Codice A1911A
D.D. 29 dicembre 2023, n. 599
Iniziativa NextGenerationEU - PNRR M1C1|1.5 ''Cybersecurity''. contributo PNRR finanziato da ACN a valere sull'Avviso 3/2022. Affidamento dei servizi relativi all' Intervento 3A, iniziativa ''ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI'' - CUP: J14F22001120006 tramite Adesione all'Accordo Quadro ''ID 2296 - Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni - Lotto 1''...

REGIONE PIEMONTE

ATTO DD 599/A1911A/2023 DEL 29/12/2023

DETERMINAZIONE DIRIGENZIALE
A19000 - COMPETITIVITA' DEL SISTEMA REGIONALE
A1911A - Sistema informativo regionale

OGGETTO: Iniziativa NextGenerationEU – PNRR M1C1|1.5 “Cybersecurity”. contributo PNRR finanziato da ACN a valere sull’Avviso 3/2022. Affidamento dei servizi relativi all’ Intervento 3A, iniziativa “ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI” – CUP: J14F22001120006 tramite Adesione all’Accordo Quadro “ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni – Lotto 1”, CIG A03A642A24, per un totale di € 75.988,64. Accertamento di complessivi € 59.899,84 sul cap. 20495/2024. Imp. di spesa di € 59.899,84 sul cap. di spesa 207164/2024 a favore di Accenture S.p.a.. Imp. di spesa di € 15.346,24 sul cap. di spesa 106601/2024 a favore di Accenture S.p.a.. Imp. di spesa di € 247,52 sul cap. di spesa 106601/2024 a favore di Fastweb S.p.A.. Imp. di spesa di € 247,52 sul cap. di spesa 106601/2024 a favore di Fincantieri NextTech S.p.A. Imp. di spesa di € 247,52 sul cap. di spesa 106601/2024 a favore di DEAS-Difesa e Analisi Sistemi S.p.A.

Premesso che:

l'Unione Europea, all'interno del programma Next Generation EU, per rispondere alla crisi pandemica provocata dal Covid-19, ha previsto un pacchetto di finanziamenti pari a 750 miliardi di euro ed ha approvato il Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, che istituisce il Dispositivo per la Ripresa e la Resilienza quale principale componente del suddetto programma;

tale strumento, con una durata prevista di sei anni (dal 2021 al 2026) e di dimensione finanziaria pari a 672,5 miliardi di euro, è finalizzato alla realizzazione di programmi di investimenti e di riforme coerenti, ai sensi dell'articolo 17, paragrafo 3, del Regolamento sopra citato, con le pertinenti sfide e priorità specifiche per Paese individuate nell'ambito del semestre europeo, con le sfide e le priorità individuate nelle Raccomandazioni del Consiglio sulla politica economica della zona euro, con i Programmi Nazionali di Riforma nell'ambito del semestre europeo, i piani nazionali per l'energia e il clima, i piani territoriali per una transizione giusta, i piani di attuazione

della garanzia per i giovani, gli accordi di partenariato ed i programmi operativi cofinanziati con i fondi europei;

gli obiettivi generali del Dispositivo per la Ripresa e la Resilienza sono, ai sensi dell'articolo 4 del Reg. (EU) 2021/241 i seguenti :

1. promuovere la coesione economica, sociale e territoriale dell'Unione migliorando la resilienza, la preparazione alle crisi, la capacità di aggiustamento e il potenziale di crescita degli Stati membri;
2. attenuare l'impatto sociale ed economico della crisi, in particolare sulle donne, contribuendo all'attuazione del pilastro europeo dei diritti sociali;
3. sostenere la transizione verde contribuendo al raggiungimento degli obiettivi climatici dell'Unione per il 2030 nonché della neutralità climatica dell'UE entro il 2050;
4. sostenere la transizione digitale, contribuendo in tal modo alla convergenza economica e sociale, ripristinare il potenziale di crescita delle economie dell'Unione, incentivare la creazione di posti di lavoro nel periodo successivo alla crisi del Covid- 19;
5. ripristinare e promuovere la crescita sostenibile e l'integrazione delle economie dell'Unione e incentivare la creazione di posti di lavoro di alta qualità, nonché contribuire all'autonomia strategica dell'Unione unitamente a un'economia aperta, generando un valore aggiunto europeo;

l'articolo 17 del Regolamento in parola prevede che i singoli Stati membri elaborino un Piano Nazionale di Ripresa e Resilienza (PNRR), da trasmettere, ai sensi del successivo articolo 18, alla Commissione europea entro il 30 aprile 2021;

il Piano Nazionale di Ripresa e Resilienza, presentato dall'Italia in data 30 aprile 2021, è strutturato in sei Missioni, a loro volta suddivise in componenti:

1. Digitalizzazione, innovazione, competitività, cultura e turismo;
2. Rivoluzione verde e transizione ecologica;
3. Infrastrutture per una mobilità sostenibile;
4. Istruzione e ricerca;
5. Inclusione e coesione;
6. Salute;

la governance del PNRR, articolata su più livelli, è disciplinata dal Decreto legge 31 maggio 2021, n. 77 convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108;

a conclusione di un articolato processo di raccolta e clusterizzazione delle proposte da parte delle Regioni e delle Province autonome, la Conferenza delle Regioni e delle Province autonome ha individuato le priorità comuni che sono state trasmesse al Governo il 28 dicembre 2020;

il Piano nazionale di ripresa e resilienza (PNRR) è stato approvato con Decisione del Consiglio ECOFIN del 13 luglio 2021 e notificato all'Italia dal Segretariato generale del Consiglio con nota LT161/21 del 14 luglio 2021;

con decreto-legge 14 giugno 2021 n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è stata istituita l' Agenzia per la Cybersicurezza Nazionale (ACN);

il Decreto del Ministro dell'Economia e delle Finanze del 6 agosto 2021, relativo all'assegnazione delle risorse in favore di ciascuna Amministrazione titolare degli interventi del PNRR e corrispondenti milestone e target, ha individuato la Presidenza del Consiglio dei ministri quale Amministrazione titolare della Missione 1, Componente 1, Investimento 1.5 recante "Cybersicurezza"; la dotazione finanziaria complessiva per l'Investimento 1.5 ammonta ad € 623.000.000,00;

con Accordo stipulato dall'Agenzia per la Cybersicurezza Nazionale con il Dipartimento per la trasformazione digitale, ai sensi dell'articolo 5, comma 6, del D.lgs. n. 50/2016, n. 34/2021 del 14 dicembre 2021, di cui al prot. ACN n. 896 del 15 dicembre 2021, è stato disciplinato lo svolgimento in collaborazione delle attività di realizzazione dell'<<Investimento 1.5>>, registrato dalla Corte dei Conti il 18/01/2022 al n. 95;

con nota prot. 347 del 19 gennaio 2022, l'Autorità delegata per la sicurezza della Repubblica e la cybersicurezza ha approvato il documento di indirizzo strategico recante la "Strategia di finanziamento mediante Avvisi Pubblici", predisposto dall'Agenzia per la Cybersicurezza Nazionale, sentita la Presidenza del Consiglio del ministri – Dipartimento per la trasformazione digitale;

il traguardo e l'obiettivo da perseguire in relazione all'Investimento 1.5, riportato nel documento di indirizzo strategico sopra richiamato, è il seguente: M1C1-19 (target finale UE) "Supporto all'aggiornamento delle misure di sicurezza - 50 strutture di sicurezza adeguate entro dicembre 2024";

per procedere all'attuazione degli interventi previsti dalla Missione 1, Componente 1, Investimento 1.5, è stato deciso di procedere mediante la selezione di progetti "a regia" con Avviso Pubblico valutativo con graduatoria, al fine di individuare i Soggetti attuatori delle proposte progettuali riguardanti la realizzazione di interventi di potenziamento della resilienza cyber per le Pubbliche Amministrazioni;

con determinazione n. 1816 del 02/03/2022 del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, è stato approvato l'Avviso pubblico n. 01/2022 avente ad oggetto "Avviso pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber degli Organi Costituzionali e di rilievo Costituzionale, delle Agenzie Fiscali e delle Amministrazioni facenti parte del Nucleo per la cybersicurezza a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" - Codice d'investimento M1C1I1.5";

in linea con quanto previsto nel sopra citato documento di indirizzo strategico recante la "Strategia di finanziamento mediante Avvisi Pubblici", l'Agenzia per la Cybersicurezza Nazionale ha ritenuto di ampliare la platea di Soggetti ammessi alla partecipazione, individuando quali Soggetti destinatari le Regioni, i Comuni capoluogo facenti parte di Città metropolitane ex legge 7 aprile 2014, n. 56, i Comuni capoluogo delle Città metropolitane istituite nelle Regioni a statuto speciale e le Province autonome;

l'Agenzia per la Cybersicurezza Nazionale ha pertanto ritenuto necessario procedere con l'approvazione e l'indizione di un nuovo Avviso Pubblico (n. 03/2022) recante "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" - Codice d'investimento M1C1 I1.5" e dei relativi allegati, con l'obiettivo di dotare i Soggetti attuatori dei necessari strumenti e processi per una gestione del rischio cyber in linea con le migliori prassi nazionali e internazionali;

la dotazione finanziaria dell'Avviso, in scadenza al 30 settembre 2022,ammonta complessivamente ad € 45.000.000,00, a valere sull'Investimento 1.5 "Cybersecurity", Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo", Componente 1 – "Digitalizzazione, Innovazione e

Sicurezza nella P.A.", Misura 1 – "Digitalizzazione P.A." del PNRR;

l'importo massimo ammissibile a finanziamento è pari a € 1.000.000,00 per progetto e comunque limitato in
€ 2.000.000,00 per Soggetto proponente e potrà essere erogato un contributo in misura pari al 100% delle spese ritenute ammissibili indicate nell'avviso, nel rispetto dei predetti massimali.

Ritenuto opportuno promuovere interventi di potenziamento della resilienza cyber, per aumentare i livelli di sicurezza ed affidabilità dei sistemi informativi, anche tenendo conto che la digitalizzazione dei processi, prodotti e servizi caratterizza molte delle politiche e degli interventi di riforma del Piano Nazionale di Ripresa e Resilienza (PNRR) e le linee guida a livello nazionale per l'introduzione di piattaforme digitali per l'ammodernamento della Pubblica Amministrazione, anche a supporto del lavoro agile, e che le politiche volte alla digitalizzazione della Pubblica Amministrazione richiedono un rafforzamento sempre crescente della sicurezza informatica secondo gli indirizzi formulati dall'Agenzia per la Cybersicurezza Nazionale, anche alla luce del percorso di graduale trasferimento del personale regionale che attualmente occupa diverse sedi presenti nel comune di Torino, nella nuova sede unica degli uffici della Giunta regionale.

Dato atto che:

al fine di presentare la candidatura al predetto Avviso Pubblico, la Direzione regionale Competitività del Sistema Regionale ha elaborato due proposte progettuali, predisposte rispettivamente dal Settore "Servizi Infrastrutturali e Tecnologici" e dal Settore "Sistema Informativo Regionale" per un importo complessivo previsto pari a € 1.979.500,00, finalizzate ad accrescere il livello di sicurezza informatica e di consapevolezza del rischio cyber dell'Amministrazione Regionale, come di seguito riportato:

- la prima proposta progettuale, denominata "Postazioni di lavoro e rete regionale; l'evoluzione in sicurezza", di importo stimato pari a € 984.400,00, è di carattere infrastrutturale, riguarda l'analisi della postura di sicurezza degli strumenti tecnologici di lavoro del personale (postazioni, ambienti di virtualizzazione, reti) e l'attuazione degli interventi necessari al rafforzamento della resilienza, quali l'implementazione di servizi di monitoraggio e di sicurezza intelligenti a beneficio sia delle sedi regionali sul territorio, sia dell'importante sede del palazzo unico. Il progetto prevede anche il rafforzamento della conoscenza, della cultura sulla sicurezza presso gli utilizzatori, con l'obiettivo di sviluppare ulteriormente la consapevolezza delle minacce cyber e di adeguare i comportamenti organizzativi correlati;
- la seconda proposta progettuale, denominata "Transizione digitale e servizi sicuri", di importo stimato pari a € 995.100,00, opera sul fronte della messa in sicurezza dei servizi digitali e prevede l'analisi di vulnerabilità, la pianificazione e la realizzazione di interventi di mitigazione del rischio di un portafoglio composto dai servizi applicativi più rilevanti per la Regione. Il progetto contempla la definizione delle strategie tecnico-organizzative e la predisposizione del piano di continuità operativa previsto dalla norma ISO 22301:2019. Si prevede anche in questo ambito di realizzare azioni di rafforzamento delle conoscenze e delle pratiche del personale regionale in termini di sicurezza nella gestione dei dati e dei servizi digitali erogati all'utenza.

con Deliberazione n. 6-5680 del 27 settembre 2022, la Giunta Regionale, nel ritenere di aderire all'Avviso n. 03/2022 pubblicato dall'Agenzia per la Cybersicurezza Nazionale per la presentazione di proposte di interventi di potenziamento della resilienza cyber, disponendo di presentare le due proposte di interventi sopra esposte di potenziamento della resilienza cyber, ha demandato alla Direzione regionale Competitività del Sistema Regionale, Settore "Sistema Informativo Regionale" e Settore "Servizi Infrastrutturali e Tecnologici" l'adozione degli atti e dei provvedimenti necessari per l'attuazione della deliberazione stessa, in particolare, la cura degli adempimenti formali

connessi alla partecipazione all'avviso, nonché l'eventuale rimodulazione tecnica delle proposte al fine di allinearle all'esito delle istruttorie ed ai relativi stanziamenti dei fondi;

in ottemperanza alla Deliberazione n. 6-5680 del 27 settembre 2022, con invio tramite posta elettronica certificata, è stata inoltrata in data 29 settembre 2022 all'Agenzia per la Cybersicurezza Nazionale la richiesta formale di presentazione delle due proposte di partecipazione a firma del Presidente della Regione Piemonte, Alberto Cirio, allegando i due progetti sopra descritti;

con determina dell'Agenzia per la Cybersicurezza Nazionale prot. n. 31275 del 20 dicembre 2022, avente ad oggetto *«Avviso pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane e delle Province autonome a valere sul PNRR, Missione 1 – Componente 1 – Investimento 1.5 «Cybersecurity» - Codice d'investimento «M1C1I1.5». Determina di ammissione ed esclusione delle istanze pervenute*, si indicava l'ammissione al prosieguo della valutazione di n. 76 istanze, comprendendo le due inviate da Regione Piemonte;

con determinazione dell'Agenzia per la Cybersicurezza Nazionale prot. n. 3429 del 20 gennaio 2023 (rettificata con Determinazione prot. ACN n .7591 del 23 febbraio 2023) *Avviso Pubblico n. 03/2022 per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane e delle Province autonome a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" – Codice "d'investimento M1C1I1.5". Determina per l'approvazione della graduatoria finale e di destinazione delle risorse delle proposte progettuali ammesse e totalmente finanziabili (Allegato A), proposte progettuali ammesse e parzialmente finanziabili (Allegato B), proposte progettuali idonee ma non finanziabili (Allegato C), elenco delle proposte progettuali non ammesse (Allegato D),* l'Agenzia per la Cybersicurezza Nazionale approvava la graduatoria definitiva a valere sull'Avviso n.3/2022, dalla quale si evinceva che entrambi i progetti presentati da Regione Piemonte risultavano nell'elenco delle proposte progettuali ammesse e totalmente finanziabili;

con Determinazione prot. ACN n. 7591 del 23 febbraio 2023 dell'Agenzia per la Cybersicurezza Nazionale viene rettificata la determinazione prot. n. 3429 del 20 gennaio 2023, confermando comunque la presenza nella graduatoria definitiva a valere sull'Avviso n.3/2022 di entrambi i progetti presentati da Regione Piemonte quali proposte progettuali ammesse e totalmente finanziabili;

con invio tramite posta elettronica certificata in data 17 febbraio 2023, Regione Piemonte ha trasmesso il documento "Atto d'Obbligo" a firma del Presidente della Regione Piemonte, che, contestualmente all'accettazione del finanziamento concesso dall'Agenzia per la Cybersicurezza Nazionale, impegna l'Ente alla realizzazione e completamento dei due progetti "Postazioni di lavoro e rete regionale; l'evoluzione in sicurezza" e "Transizione digitale e servizi sicuri", secondo i requisiti e i vincoli previsti dall'Avviso n. 3 sopra citato;

con invio tramite posta elettronica certificata in data 24/02/2023, Regione Piemonte ha trasmesso

- il documento "COMUNICAZIONE AVVIO ATTIVITÀ E/O RICHIESTA DI ANTICIPAZIONE" a firma del Dirigente del Settore "Sistema Informativo" A1911A" nel quale si attestava che le attività relative al progetto "Transizione digitale e servizi sicuri" sono state avviate in data 22/02/2023, in conformità con le indicazioni dell'Avviso Pubblico di riferimento;
- il documento "RICHIESTA MODIFICA PROGETTO" a firma del Dirigente del Settore

"Sistema Informativo" A1911A" nel quale si adegua il cronoprogramma del progetto "Transizione digitale e servizi sicuri" in base alla variazione della data di avvio dovuta alle tempistiche di approvazione del progetto in oggetto da parte di ACN, variazioni che non comportano una modifica sostanziale del progetto;

con comunicazione via PEC in data 17/04/2023, prot. del Settore n. 4214/2023, ACN ha approvato la richiesta di modifica progetto e quindi del nuovo cronoprogramma;

con invio tramite posta elettronica certificata in data 06/12/2023, Regione Piemonte ha trasmesso il documento "RICHIESTA MODIFICA PROGETTO" a firma del Dirigente del Settore "Sistema Informativo" A1911A" nel quale, al fine di migliorare il dispiegamento dei servizi inclusi nell'intervento 3B del progetto "Transizione digitale e servizi sicuri", si adegua il cronoprogramma di tale intervento, portandone la conclusione al terzo quarto del 2024; tale ripianificazione non comporta una modifica sostanziale del progetto;

Considerato che

l'importo complessivo dei due progetti ("Postazioni di lavoro e rete regionale; l'evoluzione in sicurezza", affidato al Settore A1910, e "Transizione digitale e servizi sicuri", affidato al settore A1911), finanziati da ACN a valere sull'Avviso 3/22 per un totale di Euro 1.979.500,00, prevede una spesa di Euro 1.272.750,00 per l'anno 2023 e Euro 706.750,00 per l'anno 2024;

Considerato inoltre che

- il progetto denominato "TRANSIZIONE DIGITALE E SERVIZI SICURI", inserito e finanziato a valere sulle risorse PNRR, dell'importo complessivo di € 995.100,00, prevede al suo interno differenti iniziative, volte alla messa in sicurezza dei servizi digitali; prevede l'analisi di vulnerabilità e la pianificazione/realizzazione di interventi di mitigazione del rischio di un portafoglio composto dai servizi applicativi più rilevanti per la Regione. Il progetto contempla la definizione delle strategie tecnico- organizzative e la predisposizione del piano di continuità operativa previsto dalla norma ISO 22301:2019. Si prevede anche in questo ambito di realizzare azioni di rafforzamento delle conoscenze e delle pratiche del personale regionale in termini di sicurezza nella gestione dei dati e dei servizi digitali erogati all'utenza, di erogare servizi ICT compositi e integrati atti a garantire la funzionalità del sistema informativo regionale e il suo adeguamento alle norme e disposizioni locali e nazionali, secondo i paradigmi della digitalizzazione nell'ambito PA;
- con determinazione dirigenziale 200/A1911A/2023 del 15 maggio 2023 è stata approvata la PTE di iniziativa "ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI" che prevede i seguenti interventi:
  - intervento 1A – Postura della sicurezza applicativi perimetro regionale
  - intervento 1B – Individuazione e analisi vulnerabilità su perimetro applicativi prefissato e piano di remediation
  - intervento 2A – Revisione/integrazione delle procedure e policy
  - intervento 2B – Business Impact Analysis a supporto della continuità operativa
  - intervento 3A – Security awareness e formazione
  - intervento 4A – Realizzazione degli strumenti analisi vulnerabilità filiera automation ed interventi mitigazione
  - intervento 4B – Evoluzione piattaforma di identità digitale
- nella determinazione sopra citata è stato affidato secondo quanto definito dalla "Convenzione quadro per gli affidamenti diretti al CSI Piemonte per la prestazione di servizi in regime di esenzione IVA", per il periodo 1 gennaio 2022 – 31 dicembre 2026, approvata con deliberazione di Giunta regionale n. 21-4474 del 29 dicembre 2021 il solo intervento 4B –

Evoluzione piattaforma di identità digitale, risulta quindi necessario provvedere all'attivazione di un ulteriore parte dell'attività progettuale;

- con successiva determinazione dirigenziale 393/A1911A/2023 del 26 settembre 2023 venivano affidati, inoltre al CSI Piemonte, i servizi relativi agli interventi:

- 1A - Postura della sicurezza applicativi perimetro regionale
- 2A - Revisione/integrazione delle procedure e policy
- 2B - Business Impact Analysis a supporto della continuità operativa
- 4A - Realizzazione degli strumenti analisi vulnerabilità filiera automation ed interventi mitigazione

relativi all' iniziativa "ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI";

- risultano quindi ancora da affidare gli interventi

- 1B – Individuazione e analisi vulnerabilità su perimetro applicativi prefissato e piano di remediation
- 3A – Security awareness e formazione

Richiamato

- l'art. 26 della legge 23 dicembre 1999, n° 488 che ha affidato al Ministero dell' Economia e delle Finanze (MEF) il compito di stipulare Convenzioni con le quali il fornitore prescelto, nel rispetto delle vigenti normative per la scelta del contraente, si impegna ad accettare Ordinativi di Fornitura deliberati dalle Pubbliche Amministrazioni individuate dall'art. 1 del D.lgs. n. 165/2001, e che le predette amministrazioni utilizzano la Convenzione sino a concorrenza dell'importo massimo complessivo stabilito dalla Convenzione medesima ed ai prezzi e condizioni ivi previsti, fermo restando quanto previsto dall'art. 1, comma 449, della legge

- l'articolo 2, comma 225, Legge 23 dicembre 2009, n. 191, consente a Consip S.p.A. di concludere Accordi Quadro a cui le Stazioni Appaltanti, possono fare ricorso per l' acquisto di beni e di servizi;

Considerato che

- Consip S.p.A. ha attivato l'iniziativa "Sicurezza da remoto", che è stata bandita ai sensi dell'art. 4, comma 3 quater del d.l. 95/2012, ove Consip S.p.a. svolge altresì le attività di centrale di committenza relative alle Reti telematiche delle pubbliche amministrazioni, al Sistema pubblico di connettività ai sensi del decreto legislativo 7 marzo 2005, n. 82, e alla Rete internazionale delle pubbliche amministrazioni ai sensi del decreto medesimo nonché ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311.

- Tale iniziativa si affianca alle gare strategiche ai fini dell'attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione nelle versioni 2018-2020 e successive, nell'attuazione del processo di trasformazione digitale del Paese.

- L'Accordo Quadro "ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni – Lotto 1", incardinato in questa iniziativa, prevede una modalità di affidamento dei Contratti Esecutivi, tramite ordinativo di fornitura a condizioni tutte fissate; a tal fine è disponibile la documentazione necessaria per le attività di definizione del "Piano dei fabbisogni" e successivo "Piano Operativo". Si compone di due Lotti uno dedicato ai servizi di sicurezza e l'altro a quello di compliance di controllo.

- L'Accordo Quadro relativo al Lotto 1 CIG 88846293CA, dedicato ai Servizi di Sicurezza da Remoto, è stato aggiudicato in via definitiva ed efficace in data 24/05/2022, laddove il relativo

contratto con il fornitore aggiudicatario è stato stipulato il 04/08/2022; l'Accordo Quadro di cui trattasi è pertanto attivo dal 26/09/2022 ed ha durata complessiva di 24 mesi.

I fornitori aggiudicatari del Lotto 1 di interesse sono, per le Pubbliche Amministrazioni Locali (PAL), il RTI così costituito:
- **Accenture S.p.A.**, sede legale in Milano, Via Privata Nino Bonnet n. 10, capitale sociale Euro 1.843.248,60, iscritta al Registro delle Imprese di Milano-Monza-Brianza-Lodi al n. MI-1652886, 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, capitale sociale Euro 12.000.000,00, iscritta al Registro delle Imprese di Milano-Monza-Brianza-Lodi al n. MI-1591912, P. IVA 12878470157;
- **Fincantieri NextTech S.p.A.**, con sede legale in Milano, Via Carlo Ottavio Cornaggia n. 10, capitale sociale Euro 12.000.000,00, iscritta al Registro delle Imprese di Milano-Monza-Brianza-Lodi al n. MI-2073993, P. IVA 00890740111;
- **DEAS- Difesa e Analisi Sistemi S.p.A.**, con sede legale in Roma Via della Colonna Antonina n. 46, capitale sociale Euro 150.000,00, iscritta al Registro delle Imprese di Roma al n. RM-1558212, P. IVA 14961281004
giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott.ssa Paola Cardelli repertorio n. 27351 del 10 marzo 2022;

Dato atto che, ai sensi dell'art. 226, comma 2, d. Lgs 36/2023 del Nuovo Codice dei Contratti Pubblici, rubricato "abrogazioni e disposizioni finali ", viene espressamente disposto che"le disposizioni di cui al decreto legislativo n. 50 del 2016 continuano ad applicarsi esclusivamente ai procedimenti in corso. A tal fine, per procedimenti in corso si intendono: a) 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;"

Preso atto che l'accordo quadro tra CONSIP S.p.A. e il RTI costituito dalle azienda Accenture S.p.A., Fincantieri Nextech S.p.A., Fasteweb S.p.A., Deas, Difesa e Analisi Sistemi S.p.A. è stato stipulato e sottoscritto a seguito di procedura avviata nell'anno 2019, prima dell'entrata in vigore del Nuovo Codice (D.Lgs. 36/2023) in vigore dal 01.07.2023, per l'affidamento dei singoli contratti esecutivi valgono le disposizioni del precedente Codice dei Contratti Pubblici, D.Lgs. 50/2016 s.m.i.;

Tenuto conto che rispetto all'iniziativa "ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI" risulta ancora da affidare l'intervento "3A – Security awareness e formazione";

Rilevato che nell'Accordo Quadro Accordo Quadro ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni" è presente il servizio denominato "L1.S9 - Servizio di Formazione e Security awareness"; esso offre un programma di formazione in modalità e-learning, che garantisce lo sviluppo graduale della conoscenza delle minacce cyber attraverso un approccio maggiormente inclusivo ed innovativo, integrando le lezioni e-learning con brevi filmati, casi d'uso, gaming, percorsi di apprendimento con premialità al raggiungimento degli obiettivi formativi. Questo processo di apprendimento è pensato per mantenere nel tempo le conoscenze acquisite e fornire un costante aggiornamento sull'evoluzione delle minacce, con un approccio verso l'utente più dinamico ed integrato.

Tenuto altresì conto

- che il Lotto 1 dell'Accordo Quadro "ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e

Controllo per le Pubbliche amministrazioni – Lotto 1" stipulato, ai sensi dell'art. 54, comma 4, lett. a) D.Lgs. 50/2016 allora vigente, dalla Consip S.p.A. con il RTI Accenture S.p.A., Fincantieri Nextech S.p.A., Fasteweb S.p.A., Deas, Difesa e Analisi Sistemi S.p.A., include i servizi necessari per gli scopi che si prefigge di raggiungere questa Amministrazione attraverso l'iniziativa "ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI", intervento "3A – Security awareness e formazione"; essi sono quelli previsti nel finanziamento afferente al progetto denominato "Transizione digitale e servizi sicuri" ed affidato al Settore A1911A, intervenendo sull'aspetto del progetto riguardante l'"aumento della security awareness", cioè il livello di consapevolezza dei rischi di sicurezza cui sono esposti gli utenti della PA. Saranno rafforzate le competenze e le pratiche del personale, con un focus sulla gestione dei dati e dei servizi erogati"; Regione Piemonte ritiene infatti che la formazione dei dipendenti su tematiche di cyber security è uno degli aspetti fondamentali per sensibilizzare il personale delle PA sulle tematiche inerenti alla sicurezza delle informazioni ed evitare che comportamenti non adeguati dei singoli soggetti possano compromettere la sicurezza dell'intero sistema.

- delle Modalità di adesione all'Accordo Quadro che prevedono le seguenti fasi:
  1. l'inoltro del Piano dei Fabbisogni al fornitore
  2. l'accettazione del Piano Operativo da parte del Fornitore
  3. la sottoscrizione di un contratto esecutivo tra le parti

- che tutto l'iter amministrativo sarà gestito tramite scambio di PEC, come previsto nell'Accordo quadro "ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni – Lotto 1" stesso;

- che il Settore Sistema Informativo Regionale ha inoltrato, mediante invio PEC, nostro protocollo 15672/2023 del 11/12/2023 il Piano dei Fabbisogni, contenente le esigenze e i servizi che si intendono attivare, gli obiettivi che l'ente si prefigge di raggiungere, i benefici conseguenti all'attivazione, gli elementi qualitativi e quantitativi dei servizi e la pianificazione degli stessi.

- che tali obiettivi vengono tradotti nel Piano dei Fabbisogni inviato da Regione Piemonte utilizzando i servizi previsti nell'Accordo Quadro denominati "L1.S9 – FORMAZIONE E SECURITY AWARENESS", e precisamente:

- "Formazione 1": una formazione di livello medio base per la totalità dei dipendenti Regionali (stimata in 2450) unità, della durata di 9 mesi, finanziato attraverso i fondi stanziati dall'Avviso 3/2022 a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 per il progetto "Transizione digitale e servizi sicuri",
- "Formazione 2": una ulteriore formazione a livello avanzato per dipendenti con ruoli di responsabilità e incarichi affini a tematiche evolute di cybersicurezza (stimata in 245 unità), della durata di 15 mesi, finanziato con fondi Regionali

Verificato che il Piano Operativo trasmesso dal forniture Accenture e assunto agli atti del Settore con prot. 15907/2023 del 14/12/2023 soddisfa le necessità dell'Amministrazione e che lo stesso prevede:

- la seguente distribuzione delle attività a carico delle singole aziende componenti l'RTI:

Azienda RTI	**Percentuale attività**
Accenture	99,01%
Fasweb	0,33%
Fincantieri	0,33%
DEAS	0,33%

- il seguente quadro economico di riferimento:

Azienda RTI	**Totale "Formazione 1"**	**Totale "Formazione 2"**	**Totali**
Accenture	€ 59.899,84	€ 15.346,24	€ 75.246,08
Fasweb	€ 0,00	€ 247,52	€ 247,52
Fincantieri	€ 0,00	€ 247,52	€ 247,52
DEAS	€ 0,00	€ 247,52	€ 247,52
Totali	€ 59.899,84	€ 16.088,80	€ 75.988,64

per complessivi € 75.988,64, IVA esente ai sensi del combinato disposto dell'art. 10 del D.P.R. 633/72 e dell'art. 14 della Legge 537/93;

Dato atto che:

- come previsto dall'art. 29 del Accordo Quadro "ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni – Lotto 1", 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. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010;

- le Amministrazioni Beneficiarie sono tenute, pertanto, 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.
- il valore complessivo del presente affidamento è pari ad € 75.988,64, e di conseguenza il valore del contributo dovuto dall'Amministrazione Beneficiaria Regione Piemonte verso Consip S.p.A. ammonta ad € 607,91;
- le modalità operative di pagamento del predetto contributo sono rese note alle Amministrazioni contraenti a mezzo di apposita comunicazione sul sito internet della Consip S.p.A. (www.consip.it);
- detto contributo è considerato fuori campo dell'applicazione dell'IVA, ai sensi dell'art.2 del D.P.R. 633 del 1972 e pertanto non è prevista nessuna emissione di fattura. Gli stessi non rientrano inoltre nell'ambito di applicazione della tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136.

Ritenuto opportuno, alla luce di quanto sopra esposto, procedere all'attivazione dell'Accordo Quadro "ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni – Lotto 1", per la realizzazione dei sottoelencati obiettivi, a cui corrispondono i relativi servizi inclusi nell'AQ medesimo, per una spesa complessiva di € 75.988,64 esente IVA;

Col presente atto, pertanto, si intende:

- approvare il Piano Operativo trasmesso dal RTI Accenture S.p.A./Fastweb S.p.A./Fincantieri NextTech S.p.A./DEAS- Difesa e Analisi Sistemi S.p.A., assunto al protocollo del Settore al n.15907/2023 del 14/12/2023 ed allegato alla presente, contenente gli obiettivi definitivi dall'Amministrazione nel proprio Piano dei Fabbisogni, il cronoprogramma delle attività, le modalità di esecuzione e di erogazione dei servizi;

- approvare la bozza di Contratto esecutivo, allegato alla presente e redatto sulla base del template messo a disposizione da Consip, contenente le condizioni generali di realizzazione dei servizi;
- affidare al RTI Accenture S.p.A./Fastweb S.p.A./Fincantieri NextTech S.p.A./DEAS- Difesa e Analisi Sistemi S.p.A., nell'ambito del "ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni – Lotto 1", la realizzazione dei servizi "L1.S9 – FORMAZIONE E SECURITY AWARENESS" nelle modalità sopra definite;
- accertare la somma di Euro 59.899,84 sul capitolo in entrata 20495, Tipologia 200: Contributi agli investimenti, Categoria 4020100 – Contributi agli investimenti da amministrazioni pubbliche, sul capitolo 20495 del Bilancio Finanziario Gestionale 2023-2025, annualità 2024, p.d.c. E.4.02.01.01.001;
- impegnare, contestualmente, la somma complessiva di € 75.988,64 IVA esente, a favore dei singoli componenti del RTI, secondo le relative quote di competenza, desunte dai documenti contrattuali in esame (così come indicate nel Piano Operativo e confermate dalla capogruppo mandataria con nota assunta al prot. n.16007/A1911A/2023 del 18/12/2023) come nel seguito indicato:

sul capitolo di spesa 207164 (Missione 01, Programma 0112), l'importo complessivo di Euro 59.899,84 IVA esente del bilancio finanziario gestionale 2023-2025, annualità 2024 - P.d.C. U.2.02.03.02.001 - a favore di Accenture S.p.A. - codice beneficiario 73660;

sul capitolo di spesa 106601 del Bilancio finanziario gestionale 2023-2025, annualità 2024 (Missione 01 Programma 0110 - P.d.C. U.1.03.02.04.999) l'importo complessivo di Euro 16.088,80, secondo la seguente modalità:

Impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano di Euro 15.346,24 IVA esente a favore di Accenture S.p.A. - codice beneficiario 73660

Impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano di Euro € 247,52 IVA esente a favore di Fastweb S.p.A. - codice beneficiario 96711

Impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano di Euro € 247,52 IVA esente a favore di Fincantieri NextTech S.p.A. - codice beneficiario 385478

Impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano di Euro € 247,52 IVA esente a favore di DEAS - Difesa e Analisi Sistemi S.p.A. - codice beneficiario 385479

- impegnare, la somma complessiva di € 607,91 fuori campo applicazione Iva, del Bilancio finanziario gestionale 2023-2025, annualità 2024, a favore di Consip S.p.a. (codice beneficiario 379908), mediante impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano (Missione 01 Programma 0110 - P.d.C. U.1.03.02.04.999) quale 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.

Dato atto che:

- all'intervento in oggetto, tramite procedura online del Comitato Interministeriale per la Programmazione Economica, è stato assegnato il Codice Unico di progetto di investimento

Pubblico (CUP) J14F22001120006;

- l’accertamento è assunto con il presente provvedimento sul Capitolo 20495/2023 del Bilancio Finanziario Gestionale 2023-2025 - P.d.C E.4.02.01.01.000 e trattasi di natura non ricorrente.
- l’entrata che si accerta con il presente provvedimento è vincolata al finanziamento della spesa relativa a “ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI. Affidamento dei servizi relativi all’Intervento 3B – CUP: J14F22001120006”, che viene registrata contestualmente all'impegno (riferimento numero codice progetto 2023/22).

L’accertamento non è stato già assunto con precedenti atti.

Dato atto, inoltre, che:

- i suddetti impegni sono assunti nei limiti delle risorse stanziate ed autorizzate sulla dotazione finanziaria dei competenti capitoli di spesa del Bilancio Finanziario Gestionale 2023-2025;
- i suddetti impegni sono assunti secondo il principio della competenza finanziaria di cui al D.Lgs. n. 118/2011 e.sm.i. (allegato n. 4.2) e la relativa obbligazione è esigibile nell'esercizio 2024;
- trattasi di spesa non ricorrente;
- la competenza economica coincide con quella finanziaria;

- gli impegni sono relativi a risorse di derivazione statale (Codice progetto 2023/22)

- il programma dei pagamenti è compatibile con il relativo stanziamento di bilancio, secondo quanto previsto dall'art. 56, comma 6 del D.Lgs. n. 118/2011 e s.m.i. e dall'art. 27 del Regolamento regionale di contabilità n. 9/2021
- il presente provvedimento non determina oneri impliciti per il bilancio regionale.

Attestata la regolarità amministrativa del presente provvedimento ai sensi della DGR n. 1-4046 del 17/10/2016, come modificata dalla DGR 1-3361 del 14 giugno 2021.

IL DIRIGENTE

Richiamati i seguenti riferimenti normativi:

- Legge n. 241 del 7 agosto 1990 e successive modifiche e integrazioni, "Norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- D.Lgs. n. 165 del 30 marzo 2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";
- D.Lgs. n. 118 del 23 giugno 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 articoli 1 e 2 della legge 5 maggio 2009, n. 42 " e smi;
- Legge n. 190 del 6 novembre 2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione;
- D.Lgs. n. 33 del 14 marzo 2013 "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- D.Lgs. n. 82 del 7 marzo 2005 "Codice dell'Amministrazione Digitale" e s.m.i.;
- D.Lgs. n. 36 del 31 marzo 2023 "Codice dei contratti pubblici";
- D.Lgs. n. 50 del 30 giugno 2016 "Codice degli appalti pubblici e dei contratti di concessione" e s.m.i., in quanto compatibile;
- Legge regionale n. 23 del 28 luglio 2008 "Disciplina dell'organizzazione degli uffici regionali e disposizioni concernenti la dirigenza ed il personale" e s.m.i.;

- Legge regionale n. 9 del 26 marzo 2009 "Norme in materia di pluralismo informatico sull'adozione e la diffusione del software libero e sulla portabilità dei documenti informatici nella pubblica amministrazione";
- D.G.R. n.3 - 6447 del 31 gennaio 2023 "Approvazione del Piano Integrato di Attività e Organizzazione (PIAO) della Giunta regionale del Piemonte per gli anni 2023- 2025 e della tabella di assegnazione dei pesi degli obiettivi dei Direttori del ruolo della Giunta regionale per l'anno 2023" dando atto che nel PIAO è confluito il Piano Triennale di prevenzione della Corruzione e della Trasparenza;
- Regolamento n. 9 del 16 luglio 2021 " Regolamento regionale di contabilità della Giunta regionale. Abrogazione del regolamento regionale 5 dicembre 2001, n. 18";
- DGR n. 38-6152 del 2 dicembre 2022 "Approvazione linee guida per le attività di ragioneria relative al controllo preventivo sui provvedimenti dirigenziali. Revoca allegati A, B, D della dgr 12-5546 del 29 agosto 2017;
- Legge regionale n. 5 del 24 aprile 2023 "Disposizioni per la formazione del bilancio annuale di previsione 2023-2025 (Legge di stabilità regionale 2023)";
- Legge regionale n. 6 del 24 aprile 2023 "Bilancio di previsione finanziario 2023-2025";
- DGR n.1-6763 del 27 aprile 2023 "Legge regionale 24 aprile 2023, n. 6 "Bilancio di previsione finanziario 2023-2025". Approvazione del Documento Tecnico di Accompagnamento e del Bilancio Finanziario Gestionale 2023-2025";
- D.G.R. 20 dicembre 2018, n. 35-8188 "Nomina del Responsabile della transizione alla modalita' operativa digitale della Regione, ai sensi dell'art. 17, commi 1 e 1 ter, del decreto legislativo 82/2005 (Codice Amministrazione Digitale)";
- Legge 13 agosto 2010 n. 136 "Piano straordinario contro le mafie, nonché delega al Governo in materia di normativa antimafia";
- D.Lgs. 1 dicembre 2009, n. 177, come disciplinato dal D.P.C.M. 23 giugno 2010;

determina

per le considerazioni di cui alla premessa, che interamente si richiamano:

- di dare atto che CONSIP S.p.A., a seguito di pubblicazione di specifico Bando di Gara, ha stipulato in data 04/08/2022 ai sensi dell’art. 54 comma 4 lett. a) del D.Lgs. 50/2016, un Accordo Quadro “ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni – Lotto 1” con il fornitore individuato: RTI Accenture S.p.A./Fastweb S.p.A./Fincantieri NextTech S.p.A./DEAS- Difesa e Analisi Sistemi S.p.A.;

- di dare atto che, in virtù del fatto che l’accordo quadro tra CONSIP S.p.A. e il RTI costituito è stato stipulato e sottoscritto antecedentemente alla data di entrata in vigore del nuovo Codice degli Appalti, avvenuta con D.Lgs. 36/2023 in vigore dal 01.07.2023, per l’affidamento di cui al presente provvedimento valgono le disposizioni del precedente Codice dei Contratti, D.Lgs. 50/2016 s.m.i.;

- di aderire per le motivazioni indicate in premessa che interamente si richiamano, all’Accordo Quadro “ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni – Lotto 1” indicato al punto precedente, per la realizzazione dei obiettivi sopra esposti, mediante la fornitura dei servizi “L1.S9 – FORMAZIONE E SECURITY AWARENESS”, e precisamente:

- “Formazione 1”: una formazione di livello medio base per la totalità dei dipendenti Regionali (stimata in 2450) unità, della durata di 9 mesi, finanziato attraverso i fondi stanziati dall’Avviso 3/2022 a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” M1C1I1.5 per il progetto “Transizione digitale e servizi sicuri”,
- “Formazione 2”: una ulteriore formazione a livello avanzato per dipendenti con ruoli di responsabilità e incarichi affini a tematiche evolute di cybersicurezza (stimata in 245 unità), della durata di 15 mesi, finanziato con fondi Regionali

per gli importi ivi indicati:

Azienda RTI	**Totale “Formazione 1”**	**Totale “Formazione 2”**	**Totali**
Accenture S.p.A.	€ 59.899,84	€ 15.346,24	€ 75.246,08
Fastweb S.p.A.	€ 0,00	€ 247,52	€ 247,52
Fincantieri NextTech S.p.A.	€ 0,00	€ 247,52	€ 247,52
DEAS- Difesa e Analisi Sistemi S.p.A.	€ 0,00	€ 247,52	€ 247,52
Totali	€ 59.899,84	€ 16.088,80	€ 75.988,64

per complessivi € 75.988,64, esenti IVA;

- di approvare, con il presente atto, **il Piano Operativo** (trasmesso dal Fornitore e assunto agli atti del Settore con prot. n. 15907/2023 del 14/12/2023) ed allegato alla presente, contenente gli obiettivi definitivi dall’Amministrazione nel proprio Piano dei Fabbisogni, il cronoprogramma delle attività, le modalità di esecuzione e di erogazione dei servizi;

- di approvare la **bozza di Contratto esecutivo** allegato al presente atto;

- di dare atto che all’intervento relativo al progetto denominato “TRANSIZIONE DIGITALE E SERVIZI SICURI”, inserito e finanziato a valere sulle risorse PNRR, dell’importo complessivo di € 995.100,00, è stato assegnato il seguente il Codice Unico di Progetto di investimento pubblico CUP J14F22001120006;

- di accertare la somma di Euro 59.899,84 sul capitolo in entrata 20495, Tipologia 200: Contributi agli investimenti, Categoria 4020100 – Contributi agli investimenti da amministrazioni pubbliche, come segue:

Euro 59.899,84 sul capitolo 20495 del Bilancio Finanziario Gestionale 2023-2025, annualità 2024, p.d.c. E.4.02.01.01.001;

la cui transazione elementare è riportata nell'Appendice A "Elenco registrazioni contabili", facente parte integrante formale e sostanziale del presente provvedimento.
Il soggetto versante è l'Agenzia per la Cybersicurezza Nazionale (C.F.: 96501130585) - codice versante 382090;

- di affidare l’ “intervento 3A – Security awareness e formazione” dell’ iniziativa “ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI” al RTI Accenture S.p.A./Fastweb

S.p.A./Fincantieri NextTech S.p.A./DEAS- Difesa e Analisi Sistemi S.p.A., nell'ambito del AQ "ID 2296 – Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche amministrazioni – Lotto 1", per la realizzazione dei servizi "L1.S9 – FORMAZIONE E SECURITY AWARENESS" come definiti nel Piano Operativo;

- di impegnare a favore dei singoli componenti del RTI, secondo le relative quote di competenza, desunte dai documenti contrattuali in esame (così come indicate nel Piano Operativo e confermate dalla capogruppo mandataria Accenture S.p.a. con nota assunta al prot. n. 16007/A1911A/2023 del 18/12/2023), come nel seguito indicato, la somma complessiva di € 75.988,64 IVA esente:

- impegno di Euro 59.899,84 iva esente sul cap. 207164 del Bilancio Finanziario Gestionale 2023 - 2025, annualità 2024 - P.d.C. U.2.02.03.02.001 a favore di Accenture S.p.A. - Via Privata Nino Bonnet n. 10, Milano - C.F. e P.IVA 13454210157 (codice beneficiario 73660);
- impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano di Euro 15.346,24 esente IVA sul capitolo 106601/2024 del Bilancio Finanziario Gestionale 2023 - 2025, annualità 2024 - P.d.C. U.1.03.02.04.999 a favore di Accenture S.p.A. - Via Privata Nino Bonnet n. 10, Milano - C.F. e P.IVA 13454210157 (codice beneficiario 73660);
- impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano di Euro 247,52 esente IVA sul capitolo 106601/2024 del Bilancio Finanziario Gestionale 2023 - 2025, annualità 2024 - P.d.C. U.1.03.02.04.999 a favore di Fastweb S.p.A (codice beneficiario 96711);
- impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano di Euro 247,52 esente IVA sul capitolo 106601/2024 del Bilancio Finanziario Gestionale 2023 - 2025, annualità 2024 - P.d.C. U.1.03.02.04.999 a favore di Fincantieri NextTech S.p.A. (codice beneficiario 385478);
- impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano di Euro 247,52 esente IVA sul capitolo 106601/2024 del Bilancio Finanziario Gestionale 2023 - 2025, annualità 2024 - P.d.C. U.1.03.02.04.999 a favore di DEAS- Difesa e Analisi Sistemi S.p.A. (codice beneficiario 385479);

- di effettuare impegno delegato Direzione A1000A - DIREZIONE DELLA GIUNTA REGIONALE Settore A1007E - Sviluppo e Capitale umano Euro 607,91 fuori campo applicazione IVA sul capitolo 106601/2024 del Bilancio Finanziario Gestionale 2023 - 2025, annualità 2024 - P.d.C. U.1.03.02.04.999 a favore di Consip S.p.A. (codice beneficiario 379908) in assolvimento del 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;

le cui transazioni elementari sono riportate nell'Appendice A "Elenco registrazioni contabili", facente parte integrante formale e sostanziale del presente provvedimento;

- di dare atto che i pagamenti a favore del RTI saranno soggetti alla disciplina dell'art. 3 Legge n. 136/2010, così come modificata dal D.L. n. 187/2010 convertito con Legge n. 217/2010 (Tracciabilità dei flussi finanziari) e che al presente affidamento è stato assegnato il CIG derivato A03A642A24;

- di prendere atto della regolarità contributiva dei componenti il RTI come da DURC indicati in seguito:

- Accenture S.p.A. Numero Protocollo INAIL_40557778, data richiesta 02/10/2023, scadenza validità 30/01/2024;
- Fastweb S.p.A. Numero Protocollo INPS_37834413, data richiesta 29/09/2023, scadenza validità 27/01/2024;
- Fincantieri NextTech S.p.A. Numero Protocollo INPS_37960010, data richiesta 09/10/2023,

scadenza validità 06/02/2024;
- DEAS- Difesa e Analisi Sistemi S.p.A. Numero Protocollo INAIL_40422750, data richiesta 24/09/2023, scadenza validità 22/01/2024

- di individuare il funzionario regionale Dott. Domenico Festa quale Direttore Esecutivo del Contratto, ai sensi dell'art. 111, comma 2 D.Lgs. 50/2016 e del Decreto 7 Marzo 2018, n. 49 del Ministero delle Infrastrutture e dei Trasporti "Regolamento recante: «Approvazione delle linee guida sulle modalità di svolgimento delle funzioni del direttore dei lavori e del direttore dell'esecuzione», in quanto compatibili;

- di dare atto che il Responsabile Unico del Procedimento è il Dott. Giorgio CONSOL, Responsabile del Settore Sistema Informativo Regionale A1911A;

- di attestare l'avvenuta verifica dell'insussistenza, anche potenziale, di situazioni di conflitto di interesse, così come risulta dalle allegate dichiarazioni agli atti del fascicolo istruttorio;

La presente determinazione sarà pubblicata sul B.U.R.P., ai sensi dell'art. 61 dello Statuto e dell'art. 5 della L.R. 22/2010, nonché ai sensi dell'articolo 23, comma 1, lett. b) e dell'art. 37 del D.Lgs. 33/2013 sul sito di Regione Piemonte, sezione "Amministrazione trasparente":
Contraenti:
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
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
DEAS- Difesa e Analisi Sistemi S.p.A., con sede legale in Milano, Piazza degli Affari n.3, P. IVA 14961281004

Importo: Euro 75.988,64 IVA Esente
Responsabile del Procedimento: Dott. Giorgio CONSOL
Modalità individuazione contraenti: Affidamento tramite adesione ad Accordo Quadro Consip

Avverso la presente determinazione è possibile ricorrere al Tribunale Amministrativo regionale entro 30 giorni dalla data di comunicazione o piena conoscenza dell'atto, secondo quanto previsto all'art. 120 del Decreto legislativo n. 104 del 2 luglio 2010 (Codice del processo amministrativo).

IL DIRIGENTE (A1911A - Sistema informativo regionale)
Firmato digitalmente da Giorgio Consol

Si dichiara che sono parte integrante del presente provvedimento gli allegati riportati a seguire [1], archiviati come file separati dal testo del provvedimento sopra riportato:

1. ID_2296__Schema_di_Contratto_Esecutivo_RegionePiemonte.pdf
2. RegionePiemonte_AQSEC-2296L1-Piano_Operativo_v_Livello1.pdf — Allegato

1 L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento

REGIONE PIEMONTE

CONTRATTO ESECUTIVO – LOTTO 1SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI (ID 2296)

CIG: 88846293CA

CIG "derivato": A03A642A24

INDICE

CONTRATTO ESECUTIVO

TRA

Regione Piemonte, con sede in Torino, Piazza Piemonte, 1, C.F. 80087670016, in persona del Dott. Giorgio CONSOL, Dirigente del Settore Sistema Informativo Regionale – Direzione Competitività del Sistema Regionale (nel seguito per brevità anche "**Amministrazione**")

E

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, i P. IVA 12878470157; - **Fincantieri NextTech S.p.A.**, con sede legale in Milano, Via Carlo Ottavio Cornaggia n. 10, P. IVA 00890740111; - **DEAS- Difesa e Analisi Sistemi S.p.A.**, con sede legale in Milano, Piazza degli Affari n.3, P. IVA 14961281004, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott.ssa Paola Cardelli repertorio n. 27351 del 10 marzo 2022; (nel seguito per brevità congiuntamente anche "Fornitore" o "Impresa)

PREMESSO CHE

(A) l'art. 4, comma 3-quater, del D.L. n. 95/2012, come convertito con modificazioni dalla Legge n. 135/2012, ha stabilito che Consip S.p.A. svolge altresì le attività di centrale di committenza relativamente "ai contratti-quadro ai sensi dell'articolo 1, comma 192, della legge 30 dicembre 2004, n. 311";

(B) L'articolo 2, comma 225, Legge 23 dicembre 2009, n. 191, consente a Consip S.p.A. di concludere Accordi Quadro a cui le Stazioni Appaltanti, possono fare ricorso per l'acquisto di beni e di servizi.

(C) Peraltro, l'utilizzazione dello strumento dell'Accordo Quadro e, quindi, una gestione in forma associata della procedura di scelta del contraente, mediante aggregazione della domanda di più soggetti, consente la razionalizzazione della spesa di beni e servizi, il supporto alla programmazione dei fabbisogni, la semplificazione e standardizzazione delle procedure di acquisto, il conseguimento di economie di scala, una maggiore trasparenza delle procedure di gara, il miglioramento della responsabilizzazione e del controllo della spesa, un incremento della specializzazione delle competenze, una maggiore efficienza nell'interazione fra Amministrazione e mercato e, non ultimo, un risparmio nelle spese di gestione della procedura medesima.

(D) In particolare, in forza di quanto stabilito dall'art. 1, comma 514, della legge 28 dicembre 2015, n.208 (Legge di stabilità 2016) ,"Ai fini di cui al comma 512," – e quindi per rispondere alle esigenze delle amministrazioni pubbliche e delle 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. 19 – "Consip S.p.A. o il soggetto aggregatore interessato sentita l'Agid per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al

predetto Piano. […] Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni".

(E) L'art. 20, comma 4, del D.L. n. 83/2012, come convertito con modificazioni dalla Legge 7 agosto 2012, n. 134, ha affidato a Consip S.p.A., a decorrere dalla data di entrata in vigore della legge di conversione del decreto medesimo, "le attività amministrative, contrattuali e strumentali già attribuite a DigitPA, ai fini della realizzazione e gestione dei progetti in materia, nel rispetto delle disposizioni del comma 3".

(F) Ai fini del perseguimento degli obiettivi di cui al citato Piano triennale per l'informatica nella Pubblica Amministrazione, e che in esecuzione di quanto precede, Consip S.p.A., in qualità di stazione appaltante e centrale di committenza, ha indetto con Bando di gara pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 108 del 17/09/e nella Gazzetta Ufficiale dell'Unione Europea n. S 178 del 14/09/2021,una procedura aperta per la stipula di un Accordo Quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, ai sensi dell'art. 54, comma 4, lett. a) del D. Lgs. n. 50/2016, con più operatori.

(G) Il Fornitore è risultato aggiudicatario della quota PAL del Lotto 1 della predetta gara, ed ha stipulato il relativo Accordo Quadro in data 26/07/2022.

(H) In applicazione di quanto stabilito nel predetto Accordo Quadro, ciascuna Amministrazione Contraente utilizza il medesimo per la stipula di Contratti esecutivi, secondo quanto disciplinato nell'Accordo Quadro stesso.

(I) L'Amministrazione Contraente ha svolto ogni attività prodromica necessaria alla stipula del presente Contratto esecutivo, in conformità alle previsioni di cui al Capitolato Tecnico Generale.

(J) Il Fornitore dichiara che quanto risulta dall'Accordo Quadro e dai suoi allegati, ivi compreso il Capitolato d'Oneri ed il Capitolato Tecnico (Generale e Speciale) dell'Accordo Quadro, nonché dal presente Contratto esecutivo e dai suoi allegati, definisce in modo adeguato e completo gli impegni assunti con la firma del presente Contratto, nonché l'oggetto dei prodotti e dei servizi connessi da fornire e, in ogni caso, che ha potuto acquisire tutti gli elementi per una idonea valutazione tecnica ed economica degli stessi e per la formulazione dell'offerta che ritiene pienamente remunerativa;

(K) L'Amministrazione contraente dichiara che il presente contratto sarà finanziato prevalentemente attraverso i fondi stanziati dall'Agenzia per la Cybersicurezza Nazionale tramite l'Avviso 3/2022 a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 per il progetto di Regione Piemonte "Transizione digitale e servizi sicuri". La gestione dell'intervento rientra quindi a pieno titolo nella gestione dei progetti PNRR (REGOLAMENTO (UE) 2021/241 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 12 febbraio 2021) , e le parti dovranno rispettare tutte le richieste previste nel bando Avviso 3/2022 a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5 (rendicontazioni, modalità di fatturazione, loghi "NextgenerationEU" sulle comunicazioni tra le parti), come esplicitato nelle "Linee guida per soggetti attuatori individuati tramite avvisi pubblici – Manuale Operativo" emanate dall' Agenzia per la Cybersicurezza Nazionale.

(L) il CIG del presente Contratto Esecutivo è il seguente:

CIG: 88846293CA - CIG "derivato": A03A642A24;

(M) il CUP (Codice Unico Progetto) del presente Contratto Esecutivo è il seguente: **J14F22001120006**;

TUTTO CIÒ PREMESSO SI CONVIENE E SI STIPULA QUANTO SEGUE:

1. DEFINIZIONI

1.1 I termini contenuti nel presente Contratto esecutivo hanno il significato specificato nell'Accordo Quadro e nei relativi Allegati, salvo che il contesto delle singole clausole disponga diversamente.

1.2 I termini tecnici contenuti nel presente Contratto esecutivo hanno il significato specificato nel Capitolato Tecnico Generale e Speciale, salvo che il contesto delle singole clausole disponga diversamente.

1.3 Il presente Contratto esecutivo è regolato:

a) dalle disposizioni del presente atto e dai suoi allegati, che costituiscono la manifestazione integrale di tutti gli accordi intervenuti tra il Fornitore e l'Amministrazione relativamente alle attività e prestazioni contrattuali;
b) dalle disposizioni dell'Accordo Quadro e dai suoi allegati;
c) dalle disposizioni del D.Lgs. 50/2016 e s.m.i. e relative prassi e disposizioni attuative;
d) dalle disposizioni di cui al D.Lgs. n. 82/2005;
e) dal codice civile e dalle altre disposizioni normative in vigore in materia di contratti di diritto privato.

2. VALORE DELLE PREMESSE E DEGLI ALLEGATI

2.1 Le premesse di cui sopra, gli atti e i documenti richiamati nelle medesime premesse e nella restante parte del presente atto, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del presente Contratto esecutivo.

2.2 Costituiscono, altresì, parte integrante e sostanziale del presente Contratto esecutivo:

- l'Accordo Quadro,
- gli Allegati dell'Accordo Quadro,
- l'**Allegato 1** "Piano Operativo" approvato, l'**Allegato 2** "Piano dei Fabbisogni", di cui al paragrafo 6.4 del Capitolato Tecnico Parte Generale (Allegato all'Accordo Quadro).

2.3 In particolare, per ogni condizione, modalità e termine per la prestazione dei servizi oggetto del presente Contratto Esecutivo che non sia espressamente regolata nel presente atto, vale tra le Parti quanto stabilito nell'Accordo Quadro, ivi inclusi gli Allegati del medesimo, con il quale devono intendersi regolati tutti i termini del rapporto tra le Parti.

2.4 Le Parti espressamente convengono che il predetto Accordo Quadro, ha valore di regolamento e pattuizione per il presente Contratto esecutivo. Pertanto, in caso di contrasto tra i principi dell'Accordo Quadro e quelli del Contratto esecutivo, i primi prevarranno su questi ultimi, salvo diversa espressa volontà derogativa delle parti manifestata per iscritto.

3. OGGETTO DEL CONTRATTO ESECUTIVO

3.1 Il presente Contratto esecutivo definisce i termini e le condizioni che, unitamente alle disposizioni contenute nell'Accordo Quadro, regolano la prestazione in favore dell'Amministrazione da parte del Fornitore dei seguenti servizi: **L1.S9 Formazione e**

Security Awareness, come riportati nel Piano Operativo approvato di cui all'Allegato 1 e nel Piano dei Fabbisogni di cui all'Allegato 2 al presente documento.

3.2 I predetti servizi dovranno essere erogati con le modalità ed alle condizioni stabilite nel presente Contratto esecutivo e nell'Accordo Quadro e relativi allegati.

3.3 Sono designati quale Responsabile unico del procedimento, ai sensi dell'art. 31 del D. Lgs. n. 50/2016 il Dott. Giorgio Consol e Direttore dell'esecuzione ai sensi dell'art. 101 del D. Lgs. n. 50/2016 il Dott. Domenico Festa.

3.4 L'affidatario si impegna a rispettare tutti i requisiti tecnici e ambientali previsti dalla normativa europea e nazionale in ottemperanza al principio di non arrecare un danno significativo all'ambiente "Do No Significant Harm" (DNSH), ivi incluso l'impegno a consegnare all'Amministrazione la documentazione a comprova del rispetto dei suddetti requisiti.

4. EFFICACIA E DURATA

4.1 Il presente Contratto esecutivo spiega i suoi effetti dalla data della sua sottoscrizione ed avrà termine allo spirare di 24 mesi dalla data di conclusione delle attività di presa in carico.

4.2 Le Amministrazioni possono, nei limiti di quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016, chiedere al Fornitore prestazioni supplementari rispetto al Contratto esecutivo, che si rendano necessarie, ove un cambiamento del contraente produca entrambi gli effetti di cui all'art. 106, comma 1, lettera b), D. Lgs. n. 50/2016; l'Amministrazione comunicherà ad ANAC tale modifica entro i termini di cui all'art. 106, comma 8, del medesimo decreto.

4.3 Le Amministrazioni possono apportare modifiche al contratto esecutivo ove siano soddisfatte tutte le condizioni di cui all'art. 106, comma 1, lettera c), D. Lgs. 50/2016, fatto salvo quanto previsto all'art. 106, comma 7, del D. Lgs. n. 50/2016. Al ricorrere delle condizioni di cui all'art. 106, comma 14, del D. Lgs. 50/2016 l'Amministrazione comunicherà ad ANAC tale modifica entro i termini e con le modalità ivi indicati. In entrambi i casi sopra descritti, l'Amministrazione eseguirà le pubblicazioni prescritte dall'art. 106, comma 5, del D. Lgs. n. 50/2016.

4.4 Le Amministrazioni potranno apportare le modifiche di cui art. 106, comma 1, lett. d), del D. Lgs. n. 50/2016, nel pieno rispetto di tale previsione normativa.

4.5 Ai sensi dell'art. 106, comma 12, del D.Lgs. n. 50/2016, ove ciò si renda necessario in corso di esecuzione, l'Amministrazione potrà imporre al Fornitore affidatario del Contratto esecutivo un aumento o una diminuzione delle prestazioni fino a concorrenza di un quinto dell'importo del contratto alle stesse condizioni ed agli stessi prezzi unitari previsti nel presente contratto. In tal caso, il Fornitore non può far valere il diritto alla risoluzione del contratto.

5. GESTIONE DEL CONTRATTO ESECUTIVO

5.1 Ai fini dell'esecuzione del presente Contratto esecutivo, il Fornitore ha nominato come Responsabile Unico delle Attività Contrattuali (RUAC) e come Referente/i Tecnico/i per l'erogazione dei servizi rispettivamente: l'Ing. Mattia Cinacchi e la dott.ssa Camilla Sormani

5.2 I compiti demandati alle suddette figure del Fornitore sono declinati al paragrafo 7.2 del Capitolato Tecnico Generale dell'Accordo Quadro.

5.3 Le attività di supervisione e controllo della corretta esecuzione del presente Contratto esecutivo, in relazione ai servizi richiesti, sono svolte dall'Amministrazione,

eventualmente d'intesa con i soggetti indicati nell'Allegato Governance al Capitolato Tecnico Generale dell'Accordo Quadro.

6. PRESA IN CARICO E TRASFERIMENTO DEL KNOW HOW

6.1 Il Fornitore, a decorrere dalla data di stipula del presente Contratto esecutivo, dovrà procedere alla attività di presa in carico con le modalità indicate nel Capitolato Tecnico Speciale dell'Accordo Quadro.

6.2 L'attivazione dei servizi avverrà nei tempi e nei modi di cui al Capitolato Tecnico Generale e Speciale dell'Accordo Quadro, al Piano dei Fabbisogni ed al Piano Operativo.

6.3 In base ai servizi richiesti da parte dell'Amministrazione contraente, alla scadenza del presente Contratto esecutivo o in caso di risoluzione o recesso dallo stesso, il Fornitore si impegna a porre in essere tutte le attività per il passaggio di consegne di fine fornitura (phase-out), finalizzato al trasferimento all'Amministrazione, o a terzi da essa indicati, del know-how e delle competenze maturate nella conduzione delle attività, secondo quanto previsto nel paragrafo 7.3 del Capitolato Tecnico Speciale (2A).

7. LOCALI MESSI A DISPOSIZIONE DALL'AMMINISTRAZIONE CONTRAENTE

7.1 L'Amministrazione Contraente provvede ad indicare e mettere a disposizione del Fornitore, in comodato gratuito ed in uso non esclusivo, locali idonei alla installazione degli eventuali apparati del Fornitore necessari all'erogazione dei servizi richiesti, con le modalità indicate nel Piano dei Fabbisogni e nel Piano Operativo.

7.2 L'Amministrazione Contraente garantisce al Fornitore:

- lo spazio fisico necessario per l'alloggio delle apparecchiature ed idoneo ad ospitare le apparecchiature medesime;
- l'alimentazione elettrica delle apparecchiature di adeguata potenza; sarà cura del Fornitore provvedere ad adottare ogni misura per garantire la continuità della alimentazione elettrica.

7.3 Il Fornitore provvede a visitare i locali messi a disposizione dall'Amministrazione Contraente ed a segnalare, prima della data di disponibilità all'attivazione, l'eventuale inidoneità tecnica degli stessi.

7.4 L'Amministrazione Contraente consentirà al personale del Fornitore o a soggetti da esso indicati, muniti di documento di riconoscimento, l'accesso ai propri locali per eseguire eventuali operazioni rientranti nell'oggetto del presente Contratto esecutivo. Le modalità dell'accesso saranno concordate fra le Parti al fine di salvaguardare la legittima esigenza di sicurezza dell'Amministrazione Contraente. Il Fornitore è tenuto a procedere allo sgombero, a lavoro ultimato, delle attrezzature e dei materiali residui.

7.5 L'Amministrazione Contraente, successivamente all'esito positivo delle verifiche di conformità a fine contratto, porrà in essere quanto possibile affinché gli apparati del Fornitore presenti nei suoi locali non vengano danneggiati o manomessi, pur non assumendosi responsabilità se non quelle derivanti da dolo o colpa grave del proprio personale.

8. VERIFICHE DI CONFORMITA'

8.1 Nel periodo di efficacia del presente Contratto esecutivo, l'Amministrazione Contraente procederà ad effettuare la verifica di conformità delle prestazioni oggetto del Contratto esecutivo per la verifica della corretta esecuzione delle prestazioni contrattuali, con le modalità e le specifiche stabilite nell'Accordo Quadro e nel Capitolato Tecnico Generale e Speciale ad esso allegati.

9. PENALI

9.1 L'Amministrazione potrà applicare al Fornitore le penali dettagliatamente descritte e regolate nell'Accordo Quadro, qui da intendersi integralmente trascritte.

9.2 Per le modalità di contestazione ed applicazione delle penali vale tra le Parti quanto stabilito all'articolo 12 dell'Accordo Quadro.

10. CORRISPETTIVI

10.1 Il corrispettivo complessivo, calcolato sulla base del dimensionamento dei servizi indicato del Piano dei Fabbisogni e nel Piano Operativo, è pari a 75.988,64 € settantacinquemilanovecentoottantaotto,64 .

10.2 I corrispettivi unitari per singolo servizio, dovuti al Fornitore per la fornitura dei servizi prestati in esecuzione del presente Contratto esecutivo sono determinati in ragione dei prezzi unitari stabiliti nell'Allegato "C" all'Accordo Quadro "Corrispettivi e Tariffe".

10.3 Il corrispettivo contrattuale si riferisce alla esecuzione dei servizi a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali.

10.4 I corrispettivi contrattuali sono stati determinati a proprio rischio dal Fornitore in base ai propri calcoli, alle proprie indagini, alle proprie stime, e sono, pertanto, fissi ed invariabili indipendentemente da qualsiasi imprevisto o eventualità, facendosi carico il Fornitore medesimo di ogni relativo rischio e/o alea. Il Fornitore non potrà vantare diritto ad altri compensi, ovvero ad adeguamenti, revisioni o aumenti dei corrispettivi come sopra indicati.

10.5 Tali corrispettivi sono dovuti dall'Amministrazione Contraente al Fornitore a decorrere dalla "Data di accettazione" della fornitura e successivamente all'esito positivo della verifica di conformità della singola prestazione.

11. FATTURAZIONE E PAGAMENTI

11.1 La fattura relativa ai corrispettivi maturati secondo quanto previsto al precedente art. 10 viene emessa ed inviata dal Fornitore ad esito positivo della verifica di conformità, che avverrà al termine dei 2 periodi di formazione previsti nel Piano Operativo.

Per quanto riguarda la fattura relativa al primo periodo di formazione definito nel Piano Operativo, interamente a carico di Accenture S.p.a. e finanziato tramite fondi previste nel bando Avviso 3/2022 a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5, essa dovrà contenere tutte le informazioni previste nel modulo "MOA-12_Format Indicazioni fatturazione", allegato alle "Linee guida per soggetti attuatori individuati tramite avvisi pubblici – Manuale Operativo".

Relativamente alla fatturazione riguardante il secondo periodo di formazione, le singole Società costituenti il Raggruppamento, salva ed impregiudicata la responsabilità solidale delle società raggruppate nei confronti dell'Amministrazione, potranno provvedere ciascuna alla fatturazione "pro quota" delle attività effettivamente prestate. Le Società componenti il Raggruppamento potranno fatturare solo le attività effettivamente svolte, corrispondenti alla ripartizione delle attività.

La società mandataria del Raggruppamento medesimo è obbligata a trasmettere, in maniera unitaria e previa predisposizione di apposito prospetto riepilogativo delle attività e delle competenze maturate, le fatture relative all'attività svolta da tutte le imprese raggruppate. Ogni singola fattura dovrà contenere la descrizione di ciascuno dei servizi / attività / fasi / prodotti a cui si riferisce.

11.2 Ciascuna fattura dovrà essere emessa nel rispetto di quanto prescritto nell'Accordo

Quadro e, a riguardo del primo periodo di formazione, come esplicitato nelle “Linee guida per soggetti attuatori individuati tramite avvisi pubblici – Manuale Operativo” emanate dall’ Agenzia per la Cybersicurezza Nazionale relativamente all’Avviso 3/2022 a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” M1C1I1.5.

11.3 I corrispettivi saranno accreditati, a spese del Fornitore, sui seguenti conto corrente:

il Fornitore dichiara che i predetti conti operano nel rispetto della Legge 13 agosto 2010 n. 136 e si obbliga a comunicare le generalità e il codice fiscale del/i delegato/i ad operare sul/i predetto/i conto/i all’Amministrazione all’atto del perfezionamento del presente Contratto Esecutivo.

11.4 l’art. 35, comma 18, del Codice non si applica

12. GARANZIA DELL’ESATTO ADEMPIMENTO

12.1 Il Fornitore ha prestato garanzia definitiva rilasciata in data _____ dalla _____ avente n. _____ di importo pari ad Euro _____= (_____/00) che copre le obbligazioni assunte con il presente contratto, il risarcimento dei danni derivanti dall'eventuale inadempimento delle stesse obbligazioni, nonché il rimborso delle somme pagate in più all'esecutore rispetto alle risultanze della liquidazione finale, salva comunque la risarcibilità del maggior danno verso l'appaltatore, nonché, ove esistente, le obbligazioni assunte con il Patto di integrità.

12.2 L’Amministrazione ha inoltre il diritto di valersi della garanzia definitiva, nei limiti dell'importo massimo garantito: i) per l'eventuale maggiore spesa sostenuta per il completamento delle prestazioni nel caso di risoluzione del contratto disposta in danno dell’esecutore; ii) per provvedere al pagamento di quanto dovuto dal Fornitore per le inadempienze derivanti dalla inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori comunque presenti nei luoghi dove viene eseguito il contratto ed addetti all'esecuzione dell'appalto.

12.3 L’Amministrazione ha diritto di incamerare la garanzia, in tutto o in parte, per i danni che essa affermi di aver subito, senza pregiudizio dei suoi diritti nei confronti del Fornitore per la rifusione dell’ulteriore danno eventualmente eccedente la somma incamerata.

12.4 La garanzia prevede espressamente la rinuncia della preventiva escussione del debitore principale, la rinuncia all’eccezione di cui all’art. 1957, comma 2 del codice civile, nonché l’operatività della garanzia medesima entro 15 giorni, a semplice richiesta scritta.

12.5 Il Fornitore si impegna a tenere valida ed efficace la garanzia, mediante rinnovi e proroghe, per tutta la durata del presente contratto e, comunque, sino al perfetto adempimento delle obbligazioni assunte in virtù del presente contratto, pena la risoluzione di diritto del medesimo.

12.6 L'Amministrazione può richiedere al Fornitore la reintegrazione della garanzia ove questa sia venuta meno in tutto o in parte entro il termine di 10 (dieci) giorni dalla richiesta; in caso di inottemperanza, l'Amministrazione conseguirà la reintegrazione trattenendo quanto necessario dai corrispettivi dovuti al Fornitore.

12.7 La garanzia sarà progressivamente svincolata a misura dell'avanzamento dell'esecuzione contrattuale, nel limite massimo dell'80 per cento dell'iniziale importo garantito, secondo quanto stabilito dall'art. 103, comma 5, del D. Lgs. n. 50/2016, previa deduzione di crediti dell'Amministrazione verso il Fornitore e subordinatamente alla preventiva consegna, da parte del Fornitore all'Istituto garante, di un documento, in originale o copia autentica, attestante l'avvenuta esecuzione delle prestazioni contrattuali. Tale documento è emesso periodicamente dall'Amministrazione in ragione delle verifiche di conformità svolte. Il fornitore dovrà inviare per conoscenza all'Amministrazione la comunicazione che invia al Garante ai fini dello svincolo. Il Garante dovrà comunicare all'Amministrazione il valore dello svincolo. L'Amministrazione si riserva di verificare la correttezza degli importi svincolati e di chiedere al Fornitore ed al Garante in caso di errore un'integrazione.

12.8 L'ammontare residuo della garanzia definitiva deve permanere fino alla data di emissione del certificato di verifica di conformità attestante la corretta esecuzione del Contratto esecutivo.

12.9 Resta fermo tutto quanto previsto dall'art. 103 del D. Lgs. n. 50/2016.

13. SUBAPPALTO

13.1 L'Impresa si è riservata di affidare in subappalto, nella misura di 50%, l'esecuzione delle seguenti prestazioni: L1.S9 Formazione e Security Awareness, salvo quanto previsto dall'art. 105, comma 12, del d. lgs. n. 50/2016.

13.2 L'Impresa si impegna a depositare presso Consip S.p.A., almeno venti giorni prima della data di effettivo inizio dell'esecuzione delle attività oggetto del subappalto: i) l'originale o la copia autentica del contratto di subappalto che deve indicare puntualmente l'ambito operativo del subappalto sia in termini prestazionali che economici; ii) dichiarazione attestante il possesso da parte del subappaltatore dei requisiti richiesti dalla documentazione di gara, per lo svolgimento delle attività allo stesso affidate, ivi inclusi i requisiti di ordine generale di cui all'articolo 80 del D. Lgs. n. 50/2016; iii) dichiarazione dell'appaltatore relativa alla sussistenza o meno di eventuali forme di controllo o collegamento a norma dell'art. 2359 c.c. con il subappaltatore; se del caso, v) documentazione attestante il possesso da parte del subappaltatore dei requisiti di qualificazione/certificazione prescritti dal D. Lgs. n. 50/2016 per l'esecuzione delle attività affidate.

13.3 In caso di mancato deposito di taluno dei suindicati documenti nel termine all'uopo previsto, Consip S.p.A. procederà a richiedere al Fornitore l'integrazione della suddetta documentazione. Resta inteso che la suddetta richiesta di integrazione comporta l'interruzione del termine per la definizione del procedimento di autorizzazione del subappalto, che ricomincerà a decorrere dal completamento della documentazione.

13.4 I subappaltatori dovranno mantenere per tutta la durata del presente contratto, i requisiti richiesti per il rilascio dell'autorizzazione al subappalto. In caso di perdita dei detti requisiti Consip S.p.A. revocherà l'autorizzazione.

13.5 L'impresa qualora l'oggetto del subappalto subisca variazioni e l'importo dello stesso sia incrementato nonché siano variati i requisiti di qualificazione o le certificazioni deve acquisire una autorizzazione integrativa.

13.6 Ai sensi dell'art. 105, comma 4, lett. a) del D. Lgs. n. 50/2016 e s.m.i. non sarà autorizzato il subappalto ad un operatore economico che abbia partecipato alla procedura di affidamento dell'Accordo Quadro.

13.7 Per le prestazioni affidate in subappalto: il subappaltatore, ai sensi dell'art. 105, comma 14, del Codice, deve garantire gli stessi standard qualitativi e prestazionali previsti nel contratto di appalto e riconoscere ai lavoratori un trattamento economico e normativo non inferiore a quello che avrebbe garantito il contraente principale, inclusa l'applicazione dei medesimi contratti collettivi nazionali di lavoro, qualora le attività oggetto di subappalto coincidano con quelle caratterizzanti l'oggetto dell'appalto ovvero riguardino le lavorazioni relative alle categorie prevalenti e siano incluse nell'oggetto sociale del contraente principale;

13.8 L'Amministrazione contraente, sentito il direttore dell'esecuzione, provvede alla verifica dell'effettiva applicazione degli obblighi di cui al presente comma. Il Fornitore è solidalmente responsabile con il subappaltatore degli adempimenti, da parte di questo ultimo, degli obblighi di sicurezza previsti dalla normativa vigente.

13.9 Il Fornitore e il subappaltatore sono responsabili in solido, nei confronti dell'Amministrazione Contraente, in relazione alle prestazioni oggetto del contratto di subappalto.

13.10 L'Impresa è responsabile in solido con il subappaltatore nei confronti dell'Amministrazione contraente dei danni che dovessero derivare ad essa o a terzi per fatti comunque imputabili ai soggetti cui sono state affidate le suddette attività. In particolare, il Fornitore e il subappaltatore si impegnano a manlevare e tenere indenne la Consip e l'Amministrazione da qualsivoglia pretesa di terzi per fatti e colpe imputabili al subappaltatore o ai suoi ausiliari derivanti da qualsiasi perdita, danno, responsabilità, costo o spesa che possano originarsi da eventuali violazioni del Regolamento 679/2016.

13.11 Il Fornitore è responsabile in solido dell'osservanza del trattamento economico e normativo stabilito dai contratti collettivi nazionale e territoriale in vigore per il settore e per la zona nella quale si eseguono le prestazioni da parte del subappaltatore nei confronti dei suoi dipendenti, per le prestazioni rese nell'ambito del subappalto. Il Fornitore trasmette all'Amministrazione contraente prima dell'inizio delle prestazioni la documentazione di avvenuta denunzia agli enti previdenziali, inclusa la Cassa edile, ove presente, assicurativi e antinfortunistici, nonché copia del piano della sicurezza di cui al D. Lgs. n. 81/2008. Ai fini del pagamento delle prestazioni rese nell'ambito dell'appalto o del subappalto, la stazione appaltante acquisisce d'ufficio il documento unico di regolarità contributiva in corso di validità relativo a tutti i subappaltatori.

13.12 Il Fornitore è responsabile in solido con il subappaltatore in relazione agli obblighi retributivi e contributivi, ai sensi dell'art. 29 del D. Lgs. n. 276/2003, ad eccezione del caso in cui ricorrano le fattispecie di cui all'art. 105, comma 13, lett. a) e c), del D. Lgs. n. 50/2016.

13.13 Il Fornitore si impegna a sostituire i subappaltatori relativamente ai quali apposita verifica abbia dimostrato la sussistenza dei motivi di esclusione di cui all'articolo 80 del D. Lgs. n. 50/2016.

13.14 L'Amministrazione Contraente corrisponde direttamente al subappaltatore, al cottimista, al prestatore di servizi ed al fornitore di beni o lavori, l'importo dovuto per le prestazioni dagli stessi eseguite nei seguenti casi: a) quando il subappaltatore o il cottimista è una microimpresa o piccola impresa; b) in caso di inadempimento da parte dell'appaltatore; c) su richiesta del subappaltatore e se la natura del contratto lo consente. In caso contrario, salvo diversa indicazione del direttore dell'esecuzione, il Fornitore si obbliga a trasmettere all'Amministrazione contraente entro 20 giorni dalla data di ciascun pagamento da lui effettuato nei confronti dei subappaltatori, copia delle fatture quietanzate relative ai pagamenti da essa via via corrisposte al subappaltatore.

13.15 L'esecuzione delle attività subappaltate non può formare oggetto di ulteriore subappalto.

13.16 In caso di inadempimento da parte dell'Impresa agli obblighi di cui ai precedenti commi, l'Amministrazione può risolvere il Contratto esecutivo, salvo il diritto al risarcimento del danno.

13.17 Ai sensi dell'art. 105, comma 2, del D. Lgs. n. 50/2016, il Fornitore si obbliga a comunicare all'Amministrazione il nome del subcontraente, l'importo del contratto, l'oggetto delle prestazioni affidate.

13.18 Il Fornitore si impegna a comunicare all'Amministrazione, prima dell'inizio della prestazione, per tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione del contratto, il nome del sub-contraente, l'importo del sub-contratto, l'oggetto del lavoro, servizio o fornitura affidati. Sono, altresì, comunicate eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto.

13.19 Non costituiscono subappalto le fattispecie di cui al comma 3 dell'art. 105 del d. lgs. n. 50/2016 e s.m.i.. Nel caso in cui l'Impresa intenda ricorrere alle prestazioni di soggetti terzi in forza di contratti continuativi di cooperazione, servizio e/o fornitura gli stessi devono essere stati sottoscritti in epoca anteriore all'indizione della procedura finalizzata all'aggiudicazione del contratto e devono essere consegnati all'Amministrazione prima o contestualmente alla sottoscrizione del Contratto.

13.20 Per tutto quanto non previsto si applicano le disposizioni di cui all'art. 105 del D.Lgs. 50/2016.

13.21 Restano fermi tutti gli obblighi e gli adempimenti previsti dall'art. 48-bis del D.P.R. 602 del 29 settembre 1973 nonché dai successivi regolamenti.

13.22 L'Amministrazione provvederà a comunicare al Casellario Informatico le informazioni di cui alla Determinazione dell'Autorità di Vigilanza sui Contratti Pubblici (ora A.N.AC) n. 1 del 10/01/2008.

RISOLUZIONE E RECESSO

13.23 Le ipotesi di risoluzione del presente Contratto esecutivo e di recesso sono disciplinate, rispettivamente, agli artt. 14 e 15 dell'Accordo Quadro, cui si rinvia, nonché agli artt. "SUBAPPALTO" "TRASPARENZA DEI PREZZI", "TRACCIABILITÀ DEI FLUSSI FINANZIARI" e "TRATTAMENTO DEI DATI PERSONALI" del presente Documento.

14. FORZA MAGGIORE

14.1 Nessuna Parte sarà responsabile per qualsiasi perdita che potrà essere patita dall'altra Parte a causa di eventi di forza maggiore (che includono, a titolo esemplificativo, disastri naturali, terremoti, incendi, fulmini, guerre, sommosse, sabotaggi, atti del Governo,

autorità giudiziarie, autorità amministrative e/o autorità di regolamentazione indipendenti) a tale Parte non imputabili.

14.2 Nel caso in cui un evento di forza maggiore impedisca la prestazione dei servizi da parte del Fornitore, l'Amministrazione, impregiudicato qualsiasi diritto ad essa spettante in base alle disposizioni di legge sull'impossibilità della prestazione, non dovrà pagare i corrispettivi per la prestazione dei servizi fino a che i servizi non siano ripristinati e, ove possibile, avrà diritto di affidare l'erogazione dei servizi in questione ad altro fornitore assegnatario per una durata ragionevole secondo le circostanze.

14.3 L'Amministrazione si impegna, inoltre, in tale eventualità a compiere le azioni necessarie al fine di risolvere tali accordi, non appena il Fornitore le comunichi di essere in grado di erogare nuovamente i servizi.

15. RESPONSABILITA' CIVILE E POLIZZA ASSICURATIVA

15.1 Fermo restando quanto previsto dall'Accordo Quadro, il Fornitore assume in proprio ogni responsabilità per infortunio o danni eventualmente subiti da parte di persone o di beni, tanto del Fornitore quanto dell'Amministrazione o di terzi, in dipendenza di omissioni, negligenze o altre inadempienze attinenti all'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi.

15.2 A fronte dell'obbligo di cui al precedente comma, il Fornitore ha presentato polizza/e assicurativa/e conforme/i ai requisiti indicati nella Richiesta di Offerta (conformi all'allegato di gara dell'AQ).

15.3 Resta ferma l'intera responsabilità del Fornitore anche per danni coperti o non coperti e/o per danni eccedenti i massimali assicurati dalle polizze di cui al precedente comma 2.

15.4 Con specifico riguardo al mancato pagamento del premio, ai sensi dell'art. 1901 del c.c., l'Amministrazione si riserva la facoltà di provvedere direttamente al pagamento dello stesso, entro un periodo di 60 giorni dal mancato versamento da parte del Fornitore ferma restando la possibilità dell'Amministrazione di procedere a compensare quanto versato con i corrispettivi maturati a fronte delle attività eseguite.

15.5 Qualora il Fornitore non sia in grado di provare in qualsiasi momento la piena operatività delle coperture assicurative di cui al precedente comma 2 e qualora l'Amministrazione non si sia avvalsa della facoltà di cui al precedente comma 4, il Contratto potrà essere risolto di diritto con conseguente ritenzione della garanzia prestata a titolo di penale e fatto salvo l'obbligo di risarcimento del maggior danno subito.

15.6 Resta fermo che il Fornitore si impegna a consegnare, annualmente e con tempestività, all'Amministrazione, la quietanza di pagamento del premio, atta a comprovare la validità della polizza assicurativa prodotta per la stipula del contratto o, se del caso, la nuova polizza eventualmente stipulata, in relazione al presente contratto.

16. TRASPARENZA DEI PREZZI

16.1 L'Impresa espressamente ed irrevocabilmente:

a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione del presente contratto;

b) dichiara di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi, ivi comprese le Imprese collegate o controllate, somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione del contratto stesso;

c) si obbliga a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione del presente contratto rispetto agli obblighi con esse assunti, né a compiere azioni comunque volte agli stessi fini;

d) si obbliga al rispetto di quanto stabilito dall'art. 42 del D.Lgs. n. 50/2016 al fine di evitare situazioni di conflitto d'interesse.

16.2 Qualora non risultasse conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, o il Fornitore non rispettasse gli impegni e gli obblighi di cui alle lettere c) e d) del precedente comma per tutta la durata del contratto lo stesso si intenderà risolto di diritto ai sensi e per gli effetti dell'art. 1456 cod. civ., per fatto e colpa del Fornitore, che sarà conseguentemente tenuto al risarcimento di tutti i danni derivanti dalla risoluzione e con facoltà dell'Amministrazione di incamerare la garanzia prestata.

17. ONERI FISCALI E SPESE CONTRATTUALI

17.1 Il Fornitore riconosce a proprio carico tutti gli oneri fiscali e tutte le spese contrattuali relative al presente atto, come previsto all'art. 28 dell'Accordo Quadro.

17.2 Così 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. 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.

17.3 Il valore complessivo del presente Contratto Esecutivo è quello espressamente indicato al precedente paragrafo 10.1. Di conseguenza, il valore del contributo dovuto dall'Amministrazione Beneficiaria ammonta ad € 607,91 (Euro seicentosette euro e novantuno centesimi).

17.4 In caso di incremento (entro il 20% dell'importo iniziale) del valore del Contratto esecutivo a seguito di una modifica del Piano dei Fabbisogni e del Piano Operativo approvato dall'Amministrazione Beneficiaria ai sensi dell'articolo 6 dell'Accordo Quadro, quest'ultima è tenuta a versare a Consip S.p.A., entro il termine di 30 (trenta) giorni solari dalla predetta approvazione, un ulteriore contributo nella misura prevista dall'art. 2, lettera c) (3 per mille sull'incremento tra il valore del contratto esecutivo ed il valore dell'atto aggiuntivo), del D.P.C.M. 23 giugno 2010.

A tal fine, nei casi di cui al precedente periodo, il Fornitore provvederà a comunicare all'Amministrazione e per conoscenza a Consip, entro il termine di 10 (dieci) giorni solari dalla data di approvazione del Piano Operativo incrementato, il valore aggiornato del Piano Operativo e il valore del contributo dovuto in ragione del relativo incremento.

17.5 Il pagamento del contributo, deve es sul seguente IBAN: Banca:

Detti contributi sono considerati fuori campo dell'applicazione dell'IVA, ai sensi dell'art.2, comma 3, lettera a) del D.P.R. del 1972 e pertanto non è prevista nessuna emissione di fattura; gli stessi non rientrano nell'ambito di applicazione della tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136.

18. TRACCIABILITÀ DEI FLUSSI FINANZIARI

18.1 Ai sensi e per gli effetti dell'art. 3, comma 8, della Legge 13 agosto 2010 n. 136, il Fornitore si impegna a rispettare puntualmente quanto previsto dalla predetta disposizione in ordine agli obblighi di tracciabilità dei flussi finanziari.

18.2 Ferme restando le ulteriori ipotesi di risoluzione previste dal presente contratto, si conviene che l'Amministrazione, in ottemperanza a quanto disposto dall'art. 3, comma 9 bis della Legge 13 agosto 2010 n. 136, senza bisogno di assegnare previamente alcun termine per l'adempimento, potrà risolvere di diritto il presente contratto ai sensi dell'art. 1456 cod. civ., nonché ai sensi dell'art. 1360 cod. civ., previa dichiarazione da comunicarsi all'Impresa con raccomandata a/r qualora le transazioni siano eseguite senza avvalersi del bonifico bancario o postale ovvero degli altri strumenti idonei a consentire la piena tracciabilità delle operazioni ai sensi della Legge 13 agosto 2010 n. 136.

18.3 Il Fornitore, nella sua qualità di appaltatore, si obbliga, a mente dell'art. 3, comma 8, secondo periodo della Legge 13 agosto 2010 n. 136, ad inserire nei contratti sottoscritti con i subappaltatori o i subcontraenti, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 13 agosto 2010 n. 136.

18.4 Il Fornitore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria di cui alla norma sopra richiamata è tenuto a darne immediata comunicazione all'Amministrazione e la Prefettura – Ufficio Territoriale del Governo della provincia ove ha sede l'Amministrazione.

18.5 Il Fornitore, si obbliga e garantisce che nei contratti sottoscritti con i subappaltatori e i subcontraenti, verrà assunta dalle predette controparti l'obbligazione specifica di risoluzione di diritto del relativo rapporto contrattuale nel caso di mancato utilizzo del bonifico bancario o postale ovvero degli strumenti idonei a consentire la piena tracciabilità dei flussi finanziari.

18.6 L'Impresa è tenuta a comunicare tempestivamente e comunque entro e non oltre 7 giorni dalla/e variazione/i qualsivoglia variazione intervenuta in ordine ai dati relativi agli estremi identificativi del/i conto/i corrente/i dedicato/i nonché le generalità (nome e cognome) e il codice fiscale delle persone delegate ad operare su detto/i conto/i.

18.7 Ai sensi della Determinazione dell'AVCP (ora A.N.AC.) n. 10 del 22 dicembre 2010, il Fornitore, in caso di cessione dei crediti, si impegna a comunicare il/i CIG/CUP al cessionario, eventualmente anche nell'atto di cessione, affinché lo/gli stesso/i venga/no riportato/i sugli strumenti di pagamento utilizzati. Il cessionario è tenuto ad utilizzare conto/i corrente/i dedicato/i, nonché ad anticipare i pagamenti al Fornitore mediante bonifico bancario o postale sul/i conto/i corrente/i dedicato/i del Fornitore medesimo riportando il CIG/CUP dallo stesso comunicato.

19. FORO COMPETENTE

19.1 Per tutte le questioni relative ai rapporti tra il Fornitore e l'Amministrazione, la competenza è determinata in base alla normativa vigente.

20. TRATTAMENTO DEI DATI PERSONALI

20.1 Con la sottoscrizione del presente contratto il Fornitore è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera

circolazione di tali dati (nel seguito anche “Regolamento UE”), per tutta la durata del contratto. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l’esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto del Titolare, le sole operazioni di trattamento necessarie per fornire il servizio oggetto del presente contratto, nei limiti delle finalità ivi specificate, nel rispetto del Codice Privacy, del Regolamento UE (nel seguito anche “Normativa in tema di trattamento dei dati personali”) e delle istruzioni nel seguito fornite.

20.2 Il Fornitore/Responsabile ha presentato garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l’adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali.

20.3 Le finalità del trattamento sono: erogazione del servizio L1.S9 Formazione e Security Awareness (motivi per cui il fornitore tratta i dati)

20.4 Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: dati comuni (es. dati anagrafici e di contatto)

20.5 Le categorie di interessati sono: dipendenti e collaboratori di Regione Piemonte

20.6 Nell’esercizio delle proprie funzioni, il Responsabile si impegna a:

a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;

b) trattare i dati personali per le sole finalità specificate e nei limiti dell’esecuzione delle prestazioni contrattuali;

c) trattare i dati conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d’ora in poi “persone autorizzate”; nel caso in cui ritenga che un’istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;

d) garantire la riservatezza dei dati personali trattati nell’ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:

- si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
- ricevano la formazione necessaria in materia di protezione dei dati personali;
- trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default).

f) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione

non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

g) su eventuale richiesta del Titolare, assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;

h) ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE.

j) adottare le misure minime di sicurezza ICT per le P.A. di cui alla circolare Agid n. 2/2017 del 18 aprile 2017.

20.7 Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso:

- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
- La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento tutte le misure di sicurezza previste dal presente Contratto Esecutivo e dagli altri impegni contrattualmente previsti per l'erogazione del servizio erogato, che si intendono qui integralmente richiamati.

Il Responsabile del trattamento può avvalersi di ulteriori Responsabili per delegargli attività specifiche, previa autorizzazione scritta del Titolare del trattamento. Nel caso in cui per le prestazioni del Contratto che comportano il trattamento di dati personali il Fornitore/ Responsabile ricorra a subappaltatori o subcontraenti è obbligato a nominare tali operatori a loro volta sub-Responsabili del trattamento sulla base della modalità sopra indicata e comunicare l'avvenuta nomina al titolare.
Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche

avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà risolvere il contratto con il Responsabile iniziale.

Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Amministrazione applicherà al Fornitore/Responsabile Inziale del trattamento la penale di cui all'Accordo Quadro e diffiderà lo stesso a far adottar al sub-Responsabile del trattamento tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, l'Amministrazione potrà risolvere il contratto con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno;

Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei Dati Personali e/o del Contratto (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o sub-fornitori.

20.8 Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. da 15 a 23 del Regolamento UE; qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.

20.9 Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile del trattamento e/o di suoi sub-Responsabili.

20.10 Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto;

20.11 Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le

misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, , o risulti che il Fornitore agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione l'Amministrazione applicherà la penale di cui all'Accordo Quadro e diffiderà il Fornitore ad adottare tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 c.c. l'Amministrazione potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

20.12 Il Responsabile del trattamento deve comunicare al Titolare del trattamento il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.

20.13 Al termine della prestazione dei servizi oggetto del contratto, il Responsabile su richiesta del Titolare, si impegna a: i) restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.

20.14 Il Responsabile si impegna a attuare quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" nonché Il Fornitore si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione dell'Amministrazione l'elenco aggiornato delle nomine.

20.15 In via generale, il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del presente contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.

20.16 Su richiesta del Titolare, il Responsabile si impegna ad adottare, nel corso dell'esecuzione del Contratto, ulteriori garanzie quali l'applicazione di un codice di condotta approvato o di un meccanismo di certificazione approvato di cui agli articoli 40 e 42 del Regolamento UE, quando verranno emanati. L'Amministrazione potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.

20.17 Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.

20.18 Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.

20.19 Nel caso in cui il Fornitore agisca in modo difforme o contrario alle legittime istruzione del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento risponde del danno causato agli "interessati". In tal caso, l'Amministrazione potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

20.20 Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della

normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

Letto, approvato e sottoscritto

Giorgio Consol	Nome Cognome
_____	_____
Regione Piemonte	Fornitore (RTI……)

Ai sensi e per gli effetti dell'art. 1341 c.c. il Fornitore dichiara di aver letto con attenzione e di approvare specificatamente le pattuizioni contenute negli articoli seguenti: Art. 1 Definizioni, Art. 3 Oggetto del Contratto esecutivo, Art. 4 Efficacia e durata, Art. 5 Gestione del Contratto esecutivo, Art. 6 Presa in carico e trasferimento del Know How, Art. 7 Locali messi a disposizione dell'Amministrazione contraente, Art. 8 Verifiche di conformità, Art. 9 Penali, Art. 10 Corrispettivi, Art. 11 Fatturazione e pagamenti, Art. 12 Garanzia dell'esatto adempimento, Art. 13 Subappalto, Art. 14 Condizioni e Test richiesti dal CVCN, Art. 15 Risoluzione e Recesso, Art. 16 Forza Maggiore, Art. 17 Responsabilità civile, Art. 18 Trasparenza dei prezzi, Art. 19 Oneri fiscali e spese contrattuali, Art. 20 Tracciabilità dei flussi finanziari Art. 21 Foro competente, Art. 22 Trattamento dei dati personali

Letto, approvato e sottoscritto
Nome Cognome

_____

(per il Fornitore)

Accordo quadro avente ad oggetto l'affidamento
di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni

ID 2296 - **LOTTO** 1

Piano Operativo

AQ SICUREZZA

accenture | FASTWEB | FINCANTIERI | DEAS

Rev.	Data	Descrizione delle modifiche	Autore
01	12/12/2023	Prima emissione	RTI

Tabella 1 - Registro delle versioni

Le informazioni contenute nel presente documento sono di proprietà di Accenture S.p.A., Fastweb S.p.A., Fincantieri NexTech S.p.A., Difesa e Analisi Sistemi S.p.A. e non possono, al pari di tale documento, essere riprodotte, utilizzate o divulgate in tutto o in parte a terzi senza preventiva autorizzazione scritta delle citate aziende.

Sommario

Indice delle tabelle

Indice delle figure

1 INTRODUZIONE

Regione Piemonte (nel seguito anche "Amministrazione") è un ente territoriale autonomo che esercita le funzioni amministrative, legislative ed esecutive in materia di interesse regionale, nel rispetto della Costituzione, delle leggi dello Stato e dello Statuto regionale.
In particolare, ha il compito di promuovere lo sviluppo economico, sociale e culturale del territorio, tutelando i diritti dei cittadini e le diversità locali. Si articola in organi di governo, quali il Presidente, la Giunta e il Consiglio regionale, e in organi di amministrazione, quali le Direzioni e i Settori regionali e gestisce materie di competenza esclusiva, concorrente o residuale, come la sanità, l'istruzione, il lavoro, l'ambiente, l'agricoltura, la cultura, il turismo, il territorio, le autonomie locali, le elezioni, i tributi, i fondi europei e la strategia di sviluppo sostenibile.
Collabora inoltre con le altre Regioni, lo Stato, l'Unione Europea e gli altri soggetti istituzionali, anche attraverso la partecipazione a organismi e iniziative di coordinamento e consultazione.
In tale ambito, le funzioni ICT di sviluppo del sistema informativo regionale e di erogazione dei servizi trasversali sono allocate presso la Direzione "Competitività del sistema regionale" (A1900), secondo il modello organizzativo approvato con DGR del 29 ottobre 2019, n. 4-439 e s.m.i.
In tale Direzione sono incardinati i seguenti settori regionali:

- il Settore "Sistema informativo regionale" che assume funzioni di impostazione e governo del sistema informativo nel suo complesso, ricomprendendo sia le componenti a supporto delle funzioni della Regione, sia quelle riferite al territorio (comunemente denominate Agenda digitale), con l'obiettivo di disporre di una visione integrata unitaria in ossequio a quanto richiesto dal Piano triennale nazionale e al modello di sistema informativo pubblico definito dall'Agenzia per l'Italia Digitale. Il settore cura la programmazione ICT regionale, svolge funzioni di coordinamento con soggetti ed organismi esterni (AGID, Commissione speciale agenda digitale e CISIS) ed annovera tra le competenze anche le funzioni di responsabile del monitoraggio ai sensi della circolare AGID nr. 1/2021.
- il Settore A1910A "Servizi infrastrutturali e tecnologici" a cui sono demandate, in primo luogo, le competenze relative ai servizi infrastrutturali, sistemi integrata fonia/dati, postazioni di lavoro e della connettività del territorio regionale.

Ognuno dei due settori si occupa delle tematiche di sicurezza informatica per gli ambiti di propria competenza.
Con deliberazione della Giunta regionale n. 35-8188 del 20 dicembre 2018 è stato inoltre formalmente nominato il Responsabile della transizione alla modalità digitale della Regione (RTD), ai sensi dell'art. 17, commi 1 e 1-ter, del decreto legislativo 82/2005 "Codice dell'Amministrazione digitale" al quale sono stati affidati i compiti di conduzione del processo di transizione alla modalità operativa digitale e dei conseguenti processi di riorganizzazione, finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità attraverso una maggiore efficienza ed economicità. L'RTD ha in capo, tra le altre funzioni, l'indirizzo, la pianificazione, il coordinamento e il monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture.

Regione Piemonte, infatti, ritiene opportuno promuovere interventi di potenziamento della resilienza cyber, per aumentare i livelli di sicurezza ed affidabilità dei sistemi informativi, anche tenendo conto che la digitalizzazione dei processi, prodotti e servizi, caratterizzando molte delle politiche e degli interventi di riforma del Piano Nazionale di Ripresa e Resilienza (PNRR) e le linee guida a livello nazionale per l'introduzione di piattaforme digitali per l'ammodernamento della Pubblica Amministrazione, anche a supporto del lavoro agile. Tali politiche volte alla digitalizzazione della Pubblica Amministrazione richiedono un rafforzamento sempre crescente della sicurezza informatica secondo gli indirizzi formulati dall'Agenzia per la Cybersicurezza Nazionale, anche alla luce del trasferimento del personale regionale nella nuova sede unica degli uffici della Giunta regionale, avvenuto da pochi mesi.

A riguardo dei temi sopra esposti l'Agenzia per la Cybersicurezza Nazionale (ACN), in stretto contatto con il Dipartimento per la trasformazione digitale (DTD), cura l'attuazione dell'investimento PNRR 1.5 "Cybersecurity" connettendo il mondo della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. In data 2 agosto 2022 ACN ha pubblicato l'Avviso 3/2022 sul sito Italia Domani, a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5, il quale prevede il finanziamento per un valore di 45 milioni di interventi di potenziamento della resilienza cyber destinati alle Regioni, Province Autonome e Comuni Capoluogo di Città Metropolitane.

Regione Piemonte ha partecipato a questo avviso con due progetti; ambedue sono stati approvati da ACN e sono rientrati nel perimetro del finanziamento. Uno di questi 2 progetti, denominato "Transizione digitale e servizi sicuri" ed affidato al Settore A1911A, interviene sulle seguenti aree:

- aumento della security awareness, cioè il livello di consapevolezza dei rischi di sicurezza cui sono esposti gli utenti della PA. Saranno rafforzate le competenze e le pratiche del personale, con un focus sulla gestione dei dati e dei servizi erogati;
- revisione/integrazione delle procedure e delle policy legate alla sicurezza dei servizi dell'Ente;
- analisi della postura di sicurezza dell'Ente, in particolare dei servizi applicativi individuati in un insieme predefinito di applicazioni, e produzione dei relativi report, secondo il "Framework Nazionale per la Cyber Security e la Data Protection";
- realizzazione di strumenti di analisi vulnerabilità e pianificazione/realizzazione di interventi di mitigazione;
- processi a supporto della continuità operativa: analisi delle vulnerabilità connesse alla disponibilità dei servizi attraverso la Business Impact Analysis degli stessi; definizione delle strategie tecnico-organizzative e realizzazione del piano di continuità operativa (ISO 22301:2019) e dei processi a supporto;
- evoluzione, nella logica di aumento della resilienza, della piattaforma di identità digitale per l'accesso ai servizi del Sistema Informativo regionale da parte degli utilizzatori.

1.1 Scopo

I servizi proposti nel presente Piano Operativo hanno lo scopo di indirizzare una delle aree del progetto sopra descritto, e in particolare *"aumento della security awareness, cioè il livello di consapevolezza dei rischi di sicurezza cui sono esposti gli utenti della PA. Saranno rafforzate le competenze e le pratiche del personale, con un focus sulla gestione dei dati e dei servizi erogati"*.

L'obiettivo è quindi quello di incrementare la consapevolezza dei dipendenti di Regione Piemonte sul rischio digitale e di sviluppare negli utenti 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 tramite iniziative di Security Awareness e di misurare il livello di consapevolezza raggiunto. Al fine di erogare un servizio efficace si farà leva su una serie di fattori innovativi, necessari a garantire il coinvolgimento dell'utente in funzione della percezione che questo ha della sicurezza informatica e dei rischi indotti dalla sua operatività quotidiana.

A tal fine, il presente Piano Operativo indirizza tramite il servizio L1.S9, un piano di formazione (Security Awareness Training) finalizzato a migliorare le competenze degli utenti su temi di Cyber Security ed accrescere la consapevolezza degli utenti su queste tematiche.

1.2 Ambito di Applicabilità

Il **Piano Triennale per l'informatica della Pubblica Amministrazione** è uno strumento essenziale per promuovere la trasformazione digitale dell'amministrazione italiana e del Paese e, in particolare quella della Pubblica Amministrazione (PA) italiana. Tale trasformazione dovrà avvenire nel contesto del mercato unico europeo di beni e servizi digitali, secondo una strategia che in tutta la UE si propone di migliorare l'accesso online ai beni e servizi per i consumatori e le imprese e creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi per massimizzare il potenziale di crescita dell'economia digitale europea. In tale contesto dove quindi i servizi digitali rappresentano un elemento indispensabile per il funzionamento di un Paese, la PA ne è parte fondamentale e indispensabile.

È ampiamente noto che la minaccia cibernetica è sempre più attiva e cresce continuamente in qualità e quantità minacciando infrastrutture critiche, processi digitali e rappresentando anche un elevato rischio di natura militare visto l'utilizzo che è sempre più diffuso verso quello che chiamiamo il perimetro di sicurezza cibernetico. In questo scenario di notevole fermento, il Piano delle Gare Strategiche ICT, concordato tra Consip e AgID, ha l'obiettivo, tra le altre cose, di mettere a disposizione delle Pubbliche Amministrazioni delle specifiche iniziative finalizzate all'acquisizione di prodotti e di servizi nell'ambito della sicurezza informatica, facilitando l'attuazione del Piano Triennale e degli obiettivi del PNRR in ambito, restando in linea con le disposizioni normative relative al settore della cybersicurezza. Il Piano mantiene l'attenzione rispetto al passato ponendosi anche il cruciale

problema della protezione del dato. Questo elemento è fondamentale perché tale protezione è strettamente connessa alla sua qualità e agire correttamente consente di attuare anche gli obblighi normativi europei in materia di protezione dei dati personali (GDPR).

Il Piano si focalizza sulla **Cyber Security Awareness**, poiché tale consapevolezza fa scaturire azioni organizzative indispensabili per mitigare il rischio connesso alle potenziali minacce informatiche. Nella PA ci sono frequenti attacchi a portali che bloccano i servizi erogati e costituiscono danno di immagine. È in crescita anche il fenomeno denominato data breach (violazione dei dati) che rappresenta anche una grave violazione del GDPR. Le azioni stabilite nel Piano sono tutte indispensabili rispetto allo scenario possibile. Oltre agli attori coinvolti nel Piano resta indispensabile e cruciale il supporto del Garante per la protezione dei dati personali quantomeno per verificare se la PA ha nominato un adeguato DPO (figura obbligatoria per il GDPR) ed è organizzata, almeno ai minimi termini, in linea con le regole del GDPR (Regolamento europeo 679/2016). Il Piano affida a Linee guida e regole specifiche ma anche alle strutture specifiche di AgID il supporto alle Pubbliche Amministrazioni.

In particolare, AgID ha concordato l'indirizzo strategico per la progettazione della presente iniziativa con particolare riferimento sui contenuti tecnici e sui meccanismi di coordinamento e controllo dell'utilizzo dello strumento di acquisizione; Consip S.p.A., in qualità di soggetto Stazione Appaltante, ha aggregato i fabbisogni e predisposto la procedura di gara e gestirà la stipula dei contratti per le amministrazioni centrali e locali. Le PA devono intraprendere misure ed azioni per l'avvio di progetti finalizzati alla trasformazione digitale dei propri servizi in base al Modello strategico evolutivo dell'informatica della PA e ai principi definiti nel Piano Triennale.

In capo ai Fornitori è la responsabilità di supportare le Amministrazioni mediante i servizi resi disponibili dalla presente iniziativa e supportare i soggetti deputati al coordinamento e controllo, secondo quanto previsto dalla documentazione di gara.

Il RTI ha basato il modello di tali servizi sul National Institute of Standards and Technology (NIST) Cyber Security Framework (principale standard di sicurezza in ambito cyber, anche il framework nazionale si basa su di esso), arricchito dai principali standard e best practice di settore (ISO 27001, NERC-CIP, MITRE ATT&CK, ISF, SANS, ITIL e COBIT), integrando i requisiti normativi cogenti (es. GDPR/Privacy, NIS) e, come fattore abilitante nel contesto della PA, è allineato al Framework Nazionale per la Cybersecurity e la Data Protection.

In particolare, nella figura sottostante è riportata la mappatura dei servizi offerti al Framework, al fine di illustrare come tali servizi siano funzionali a ciascuna area del Framework.

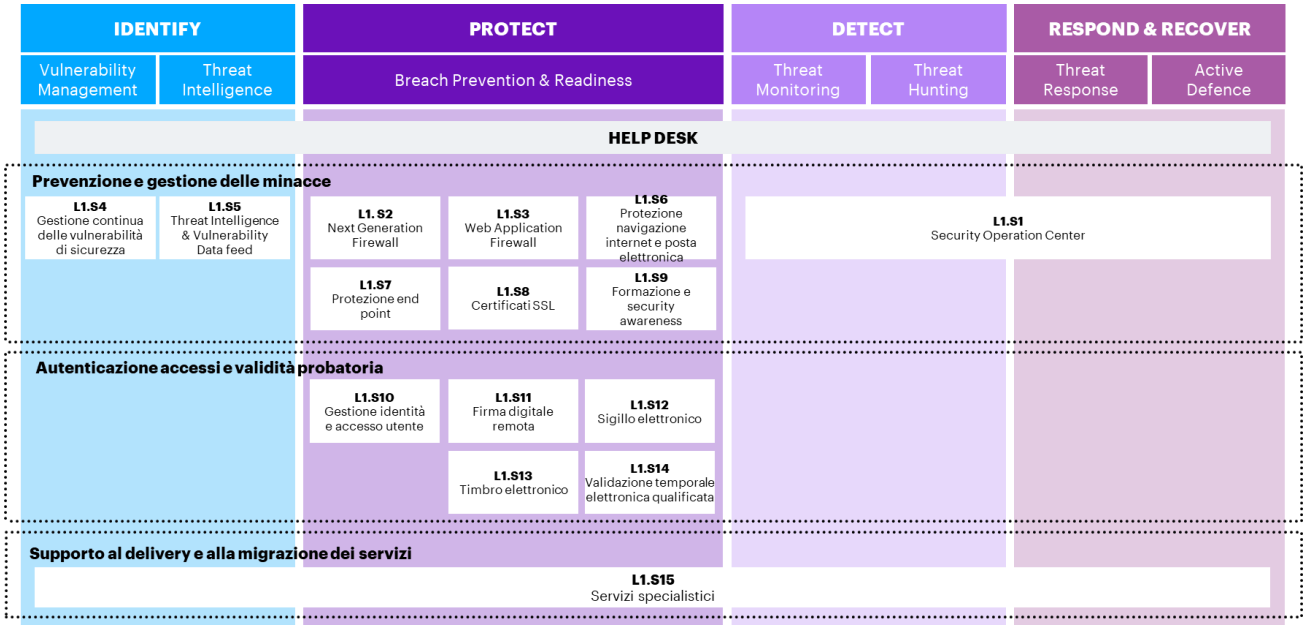

Figura 1 - Mappatura Servizi di Sicurezza e Framework NIST

In linea con le previsioni del Piano Triennale e al fine di indirizzare e governare la trasformazione digitale della PA italiana, sono previste la definizione e l'implementazione di misure di governance centralizzata, anche mediante la costituzione di **Organismi di coordinamento e controllo**, finalizzati alla direzione strategica e alla direzione tecnica della stessa. In particolare, le attività di direzione strategica prevedono il coinvolgimento di soggetti istituzionali, mentre nell'ambito delle attività di direzione tecnica

saranno coinvolti anche soggetti non istituzionali, individuati nei Fornitori Aggiudicatari della presente acquisizione. Si precisa che per "Organismi di coordinamento e controllo", si intendono i soggetti facenti capo alla Presidenza del Consiglio e/o al Ministero per l'Innovazione tecnologica e la Digitalizzazione (es: Agid, Team Digitale), che, in base alle funzioni attribuite ex lege, sono ad oggi deputati, per quanto di rispettiva competenza, al monitoraggio e al controllo delle iniziative rientranti nel Piano Triennale per l'informatica nella Pubblica Amministrazione. Nell'ambito di tali Organismi è ricompresa altresì Consip S.p.A., per i compiti di propria competenza. Rimangono salve eventuali modifiche organizzative che interverranno a livello istituzionale nel corso della durata del presente Accordo Quadro.

Gli Organismi di coordinamento e controllo saranno normati da appositi Regolamenti che, resi disponibili alla stipula dei contratti relativi alla presente iniziativa o appena possibile, definiranno gli aspetti operativi delle attività di coordinamento e controllo, sia tecnico che strategico.

I meccanismi di governance sopra introdotti e applicati anche a tutte le iniziative afferenti al Piano Triennale riguarderanno:

- i processi di procurement, veicolati attraverso gli strumenti di acquisizione messi a disposizione da Consip;
- l'inquadramento o categorizzazione degli interventi delle Amministrazioni, realizzati mediante la sottoscrizione di uno o più contratti esecutivi afferenti alle iniziative del Piano Strategico, nel framework del Piano Triennale;
- l'individuazione, da parte delle Amministrazioni beneficiarie, secondo quanto fornito in documentazione di gara, degli indicatori di digitalizzazione coi quali gli Organismi di coordinamento e controllo analizzeranno e valuteranno gli interventi realizzati dalle Amministrazioni con i contratti afferenti alle Gare strategiche;
- la valutazione e l'attuazione della revisione dei servizi previsti dagli Accordi Quadro e/o dei relativi prezzi, per le Gare Strategiche che lo prevedono in documentazione di gara e in funzione dell'evoluzione tecnologica del mercato e/o della normativa applicabile;
- l'analisi e la verifica di coerenza, rispetto al perimetro di ogni Gara Strategica, degli interventi delle Amministrazioni realizzati mediante contratti attuativi afferenti alle Gare Strategiche;
- le modalità e le tempistiche con cui i fornitori dovranno consegnare i dati relativi ai contratti esecutivi, con particolare riferimento alla fase di chiusura degli Accordi Quadro.

L'iniziativa in oggetto si affianca alle gare strategiche previste da AgID ai fini dell'attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione nelle versioni 2018-2020 e successive, nell'attuazione del processo di trasformazione digitale del Paese. Storicamente, il Sistema Pubblico di Connettività (SPC) ha seguito la rete unitaria della pubblica amministrazione (RUPA), nata con l'intento di connettere le pubbliche amministrazioni, almeno quelle centrali. Il Sistema Pubblico di Connettività (SPC), è posto alla base delle infrastrutture materiali dell'architettura disegnata nel Piano Triennale l'informatica nella Pubblica Amministrazione 2017-2019 di AgID, il cosiddetto Modello Strategico. È un sistema composto da molti servizi stratificati, dalla connettività ai servizi Cloud, ed è stato aggiornato nel 2016 con nuove gare Consip SPC2, SPC Cloud ampliando il portafoglio dei servizi e delle infrastrutture.

L'iniziativa Sicurezza da remoto si pone un **duplice obiettivo**:

- quello di garantire la continuità e l'evoluzione dei servizi già previsti nella precedente iniziativa SPC Cloud – Lotto 2 avente ad oggetto servizi di sicurezza volti alla protezione dei sistemi informativi in favore delle Pubbliche Amministrazioni, nell'ambito del Sistema pubblico di connettività;
- quello di rendere disponibili alle Amministrazioni servizi con carattere di innovazione tecnologica per l'attuazione del Codice dell'Amministrazione Digitale, nonché del Piano Triennale ICT della PA.

Lo scenario è contestualmente caratterizzato dalla presenza di due Lotti dedicati ai servizi di Sicurezza da remoto e servizi di Compliance e controllo. Tale specializzazione si innesta in considerazione dei diversi obiettivi a cui i due Lotti rispondono.
In particolare:

- il **Lotto di servizi di Sicurezza da remoto (Lotto 1)** ha 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;
- il **Lotto di servizi di Compliance e controllo (Lotto 2)** ha l'obiettivo di mettere a disposizione delle Amministrazioni servizi - erogati "on-site" in logica di progetto – finalizzati alla elaborazione di un "progetto di sicurezza" che identifica lo stato di

salute della sicurezza del sistema informativo dell'Amministrazione e nel controllo imparziale sulla corretta esecuzione dei servizi di sicurezza del Lotto 1 nonché sulla efficacia delle misure di sicurezza attuate, a partire dalla fase di acquisizione degli stessi sino alla loro esecuzione a regime.

In riferimento a quanto sopra riportato, **Regione Piemonte**, intende avvalersi dei **servizi di Sicurezza da Remoto** previsti per il **Lotto 1**, secondo i termini e le condizioni dell'**Accordo Quadro per l'Affidamento di Servizi da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni – Lotto 1 ID2296 –** (Accordo Quadro o AQ), senza riaprire il confronto competitivo tra gli operatori economici parti dell'Accordo Quadro ("AQ a condizioni tutte fissate").

Nell'ambito di tale lotto, si riportano di seguito i **servizi fruibili**, così come previsto dall'Accordo Quadro:

- L1.S1 - Security Operation Center (SOC)
- L1.S2 - Next Generation Firewall
- L1.S3 - Web Application Firewall
- L1.S4 - Gestione continua delle vulnerabilità di sicurezza
- L1.S5 - Threat Intelligence & Vulnerability Data Feed
- L1.S6 - Protezione navigazione Internet e Posta elettronica
- L1.S7 - Protezione degli endpoint
- L1.S8 - Certificati SSL
- L1.S9 - Servizio di Formazione e Security awareness
- L1.S10 - Gestione dell'identità e l'accesso utente
- L1.S11 - Firma digitale remota
- L1.S12 - Sigillo elettronico
- L1.S13 - Timbro elettronico
- L1.S14 - Validazione temporale elettronica qualificata
- L1.S15 - Servizi specialistici

A tal fine, **Regione Piemonte** ha individuato il Raggruppamento Temporaneo di Imprese (RTI o Fornitore) composto da Accenture S.p.A. (Accenture, impresa mandataria), Fastweb S.p.A. (Fastweb), Fincantieri NexTech S.p.A. (Fincantieri), e Difesa e Analisi Sistemi S.p.A. (DEAS) , quale aggiudicatario dell'Accordo Quadro che effettuerà la prestazione, sulla base di decisione motivata in relazione alle specifiche esigenze dell'amministrazione e in relazione a quanto stipulato nell'Accordo Quadro di riferimento.

1.3 Assunzioni

ID	AMBITO	ASSUNZIONE
1	Adeguamenti Normativi	A fronte di eventuali novità di carattere normativo che riguardano i processi e i sistemi oggetto della presente fornitura, dovranno essere valutati e condivisi tra Regione Piemonte e fornitore gli eventuali interventi progettuali da attivare/modificare nonché gli impatti in termini di Piano di Lavoro Generale

Tabella 2 - Assunzioni

2 RIFERIMENTI

2.1 Normativa di riferimento

Trovano applicazione le normative e gli standard internazionali riportate al "Capitolato Tecnico Generale" (§ 4.6) [DA-1].

2.2 Documenti Applicabili

Rif.	Titolo
DA-1.	ALLEGATO 1 - CAPITOLATO TECNICO GENERALE - Gara a procedura aperta per la conclusione di un accordo quadro, ai sensi del d.lgs. 50/2016 e s.m.i., suddivisa in 2 lotti e avente ad oggetto l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni.
DA-2.	ALLEGATO 2A - CAPITOLATO TECNICO SPECIALE SERVIZI DI SICUREZZA DA REMOTO
DA-3.	Accordo Quadro
DA-4.	Offerta Tecnica – Lotto 1 GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
DA-5.	Appendice 1 al CTS Lotto 1_Indicatori di qualità - ID 2296 - Gara Sicurezza da remoto
DA-6.	Piano dei Fabbisogni

Tabella 3 - Documenti Applicabili

3 DEFINIZIONI E ACRONIMI

3.1 Acronimi

Definizione	Descrizione
Accordo Quadro (AQ)	L'Accordo Quadro stipulato tra il/i Fornitore/i aggiudicatario/i e Consip S.p.A. all'esito della procedura di gara di prima fase
Aggiudicatario / Fornitore	Se non diversamente indicato vanno intesi gli aggiudicatari previsti per ciascun AQ per ciascuno dei Lotti della fornitura
Amministrazioni	Pubbliche Amministrazioni
Amministrazione Aggiudicatrice	Consip S.p.A.
Amministrazione/i Contraente/i	Pubbliche Amministrazioni che hanno siglato o intendono affidare un contratto esecutivo con il Fornitore per l'erogazione di uno dei servizi oggetto dell'Accordo Quadro
Capitolato Tecnico Generale	Documento che definisce il funzionamento e i requisiti comuni ai lotti oggetto della presente iniziativa
Capitolati Tecnici Speciali	Integrano il Capitolato Tecnico Generale e definiscono i contenuti di dettaglio e i requisiti minimi in termini di quantità, qualità e livelli di servizio, relativamente al Lotto 1 avente ad oggetto i Servizi di Sicurezza da remoto e al Lotto 2 avente ad oggetto i Servizi di Compliance e controllo
Collaudo e verifica di Conformità	Effettuati dall'Amministrazione e corrispondenti alla valutazione con verifica di merito dei prodotti consegnati
Componente	Il singolo elemento della configurazione di un sistema sottoposto a monitoraggio
Contratto Esecutivo	Il Contratto avente ad oggetto Servizi di Sicurezza da remoto, di Compliance e di Controllo per le Pubbliche Amministrazioni (Lotto 1)
Piano dei Fabbisogni	Il documento inviato dall'Amministrazione al Fornitore, al quale l'Amministrazione medesima affida il singolo Contratto Esecutivo e nel quale dovranno essere riportate, tra l'altro, le specifiche esigenze dell'Amministrazione che hanno portato alla scelta del fornitore
Piano Operativo	Il documento, inviato dal Fornitore all'Amministrazione, contenente la traduzione operativa dei fabbisogni espressi dall'Amministrazione con le modalità indicate nel presente documento
Prodotto della Fornitura	Tutto ciò che viene realizzato dal fornitore. Comprende tutta la documentazione contrattuale e gli artefatti come definiti nell'appendice Livelli di servizio
Modalità di erogazione da remoto	Servizio erogato - in modalità *managed* - attraverso i Centri Servizi del Fornitore
Modalità di lavoro *On-site*	Servizio erogato presso le strutture dell'Amministrazione contraente o altre strutture indicate dalla stessa o in alternativa presso la sede del Fornitore
Milestone	In ingegneria del software e Project Management indica ciascun traguardo intermedio e il traguardo finale dello svolgimento del progetto. Sono i punti di controllo all'interno di ciascuna fase oppure di consegna di specifici deliverable o raggruppamenti di deliverable. Sono normalmente attività considerate convenzionalmente a durata zero che servono per isolare nella schedulazione i principali momenti di verifica e validazione. Di fatto ciascun punto di controllo serve per approvare quanto fatto a monte della milestone ed abilitare le attività previste a valle della milestone
Sistema	Per Sistema si intende la singola immagine del sistema operativo, comprensiva di tutte le periferiche fisiche e/o logiche e di tutti i prodotti e/o servizi necessari al corretto funzionamento delle applicazioni, oppure l'insieme delle componenti HW e SW inserite in un unico chassis atto alla interconnessione e l'estensione di reti TLC (ad esempio apparati che gestiscono i primi quattro livelli della pila ISO-OSI)
Centro Servizi (CS)	La/e sede/i da cui l'Aggiudicatario eroga i servizi in modalità "da remoto" di cui al presente Capitolato per lo specifico Lotto di fornitura
Perimetro di Sicurezza Nazionale Cibernetica	Ai sensi del DL. Del 21 settembre 2002 n.105, il Perimetro è composto dai sistemi informativi e dai servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali

Tabella 4 - Definizioni

Vocabolo	Titolo
AgID	Agenzia per l'Italia Digitale
AQ	Accordo Quadro
BC	Business Continuity
CE	Contratto Esecutivo
CS	Centro Servizi
CTS	Capitolato Tecnico Speciale
DA	Documenti Applicabili
DDoS	Distributed Denial-of-Service
DR	Disaster Recovery
HVAC	Heating, Ventilation and Air Conditioning
HW	Hardware
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LRP	Livello di Rischio Previsto
LRR	Livello di Rischio Residuo
MGMT	Management
MPLS	MultiProtocol Label Switching
NDA	Non-Disclosure Agreement
OLO	Other Licensed Operators
PA	Pubblica Amministrazione
PEC	Posta Elettronica Certificata
PMO	Project Management Office
RPO	Recovery Point Objective
RTI	Raggruppamento Temporaneo di Impresa
RTO	Recovery Time Objective
SAN	Storage Area Network
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SIEM	Security Information and Event Management
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività
SSL	Secure Sockets Layer
SW	Software
UPS	Uninterruptible Power Supply
UTP	Unified Threat Protection
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network

Tabella 5 - Acronimi

4 ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

Di seguito trova descrizione l'organizzazione dell'RTI per l'erogazione dei servizi richiesti da Regione Piemonte nel Piano dei Fabbisogni.

L'approccio organizzativo che il RTI propone è volto a garantire:

- la gestione dell'Accordo Quadro (AQ) nel suo complesso, con ruoli di organizzazione, indirizzo e controllo dei diversi Contratti Esecutivi (CE) attivati (Governo dell'AQ);
- il coordinamento dei singoli CE e l'erogazione dei servizi richiesti per ciascuno di essi (Gestione dei CE);
- la capacità di adattarsi dinamicamente alle necessità della singola PA in base, ad esempio, alla maturità della stessa in ambito Cybersecurity, alle dimensioni, al contesto tecnologico, alla tipologia di dati trattati, alla distribuzione geografica e all'appartenenza del Perimetro di Sicurezza Cibernetico Nazionale.

L'organizzazione del RTI proposta per la conduzione dell'Accordo Quadro è mostrata nella figura di seguito riportata:

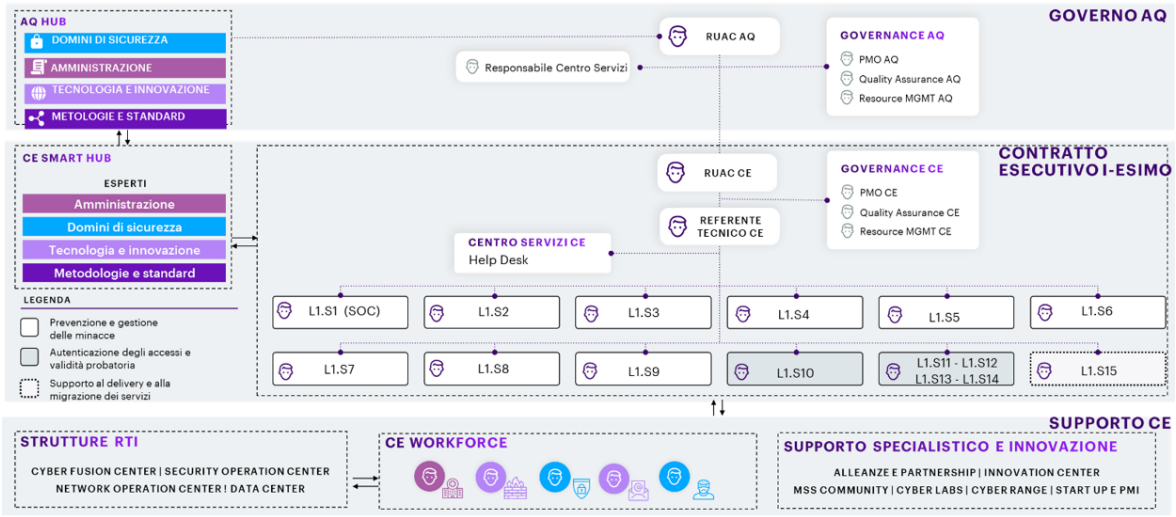

Figura 2 - Organizzazione dell'AQ proposta dal RTI

L'organigramma proposto prevede che il coordinamento delle attività del presente Accordo Quadro venga svolto dal Responsabile Unico della Attività Contrattuali dell'Accordo Quadro.

Il modello proposto si articola sui tre livelli di seguito illustrati:

- **Livello di Governo dell'AQ -** rappresenta il livello organizzativo più elevato per la gestione e il coordinamento dell'intera Fornitura. È presieduto dal Responsabile Unico delle Attività Contrattuali dell'AQ (RUAC AQ), che svolge un'azione di indirizzo e controllo strategico in ottica di gestione unitaria dei CE. Il RUAC AQ è designato dalla mandataria, presiede il Comitato di Coordinamento del RTI composto da figure manageriali delle aziende in esso contenute e dal Responsabile del Centro Servizi, che insieme definiscono la strategia di AQ e assicurano una visione unica e integrata dell'andamento dei servizi oggetto di gara, garantendo al tempo stesso la qualità complessiva dei CE per conseguire la piena soddisfazione delle PA.
  Il RUAC AQ è il principale riferimento del RTI per Consip, rappresenta inoltre il RTI all'interno dell'Organismo Tecnico di Coordinamento e Controllo ed è quindi la principale interfaccia verso i soggetti istituzionali su tutte le tematiche contrattuali. È supportato dal team di Governance AQ che include strutture/ruoli aggiuntivi (offerti senza oneri aggiuntivi) quali: Project Management Office, Quality Assurance e Resource Management.
- **Livello dei Contratti Esecutivi -** è progettato per adattarsi alle diverse tipologie di PA che aderiranno, garantendo la qualità e fornendo la maggiore flessibilità possibile per l'erogazione dei servizi. A tale livello sono coordinati ed erogati i servizi previsti per ogni CE ed è prevista la presenza di:
  - ❖ un Responsabile unico delle attività contrattuali del CE (RUAC CE);

- un Referente Tecnico CE;
- un team di Governance CE;
- un Help Desk dedicato all'assistenza dei Referenti identificati dall'Amministrazione,
- team responsabili dell'erogazione dei servizi previsti.

Il RUAC CE ha una responsabilità speculare a quella del RUAC AQ e rappresenta la principale interfaccia verso le singole PA per tutte le tematiche contrattuali, avendo allo stesso tempo compiti di raccordo tra i due livelli.
Il Referente Tecnico CE è responsabile del corretto svolgimento delle attività e dei servizi e il relativo livello di qualità di erogazione per il singolo CE ed è supportato dal team di Governance CE (PMO CE, Quality Assurance CE e Resource Management CE).
I Team responsabili dell'erogazione dei servizi, composti da professionisti di settore, hanno l'ulteriore supporto dei maggiori esperti di tematica del RTI (Subject Matter Expert) per assicurare omogeneità di metodologie e innovazione continua in base all'evoluzione del contesto.

- **Livello Supporto CE -** garantisce due tipi di supporto:
  - *Scalabilità* - La CE Workforce comprende le strutture di appartenenza delle risorse assegnate ai CE, quali Cyber Fusion Center/Security Operation Center/Network Operation Center/Data Center, la cui dimensione garantisce flessibilità e scalabilità adeguata alle esigenze (es. aumento della domanda, complessità progettuale, contesto tecnologico, sensibilità dei dati);
  - *Supporto specialistico e innovazione* - Garantito da:
    - ✓ i CdC tecnologici (es. infrastruttura, rete, applicazioni, DB, S.O., sistemi di virtualizzazione e HW);
    - ✓ i Cyber Labs di Accenture, operanti a livello globale per introdurre nuove tecnologie di sicurezza tramite prove di laboratorio che ne facilitano l'integrazione sui sistemi cliente, e i centri di ricerca e sviluppo in ambito cyber di Fastweb (FDA-Fastweb Digital Academy), Fincantieri e DEAS;
    - ✓ il network di start-up e PMI innovative;
    - ✓ le partnership con i principali vendor in materia sicurezza;
    - ✓ le MSS COMMUNITY, specializzate per ambito (es. Application Security, Digital Identity, Threat Operations, Cloud Security, Continuous Risk Management), tecnologia delle soluzioni offerte e/o presenti presso le PA richiedenti, tematica (es. ambiti Difesa, Sanità);
    - ✓ i Cyber Range (Poligoni Cibernetici) di Accenture e DEAS;
    - ✓ i laboratori di test plant di Fastweb utilizzati per testare gli apparati di sicurezza, così come nella verifica della conformità dei prodotti effettuata dai CVCN (Centro di Valutazione e Certificazione Nazionale) e CV. In particolare, per la capacità del RTI di supportare Consip, le PA e gli organismi istituzionali (es. AgID, Agenzia per la Cyber Sicurezza Nazionale) in materia di Innovazione.
- **AQ HUB e CE SMART HUB -** Strutture aggiuntive composte da esperti di diversi ambiti, con il compito di stimolare e promuovere, rispettivamente a livello di AQ e di CE, l'innovazione e le competenze tecnologiche nell'erogazione dei servizi, rafforzare il livello di conoscenze nei vari domini di sicurezza e di awareness verso le PA anche rispetto alle opportunità offerte dal contratto, garantire la conformità a standard e best practice di settore.

Per quanto concerne invece i **Centri Servizi**, questi vengono coordinati da uno specifico Responsabile che opera a livello "Governo AQ" e in accordo ai seguenti criteri:

- struttura organizzativa unica che assume la responsabilità dell'erogazione del servizio per tutte le sedi operative;
- assegnazione di responsabilità specifiche centralizzate, a livello di CS e a diretto riporto del responsabile del CS, in merito alla gestione della sicurezza informatica e della continuità operativa;
- assegnazione di responsabilità specifiche distribuite, a livello di sede operativa, in merito alla sicurezza fisica e alla gestione ambientale ed energetica.

4.1 Attività in carico alle aziende del RTI

Nell'ambito della specifica fornitura le attività saranno svolte dalle aziende secondo la ripartizione seguente:

SERVIZIO	ACCENTURE	FASTWEB	FINCANTIERI	DEAS
L1.S9 – Formazione e Security Awareness	X	X	X	X
TOTALE (%)	99,01%	0,33%	0.33%	0.33%
TOTALE (€)	75.246,08 €	247,52 €	247,52 €	247,52 €

Tabella 6 - Ripartizione attività in carico

4.2 Organizzazione e figure di riferimento del Fornitore

Nella tabella che segue sono riportate le principali figure di riferimento del Fornitore, cui ruoli e responsabilità sono stati illustrati nella parte introduttiva del Capitolo:

FIGURE DI RIFERIMENTO E REFERENTI DEL FORNITORE
RUAC AQ
GOVERNANCE AQ (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
RESPONSABILE CENTRO SERVIZI
RESPONSABILE DI SICUREZZA INFORMATICA E CONTINUITÀ OPERATIVA
RESPONSABILE DI SEDE OPERATIVA
RUAC CE
GOVERNANCE CE (PROJECT MANAGEMENT OFFICE, QUALITY ASSURANCE, RESOURCE MANAGEMENT)
REFERENTE TECNICO CE
RESPONSABILI DELL'EROGAZIONE DEI SERVIZI

Tabella 7 - Figure di riferimento e referenti del Fornitore

4.3 Luogo di erogazione e di esecuzione della Fornitura

In base alla modalità di esecuzione dei servizi le prestazioni contrattuali dovranno essere svolte come indicato nel Piano dei Fabbisogni sempre da remoto attraverso i Centri Servizi del Fornitore.

5 AMBITI E SERVIZI

5.1 Ambiti di intervento

Il presente Piano Operativo riguarda l'erogazione del servizio **L1.S9 Formazione e Security Awareness**, servizio volto a sensibilizzare il personale dell'Amministrazione su vari aspetti relativi alla sicurezza delle informazioni, finalizzato ad accrescere il livello di consapevolezza ed elevare il livello di sicurezza dell'Amministrazione stessa.
Come indicato nel Piano dei Fabbisogni dall'Amministrazione l'ambito di intervento riguarda in particolare:

- una formazione di livello medio base per la totalità dei dipendenti Regionali (2450 utenti), durante i primi 9 mesi di servizio.
- una ulteriore formazione a livello avanzato per dipendenti con ruoli di responsabilità e incarichi affini a tematiche evolute di cybersicurezza (per un totale di 245 utenti), da erogarsi a partire dal decimo mese di servizio fino al termine dello stesso.

Le attività di formazione saranno erogate con il supporto della piattaforma CyberGuru e saranno destinate ad accrescere la consapevolezza degli utenti partecipanti sulle tematiche di sicurezza e fornire strumenti utili per favorire un comportamento adeguato in caso di attacchi informatici. Il servizio fa inoltre leva su specifici fattori innovativi, quali:

- assessment delle competenze dell'utente prima dell'esecuzione degli interventi di awareness con l'obiettivo di definire azioni adeguate e motivanti nel percorso di formazione;
- coinvolgimento dell'utente tramite diversi canali e strumenti, specificamente definiti in funzione delle caratteristiche ricoperte nell'organizzazione delle PA e dei rischi di sicurezza ad esso pertinenti;
- utilizzo di canali e-learning che facilitano l'accesso continuativo ai servizi e coinvolgono l'utente in percorsi di formazione progressivi nel tempo, con contenuti che possono essere usufruiti secondo le disponibilità operative;
- sviluppo di contenuti formativi tramite le agenzie di Accenture dedicate al mondo della comunicazione e dell'interattività così da fornire format e qualità di contenuti video e grafici adeguati ad ottenere un forte livello di engagement sulla tematica;
- adozione di strumenti di verifica del livello di formazione acquisito sulla base di meccanismi basati su analytics e AI per la somministrazione di test di verifica specifici, simulazioni (real life assessment) e certificazione / riconoscimento dei risultati raggiunti;
- disponibilità di personale altamente specializzato e certificato su tematiche di sicurezza informatica e continuità operativa (certificazioni ISO 27001, ISO 22310, CSX, CISA, CISSP, CISM) che predispone, sviluppa specificamente ed eroga i contenuti formativi.

5.2 Servizi

SERVIZIO	FASCIA	QUANTITÀ I ANNO	QUANTITÀ II ANNO
L1.S9 - Formazione e Security Awareness	**gg/p Team ottimale**	**242**	**65**

Tabella 8 - Servizi

5.3 Indicatore di progresso

Di seguito l'indicatore di progresso identificato in questa fase per l'erogazione della fornitura:

Denominazione	Indicatore di progresso		
Aspetto da valutare	Grado di mappatura di ciascuna classe di controlli ABSC delle misure minime di sicurezza AGID		
Unità di misura	Numero di Controlli	**Fonte dati**	Piano dei Fabbisogni o Piano di lavoro Generale
Periodo di riferimento	Momento di Pianificazione dell'intervento	**Frequenza di misurazione**	Per ogni intervento pianificato
Dati da rilevare	*N1: numero di controlli relativi alla specifica classe ABSC soddisfatti attraverso l'intervento* *NT: numero totale di controlli relativi alla specifica classe previsti dalle misure minime di sicurezza AGID*		
Regole di campionamento	Nessuna		
Formula	$Ip = (N_1 - N_0)/N_T$		
Regole di arrotondamento	Nessuna		
Valore di soglia	*N0: numero di controlli relativi alla specifica classe soddisfatti prima dell'intervento;*		
Applicazione	Amministrazione Contraente		

Tabella 9 - Schema definizione Indicatore di Progresso

Tale indicatore sarà oggetto di revisione con l'Amministrazione a valle della fase di presa in carico. In particolare, sarà attivato uno specifico tavolo di lavoro mirato a:

- valutare il grado di maturità digitale dei servizi offerti e il grado di maturità atteso;
- consolidare l'indicatore;
- definire le misure iniziali dell'indicatore;
- stabilire i target e cioè le misure attese alla fine del contratto.

6 SOLUZIONE PROPOSTA

6.1 Descrizione dei servizi richiesti

L1.S9 – Formazione e Security Awareness

Il servizio "Formazione e Security awareness" è mirato a sensibilizzare il personale dell'Amministrazione su svariati aspetti della 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 negli utenti 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.
Il servizio prevede, in particolare, l'erogazione di giornate/uomo offerte con l'ausilio della piattaforma Cyberguru, per attività di formazione (Security Awareness Training) in formato multimediale interattivo con i seguenti obiettivi:

- rendere consapevoli gli utenti su cos'è una minaccia informatica (in particolare con tecniche di Phishing),
- informare su come possa essere veicolata una tale minaccia informatica
- informare su come detta minaccia informatica possa arrecare danni materiali ed immateriali all'Amministrazione.

I servizi di formazione saranno erogati in conformità a quanto indicato nella tabella oraria indicata al par. 8.9 del Capitolato Tecnico Speciale e prevederanno 2 specifiche iniziative:

- una formazione di livello medio base per la totalità dei dipendenti Regionali (2450 utenti), durante i primi 9 mesi di servizio, con il supporto dei contenuti della piattaforma Cyberguru dei livelli 1 e 2.
- una ulteriore formazione a livello avanzato per dipendenti con ruoli di responsabilità e incarichi affini a tematiche evolute di cybersicurezza (per un totale di 245 utenti), da erogarsi a partire dal decimo mese di servizio fino al termine dello stesso, con il supporto dei contenuti della piattaforma Cyberguru del livello 3.

Gli utenti potranno accedere tramite le credenziali comunicate ad avvio del servizio alla piattaforma di Cyberguru che prevede una struttura modulare che include:

- Una sezione di Awareness: un innovativo sistema integrato di e-Learning che consente di coinvolgere tutta l'organizzazione in un percorso di apprendimento che sia al contempo educativo e stimolante;
- Una sezione Phishing: un innovativo sistema di e-training, in funzione AntiPhishing, che produce risultati efficaci grazie alla sua metodologia di training on the job e alle caratteristiche di automazione e Machine Learning;
- Una sezione Informativa: un percorso di formazione video basato su una metodologia induttiva e realizzato con tecniche di produzione avanzata e con uno storytelling particolarmente coinvolgente.

6.2 Utenza interessata / coinvolta

Il personale dell'Amministrazione stessa.

6.3 Eventuali riferimenti / vincoli normativi

Non applicabile.

7 PIANO DI PROGETTO

7.1 Cronoprogramma

L'erogazione dei servizi avrà durata 24 mesi, a decorrere dalla data di conclusione delle attività di presa in carico T0 (data di firma del contratto esecutivo + periodo di presa in carico), come indicato nella seguente tabella:

	ANNO I												ANNO II											
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
L1.S9 - Formazione e Security Awareness																								

Tabella 10 - Cronoprogramma

7.2 Data di Attivazione e Durata del Servizio

Il contratto esecutivo dispiegherà i suoi effetti dalla data di stipula e avrà una durata di 36 mesi decorrenti dalla data di conclusione delle attività di presa in carico dei servizi.

7.3 Gruppo di Lavoro

L'approccio organizzativo individuato e descritto all'interno del Capitolo 4 consente di predisporre team e organizzazioni del lavoro secondo condizioni ad hoc per ogni progetto, secondo i carichi di lavoro previsti nella progettualità condivisa ma facilmente scalabili, qualora in corso d'opera maturassero condizioni tali da richiedere una modifica al numero dei team, delle risorse o del perimetro d'intervento. Una volta individuate le peculiarità dell'Amministrazione contraente, la selezione del gruppo di lavoro avviene analizzando il contesto della stessa sia dal punto di vista tecnologico, individuando il personale maggiormente qualificato sulle tecnologie e sui prodotti già in uso o attese, che tematico, andando ad identificare le figure professionali con esperienze e competenze nel settore pubblico.

7.4 Modalità di esecuzione dei Servizi

Per la modalità di esecuzione dei servizi è possibile far riferimento al Capitolo 8 del Capitolato Tecnico Speciale. In generale, a partire dal Piano di Lavoro Generale, l'Amministrazione richiederà la stima ed il Piano di Lavoro del singolo stream progettuale (obiettivo), fornendo la documentazione di supporto ed i macro-requisiti per poter effettuare una stima dell'obiettivo.
Di seguito si riporta una tabella di sintesi con le principali milestone per ogni servizio:

MILESTONE	DESCRIZIONE	ATTORE
Richiesta stima e Piano di Lavoro	Richiesta al fornitore di procedere alla stima dei tempi e costi del servizio	**Amministrazione**
Stima (pre-dimensionamento)	Comunicazione dei tempi e dei costi previsti per servizio	**RTI**
Collaudo	Esecuzione del collaudo dei servizi per cui è stato richiesto	**RTI**
Attivazione	Individuazione del ciclo di vita ed avvio del fornitore a	**Amministrazione**

MILESTONE	DESCRIZIONE	ATTORE
	procedere con le attività sul servizio. Al momento dell'attivazione saranno noti elementi caratteristici ai quali si associa una valutazione di complessità	
Consegna	Rilascio degli artefatti previsti dal piano di lavoro, sia intermedi che finali	**RTI**
Approvazione e Verifica di Conformità	Riscontro degli artefatti consegnati in quantità e tipologia (ricevuta), senza valutazione di contenuto	**Amministrazione**
Accettazione e Verifica di Conformità	Verifica e validazione dei prodotti intermedi di servizio, previa verifica di merito. Certificazione della corretta esecuzione del servizio relativamente ai prodotti oggetto di approvazione	**Amministrazione**
Valutazione difettosità all'avvio e Verifica di Conformità	Verifica della piena fruizione delle funzionalità e dei servizi da parte dell'utente (cittadino/ impresa/ operatore amministrativo/ decisore/ fruitore) tramite l'esame della quantità e della tipologia di malfunzionamenti e non conformità rilevati durante il periodo di avvio in esercizio. Certificazione della corretta esecuzione del servizio	**Amministrazione**

Tabella 11 - Descrizione milestone per obiettivo

Per il Governo della Fornitura, si propone l'adozione delle pratiche di seguito descritte:

- **Stato avanzamenti lavori – tecnico.** Con cadenza mensile (o su richiesta dell'Amministrazione) per le attività progettuali e mensile (o su richiesta dell'Amministrazione) per quelle continuative, verrà prodotto un report di sintesi che sarà discusso nel corso di un meeting ad hoc con l'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.

7.5 Modalità di ricorso al Subappalto da parte del Fornitore

Di seguito sono elencate, per ogni azienda del RTI, le attività fra quelle oggetto del presente Piano Operativo, che detta azienda intende subappaltare e relativa quota massima per l'insieme di tali attività.

La quota massima di attività subappaltabile – o concedibile in cottimo – da parte del RTI è pari al 50% dell'importo complessivo previsto dal contratto. Di seguito è riportato l'elenco delle attività / prestazioni per parti delle quali il RTI intende ricorrere al subappalto:

SERVIZIO	AZIENDA	QUOTA MASSIMA SUBAPPALTABILE
L1.S9 – Formazione e Security Awareness	**Accenture**	**50%**
L1.S9 – Formazione e Security Awareness	**Fastweb**	**50%**
L1.S9 – Formazione e Security Awareness	**Deas**	**50%**
L1.S9 – Formazione e Security Awareness	**Fincantieri**	**50%**

Tabella 12 - Modalità di ricorso al Subappalto da parte del Fornitore

8 DIMENSIONAMENTO ECONOMICO

8.1 Modalità di erogazione dei Servizi

Di seguito sono riportate per ogni servizio le metriche di misura e le modalità di erogazione e consuntivazione.

ID SERVIZIO	METRICA	MODALITÀ EROGAZIONE	MODALITÀ CONSUNTIVAZIONE	PERIODICITÀ CONSUNTIVAZIONE	PREZZO UNITARIO OFFERTO	QUANTITÀ TOTALE	VALORE ECONOMICO TOTALE
L1.S9	gg/p Team ottimale	Remoto	Progettuale/ a corpo	Mensile	247,52	242 (I anno) 65 (II anno)	75.988,64 €

Tabella 13 - Quadro economico di riferimento

L'importo complessivo dell'ordinativo di fornitura ammonta a **75.988,64 €** (IVA Esclusa).

8.2 Indicazioni in ordine alla fatturazione ed ai termini di pagamento

La fatturazione sarà eseguita in accordo con quanto previsto nello Schema di Contratto Esecutivo. Per quanto concerne i termini di pagamento si fa riferimento a quanto previsto nell'Accordo Quadro.

9 ALLEGATI

9.1 Piano di Lavoro Generale

Per il piano di lavoro generale si rimanda all'allegato Piano di Lavoro Generale.

9.2 Piano di Presa in Carico

Per il piano di presa in carico si rimanda all'allegato Piano di Presa in Carico.

9.3 Piano della Qualità Specifico

Per il piano di qualità specifico si rimanda al documento denominato Piano della Qualità Specifico.

9.4 Curriculum Vitae dei Referenti

Si allega, nel Piano di Lavoro Generale, il CV del RUAC di CE. Per quanto concerne il Referente Tecnico di CE, il relativo nominativo sarà fornito per la stipula del CE ed il relativo CV sarà fornito entro 5 giorni dalla stipula.

9.5 Misure di Sicurezza poste in essere

Per le misure di sicurezza poste in essere si rimanda al Piano di Sicurezza del Centro Servizi.

9.6 Documentazione relativa al principio "Do No Significant Harm" (DNSH)

Si allega la documentazione trasmessa a Consip tramite pec in data 11/11/2022, relativa al principio "Do No Significant Harm" (DNSH).

REGIONE PIEMONTE

APPENDICE A – ELENCO REGISTRAZIONI CONTABILI

REGISTRAZIONI CONTABILI DELLA DETERMINAZIONE DIRIGENZIALE

ATTO DD 599/A1911A/2023 DEL 29/12/2023

Impegno N.: 2024/6191
Descrizione: INTERVENTO 3A - SECURITY AWARENESS E FORMAZIONE
Importo (€): 59.899,84
Cap.: 207164 / 2024 - PNRR - MISSIONE M1, COMPONENTE C1, INVESTIMENTO1.5 "CYBERSECURITY - PROGETTO ANALISI, REVISIONE E POTENZIAMENTO DEL PERIMETRO DI SICUREZZA RIFERITO A POSTAZIONI DI LAVORO E RETE REGIONALE" - SOFTWARE
Macro-aggregato: Cod. 2020000 - Investimenti fissi lordi e acquisto di terreni
CIG: A03A642A24
CUP: J14F22001120006
Soggetto: Cod. 73660
PdC finanziario: Cod. U.2.02.03.02.001 - Sviluppo software e manutenzione evolutiva
COFOG: Cod. 01.3 - Servizi generali
Tipo finanziamento: Cod. S - FONDI STATALI
Trans. UE: Cod. 4 - per le spese finanziate da trasferimenti statali correlati ai finanziamenti dell'Unione europea
Natura ricorrente: Cod. 4 - Non ricorrente
Perimetro sanitario: Cod. 3 - per le spese delle gestione ordinaria della regione
Debito SIOPE: Cod. CO - Commerciale
Titolo: Cod. 2 - Spese in conto capitale
Missione: Cod. 01 - Servizi istituzionali, generali e di gestione
Programma: Cod. 0112 - Politica regionale unitaria per i servizi istituzionali, generali e di gestione (solo per le Regioni)

REGIONE PIEMONTE

APPENDICE A – ELENCO REGISTRAZIONI CONTABILI

REGISTRAZIONI CONTABILI DELLA DETERMINAZIONE DIRIGENZIALE

ATTO DD 599/A1911A/2023 DEL 29/12/2023

Impegno N.: 2024/6204
Descrizione: NEXTGENERATIONEU - PNRR M1C1|1.5 "CYBERSECURITY". INTERVENTO 3A, INIZIATIVA "ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI". ADESIONE ALL'AQ "ID 2296 - SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PA - LOTTO 1" IMPEGNO DI SPESA A FAVORE DI ACCENTURE SPA € 15.346,24 CAP. 106601/2024
Importo (€): 15.346,24
Cap.: 106601 / 2024 - INTERVENTI ORDINARI E STRAORDINARI PER LA FORMAZIONE E L'AGGIORNAMENTO PROFESSIONALE DEI DIPENDENTI REGIONALI. SPESE PER L'ACQUISTO DI METODOLOGIE E MATERIALI DIDATTICI, PARTECIPAZIONI O CONTRIBUTI A SPERIMENTAZIONI E STUDI, PROGETTAZIONE, ISTITUZIONE, SVOLGIMENTO DI ATTIVITA' FORMATIVE INTERNE, PARTECIPAZIONE DI DIPENDENTI REGIONALI A CORSI, CONVEGNI DI STUDI,SEMINARI ED ALTRE INIZIATIVE DI FORMAZIONE PROFESSIONALE,ANCHE ORGANIZZATE DA ENTI ESTERNI (C.C.N.L. PER GLI ANNI 1998-2001, COMPARTO DEL PERSONALE DELLE REGIONI ED AUTONOMIE LOCALI).
Macro-aggregato: Cod. 1030000 - Acquisto di beni e servizi
CIG: A03A642A24
CUP: J14F22001120006
Soggetto: Cod. 73660
PdC finanziario: Cod. U.1.03.02.04.999 - Acquisto di servizi per altre spese per formazione e addestramento n.a.c.
COFOG: Cod. 01.3 - Servizi generali
Tipo finanziamento: Cod. R - FONDI REGIONALI
Trans. UE: Cod. 8 - per le spese non correlate ai finanziamenti dell'Unione europea
Natura ricorrente: Cod. 4 - Non ricorrente
Perimetro sanitario: Cod. 3 - per le spese delle gestione ordinaria della regione
Debito SIOPE: Cod. CO - Commerciale
Titolo: Cod. 1 - Spese correnti
Missione: Cod. 01 - Servizi istituzionali, generali e di gestione
Programma: Cod. 0110 - Risorse umane

REGIONE PIEMONTE

APPENDICE A – ELENCO REGISTRAZIONI CONTABILI

REGISTRAZIONI CONTABILI DELLA DETERMINAZIONE DIRIGENZIALE

ATTO DD 599/A1911A/2023 DEL 29/12/2023

Impegno N.: 2024/6205
Descrizione: NEXTGENERATIONEU - PNRR M1C1|1.5 "CYBERSECURITY". INTERVENTO 3A, INIZIATIVA "ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI". ADESIONE ALL'AQ "ID 2296 - SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PA - LOTTO 1" IMPEGNO DI SPESA A FAVORE DI FASTWEB SPA € 247,52 CAP. 106601/2024
Importo (€): 247,52
Cap.: 106601 / 2024 - INTERVENTI ORDINARI E STRAORDINARI PER LA FORMAZIONE E L'AGGIORNAMENTO PROFESSIONALE DEI DIPENDENTI REGIONALI. SPESE PER L'ACQUISTO DI METODOLOGIE E MATERIALI DIDATTICI, PARTECIPAZIONI O CONTRIBUTI A SPERIMENTAZIONI E STUDI, PROGETTAZIONE, ISTITUZIONE, SVOLGIMENTO DI ATTIVITA' FORMATIVE INTERNE, PARTECIPAZIONE DI DIPENDENTI REGIONALI A CORSI, CONVEGNI DI STUDI,SEMINARI ED ALTRE INIZIATIVE DI FORMAZIONE PROFESSIONALE,ANCHE ORGANIZZATE DA ENTI ESTERNI (C.C.N.L. PER GLI ANNI 1998-2001, COMPARTO DEL PERSONALE DELLE REGIONI ED AUTONOMIE LOCALI).
Macro-aggregato: Cod. 1030000 - Acquisto di beni e servizi
CIG: A03A642A24
CUP: J14F22001120006
Soggetto: Cod. 96711
PdC finanziario: Cod. U.1.03.02.04.999 - Acquisto di servizi per altre spese per formazione e addestramento n.a.c.
COFOG: Cod. 01.3 - Servizi generali
Tipo finanziamento: Cod. R - FONDI REGIONALI
Trans. UE: Cod. 8 - per le spese non correlate ai finanziamenti dell'Unione europea
Natura ricorrente: Cod. 4 - Non ricorrente
Perimetro sanitario: Cod. 3 - per le spese delle gestione ordinaria della regione
Debito SIOPE: Cod. CO - Commerciale
Titolo: Cod. 1 - Spese correnti
Missione: Cod. 01 - Servizi istituzionali, generali e di gestione
Programma: Cod. 0110 - Risorse umane

REGIONE PIEMONTE

APPENDICE A – ELENCO REGISTRAZIONI CONTABILI

REGISTRAZIONI CONTABILI DELLA DETERMINAZIONE DIRIGENZIALE

ATTO DD 599/A1911A/2023 DEL 29/12/2023

Impegno N.: 2024/6206
Descrizione: NEXTGENERATIONEU - PNRR M1C1|1.5 "CYBERSECURITY". INTERVENTO 3A, INIZIATIVA "ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI". ADESIONE ALL'AQ "ID 2296 - SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PA - LOTTO 1" IMPEGNO DI SPESA A FAVORE DI FINCANTIERI NEXTECH S.P.A. € 247,52 CAP. 106601/2024
Importo (€): 247,52
Cap.: 106601 / 2024 - INTERVENTI ORDINARI E STRAORDINARI PER LA FORMAZIONE E L'AGGIORNAMENTO PROFESSIONALE DEI DIPENDENTI REGIONALI. SPESE PER L'ACQUISTO DI METODOLOGIE E MATERIALI DIDATTICI, PARTECIPAZIONI O CONTRIBUTI A SPERIMENTAZIONI E STUDI, PROGETTAZIONE, ISTITUZIONE, SVOLGIMENTO DI ATTIVITA' FORMATIVE INTERNE, PARTECIPAZIONE DI DIPENDENTI REGIONALI A CORSI, CONVEGNI DI STUDI,SEMINARI ED ALTRE INIZIATIVE DI FORMAZIONE PROFESSIONALE,ANCHE ORGANIZZATE DA ENTI ESTERNI (C.C.N.L. PER GLI ANNI 1998-2001, COMPARTO DEL PERSONALE DELLE REGIONI ED AUTONOMIE LOCALI).
Macro-aggregato: Cod. 1030000 - Acquisto di beni e servizi
CIG: A03A642A24
CUP: J14F22001120006
Soggetto: Cod. 385478
PdC finanziario: Cod. U.1.03.02.04.999 - Acquisto di servizi per altre spese per formazione e addestramento n.a.c.
COFOG: Cod. 01.3 - Servizi generali
Tipo finanziamento: Cod. R - FONDI REGIONALI
Trans. UE: Cod. 8 - per le spese non correlate ai finanziamenti dell'Unione europea
Natura ricorrente: Cod. 4 - Non ricorrente
Perimetro sanitario: Cod. 3 - per le spese delle gestione ordinaria della regione
Debito SIOPE: Cod. CO - Commerciale
Titolo: Cod. 1 - Spese correnti
Missione: Cod. 01 - Servizi istituzionali, generali e di gestione
Programma: Cod. 0110 - Risorse umane

REGIONE PIEMONTE

APPENDICE A – ELENCO REGISTRAZIONI CONTABILI

REGISTRAZIONI CONTABILI DELLA DETERMINAZIONE DIRIGENZIALE

ATTO DD 599/A1911A/2023 DEL 29/12/2023

Impegno N.: 2024/6207
Descrizione: NEXTGENERATIONEU - PNRR M1C1|1.5 "CYBERSECURITY". INTERVENTO 3A, INIZIATIVA "ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI". ADESIONE ALL'AQ "ID 2296 - SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PA - LOTTO 1" IMPEGNO DI SPESA A FAVORE DI DEAS - DIFESA E ANALISI SISTEMI S.P.A. € 247,52 CAP. 106601/2024
Importo (€): 247,52
Cap.: 106601 / 2024 - INTERVENTI ORDINARI E STRAORDINARI PER LA FORMAZIONE E L'AGGIORNAMENTO PROFESSIONALE DEI DIPENDENTI REGIONALI. SPESE PER L'ACQUISTO DI METODOLOGIE E MATERIALI DIDATTICI, PARTECIPAZIONI O CONTRIBUTI A SPERIMENTAZIONI E STUDI, PROGETTAZIONE, ISTITUZIONE, SVOLGIMENTO DI ATTIVITA' FORMATIVE INTERNE, PARTECIPAZIONE DI DIPENDENTI REGIONALI A CORSI, CONVEGNI DI STUDI,SEMINARI ED ALTRE INIZIATIVE DI FORMAZIONE PROFESSIONALE,ANCHE ORGANIZZATE DA ENTI ESTERNI (C.C.N.L. PER GLI ANNI 1998-2001, COMPARTO DEL PERSONALE DELLE REGIONI ED AUTONOMIE LOCALI).
Macro-aggregato: Cod. 1030000 - Acquisto di beni e servizi
CIG: A03A642A24
CUP: J14F22001120006
Soggetto: Cod. 385479
PdC finanziario: Cod. U.1.03.02.04.999 - Acquisto di servizi per altre spese per formazione e addestramento n.a.c.
COFOG: Cod. 01.3 - Servizi generali
Tipo finanziamento: Cod. R - FONDI REGIONALI
Trans. UE: Cod. 8 - per le spese non correlate ai finanziamenti dell'Unione europea
Natura ricorrente: Cod. 4 - Non ricorrente
Perimetro sanitario: Cod. 3 - per le spese delle gestione ordinaria della regione
Debito SIOPE: Cod. CO - Commerciale
Titolo: Cod. 1 - Spese correnti
Missione: Cod. 01 - Servizi istituzionali, generali e di gestione
Programma: Cod. 0110 - Risorse umane

REGIONE PIEMONTE

APPENDICE A – ELENCO REGISTRAZIONI CONTABILI

REGISTRAZIONI CONTABILI DELLA DETERMINAZIONE DIRIGENZIALE

ATTO DD 599/A1911A/2023 DEL 29/12/2023

Impegno N.: 2024/6209
Descrizione: NEXTGENERATIONEU - PNRR M1C1|1.5 "CYBERSECURITY". INTERVENTO 3A, INIZIATIVA "ICT_0_07 TRANSIZIONE DIGITALE E SERVIZI SICURI". ADESIONE ALL'AQ "ID 2296 - SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PA - LOTTO 1" IMPEGNO DI SPESA A FAVORE DI CONSIP S.P.A. € 607,91 CAP. 106601/2024
Importo (€): 607,91
Cap.: 106601 / 2024 - INTERVENTI ORDINARI E STRAORDINARI PER LA FORMAZIONE E L'AGGIORNAMENTO PROFESSIONALE DEI DIPENDENTI REGIONALI. SPESE PER L'ACQUISTO DI METODOLOGIE E MATERIALI DIDATTICI, PARTECIPAZIONI O CONTRIBUTI A SPERIMENTAZIONI E STUDI, PROGETTAZIONE, ISTITUZIONE, SVOLGIMENTO DI ATTIVITA' FORMATIVE INTERNE, PARTECIPAZIONE DI DIPENDENTI REGIONALI A CORSI, CONVEGNI DI STUDI,SEMINARI ED ALTRE INIZIATIVE DI FORMAZIONE PROFESSIONALE,ANCHE ORGANIZZATE DA ENTI ESTERNI (C.C.N.L. PER GLI ANNI 1998-2001, COMPARTO DEL PERSONALE DELLE REGIONI ED AUTONOMIE LOCALI).
Macro-aggregato: Cod. 1030000 - Acquisto di beni e servizi
CIG: A03A642A24
CUP: J14F22001120006
Soggetto: Cod. 379908
PdC finanziario: Cod. U.1.03.02.04.999 - Acquisto di servizi per altre spese per formazione e addestramento n.a.c.
COFOG: Cod. 01.3 - Servizi generali
Tipo finanziamento: Cod. R - FONDI REGIONALI
Trans. UE: Cod. 8 - per le spese non correlate ai finanziamenti dell'Unione europea
Natura ricorrente: Cod. 4 - Non ricorrente
Perimetro sanitario: Cod. 3 - per le spese delle gestione ordinaria della regione
Debito SIOPE: Cod. NC - Non commerciale
Titolo: Cod. 1 - Spese correnti
Missione: Cod. 01 - Servizi istituzionali, generali e di gestione
Programma: Cod. 0110 - Risorse umane

Accertamento N.: 2024/405
Descrizione: INZIATIVA NEXTGENERATIONEU CONTRIBUTO PNRR FINANZIATO DA ACN INTERVENTO 3A INIZIATIVA ICT_0_07 TRASIZIONE DIGITALE E SERVIZI SICURI
Importo (€): 59.899,84
Cap.: 20495 / 2024 - PNRR - MISSIONE M1, COMPONENTE C1, INVESTIMENTO 1.5 "CYBERSECURITY"
Soggetto: Cod. 382090
PdC finanziario: Cod. E.4.02.01.01.001 - Contributi agli investimenti da Ministeri
Tipo finanziamento: Cod. S - FONDI STATALI
Trans. UE: Cod. 1 - per le entrate derivanti da trasferimenti destinate al finanziamento dei progetti comunitari provenienti da amministrazioni pubbliche e da altri soggetti
Natura ricorrente: Cod. 2 - Non ricorrente
Perimetro sanitario: Cod. 1 - per le entrate delle gestione ordinaria della regione
Titolo: Cod. 4 - ENTRATE IN CONTO CAPITALE
Tipologia: Cod. 4020000 - Tipologia 200: Contributi agli investimenti