% compresa, riferita all'incarico per servizi informatici, è assicurata dagli accertamenti di entrata disposti al punto 13, a carico del Bilancio regionale per l'annualità 2024;
23. di attestare la copertura dell'obbligazione assunta per una spesa pari ad EURO 6.147,54 (fuori campo dell'applicazione dell'IVA, ai sensi dell'art.2, comma 3, lettera a) del D.P.R. del 1972) a carico del Bilancio regionale per l'annualità 2024, come specificato al punto 20) del presente dispositivo;
24. di dare atto che il contratto pluriennale che viene sottoscritto a seguito della presente procedura di spesa genererà spesa corrente ed è necessario a garantire la continuità dei servizi connessi con le funzioni fondamentali dell'Amministrazione (art 10, comma 3, lett. a) del D.lgs 118/2011);
25. di dare atto che alla liquidazione si procederà ai sensi dell'art. 44 e seguenti della L.R. n. 39/2001, previo accertamento della regolare esecuzione e su presentazione di regolare fattura;
26. di attestare, ai sensi dell'art. 56, punto 6, del D.Lgs. n. 118/2011 e ss.mm.ii., che il programma dei pagamenti è compatibile con gli stanziamenti di bilancio di previsione 2023-2025, e con le regole di finanza pubblica;
27. di attestare che si provvederà a comunicare al destinatario della spesa le informazioni relative all'impegno assunte con il presente provvedimento (art. 56, punto 7, del D.Lgs. n. 118/2011 e ss.mm.ii.);
28. di attestare la regolarità amministrativa del provvedimento;
29. di trasmettere il presente atto alla Direzione Bilancio e Ragioneria per l'apposizione del visto di regolarità contabile al fine del perfezionamento e dell'efficacia;
30. di dare atto che il presente provvedimento è soggetto a pubblicazione ai sensi degli artt. 23 e 37 del D.Lgs. 14 marzo 2013 n. 33 e dell'art. 29 del D.Lgs. n. 50/2016;
31. di disporre la pubblicazione integrale del presente Decreto nel Bollettino Ufficiale della Regione del Veneto, omettendo l'**Allegato A.**

Idelfo Borgo

Allegato (*omissis)*