Codice A1910A
D.D. 27 dicembre 2023, n. 586
Piano Nazionale di Ripresa e Resilienza, Missione 1 - Componente 1 - Investimento 1.5 ''Cybersecurity'' M1C1I1.5. Contributo finanziato dall'Agenzia per la Cybersicurezza Nazionale a valere sull'Avviso 3/2022. Approvazione PTE ''ICT_1_03 Postazioni di Lavoro e Rete Regionale: l'evoluzione in sicurezza'' e affidamento delle attività di cui alle Schede Tecniche allegate alla PTE (Interventi 1A, 2A, 2B, 3A, 4A1, 4A2...

ATTO DD 586/A1910A/2023 DEL 27/12/2023

DETERMINAZIONE DIRIGENZIALE
A19000 - COMPETITIVITA' DEL SISTEMA REGIONALE
A1910A - Servizi infrastrutturali e tecnologici

OGGETTO: Piano Nazionale di Ripresa e Resilienza, Missione 1 - Componente 1 - Investimento 1.5 “Cybersecurity” M1C1I1.5. Contributo finanziato dall’Agenzia per la Cybersicurezza Nazionale a valere sull’Avviso 3/2022. Approvazione PTE “ICT_1_03 Postazioni di Lavoro e Rete Regionale: l’evoluzione in sicurezza” e affidamento delle attività di cui alle Schede Tecniche allegate alla PTE (Interventi 1A, 2A, 2B, 3A, 4A1, 4A2 e 4B) . Accertamento di complessivi € 483.279,85 sul cap. 20495 di cui Euro 274.079,85 annualità 2023 ed Euro 209.200,00 annualità 2024 e contestuali impegni di spesa sul cap. 207058 di Euro274.079,85 annualità 2023 ed Euro 209.200,00 annualità 2024 del Bilancio finanziario gestionale 2023-2025 a favore di CSI Piemonte. Approvazione dello schema di disciplinare d’incarico. CUP J14F22001110006.

Premesso che:

per rispondere alla crisi pandemica provocata dal Covid-19, l'Unione Europea, all'interno dello strumento finanziario denominato Next Generation EU, che prevede un pacchetto di finanziamenti pari a 750 miliardi di euro, ha approvato il Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021.
Tale strumento 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.

Alla luce di quanto sopra illustrato, Regione Piemonte ha pertanto ritenuto opportuno promuovere interventi di potenziamento della propria 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, 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 trasferimento del personale regionale nella nuova sede unica degli uffici della Giunta regionale: sull'infrastruttura da implementare insistono, infatti, sia gli ordinari servizi di rete degli Uffici, per oltre 2.000 utenti, sia i servizi di rete funzionali all'operatività di tutti gli impianti (B.M.S., ascensori, controllo accessi, videosorveglianza, impianti di sicurezza antincendio).

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 A1910A - Servizi Infrastrutturali e Tecnologici e dal Settore A1911A - 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 della 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 ha quindi aderito 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 ed ha demandato alla Direzione regionale Competitività del Sistema Regionale Settore A1911A - Sistema Informativo regionale e Settore A1910A - Servizi Infrastrutturali e Tecnologici l'adozione degli atti e dei provvedimenti necessari per l'attuazione della delibera 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 e ai relativi stanziamenti dei fondi.

In ottemperanza a tale deliberazione è stata inoltrata in data 29 settembre 2022 all'Agenzia per la

Cybersicurezza Nazionale la richiesta formale di presentazione delle due proposte di partecipazione.

Con determinazione 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, comprese le due inviate da Regione Piemonte.

Con determinazione dell'Agenzia per la Cybersicurezza Nazionale prot. n. 3429 del 20 gennaio 2023 (rettificata con successiva 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 risultava 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, veniva 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.

In data 17 febbraio 2023, Regione Piemonte ha trasmesso il documento "Atto d'Obbligo", 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.

In data 24/02/2023, il Settore A1910A - Servizi Infrastruttuali e Tecnologici ha trasmesso:
• il documento "COMUNICAZIONE AVVIO ATTIVITÀ E/O RICHIESTA DI ANTICIPAZIONE" nel quale si comunicava ad ACN che le attività relative al progetto "Postazioni di Lavoro e Rete Regionale: l'evoluzione in sicurezza" erano state avviate in data 02/02/2023, in conformità con le indicazioni del suddetto Avviso pubblico;
• il documento "RICHIESTA MODIFICA PROGETTO" anel quale si richiedeva ad ACN l'autorizzazione alla variazione del quadro finanziario e alla variazione del cronoprogramma del progetto "Postazioni di Lavoro e Rete Regionale: l'evoluzione in sicurezza" in conseguenza della variazione della data di avvio dovuta alle tempistiche di approvazione del progetto in oggetto da parte di ACN stessa, variazioni non comportanti una modifica sostanziale del progetto.

Con comunicazione via PEC in data 06/04/2023 (prot. reg. n. 3938/A1910A) ACN ha autorizzato le suddette rimodulazioni del cronoprogramma e del quadro finanziario .

Premesso, inoltre, che:

con la deliberazione di Giunta Regionale n. 21-4474 del 29 dicembre 2021, per le premesse e le motivazioni ivi contenute e richiamate espressamente nel provvedimento, è stata approvata la *"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 (repertorio n. 51 del 07.02.2022).
La citata deliberazione, dopo aver delineato il contesto normativo di riferimento per poter procedere all'approvazione della Convenzione per gli affidamenti diretti al CSI-Piemonte, evidenzia i presupposti, sia di carattere soggettivo dell'operatore economico, sia le condizioni oggettive che rendono preferibile il ricorso all'*in house providing.*

In merito ai requisiti soggettivi dell'OE, il ricorso all'in house deve avvenire nel rispetto delle disposizioni contenute nell'art. 5 del D.Lgs. 18 aprile 2016 n. 50 (Codice dei contratti pubblici), che richiama sia il D.Lgs. 19 agosto 2016 n. 175 "Testo unico in materia di società a partecipazione pubblica" s.m.i., sia le norme europee di riferimento (nello specifico la Direttiva 24/2014/UE all'art. 12, paragrafi 1,2 e 3 e la Direttiva 23/2014/UE all'art. 17, paragrafi, 1,2 e 3).

Nello specifico viene definita *in house* la società che soddisfa le seguenti condizioni:

- sia soggetta ad un controllo analogo da parte dell'amministrazione aggiudicatrice, anche in forma congiunta con altre amministrazioni(art. 5, comma 1, lett.a);
- eserciti almeno l'80% delle proprie attività a favore dell'amministrazione/i controllante/i (art. 5, comma 1 lett.b);
- non vi siano partecipazioni dirette di capitali privati che premettano l'esercizio di una influenza dominante (art. 5, comma 1 lett.c).

sulla base di quanto sopra illustrato, si può quindi affermare che il CSI-Piemonte, ente di diritto privato in controllo pubblico, opera in regime di *in house providing*, poiché possiede i requisiti soggettivi di cui sopra, peraltro, conformi a quelli indicati dalla giurisprudenza della Corte di Giustizia europea e prescritti da una consolidata giurisprudenza amministrativa che ha sempre ribadito come "la società *in house* sia equiparabile ad un ufficio interno dell'ente pubblico che l'ha costituita, sicché, non sussiste tra l'ente e la società un rapporto di alterità sostanziale, ma solo formale, ed è questa caratteristica l'unica a giustificare l'affidamento diretto, senza previa gara, di un appalto o di una concessione";

per quanto riguarda le condizioni oggettive che rendono preferibile l'attribuzione di diritti di esclusiva in luogo del ricorso al mercato, il riferimento è all'art. 192, comma 2 del Codice dei contratti pubblici, il quale prevede che negli affidamenti diretti in house sia compiuta la valutazione sulla congruità economica delle offerte, avuto riguardo all'oggetto e al valore della prestazione. Lo stesso articolo impone, altresì, alle stazioni appaltanti, per l'affidamento in house di un contratto avente ad oggetto servizi disponibili sul mercato in regime di concorrenza, l'obbligo di dare conto, nella motivazione del provvedimento di affidamento, delle ragioni del mancato ricorso al mercato, nonché dei benefici per la collettività, della forma di gestione prescelta, anche con riferimento agli obiettivi di efficienza, economicità e qualità del servizio, nonché, di ottimale impiego delle risorse pubbliche. Tale prescrizione normativa è stata opportunamente ripresa dalla Convenzione Quadro sopra citata all'articolo 6, comma 5, nel quale si fa riferimento, ai fini dell'affidamento diretto, ad un onere di motivazione "aggravato", nonché concreto, riscontrabile, pregnante sui profili della convenienza, non solo economica, della scelta.

Preso atto che:

Regione Piemonte è iscritta formalmente nell'elenco delle amministrazioni aggiudicatrici e degli enti aggiudicatori in ragione degli affidamenti in house, come da delibera ANAC n. 161 del 19

febbraio 2020; successivamente ANAC ha disposto, con Delibera 309 del 1° aprile 2020, l'integrazione della composizione degli enti che detengono il controllo analogo congiunto in relazione agli affidamenti in regime di in house providing al CSI Piemonte;

la Giunta regionale, con delibera n. 58-4509 del 29.12.2021, ha approvato la Programmazione Regionale in ambito ICT per il triennio 2021-2023 che definisce le linee di indirizzo per l'evoluzione del sistema informativo regionale;

con Determinazione n. 173 del 13.04.2023 del Settore A1911A - Sistema informativo regionale sono stati adottati i nuovi documenti tecnici, previsti dall'art. 1, comma 3, della Convenzione quadro 2022-2026;

gli atti di affidamento a favore del CSI e i relativi impegni di spesa devono avvenire nei limiti delle risorse finanziarie stanziate sui capitoli di bilancio e conseguentemente assegnate alla Direzioni regionali e in coerenza con la Programmazione Regionale in ambito ICT (approvata dalla Giunta regionale con delibera n. 58-4509 del 29.12.2021 per il triennio 2021-2023);

al fine di motivare le ragioni di mancato ricorso al mercato, per la formalizzazione degli affidamenti, è stata effettuata preliminarmente una valutazione di Congruità tecnico-economica del Catalogo e Listino dei Servizi del CSI Piemonte dell'anno 2023 (versione 1), approvato dal Consiglio di Amministrazione del Consorzio in data 21 ottobre 2022, contenente tutti i servizi erogati;

la "Valutazione della congruità tecnico economica del Catalogo e Listino dei Servizi del CSI Piemonte per l'anno 2023, è stata approvata dal Responsabile del Settore Sistema Informativo Regionale in data 07.12.2022 e trasmessa a tutte le Direzioni/Settori regionali interessati, con nota prot. 13865/A1911A in pari data; l'esito dell'istruttoria, sopra richiamata, ha messo in luce una metodologia strutturata e oggettiva mediante l'utilizzo di criteri di comparazione dei servizi e dei costi unitari del Catalogo applicati ad una chiara ed uniforme rappresentazione del mercato ICT di riferimento;

la Regione Piemonte affida in outsourcing la maggior parte delle attività relative allo sviluppo e gestione del Sistema Informativo Regionale, di cui fanno parte anche i servizi in ambito Cybersecurity per i quali CSI Piemonte riveste il ruolo di amministratore di sistema;

la convenzione Regione Piemonte-CSI è corredata da uno specifico allegato tecnico che disciplina i progetti cofinanziati con fondi SIE. Questo, aggiunto ad una consolidata esperienza pregressa relativa alla implementazione e alla gestione di progetti cofinanziati, assicura l'adeguata e tempestiva gestione degli stessi;

il ricorso all'affidamento all'in house, come descritto nel progetto "Postazioni di Lavoro e Rete Regionale: l'evoluzione in sicurezza", permette l'immediato avvio operativo delle attività, elemento determinante nel giudizio da parte dell'Agenzia per la Cybersicurezza Nazionale all'ammissione e finanziamento dei progetti presentati.

Dato atto 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 ed Euro 706.750,00 per l'anno 2024;

al fine di garantire la copertura finanziaria dei due suddetti progetti, sono stati istituiti, a seguito di specifica richiesta formulata dal Settore A1911A al Settore A1101A - Programmazione macroeconomica, bilancio e statistica, tre nuovi capitoli, uno di entrata, la cui titolarità è stata assegnata al Settore A1911A e due di spesa, con titolarità in capo ai due distinti Settori in base al progetto di propria competenza;

il progetto denominato “Postazioni di lavoro e rete regionale; l’evoluzione in sicurezza”, inserito e finanziato a valere sulle risorse PNRR, dell’importo complessivo di € 984.400,00, prevede al suo interno i seguenti interventi:
• Intervento 1: Analisi postura sicurezza e piano potenziamento
•Intervento 2: Miglioramento dei processi e dell’organizzazione di gestione della cybersecurity
• Intervento 3: Miglioramento della consapevolezza delle persone
• Intervento 4: Progettazione e sviluppo nuovi sistemi per la mitigazione del rischio;

con nota, prot. n. 1459/A1910A del 09/02/2023, il Settore Servizi Infrastrutturali e Tecnologici ha richiesto a CSI, in applicazione della Convenzione Quadro, di predisporre al riguardo apposita Proposta Tecnico Economica;

con nota prot. n. 3294 del 22/02/2023 (prot. reg. n. 2054/A1910A del 23/02/2023), CSI ha provveduto a trasmettere al Settore Servizi Infrastrutturali e Tecnologici l’“Offerta per il sistema di sicurezza perimetrale per le sedi regionali e le P.A. afferenti alla rete regionale Wi-Pie - Fornitura apparati” per un importo di € 357.000,00 oltre IVA (€ 435.540,00 o.f.i.), relativo all’Intervento n. 4, del quale rappresenta la sola componente di fornitura hardware;

con D.D. n. 282/A1910A del 30.06.2023 è stata approvata la suddetta PTE di iniziativa per la fornitura del sistema di sicurezza perimetrale ed è stata affidata a CSI tale attività (Intervento 4 – sola componente di fornitura hardware);

in coerenza con gli elementi di cui sopra, il CSI ha quindi presentato la PTE d’iniziativa “ICT_1_03 Postazioni di lavoro e Rete Regionale: l’evoluzione in sicurezza” (prot. CSI n. 16423 del 25/09/2023 - prot. del Settore 11338 del 26.09.2023) che prevede i seguenti interventi:

• Intervento 1A – Assessment Postura di sicurezza su Infrastruttura, Vulnerability Assessment, piano di remediation – *CUP J14F22001110006* - importo € 119.759,26
• Intervento 2A - Revisione di procedure e processi per la gestione del rischio cyber - *CUP J14F22001110006* - importo € 49.969,25
• Intervento n° 2B - Business Impact Analisys e Business Continuity Plan - *CUP J14F22001110006* - importo € 59.623,48
• Intervento n° 3A - Progettazione del percorso formativo, attuazione e simulazione incidenti - *CUP J14F22001110006* - importo € 59.849,43
• Intervento n° 4A1 - Securizzazione DaaS e Posti di Lavoro - *CUP J14F22001110006* - importo € 109.664,15
• Intervento n° 4A2 - NGFW per Regione ed Enti della rete Regionale - *CUP J14F22001110006* - importo € 26.658,93 (al netto di quanto già affidato con d.d. n. 282/A1910A del 30.06.2023 pari a € 435.540,00)
• Intervento n° 4B - Potenziamento del monitoraggio delle minacce Cyber per SOC e CSI regionale - *CUP J14F22001110006* - importo € 57.755,35,

per un importo complessivo pari a € 483.279,85 esente IVA, da suddividere tra le annualità 2023 e 2024 come definito nella tabella "Ripartizione Budget_baseline al 23 febbraio 2023.xlsx" agli atti

del Settore.

Con apposita nota conservata agli atti del Settore, in data 21/12/2023 gli uffici del Settore Servizi Infrastrutturali e Tecnologici A1910A e del Settore Sistema Informativo regionale A1911A hanno espresso parere positivo di congruità tecnico-economica, riferito alla succitata PTE e, in particolare, relativamente ai predetti Interventi 1A, 2A, 2B, 3A, 4A1, 4A2 e 4B, rendendo in tal modo legittimo l'affidamento diretto dei servizi ex art. 192 del D.Lgs. 50/2016.
Da tale nota risultano infatti evidenti i benefici in termini di efficienza (economica e tecnica), efficacia (qualitativa e quantitativa), economicità e qualità del servizio, in relazione alle peculiarità dei servizi descritti e agli elementi di cui all'art. 192 comma 2 del D.Lgs. 50/2016.
In particolare, il ricorso al partner tecnologico CSI-Piemonte, che riveste il ruolo di gestore e amministratore di sistema nell'ambito dello sviluppo e della gestione dei servizi di cybersecurity, garantisce da un lato la conformità, sotto il profilo tecnico, delle soluzioni tecnologiche adottate all'infrastruttura tecnica del sistema informativo regionale e, dall'altro, un aumento dell'efficacia e dell'efficienza nello svolgimento di tali servizi che devono essere erogati in forma integrata.
Il ricorso a CSI garantisce inoltre la consegna nelle modalità e nei tempi richiesti dall'Avviso 3/2022 dell'Agenzia Nazionale per la Cybersicurezza, capitalizzando le competenze acquisite nelle esperienze pregresse da parte del personale CSI-Piemonte e delle sue strutture organizzative, garantendo così una gestione ottimale delle risorse pubbliche.
CSI-Piemonte garantisce infine, dove necessario, la capacità di individuare le soluzioni di mercato più idonee ad essere inserite nella propria infrastruttura, garantendone la massima integrabilità, affidabilità della soluzione e adeguatezza alle necessità dell'Ente, per il quale riveste il ruolo di amministratore di sistema.

In tale quadro, è stato predisposto da parte del Settore scrivente il disciplinare di incarico, parte integrante e sostanziale del presente provvedimento, per l'affidamento degli interventi di cui sopra.

Tutto quanto sopra premesso, visto e considerato, con il presente provvedimento, si intende:

1) accertare dall'Agenzia per la Cybersicurezza Nazionale (cod.versante 382090) la somma complessiva di Euro 483.279,85 sul capitolo in entrata 20495 (PNRR - MISSIONE M1, COMPONENTE C1, INVESTIMENTO 1.5 "CYBERSECURITY") del Bilancio finanziario gestionale 2023-2025 - Tipologia 200: Contributi agli investimenti, Categoria 4020100 Contributi agli investimenti da amministrazioni pubbliche, P.d.C. finanziario E.4.02.01.01.001, secondo le seguenti modalità:

Euro 274.079,85 annualità 2023
Euro 209.200,00 annualità 2024

2) approvare la citata PTE di iniziativa "ICT_1_03 Postazioni di lavoro e Rete Regionale: l'evoluzione in sicurezza" (prot. del Settore 11338 del 26.09.2023) che prevede i seguenti interventi:
• Intervento 1A - Assessment Postura di sicurezza su Infrastruttura, Vulnerability Assessment, piano di remediation
• Intervento 2A - Revisione di procedure e processi per la gestione del rischio cyber
• Intervento n° 2B - Business Impact Analisys e Business Continuity Plan
• Intervento n° 3A - Progettazione del percorso formativo, attuazione e simulazione incidenti
• Intervento n° 4A1 - Securizzazione DaaS e Posti di Lavoro
• Intervento n° 4A2 - NGFW per Regione ed Enti della rete Regionale
• Intervento n° 4B - Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT regionale,

approvando,altresì, l’allegato schema di disciplinare d’incarico, parte integrante e sostanziale del presente provvedimento;

3) affidare al CSI-Piemonte (cod. beneficiario 12655) le attività di cui alle Schede Tecniche allegate alla suddetta PTE (relative agli Interventi 1A, 2A, 2B, 3A, 4A1, 4A2 e 4B), impegnando a favore dello stesso l’importo complessivo di Euro 483.279,85 sul cap. 207058 (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" – HARDWARE) del Bilancio finanziario gestionale 2023-2025 Missione 01 - Programma 0112 – PdC finanziario U.2.02.01.07.999 di cui:

Euro 274.079,85 annualità 2023
Euro 209.200,00 annualità 2024

4) approvare lo schema di disciplinare di incarico allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato A);

5) assegnare ai sig.ri Alessandro Fidanza e Fausto Grassi, funzionari del Settore A1910A - Servizi Infrastrutturali e Tecnologici, la responsabilità dell'istruttoria del procedimento in oggetto, ai sensi dell’art. 14 della L.R. n.14/2014;

6) individuare il sig. Alessandro Fidanza, funzionario del Settore A1910A - Servizi Infrastrutturali e Tecnologici, quale D.E.C. - Direttore Esecutivo del Contratto, ai sensi dell’art. 111, c. 2, del D.Lgs. n. 50/2016.

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) J14F22001110006;

- l’accertamento è assunto con il presente provvedimento sul Capitolo 20495 del Bilancio Finanziario Gestionale 2023-2025, annualità 2023 e 2024 - P.d.C E.4.02.01.01.001 - natura non ricorrente;

- l’entrata che si accerta con il presente provvedimento è vincolata al finanziamento della spesa relativa a “ICT_1_03 Postazioni di lavoro e Rete regionale: l’evoluzione in sicurezza”. Affidamento delle attività relative agli Interventi 1A, 2A, 2B, 3A, 4A1, 4A2 e 4B – CUP: J14F22001110006”, che viene registrata contestualmente all'impegno (codice progetto n. 2023/19).

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 del competente capitolo 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 le relative obbligazioni sono esigibili negli esercizi 2023 e 2024;

- trattasi di spesa di natura non ricorrente;

- la competenza economica coincide con quella finanziaria;

- l’impegno è relativo a risorse di derivazione statale e l’accertamento della correlata entrata è effettuato con questo provvedimento;

- 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.

Dato atto infine che, ai sensi dell’art. 226, c. 2, del d.lgs. 36/2023, ai procedimenti già in corso alla data del 1° luglio 2023 continuano ad applicarsi le disposizioni di cui al D.Lgs. 50/2016.

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 7 agosto 1990 n. 241 "Norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- artt. 4 e 16 D.Lgs 165/2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";
- D.Lgs. 7 marzo 2005 n. 82 e s.m.i. "Codice dell'Amministrazione Digitale";
- Legge regionale 28 luglio 2008, n. 23 artt. 4 e 17 "Disciplina dell'organizzazione degli uffici regionali e disposizioni concernenti la dirigenza ed il personale" e s.m.i.;
- Determinazione Dirigenziale n. 4/2011 dell'Autorità per la Vigilanza sui contratti pubblici di lavori, servizi e forniture aggiornata con successiva determina n. 556/2017 (risposta c.4 alle faq di ANAC in materia di tracciabilità) con la quale, tra l'altro, si escludono dall'ambito di applicazione della legge n. 136/2010 le movimentazioni di danaro derivanti da prestazioni eseguite in favore di pubbliche amministrazioni da soggetti, giuridicamente distinti dalle stesse, ma sottoposti ad un controllo analogo a quello che le medesime esercitano sulle proprie strutture (cd. affidamenti in house), con conseguente esclusione degli affidamenti diretti a società in house dall'obbligo di richiesta del codice CIG ai fini della tracciabilità;
- D.Lgs. 23 giugno 2011, n. 118 "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 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalita' nella pubblica amministrazione";
- D.Lgs. n. 33/2013 "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle PP.AA." s.m.i.;
- D.Lgs. 50/2016 e s.m.i. "Codice degli appalti pubblici e dei contratti di concessione";
- Regolamento n. 9 del 16 luglio 2021 " Regolamento regionale di contabilità della Giunta regionale. Abrogazione del regolamento regionale 5 dicembre 2001, n. 18";

- D.G.R. 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;
- D.G.R. n. 3-6447 del 30 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", riguardante il Piano Triennale di Prevenzione della corruzione (PTCP) 2023-2025;
- 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 24 aprile 2023, n. 6 "Bilancio di previsione finanziario 2023-2025";
- DGR 1- 6763 del 27/04/2023 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";
- DD n. 252 del 15/06/2023 "Presa d'atto e accettazione della cessione del credito da CSI-Piemonte a SACE Fct S.p.A, come da rogito del notaio Stucchi del 31/05/2023 rep. 17.315/12.071, registrato in Torino il 31/05/2023 al n. 25199";

determina

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

- di dare atto che all'intervento relativo al progetto denominato "Postazioni di lavoro e rete regionale; l'evoluzione in sicurezza", inserito e finanziato a valere sulle risorse PNRR, dell'importo complessivo di € 984.400,00, è stato assegnato il seguente Codice Unico di Progetto di investimento pubblico: CUP J14F22001110006;

- di approvare, ai sensi dell'art. 6 della "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", la PTE di iniziativa "ICT_1_03 Postazioni di lavoro e Rete Regionale: l'evoluzione in sicurezza" trasmessa dal CSI in data 25/09/2023 prot. n. 16423 (prot. del Settore 11338/A1910A del 26.09.2023);

- di accertare la somma complessiva di Euro 483.279,85 sul capitolo in entrata 20495 del Bilancio finanziario gestionale 2023-2025 - Tipologia 200: Contributi agli investimenti, Categoria 4020100 Contributi agli investimenti da amministrazioni pubbliche, P.d.C. finanziario E.4.02.01.01.001, secondo le seguenti modalità:

Euro 274.079,85 annualità 2023
Euro 209.200,00 annualità 2024

La 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, ai sensi dell'art. 6 della suddetta Convenzione quadro, a favore del CSI Piemonte P. IVA 01995120019 (Codice beneficiario 12655), le attività di cui alle Schede Tecniche allegate alla

suddetta PTE relative ai seguenti Interventi:

• Intervento 1A - Assessment Postura di sicurezza su Infrastruttura, Vulnerability Assessment, piano di remediation
• Intervento 2A - Revisione di procedure e processi per la gestione del rischio cyber-
• Intervento n° 2B - Business Impact Analisys e Business Continuity Plan
• Intervento n° 3A - Progettazione del percorso formativo, attuazione e simulazione incidenti
• Intervento n° 4A1 - Securizzazione DaaS e Posti di Lavoro
• Intervento n° 4A2 - NGFW per Regione ed Enti della rete Regionale
• Intervento n° 4B - Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT regionale,
per un importo complessivo pari a Euro 483.279,85, impegnando tale somma a favore dello stesso sul cap. 207058 (Missione 01 Programma 0112) del Bilancio Finanziario Gestionale 2023-2025, annualità 2023 e 2024 secondo le seguenti modalità:

Euro 274.079,85 annualità 2023
Euro 209.200,00 annualità 2024

La transazione elementare è riportata nell'Appendice A "Elenco registrazioni contabili", facente parte integrante formale e sostanziale del presente provvedimento;

- di approvare lo schema di disciplinare di incarico allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato A);

- di stabilire che si darà avvio alla fase della liquidazione della somma impegnata secondo le modalità di cui agli artt. 8, 9 e 10 della Convenzione quadro, prendendo atto che il beneficiario amministrativo è SACE FCT S.p.A.;

- di dare atto che, ai sensi della D.G.R. 13 ottobre 2014 n. 7-411, il responsabile del procedimento, di cui all’art. 31 del D.Lgs. 50/2016, è il dirigente responsabile del Settore Servizi Infrastrutturali e Tecnologici, Ing. Roberto Fabrizio;

- di assegnare ai sig.ri Alessandro Fidanza e Fausto Grassi, funzionari del Settore A1910A - Servizi Infrastrutturali e Tecnologici, la responsabilità dell'istruttoria del procedimento in oggetto, ai sensi dell’art. 14 della L.R. n.14/2014;

- di individuare il sig. Alessandro Fidanza, funzionario del Settore A1910A - Servizi Infrastrutturali e Tecnologici, quale D.E.C. - Direttore Esecutivo del Contratto, ai sensi dell’art. 111, c. 2, del D.Lgs. n. 50/2016;

- di prendere atto:

• della regolarità contributiva di CSI-Piemonte nei confronti di INPS-INAIL, come da DURC, rilasciato in data in data 02/06/2023 con validità fino al 29/01/2024, nonché della verifica negativa Equitalia del 21.12.2023 effettuata ai sensi dell’art. 48-bis del D.P.R. 602/73;

• della regolarità contributiva di SACE FCT S.p.A. nei confronti di INPS-INAIL, come da DURC, rilasciato da INAIL in data 01/10/2023 con validità fino al 29/01/2024, cessionaria del credito, così come approvato con Determinazione dirigenziale n. 252 del 15/06/2023 "Presa d'atto e accettazione della cessione del credito da CSI-Piemonte a SACE Fct S.p.A, come da rogito del notaio Stucchi del 31/05/2023 rep. 17.315/12.071, registrato in Torino il 31/05/2023 al n. 25199”.

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".

Contraente: CSI-Piemonte - P. IVA 01995120019
Importo: Euro 483.279,85 esente IVA
Resp. Procedimento: Ing. Roberto Fabrizio
Modalità ind.ne contraente: Convenzione Quadro, Rep. n. 51 del 07/02/2022

Avverso il presente provvedimento è ammesso ricorso giurisdizionale avanti al TAR entro 30 giorni dalla data di conoscenza dell'atto, secondo quanto previsto all'art. 120 del Decreto legislativo n. 104 del 2 luglio 2010 (Codice del Processo Amministrativo).

IL DIRIGENTE (A1910A - Servizi infrastrutturali e tecnologici)
Firmato digitalmente da Roberto Fabrizio

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. Discipliare_Incarico_CSI-PNRR.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

NextGenerationEU - PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 –Componente 1 – Investimento 1.5 “Cybersecurity”

ICT_1_03 - Postazioni di lavoro e rete regionale: l'evoluzione in sicurezza

Disciplinare incarico INTERVENTO/I RELATIVI all'iniziativa PTE approvata con D.D. n. xxxx/A1910A/2023 del xx/xx/2023

Con riferimento alla Vostra Proposta Tecnico Economica in argomento, acquisita agli atti dalla Regione Piemonte con prot. n. 11338/A1910A del 26/09/2023 (Prot. CSI 16423/2023 del 25/09/2023), si comunica che con la Determinazione in oggetto è stata approvata la PTE di iniziativa “ICT_1_03 Postazioni di lavoro e Rete Regionale: l’evoluzione in sicurezza” trasmessa dal CSI in data 25/09/2023 prot. n. 16423 e sono state affidate le attività relative ai seguenti interventi:

- ***Intervento: n.° 1A Assessment Postura di sicurezza su Infrastruttura, Vulnerability Assessment, piano di remediation***
- ***Intervento n° 2A Revisione di procedure e processi per la gestione del rischio cyber***
- ***Intervento n° 2B Business Impact Analisys e Business Continuity Plan***
- ***Intervento n° 3A Progettazione del percorso formativo, attuazione e simulazione incidenti***
- ***Intervento n° 4A1 Securizzazione DaaS e Posti di Lavoro***
- ***Intervento n° 4A2 NGFW per Regione ed Enti della rete Regionale***
- ***Intervento n° 4B Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT regionale,***

complementari a quanto già affidato con D.D. 282/A1910A/2023 del 30/06/2023 e relativi alla iniziativa “ICT_1_03 POSTAZIONI DI LAVORO E RETE REGIONALE: L’EVOLUZIONE IN SICUREZZA”.

Ciò premesso, tra le parti:

Committente
Regione Piemonte, Direzione Competitività del Sistema Regionale A19000, Settore A1910A – Servizi infrastrutturali e tecnologici
Responsabile di progetto: [redacted], Dirigente del Settore Servizi infrastrutturali e tecnologici.

Affidatario
CSI Piemonte, Servizi Digit
Responsabile della fornitura: [redacted]

si conviene e si stipula quanto segue

1 DISCIPLINA DEL SERVIZIO

L'espletamento del servizio è normato dal presente Disciplinare di incarico e, per quanto in esso non previsto, dalla Convenzione quadro per gli affidamenti diretti al CSI per la prestazione di servizi in regime di esenzione IVA per il periodo 1 gennaio 2022 – 31 dicembre 2026, approvata con delibera di Giunta regionale n 21-4474 del 31 dicembre 2021.

2 OGGETTO DELLA PTE

Gli interventi previsti dalla PTE saranno i seguenti:

Intervento n° 1A – Assessment della Postura di Sicurezza

Prodotto	Fornitura	Deliverable	SLA
Prodotto 1. Intervento 1A – Analisi della postura di sicurezza e piano di potenziamento	F. 1.1 -Architetture, security, evoluzione sistemi - Analisi della postura di sicurezza e Vulnerability assessment	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano dei VA; • Report dettagliato sulle analisi di postura eseguite rispetto al perimetro identificato	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance
	F.1.2 -Architetture, security, evoluzione sistemi - Piano di remediation	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano di remediation: Aree di miglioramento individuate a seguito dell'analisi di postura; • Raccomandazioni e piani d'azione per rafforzare la resilienza dell'Ente rispetto al perimetro analizzato	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance

Intervento n° 2a – Revisione di procedure e processi per la gestione del rischio cyber

Prodotto	Fornitura	Deliverable	SLA
Prodotto 1- intervento 2a - Revisione di procedure e processi per la gestione del rischio cyber	F-1.1 – Architetture, security, evoluzione sistemi - Disciplinare sull'utilizzo dei dispositivi e procedure operative	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi "del Catalogo e listino):* • Disciplinare (*Individuazione delle policy per la definizione delle regole per l'utilizzo accettabile delle risorse tecnologiche dell'Ente.* • Procedure operative standardizzate(*Definizione delle modalità di gestione della sicurezza informatica dell'Ente*	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance
	F1.2 -Architetture, security, evoluzione sistemi - Gestione proattiva della Cybersecurity	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi "del Catalogo e listino):* • Report di vulnerabilità e protocolli di gestione degli incidenti di sicurezza (descrizione delle *vulnerabilità individuate e il rischio associato ad esse, e nei protocolli di gestione degli incidenti di sicurezza definiti in linea con le migliori pratiche individuate* • Piani di mitigazione personalizzati e piani di ripristino (definizione dei	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance

		piani di mitigazione personalizzati, definiti per ogni vulnerabilità individuata e nei piani di ripristino attività definiti per garantire il ripristino delle attività in caso di incidenti di sicurezza. • Piano di comunicazione interna/esterna comunicazione in caso di incidenti di sicurezza.	

Intervento n° 2b – Business impact analysis e business continuity plan

Prodotto	Fornitura	Deliverable	SLA
Prodotto 1-intervento 2b-“Business impact analysis e business continuity plan” ”	Fornitura 1.1 – Architetture, security, evoluzione sistemi – Business Impact Analysis	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività “F” del servizio di Governace “Architetture, security, evoluzione sistemi* “*del Catalogo e listino):* • **Business Impact Analysis Report:** Questo deliverable consiste nel report di analisi di impatto relativo all’indisponibilità dei servizi infrastrutturali connessi alle postazioni di lavoro dell’Ente, con particolare riferimento alle postazioni di lavoro e alle dipendenze ad essi correlate.	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance
	Fornitura 1.2 - Architetture, security, evoluzione sistemi – Business Continuity Plan	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività “F” del servizio di Governace “Architetture, security, evoluzione sistemi* “*del Catalogo e listino):* • **Business**	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance

		Continuity Plan: comprensivo del master plan e dei diversi allegati che comprendono, tra le altre cose, di procedure specifiche, piano dei test e modulistica.	

Intervento n° 3A - Progettazione del percorso formativo, attuazione e simulazione incidenti

Prodotto	Fornitura	Deliverable	SLA
Prodotto 1 – progettazione del percorso formativo, attuazione e simulazione incidenti	F. 1.1 – Architetture, security, evoluzione sistemi- Progettazione e implementazione del percorso formativo sulla security awareness e data protection (anno 2023)	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano formativo; • Realizzazione materiali didattici e risorse di supporto al piano;	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance
	F. 1.2 - Architetture, security, evoluzione sistemi- Progettazione e svolgimento di "simulazione incidenti "(lotto 1 – Anno 2023)	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Definizione di scenari di incidenti informatici; • Report dettagliato sulle simulazioni svolte, risultati (Lotto1) • Raccomandazioni e piani d'azione per rafforzare la resilienza dell'Ente agli incidenti informatici	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance
	F. 1.3 - Architetture, security, evoluzione	Consuntivazione delle attività di supporto	

	sistemi- Progettazione e svolgimento di simulazione incidenti (lotto 2 – anno 2024	specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Definizione di scenari di incidenti informatici (Lotto2) • Report dettagliato sulle simulazioni svolte, risultati; • Raccomandazioni e piani d'azione per rafforzare la resilienza dell'Ente agli incidenti informatici	
	F.1.4 Erogazione del corso ai dipendenti e disseminazione delle tematiche Cyber e Data Protection attraverso webinar dedicati (anno 2024)	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Messa a disposizione del corso online per i dipendenti della Regione • Report di valutazione delle sessioni di formazione e dei partecipanti • Definizione calendario e agenda dei webinar; • Predisposizione materiale di supporto per erogazione webinar • Report di erogazione dei webinar	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance

Intervento n° 4A1 Securizzazione DaaS e Posti di Lavoro

Prodotto	Fornitura	Deliverable	SLA

Prodotto1 -Intervento 4.A.1 – Securizzazione Daas e Posti di Lavoro	F .1.1 – Architetture, Security, Evoluzione Sistemi- Migrazione da Windows 2012 A Windows 2019 – FASE 1	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano di migrazione delle componenti applicative client dai session host Windows 2012 R2 ai session host Windows 2019 per la prima tranche di collection. • Verbale di collaudo relativo al buon esito della migrazione dei session host Windows 2012 R2 dietro front end Windows 2019. • Verbale di collaudo relativo al buon esito della migrazione delle collection inizialmente basate su session host Windows 2012 R2.	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance
	F 1.2– Architetture, Security, Evoluzione Sistemi- SFT Multifactor Authentication – FASE 1	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Documento delle POC	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance
	F .1.3 – Architetture, Security, Evoluzione Sistemi- Migrazione da Windows 2012 A Windows 2019 – FASE 2	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano di migrazione	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance

		delle componenti applicative client dai session host Windows 2012 R2 ai session host Windows 2019, per la seconda tranche di collection. • Verbale di collaudo relativo al buon esito della migrazione delle collection inizialmente basate su session host Windows 2012 R2.	
	F 1.4– Architetture, Security, Evoluzione Sistemi- SFT Multifactor Authentication – FASE 2	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Documento Studio di Fattibilità relativo alla soluzione di MFA	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance

Intervento n° 4A2 NGFW per Regione ed Enti della rete Regionale

Prodotto	Fornitura	Deliverable	SLA
Prodotto1 -Intervento 4.a.2 – NGFW per Regione ed Enti della rete Regionale	F1.1– -Architetture, security, evoluzione sistemi -Attività per la configurazione iniziale del sistema di sicurezza perimetrale	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Verbale di installazione e collaudo relativa alla configurazione iniziale della fornitura del sistema di sicurezza perimetrale in	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance

		HA.	
	F 1.2 – -Architetture, security, evoluzione sistemi -Attività per la configurazione evoluta del sistema di sicurezza perimetrale	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* Verbale di installazione e collaudo relativa alla inizializzazione di base dei servizi Threat Prevention e URL Filtering.	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance

Intervento n° 4B regionale **Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT**

Prodotto	Fornitura	Deliverable	SLA
Prodotto 1 - Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT regionale	Fornitura 1.1 – Architetture, security, evoluzione sistemi - Studio degli ambiti di miglioramento	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Documento di analisi degli ambiti di miglioramento e potenziamento	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance
	Fornitura 1.2 - Architetture, security, evoluzione sistemi - Realizzazione delle linee d'intervento	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Documentazione attestante i nuovi processi messi in servizio per il miglioramento delle capacità dello CSIRT	RDCGOV – Rispetto Data Concordata consegna deliverable attività di Governance

3 INFORMAZIONI PER LA TRACCIATURA DEL PROGETTO

Tipologia di fondo	PNRR
Definizione/Titolo del progetto/attività	**ICT_1_03 Postazioni di lavoro e rete regionale: l'evoluzione in sicurezza:** Intervento: n.° 1A Assessment Postura di sicurezza su Infrastruttura, Vulnerability Assessment, piano di remediation - Intervento n° 2A Revisione di procedure e processi per la gestione del rischio cyber Intervento n° 2B Business Impact Analisys e Business Continuity Plan- Intervento n° 3A Progettazione del percorso formativo, attuazione e simulazione incidenti Intervento n° 4A1 Securizzazione DaaS e Posti di Lavoro Intervento n° 4A2 NGFW per Regione ed Enti della rete Regionale Intervento n° 4B Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT regionale
CUP Codice Unico di Progetto	CUP J14F22001110006

4 TEMPI DELLA FORNITURA

	Anno 2023				Anno 2024			
Interventi previsti nell'Iniziativa	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Intervento n° 1A - Assessment Postura di sicurezza su Infrastruttura, Vulnerability Assessment, piano di remediation			X	X	X	X		
Intervento n° 2A - Revisione di procedure e processi per la gestione del rischio cyber			X	X	X	X		
Intervento n° 2B - Business Impact Analisys e BC Plan			X	X	X	X	X	
Intervento n° 3A - Progettazione del percorso formativo, attuazione e simulazione incidenti			X	X	X	X		
Intervento n° 4A - Potenziamento delle infrastrutture di protezione mediante l'adozione di piattaforme HW e SW (*)	X	X	X	X	X			
Intervento n° 4A1 - Potenziamento delle infrastrutture di protezione mediante l'adozione di piattaforme HW e SW: Securizzazione DaaS e Posti di Lavoro			X	X	X			
Intervento n° 4A2 e 4A3- Potenziamento delle infrastrutture di protezione mediante l'adozione di piattaforme HW e SW: NGFW per Regione ed Enti della rete Regionale			X	X				
Intervento n° 4B - Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT regionale			X	X	X			

Si prende atto che il CSI Piemonte ha svolto, a partire dal mese di settembre 2023, attività propedeutiche agli interventi previsti nella presente PTE, nelle more del perfezionamento dell'atto di affidamento .

5 PERIMETRO ECONOMICO E VOLUMI

Si riporta nel seguito il prospetto relativo al preventivo per i servizi proposti:

Intervento n° 1A – Assessment della Postura di Sicurezza

Prodotto	Fornitura	Deliverable	Valore Economico
Prodotto 1. Intervento 1A – Analisi della postura di sicurezza e piano di potenziamento	F. 1.1 -Architetture, security, evoluzione sistemi - Analisi della postura di sicurezza e Vulnerability assessment	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano dei VA; • Report dettagliato sulle analisi di postura eseguite rispetto al perimetro identificato	89.805,68 €
	F.1.2 -Architetture, security, evoluzione sistemi - Piano di remediation	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano di remediation: Aree di miglioramento individuate a seguito dell'analisi di postura; • Raccomandazioni e piani d'azione per rafforzare la resilienza dell'Ente rispetto al perimetro analizzato	29.953,58 €

Intervento n° 2a – Revisione di procedure e processi per la gestione del rischio cyber

Prodotto	Fornitura	Deliverable	Valore Economico
Prodotto 1- intervento 2a - Revisione di procedure e processi per la gestione del rischio cyber	F-1.1 – Architetture, security, evoluzione sistemi - Disciplinare sull'utilizzo dei dispositivi e procedure operative	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi "del Catalogo e listino):* • Disciplinare (*Individuazione delle policy per la definizione delle regole per l'utilizzo accettabile delle risorse tecnologiche dell'Ente.* • Procedure operative standardizzate(*Definizione delle modalità di gestione della sicurezza informatica dell'Ente*	20.047,20 €
	F1.2 -Architetture, security, evoluzione sistemi - Gestione proattiva della Cybersecurity	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi "del Catalogo e listino):* • Report di vulnerabilità e protocolli di gestione degli incidenti di sicurezza (descrizione delle *vulnerabilità individuate e il rischio associato ad esse, e nei protocolli di gestione degli incidenti di sicurezza definiti in linea con le migliori pratiche individuate* • Piani di mitigazione personalizzati e piani di	29.922,05 €

		ripristino (definizione dei piani di mitigazione personalizzati, definiti per ogni vulnerabilità individuata e nei piani di ripristino attività definiti per garantire il ripristino delle attività in caso di incidenti di sicurezza. • Piano di comunicazione interna/esterna comunicazione in caso di incidenti di sicurezza.	

Intervento n° 2b – Business impact analysis e business continuity plan

Prodotto	Fornitura	Deliverable	Valore Economico
Prodotto 1-intervento 2b-“Business impact analysis e business continuity plan” ”	Fornitura 1.1 – Architetture, security, evoluzione sistemi – Business Impact Analysis	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività “F” del servizio di Governace “Architetture, security, evoluzione sistemi* “*del Catalogo e listino):* • **Business Impact Analysis Report:** Questo deliverable consiste nel report di analisi di impatto relativo all’indisponibilità dei servizi infrastrutturali connessi alle postazioni di lavoro dell’Ente, con particolare riferimento alle postazioni di lavoro e alle dipendenze ad essi correlate.	29.811,74 €
	Fornitura 1.2 - Architetture, security, evoluzione sistemi – Business Continuity Plan	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività “F” del servizio di Governace “Architetture, security, evoluzione sistemi* “*del Catalogo e listino):*	29.811,74 €

		• **Business Continuity Plan:** comprensivo del master plan e dei diversi allegati che comprendono, tra le altre cose, di procedure specifiche, piano dei test e modulistica.	

Intervento n° 3A - Progettazione del percorso formativo, attuazione e simulazione incidenti

Prodotto	Fornitura	Deliverable	Valore Economico
Prodotto 1 – progettazione del percorso formativo, attuazione e simulazione incidenti	F. 1.1 – Architetture, security, evoluzione sistemi- Progettazione e implementazione del percorso formativo sulla security awareness e data protection (anno 2023)	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano formativo; • Realizzazione materiali didattici e risorse di supporto al piano;	18.872,95 €
	F. 1.2 - Architetture, security, evoluzione sistemi- Progettazione e svolgimento di "simulazione incidenti "(lotto 1 – Anno 2023)	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Definizione di scenari di incidenti informatici; • Report dettagliato sulle simulazioni svolte, risultati (Lotto1) • Raccomandazioni e piani d'azione per rafforzare la resilienza dell'Ente agli incidenti informatici	10.976,05 €
	F. 1.3 - Architetture,	Consuntivazione delle	11.237,00 €

	security, evoluzione sistemi- Progettazione e svolgimento di simulazione incidenti (lotto 2 – anno 2024	attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Definizione di scenari di incidenti informatici (Lotto2) • Report dettagliato sulle simulazioni svolte, risultati; • Raccomandazioni e piani d'azione per rafforzare la resilienza dell'Ente agli incidenti informatici	
	F.1.4 Erogazione del corso ai dipendenti e disseminazione delle tematiche Cyber e Data Protection attraverso webinar dedicati (anno 2024)	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Messa a disposizione del corso online per i dipendenti della Regione • Report di valutazione delle sessioni di formazione e dei partecipanti • Definizione calendario e agenda dei webinar; • Predisposizione materiale di supporto per erogazione webinar • Report di erogazione dei webinar	18.763,43 €

Intervento n° 4A1 Securizzazione DaaS e Posti di Lavoro

Prodotto	Fornitura	Deliverable	Valore Economico

Prodotto1 -Intervento 4.A.1 – Securizzazione Daas e Posti di Lavoro	F .1.1 – Architetture, Security, Evoluzione Sistemi- Migrazione da Windows 2012 A Windows 2019 – FASE 1	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano di migrazione delle componenti applicative client dai session host Windows 2012 R2 ai session host Windows 2019 per la prima tranche di collection. • Verbale di collaudo relativo al buon esito della migrazione dei session host Windows 2012 R2 dietro front end Windows 2019. • Verbale di collaudo relativo al buon esito della migrazione delle collection inizialmente basate su session host Windows 2012 R2.	54.981,60 €
	F 1.2– Architetture, Security, Evoluzione Sistemi- SFT Multifactor Authentication – FASE 1	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Documento delle POC	28.515,76 €
	F .1.3 – Architetture, Security, Evoluzione Sistemi- Migrazione da Windows 2012 A Windows 2019 – FASE 2	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Piano di migrazione	16.748,19 €

		delle componenti applicative client dai session host Windows 2012 R2 ai session host Windows 2019, per la seconda tranche di collection. • Verbale di collaudo relativo al buon esito della migrazione delle collection inizialmente basate su session host Windows 2012 R2.	
	F 1.4– Architetture, Security, Evoluzione Sistemi- SFT Multifactor Authentication – FASE 2	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Documento Studio di Fattibilità relativo alla soluzione di MFA	9.418,59 €

Intervento n° 4A2 NGFW per Regione ed Enti della rete Regionale

Prodotto	Fornitura	Deliverable	Valore Economico
Prodotto1 -Intervento 4.a.2 – NGFW per Regione ed Enti della rete Regionale	F1.1– -Architetture, security, evoluzione sistemi -Attività per la configurazione iniziale del sistema di sicurezza perimetrale	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Verbale di installazione e collaudo relativa alla configurazione iniziale della fornitura del sistema di sicurezza perimetrale in	19.768,19 €

		HA.	
	F 1.2 – -Architetture, security, evoluzione sistemi -Attività per la configurazione evoluta del sistema di sicurezza perimetrale	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* Verbale di installazione e collaudo relativa alla inizializzazione di base dei servizi Threat Prevention e URL Filtering.	6.890,74 €

Intervento n° 4B regionale **Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT**

Prodotto	Fornitura	Deliverable	Valore Economico
Prodotto 1 - Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT regionale	Fornitura 1.1 – Architetture, security, evoluzione sistemi - Studio degli ambiti di miglioramento	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Documento di analisi degli ambiti di miglioramento e potenziamento	27.993,10 €
	Fornitura 1.2 - Architetture, security, evoluzione sistemi - Realizzazione delle linee d'intervento	Consuntivazione delle attività di supporto specialistico, con sintesi delle problematiche analizzate e risolte (*rif. Attività "F" del servizio di Governace "Architetture, security, evoluzione sistemi* "*del Catalogo e listino):* • Documentazione attestante i nuovi processi messi in servizio per il miglioramento delle capacità dello CSIRT	29.762,25 €

6 PIANO DI FATTURAZIONE

L'intervento è finanziato con Fondi PNRR, il CSI, pertanto, dovrà attenersi a quanto previsto nelle "Linee guida per i soggetti attuatori individuati tramite avvisi pubblici" redatte da ACN. Qualora si rendesse necessario adottare una diversa modalità di rendicontazione e fatturazione , il CSI dovrà adeguarsi a tale modalità, fatte salve le attività già rendicontate e fatturate.

Il pagamento è disposto entro 30 giorni dalla data di ricevimento della fattura.
Qualora il pagamento della prestazione, per cause imputabili alla Regione Piemonte, non sia effettuato entro il termine di cui al precedente comma, il ritardo costituirà base di calcolo per il riaddebito degli oneri finanziari sostenuti dal Consorzio.

Ad integrazione di quanto disciplinato al citato Documento tecnico si specifica, che **a chiusura del progetto** ed ai fini della rendicontazione UE della spesa, l'ultima fattura verrà emessa solo a seguito della determinazione dell'importo finale che sarà comprensivo: dei corrispettivi rendicontati trimestralmente al netto dei costi non ammissibili e dello scostamento dell'importo unitario delle tariffe a preventivo e quelle a consuntivo (determinato al termine dell'esercizio finanziario) .

7 COMITATO DI COORDINAMENTO (CDC)

Il Comitato di Coordinamento (CdC) ha il compito di monitorare e controllare lo stato di avanzamento delle attività previste nel presente disciplinare.
Le strutture coinvolte nel CdC sono:

- Settore A1910A Servizi infrastrutturali e tecnologici;
- Settore A1911A Sistema informativo regionale;
- CSI Piemonte.

Tali st entate all'interno del CdC da:

- o suo delegato, Dirigente del Settore A1910A, in rappresentanza del Settore A1910A con la funzione di responsabile di progetto;
- o suo delegato, Funzionario del Settore A1910A, in rappresentanza del Settore A1910A con la funzione di referente di progetto;
- o suo delegato, Funzionario del Settore A1910A, in rappresentanza del Settore A1910A con la funzione di referente di progetto;
- o suo delegato, Dirigente del Settore Sistema informativo regionale con la funzione di esperto di materia;
- o suo delegato, Funzionario del Settore Sistema informativo regionale, in rappresentanza del Settore committente con la funzione di esperto di materia;
- o suo delegato, Funzionario del Settore Sistema informativo regionale, in rappresentanza del Settore committente con la funzione di esperto di materia;
- o suo delegato, Funzionario del Settore Sistema informativo regionale, in rappresentanza del Settore committente con la funzione di esperto di materia;

- [redacted] o suo delegato, in rappresentanza del CSI-Piemonte con la funzione di responsabile della fornitura;
- [redacted] suo delegato, in rappresentanza del CSI-Piemonte con la funzione di referente;
- [redacted] o suo delegato, in rappresentanza del CSI-Piemonte con la funzione di referente;
- [redacted] o suo delegato, in rappresentanza del CSI-Piemonte con la funzione di
- [redacted] o suo delegato, in rappresentanza del CSI-Piemonte con la funzione di referente;

I ruoli dei soggetti coinvolti ed i relativi compiti sono di seguito elencati.

Referente di Progetto delSettore committente

- verificare in collaborazione con il referente del CSI Piemonte l'avanzamento del Servizio/Fornitura, riattualizzando ove necessario i piani di progetto sia dal punto di vista temporale che tecnico;
- verificare l'impegnato e il consuntivo delle attività e convalidare le risultanze finali in termini di loro rispondenza rispetto agli impegni stabiliti
- coordinare le fasi di accettazione e (eventuale) verifica di conformità che avverranno e saranno finalizzate all'accettazione del Servizio;
- assicurare la disponibilità delle risorse e delle infrastrutture necessarie all'espletamento della presente fornitura.

Referente del CSI Piemonte

- monitorare il rispetto del piano delle attività;
- monitorare la la gestione dell'andamento tecnico/economico dell'attività;
- gestire la relazione con le funzioni del committente coinvolte nel progetto;
- il coordinamento e la conduzione del gruppo di progettazione/sviluppo.

8 PIANIFICAZIONE INCONTRI DI STATO AVANZAMENTO PROGETTO

Il Comitato di Coordinamento si riunisce con cadenza **bimestrale**. In tali incontri si valuterà il corretto svolgimento delle attività in relazione alle tempistiche e ai prodotti rilasciati. Eventuali scostamenti rispetto alle tempistiche e al perimetro economico preventivato dovranno essere puntualmente rappresentati dal CSI, al fine di mettere in atto le azioni correttive da parte del Comitato stesso.

La relazione tecnica **bimestrale** di avanzamento lavori fornirà, quindi, evidenza, tramite adeguata descrizione, dell'avanzamento delle attività progettuali effettuate e che sono valorizzate nei prospetti dei rendiconti economici.

9 LIVELLI DI SERVIZIO

I livelli di servizio sono dettagliati nelle tabelle di cui al punto 2.

10 ACCETTAZIONE ORDINE

Il presente disciplinare, in assenza di osservazioni, si considera tacitamente accettato da parte del CSI entro 15 giorni solari dal ricevimento del provvedimento stesso.

11 VERIFICA DI CONFORMITA'

Il CSI Piemonte dovrà collaborare, con gli utenti e i tecnici regionali nell'attività di verifica di quanto oggetto del presente disciplinare.
Le attività di verifica saranno svolte nell'ambito dell'incontro del Comitato di Coordinamento, in cui si provvederà alla stesura ed alla sottoscrizione degli appositi verbali.
La verifica di conformità verrà eseguita prima del rilascio in esercizio dell'applicativo oggetto della fornitura del prodotto.

La fornitura si considera conclusa al rilascio in esercizio di tutti i prodotti previsti dagli interventi del presente disciplinare.

12 TITOLARITÀ DEL PRODOTTO

Le parti si danno reciprocamente atto che qualsiasi prodotto (documentazione tecnica, manuali utente, ecc…) realizzato nell'ambito del servizio, in quanto risultato originale di creazione intellettuale, è oggetto di tutela ai sensi della legge 22 aprile 1941, n. 633 ("Protezione del diritto d'autore e di altri diritti connessi al suo esercizio") e D.Lgs 30/2005. In tale contesto:

- il Committente sarà titolare del software sviluppato;
- la proprietà della soluzione informatica oggetto del contratto farà capo al Committente ;
- tutti i diritti d'autore sul software sviluppato verranno trasferiti, a seguito del completamento dell'opera, all'amministrazione committente che ne diverrà titolare;
- il fornitore mantiene il diritto morale sulla paternità dell'opera;
-

13 REPOSITORY APPLICATIVO

Tutta la documentazione di progetto ed i relativi deliverable dovranno essere depositati dal CSI in apposito repository o altro strumento individuato dal Settore A1910A e dal CSI, per la condivisione della documentazione prodotta il cui accesso è riservato al referente di progetto e Referente SIRe ICT della Direzione/Settore committente e ai funzionari del Settore Sistema Informativo regionale.

Dovranno essere rilasciati i documenti/prodotti/Deliverable di cui al punto 5 "Perimetro economico e volumi".

14 SICUREZZA E PROTEZIONE DEI DATI PERSONALI

Si rimanda quanto indicato all'art. 19 della Convenzione quadro per gli affidamenti diretti al CSI per la prestazione di servizi in regime di esenzione IVA per il periodo 1 gennaio 2022 – 31 dicembre 2026. Inoltre CSI Piemonte si impegna a rispettare quanto riportato nel paragrafo (1.4 della PTE) dal titolo "Sicurezza e protezione dei dati personali".

15 RESPONSABILITÀ ED OBBLIGHI

Dall'applicazione delle disposizioni civilistiche dettate in materia di contratto d'appalto derivano, a mero titolo esemplificativo e non esaustivo:

a) l'obbligo del Fornitore di mettere a disposizione del Committente il risultato della sua prestazione, con conseguente assunzione del rischio attinente al mancato raggiungimento del risultato medesimo;
b) l'obbligo del Fornitore di fornire la materia necessaria a compiere l'opera (art 1658 c.c.);
c) l'obbligo del Fornitore di garantire la qualità dei servizi erogati e l'assenza di difformità e vizi dei servizi, nonché l'onere del Committente di denunziare le difformità o i vizi entro i termini di legge;
d) la facoltà del Committente di recedere dal contratto, tenendo indenne il Fornitore delle spese sostenute, delle prestazioni e del mancato guadagno (art. 1671 c.c.);
e) le parti si obbligano a rispettare, altresì, ogni altra disposizione contenuta nella Convenzione quadro e nelle Procedure Operative, in coerenza con le disposizioni civilistiche in materia.

Il Fornitore riconosce a suo carico tutti gli oneri inerenti all'assicurazione del proprio personale occupato nelle lavorazioni oggetto del presente ordine e dichiara di assumere in proprio ogni responsabilità in caso di infortuni e di danni arrecati eventualmente da detto personale alle persone ed alle cose, sia dell'Amministrazione che di terzi, in dipendenza di colpa o negligenza nella esecuzione delle prestazioni stabilite.
Il Fornitore si impegna ad ottemperare a tutti gli obblighi verso i propri dipendenti in base alle disposizioni legislative e regolamentari vigenti in materia di lavoro e di assicurazione sociale, assumendo a suo carico tutti gli oneri relativi; si obbliga ad attuare nei confronti dei propri dipendenti, occupati nei lavori di cui al presente ordine, condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi di lavoro applicabili alla data di stipulazione del presente ordine, alla categoria e nella località in cui si svolgono le lavorazioni, nonché condizioni risultanti da successive modifiche od integrazioni ed in genere da ogni altro contratto collettivo successivamente stipulato per la categoria, applicabile nella località; si obbliga a continuare ad applicare i citati contratti collettivi anche dopo la loro scadenza e fino alla loro sostituzione.
I menzionati obblighi relativi ai contratti collettivi di lavoro vincolano il fornitore anche nel caso che non sia aderente alle associazioni stipulanti o receda da esse, per tutto il periodo di validità del presente contratto. In caso di violazione degli obblighi predetti e previa comunicazione al Fornitore delle inadempienze denunciate dall'Ispettorato del Lavoro, il Committente si riserva il diritto di operare una ritenuta pari, al massimo, al 20% dell'importo contrattuale; ritenuta che sarà rimborsata solo quando l'Ispettorato del Lavoro citato avrà dichiarato che il fornitore si sia posto in regola né questi potrà vantare diritto alcuno per il mancato pagamento o ritardato pagamento.

Il CSI si impegna a osservare quanto disciplinato nell'Avviso ACN 3/2022, in particolare

- a collaborare con il Committente nelle attività amministrative di monitoraggio e rendicontazione secondo quanto disposto nel citato avviso utilizzando la modulistica e le modalità definite da ACN nelle "Linee guida per i soggetti attuatori individuati tramite avvisi pubblici".

- a rispettare i principi PNRR applicabili agli interventi previsti nella PTE in oggetto:
  - principio del "non arrecare danno significativo", collaborando con il Committente nella compilazione delle apposite check lit di autocontrollo definite da ACN nelle "Linee guida per i soggetti attuatori individuati tramite avvisi pubblici";
  - principio del contributo all'obiettivo climatico e digitale (c.d. tagging);
  - conseguimento di target e milestone PNRR;
  - rispetto e promozione della parità di genere;
  - protezione e valorizzazione dei giovani.

16 RISOLUZIONE DELLE PROBLEMATICHE

Nel caso dovessero insorgere problematiche in relazione all'erogazione di singoli servizi affidati, si applica quanto previsto agli artt. 17 comma 4 e 27 comma 2 della Convenzione.

17 DOMICILI CONTRATTUALI

Si richiede che la corrispondenza relativa al presente affidamento, venga indirizzata a:

Committente:

Regione Piemonte

Direzione Competitività del Sistema Regionale A19000

Settore Servizi Infrastrutturali e Tecnologici

Piazza Piemonte, 1 – 10127 Torino

PEC: settore-ict@cert.regione.piemonte.it

Fornitore del servizio:

CSI Piemonte

Corso Unione Sovietica 216 – 10134 Torino

PEC: protocollo@cert.csi.it

Torino, 13/12/2023

Il Dirigente Settore

A1910A – Servizi Infrastrutturali e Tecnologici

(DOCUMENTO FIRMATO DIGITALMENTE)

REGIONE PIEMONTE

APPENDICE A – ELENCO REGISTRAZIONI CONTABILI

REGISTRAZIONI CONTABILI DELLA DETERMINAZIONE DIRIGENZIALE

ATTO DD 586/A1910A/2023 DEL 27/12/2023

Accertamento N.: 2023/3505
Descrizione: PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5. CONTRIBUTO FINANZIATO DALL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE A VALERE SULL'AVVISO 3/2022. APPROVAZIONE PTE "ICT_1_03 POSTAZIONI DI LAVORO E RETE REGIONALE: L'EVOLUZIONE IN SICUREZZA" TRASMESSA DAL CSI IN DATA 25/09/2023 PROT. N. 16423 - CUP: J14F22001110006 E AFFIDAMENTO DELLE ATTIVITÀ DI CUI ALLE SCHEDE TECNICHE ALLEGATE ALLA PTE (INTERVENTI 1A, 2A, 2B, 3A, 4A1, 4A2 E 4B)
Importo (€): 274.079,85
Cap.: 20495 / 2023 - 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

Accertamento N.: 2024/382
Descrizione: PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5. CONTRIBUTO FINANZIATO DALL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE A VALERE SULL'AVVISO 3/2022. APPROVAZIONE PTE "ICT_1_03 POSTAZIONI DI LAVORO E RETE REGIONALE: L'EVOLUZIONE IN SICUREZZA" TRASMESSA DAL CSI IN DATA 25/09/2023 PROT. N. 16423 - CUP: J14F22001110006 E AFFIDAMENTO DELLE ATTIVITÀ DI CUI ALLE SCHEDE TECNICHE ALLEGATE ALLA PTE (INTERVENTI 1A, 2A, 2B, 3A, 4A1, 4A2 E 4B)
Importo (€): 209.200,00
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

REGIONE PIEMONTE

APPENDICE A – ELENCO REGISTRAZIONI CONTABILI

REGISTRAZIONI CONTABILI DELLA DETERMINAZIONE DIRIGENZIALE

ATTO DD 586/A1910A/2023 DEL 27/12/2023

Impegno N.: 2023/25177
Descrizione: PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5. CONTRIBUTO FINANZIATO DALL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE A VALERE SULL'AVVISO 3/2022. APPROVAZIONE PTE "ICT_1_03 POSTAZIONI DI LAVORO E RETE REGIONALE: L'EVOLUZIONE IN SICUREZZA" TRASMESSA DAL CSI IN DATA 25/09/2023 PROT. N. 16423 - CUP: J14F22001110006 E AFFIDAMENTO DELLE ATTIVITÀ DI CUI ALLE SCHEDE TECNICHE ALLEGATE ALLA PTE (INTERVENTI 1A, 2A, 2B, 3A, 4A1, 4A2 E 4B) . ACCE
Importo (€): 274.079,85
Cap.: 207058 / 2023 - 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" - HARDWARE
Macro-aggregato: Cod. 2020000 - Investimenti fissi lordi e acquisto di terreni
Motivo assenza CIG: Affidamenti in house
CUP: J14F22001110006
Soggetto: Cod. 12655
PdC finanziario: Cod. U.2.02.01.07.999 - Hardware n.a.c.
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 586/A1910A/2023 DEL 27/12/2023

Impegno N.: 2024/6015
Descrizione: PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 - COMPONENTE 1 - INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5. CONTRIBUTO FINANZIATO DALL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE A VALERE SULL'AVVISO 3/2022. APPROVAZIONE PTE "ICT_1_03 POSTAZIONI DI LAVORO E RETE REGIONALE: L'EVOLUZIONE IN SICUREZZA" TRASMESSA DAL CSI IN DATA 25/09/2023 PROT. N. 16423 - CUP: J14F22001110006 E AFFIDAMENTO DELLE ATTIVITÀ DI CUI ALLE SCHEDE TECNICHE ALLEGATE ALLA PTE (INTERVENTI 1A, 2A, 2B, 3A, 4A1, 4A2 E 4B) . ACC
Importo (€): 209.200,00
Cap.: 207058 / 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" - HARDWARE
Macro-aggregato: Cod. 2020000 - Investimenti fissi lordi e acquisto di terreni
Motivo assenza CIG: Affidamenti in house
CUP: J14F22001110006
Soggetto: Cod. 12655
PdC finanziario: Cod. U.2.02.01.07.999 - Hardware n.a.c.
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)