Deliberazione della Giunta Regionale 27 settembre 2022, n. 6-5680

Adesione all’avviso per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Citta' metropolitane, delle Province autonome a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” M1C1I1.5, pubblicato dall’Agenzia per la Cybersicurezza Nazionale.

(omissis)

LA GIUNTA REGIONALE

a voti unanimi...

delibera

1. 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 di potenziamento della resilienza cyber sinteticamente descritte in allegato alla presente, deliberazione quale parte integrante e sostanziale, a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity” M1C1I1.5;
2. di dare atto che l'assunzione delle obbligazioni giuridiche conseguenti al presente provvedimento è subordinata all’accoglimento delle proposte da parte dell’Agenzia per la Cyber sicurezza nazionale e, pertanto, alla variazione di bilancio finalizzata a recepire, in entrata ed in uscita delle correlate spese, gli stanziamenti dei fondi, per un importo pari a euro 1.979.500,00 o per un importo inferiore, nel caso di una rimodulazione delle proposte;
3. di demandare 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 presente deliberazione, 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.

La presente deliberazione sarà pubblicata sul B.U. della Regione Piemonte ai sensi dell’art. 61 dello Statuto e dell’art. 5 della L.R. 22/2010.

(omissis)

Allegato

Allegato

Adesione all'avviso per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5, pubblicato dall'Agenzia per la Cybersicurezza Nazionale

Executive Summary

La strategia di transizione digitale della Regione Piemonte, che si concretizza nella sua programmazione a medio termine (Programma pluriennale ICT 2021-23 approvato con DGR 58-4509 del 29/12/2021), si articola nella doppia direzione di rafforzare il sistema informativo dell'Ente (SIRe) per adeguarlo alle necessità interne e alla evoluzione dei servizi e di creare le condizioni di un ecosistema digitale pubblico dell'intera PA regionale.

La Regione Piemonte ha iniziato a costruire il sistema informativo unitario della PA regionale a partire dalla programmazione europea 2007-2013 con ingenti e costanti investimenti a valere sui **POR-FESR** che hanno dato vita alle soluzioni infrastrutturali e di piattaforma che già oggi costituiscono la spina dorsale dell'ecosistema regionale. E' il caso della rete regionale a banda larga Wi-Pie, che connette tutte le strutture regionali e 80 altri Enti della PA piemontese (con circa 550 collegamenti attivi), e che ha recentemente visto l'avvio di un importante percorso di ammodernamento delle infrastrutture; del Data Center regionale in classe A; di Nivola, il cloud regionale qualificato, su cui centinaia di Comuni piemontesi hanno già avviato la migrazione dei propri servizi (anticipando l'investimento 1.2 del PNRR); di PiemonteTU, che offre un unico punto di accesso ai servizi regionali e degli enti aderenti (cfr. PNRR 1.4.1) e che permette di effettuare l'integrazione attraverso la piattaforma Notify all'App IO (cfr. PNRR 1.4.3); del polo regionale dei pagamenti PiemontePay, che permette la piena integrazione con PagoPA tramite l'intermediario tecnologico regionale (cfr. PNRR 1.4.3). Indipendentemente dallo scenario rappresentato dal PNRR, altri strumenti sono già operativi e disponibili per il territorio regionale, dalla Smart Data Platform all'Infrastruttura geografica regionale.

Sul piano del sistema informativo dell'Ente, anche in relazione ad un piano di concentrazione delle sedi di lavoro metropolitane nel Palazzo Unico Regionale (PUR), con DGR 75 - 5529 del 3/8/2022 è stato avviato un percorso di acquisizione di nuove dotazioni tecnologiche che favoriscono la possibilità di ricorso al lavoro agile, il potenziamento degli strumenti a disposizione dei lavoratori, un miglior utilizzo degli spazi (sia in termini di gestione della mobilità interna che di funzionalità legate alle attività lavorative).

L'investimento regionale nei prossimi anni, che impiegherà in maniera complementare risorse proprie dell'Ente, fondi della programmazione POR-FESR 2021-2027 e auspicabilmente del PNRR, sarà orientato all'evoluzione e al consolidamento delle traiettorie di trasformazione digitale tanto dell'Ente che della PA piemontese nel suo complesso, con particolare attenzione ai seguenti ambiti:

- **infrastrutturazione digitale**, sia in termini di infrastrutture materiali (reti a larga banda e ultra larga pubbliche, evoluzione della rete Wi-PIE, razionalizzazione dei data center e adozione del paradigma cloud), sia in termini di infrastrutture immateriali (piattaforme di pagamento, infrastruttura dati e geografica, piattaforme di interoperabilità). Il Piemonte è un territorio complesso, connotato da debolezze intrinseche derivanti dalle caratteristiche geomorfologiche, dalle rilevanti dimensioni territoriali e demografiche, dalla frammentazione amministrativa. Il valore della rete e delle infrastrutture materiali rappresenta un elemento imprescindibile per consentire una crescita omogenea e sostenibile. Regione Piemonte ha saputo svolgere un ruolo di "pioniere" attivando con tempestività, già nei primi anni 2000, gli investimenti per la creazione di una rete in banda larga (la rete Wi-PIE) a servizio di tutta la PA territoriale. Nel quadro di programmazione in corso la Regione prosegue e rafforza tali investimenti, affiancandoli ad altri finalizzati alla razionalizzazione dei data center territoriali, alla messa a disposizione di piattaforme abilitanti all'adesione verso le piattaforme nazionali, in modo da migliorare la capacità di offerta di servizi digitali da parte della Pubblica Amministrazione locale. Sfruttando le tendenze emerse in favore del paradigma cloud si sostiene un percorso di crescita del territorio verso la digitalizzazione, la continuità e la sicurezza dei servizi erogati, lo sviluppo di nuove competenze, la razionalizzazione delle risorse destinate all'ICT nonché la convergenza verso modelli comuni. Parallelamente la

Regione interviene, nell'ambito della riorganizzazione del proprio personale legata alla concentrazione in una sede unica delle principali sedi metropolitane, per completare l'evoluzione delle postazioni di lavoro (oltre 3.000) in logica Desktop As A Service, favorendo la razionalizzazione degli spazi e dell'impiego delle risorse, l'adozione di nuove modalità di lavoro, l'accrescimento della sicurezza delle attività operative dei dipendenti, dei dati e dei servizi.

- **semplificazione, dematerializzazione e digitalizzazione**: il focus è sulla precondizione rappresentata dall'amministrazione digitale senza carta e dall'attuazione del concetto "digital by default". Il processo di digitalizzazione dei servizi pubblici da una parte è favorito dalla tendenza a utilizzare le procedure telematiche da parte dell'utenza, da dinamiche di razionalizzazione della Pubblica Amministrazione per contrastare la diminuzione di risorse finanziarie e professionali; dall'altra incontra difficoltà a causa della complessità (in termini di competenze, cultura e organizzazione) del passaggio dall'analogico al digitale. Regione Piemonte intende collegare le dinamiche della dematerializzazione dei documenti e della reingegnerizzazione dei processi. In materia di competenze digitali, la Regione intende spendersi sia in qualità di facilitatore sia con proprie specifiche azioni di "assessment" e di formazione.
- **cittadino al centro:** la crescente sensibilità di cittadini e imprese verso l'utilizzo di strumenti digitali è stata favorita, in Piemonte, dall'azione pubblica per la diffusione di servizi accessibili da remoto mediante dispositivi digitali, nonché dai servizi a sostegno dell'informazione (Contact center). Regione Piemonte ha programmato azioni di razionalizzazione ed integrazione quali la messa a disposizione di servizi su PiemonteTu, in applicazione concreta del concetto di "cittadino al centro".
  Al contempo sono previste azioni di stimolo e di sensibilizzazione a supporto della domanda, con un'attenzione particolare a garantire la parità di accesso ai servizi della PA piemontese senza esclusioni.
- **monitoraggio e valore del patrimonio informativo:** Regione Piemonte ha maturato una consapevolezza rilevante sull'importanza del patrimonio informativo, realizzando una propria infrastruttura dati (la Smart Data Platform) che farà evolvere nel corso del prossimo triennio, accrescendo la consistenza, la qualità e la condivisione dell'informazione pubblica. Il focus delle iniziative più rilevanti è indirizzato verso il cittadino, con particolare riferimento al welfare e alle politiche sociali, al lavoro, al traffico e alla mobilità, verso tematiche di rilievo quali la sicurezza (ambientale e degli edifici), la gestione e la tutela del territorio, l'energia (monitoraggio piano energetico), la regia sui fondi comunitari.
- **salute digitale:** La sanità piemontese ha dimostrato una capacità di reazione che ha capitalizzato il valore del sistema e l'organizzazione già messa in campo in precedenza. Il buon livello di informatizzazione e di efficienza conseguito dal sistema sanitario regionale viene consolidato con la realizzazione del fascicolo sanitario elettronico, a condizione che siano superate, nel sistema dell'offerta, resistenze al cambiamento e carenze di integrazione ormai residuali ma comunque ancora presenti. Condizioni di contesto favorevoli sono rappresentate dall'incremento generalizzato dei servizi medici on-line, fronteggiando efficacemente i rilevanti impatti sull'utenza e sull'organizzazione dell'offerta.

In tale contesto, i due progetti che concorrono al finanziamento della misura 1.5 del PNRR hanno come obiettivo la messa in sicurezza e il rafforzamento di servizi e infrastrutture che negli anni la Regione Piemonte ha sviluppato per il proprio ente e per le altre amministrazioni del territorio.

Il **progetto *Postazioni di lavoro e rete regionale: l'evoluzione in sicurezza*** si articola in:

- evoluzione delle **postazioni di lavoro** dell'Ente in logica **Desktop As A Service**, per slegare la fruizione dei servizi dal vincolo della postazione fisica e favorire logiche di lavoro agile. L'azione specifica riguarda l'analisi della postura di sicurezza delle postazioni di lavoro dell'Ente (più di 3000), in una fase in cui il modo di lavorare si evolve, sia per il concentramento delle diverse sedi cittadine in un unico palazzo regionale, sia per la prossima completa virtualizzazione dei posti di lavoro. Ciò comporta anche l'attuazione di misure tecniche specifiche per il rafforzamento della resilienza (interventi strutturali, adozione di soluzioni tecnologiche a supporto e rafforzamento della cultura degli utenti). L'intervento prevede inoltre un programma formativo per gli utenti, che possa rafforzare la consapevolezza delle minacce cyber, ma anche la padronanza delle metodologie di

risposta e di gestione degli incidenti. I materiali realizzati saranno messi a disposizione delle altre amministrazioni del territorio, per contribuire alla diffusione della cultura cyber, come previsto dal Piano Triennale di AgID

- sviluppo ed evoluzione del **backbone regionale** (rete regionale) per l'accesso delle amministrazioni locali alla piattaforma Cloud regionale. L'intervento, attraverso la progettazione e l'implementazione di nuovi servizi di sicurezza basati su Next Generation Firewall, indirizza il rafforzamento della resilienza alle minacce della rete regionale, che eroga servizio alle sedi regionali (a breve raggruppate nel Palazzo Unico) e anche a più di 80 singole amministrazioni locali (circa 550 collegamenti di rete). In particolare, la rete garantisce a tutti gli enti la fruizione dei servizi erogati dal data center e dalla piattaforma cloud regionale. L'intervento mira quindi a potenziare ulteriormente la resilienza della rete regionale e a ridurre il rischio di minacce cyber rivolte a tutti gli enti che la utilizzano. In tale ottica verrà rafforzato anche il livello di monitoraggio del SOC (Security Operation Center, esercito dal CSI Piemonte), per garantire agli Enti strumenti, processi e competenze necessari alla gestione di minacce o incidenti di sicurezza.

L'importo complessivo del finanziamento richiesto è pari a € 984.400.

Il **progetto di *Transizione digitale e servizi sicuri*** 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 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 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 SIRe da parte dei dipendenti regionali.

L'importo complessivo del finanziamento richiesto è pari a € 995.100.

Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

REGIONE PIEMONTE

Avviso Pubblico per la presentazione di proposte per la realizzazione di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PNRR, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"

M1C1I1.5

ALLEGATO B – PIANO DI PROGETTO

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

Sezione 1 – ANAGRAFICA

Titolo del progetto	**Postazioni di lavoro e rete regionale: l'evoluzione in sicurezza**
CUP	***J14F22001110006***
Interventi ***(in conformità a quanto previsto al par. 4.1 "Caratteristiche degli Interventi di potenziamento" dell'Avviso, indicare una o più tipologie di intervento)***	☒ analisi della postura di sicurezza e piano di potenziamento; ☒ miglioramento dei processi e dell'organizzazione di gestione della cybersecurity; ☒ miglioramento della consapevolezza delle persone; ☒ progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber
Progetto già avviato o in corso di attivazione ***(in conformità a quanto previsto al par. 4 dell'Avviso, purché avviato a decorrere dal 1° febbraio 2020)***	SI ☐ indicare data di stipula_____ e CIG del/dei contratto/i _____ *Oppure* indicare riferimenti (es. determina di aggiudicazione, prot. invio Piano dei Fabbisogni) _____ NO ☒
(in caso di progetto da avviare ex novo) **Tempistiche previste per l'avvio del progetto**	< 15 gg dall'accertamento del decreto di finanziamento
Data di ultimazione dell'intervento prevista	Entro il 30 novembre 2024
Capillarità sul territorio ***(indicare se il progetto proposto coinvolge più Pubbliche Amministrazioni locali riportando la denominazione di ognuna)***	☐ **Coinvolgimento di una P.A**: ☐ **Coinvolgimento da due a cinque P.A.** *(indicare le P.A. coinvolte)*: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____ ☒ **Coinvolgimento di oltre cinque P.A.** (*indicare le P.A. coinvolte, eventualmente aggiungendo righe)*: 1. Agenzia Piemonte Lavoro

	2. Agenzia Torino 2006 3. Agenzia Mobilità Metropolitana 4. AIPO 5. ARPA 6. ARPEA 7. ASL Alessandria 8. ASL Asti 9. ASL CITTA' DELLA SALUTE 10. ASL CITTA' DI TORINO (ex ASL To2) 11. ASL CN1 12. ASL NO 13. ASL TO3 14. ASL TO4 15. ASL VCA 16. SLO S.ANNA 17. ASO 4 (AOU S. Luigi) 18. ASO AL 19. ASO CN2 20. ASO Novara 21. ATC 22. ATO 3 Torino 23. ATO 1 Verbania 24. Biblioteca Casale 25. Biblioteca Fossano 26. Biblioteca Gaetano Poggi 27. Biblioteca Gobetti 28. Biblioteca Novi Ligure 29. Biblioteca Ovada 30. Comune di Savigliano 31. Comune Vercelli 32. Comune Alessandria 33. Comune Benevagienna 34. Comune di Biella 35. Comune di Collegno 36. Comune di Fossano 37. Comune di Galliate 38. Comune di Grugliasco 39. Comune di Mondovì 40. Comune di Omegna 41. Comune di Novara

	42. Comune di Rivoli 43. Comune di Salmour 44. Comune di Torino 45. Comune di Verbania 46. Comune di Volpiano 47. Comune Domodossola 48. Comune Nichelino 49. Comune Pianezza 50. Comune Pinerolo 51. Comune Racconigi 52. Comune Rivalta 53. Consiglio Regionale 54. Consorzio Regionale Antidoping 55. IRCC Candiolo 56. IZSTO 57. Osp. Mauriziano 58. PRESIDIO SANITARIO San Camillo 59. Provincia di Alessandria 60. Provincia di Cuneo 61. Provincia TO – CMTO- 62. Provincia Vercelli 63. Provincia del VCO 64. Provincia di Biella 65. Provincia di Novara 66. REGIONE PIEMONTE 67. Unione del Fossanese 68. Unione Valle Stura 69. Università del Piemonte Orientale 70. Università di Torino 71. Politecnico di Torino
Data di ultimazione degli interventi prevista, nel rispetto del target M1C1-19 ***(indicare in GG dalla data di sottoscrizione dell'Atto d'Obbligo)***	Si stimano 730 giorni. La data di ultimazione non andrà comunque oltre il 30/11/2024

1A. Dati identificativi del Soggetto proponente	
Denominazione	Regione Piemonte

CF/P.IVA	80087670016/02843860012
sede legale (*indicare Via/Piazza, n civico e cap.)*	Piazza Castello 165, Torino 10124
posta elettronica certificata (PEC)	gabinettopresidenza-giunta@cert.regione.piemonte.it

1B. Dati identificativi del titolare del potere di impegnare il Soggetto/legale rappresentante	
Nome e Cognome	Alberto Cirio
CF	CRILRT72T06L219J
Nato a	Torino
Residente in (*indicare Via/Piazza, n civico e cap.)*	Piazza Castello 165, Torino 10124

1C. Dati identificativi del Responsabile del Progetto	
Nome e Cognome	Giorgio Consol
CF	CNSGRG65E07E379F
Nato a	Ivrea (TO)
Residente in (*indicare Via/Piazza, n civico e cap.)*	Corso Regina Margherita 174, Torino 10122
Indirizzo e-mail	giorgio.consol@regione.piemonte.it
Numero di telefono	011.4324.001

Sezione 2 – ORGANIZZAZIONE E CAPACITA' AMMINISTRATIVA DEL SOGGETTO ATTUATORE DELL'INTERVENTO

2A. Descrizione e dimensionamento delle strutture coinvolte nella gestione, attuazione e controllo dell'intervento, facendo eventualmente riferimento anche alle attività affidate in outsourcing

Max 150 parole

Regione Piemonte è dotata di due Settori dedicati alla gestione e sviluppo informatico:

- A1910A-Servizi infrastrutturali e tecnologici: 16FTE, di cui 1 unità dirigenziale Gestione dei servizi ICT trasversali alla Regione; programmazione, razionalizzazione e gestione postazioni e strumenti di lavoro della Regione; definizione e gestione delle policy di sicurezza informatica; gestione tecnica dei portali WEB e della intranet regionale; la gestione della connettività sul territorio regionale;
- A1911A-Sistema informativo regionale: 15FTE (1 unità dirigenziale) Programmazione del Sistema Informativo Regionale in coerenza con le norme, le disposizioni e gli indirizzi a livello nazionale e coordinamento del relativo sviluppo; supporto allo svolgimento delle funzioni di RTD; svolgimento delle funzioni di coordinamento e cura degli accordi con soggetti ed organismi esterni

Regione Piemonte è socio fondatore, aderente tramite Convenzione, all'in-house CSI Piemonte, a cui vengono affidate 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.

2B. Descrizione degli elementi utili a garantire la capacità amministrativa del Soggetto attuatore dell'intervento

Max 150 parole

I due settori precedentemente descritti, avvalendosi

- del RTD e del suo staff, che tra i suoi compiti ha anche quello di impulso sui progetti di innovazione tecnologica
- del partner tecnologico CSI Piemonte

ha gestito i seguenti progetti cofinanziati con Fondi Europei 2007–2013 e 2014-2020:

- Accesso ai Servizi con SPID euro 1.620.000
- YUCCA-Smart Data Platform euro 4.100.000
- PiemontePay -PagoPA euro 2.849.851
- Cloud Regionale euro 4.999.968
- Cooperazione territoriale Italia-Francia e Italia-Svizzera

comprensivi delle attività di controllo e audit di primo e secondo livello

Regione Piemonte ha inoltre istituito apposita Struttura temporanea (XST031) dedicata alla Attuazione del PNRR;

La convenzione Regione Piemonte-CSI contiene un allegato tecnico che disciplina i progetti cofinanziati con fondi europei; ciò aggiunto alla consolidata esperienza pregressa, assicura tempi rapidi di affidamento, messa in esercizio e rendicontazione dei progetti.

Sezione 3 – DESCRIZIONE DEGLI INTERVENTI

3A. Descrizione dell'ambito di esecuzione dell'intervento (es. descrizione del sistema informatico di riferimento e della struttura organizzativa; specificare la capillarità dell'intervento e quindi la modalità di coinvolgimento e/o impatto su altre amministrazioni.

Max 300 parole

Il presente intervento si sviluppa in modo funzionale ad alcune iniziative strategiche che la Regione Piemonte ha perseguito negli anni rispetto ai servizi infrastrutturali sia propri sia rivolti alle amministrazioni del territorio:

- Evoluzione dei posti di lavoro in logica Desktop As A Services per slegare la fruizione dei servizi dalla postazione fisica in ottica di maggior disponibilità e flessibilità.
- Evoluzione del backbone regionale Wi-Pie per l'accesso della PA territoriale al Data Center regionale

Nel primo ambito si prevede un ulteriore evoluzione del sistema, con utilizzo di nuovi sistemi operativi su server e con accesso allo stesso da client con sistema operativo standard e non da *thin client* specializzato. L'imminente trasferimento in una singola sede (palazzo unico) di quasi tutte le strutture metropolitane della Giunta regionale si configura come opportunità di rivalutare la postura di sicurezza del servizio legato ai Posti di Lavoro ed alla rete, attuando anche misure tecniche già individuate per il rafforzamento della resilienza (interventi strutturali, adozione di soluzioni tecnologiche a supporto e rafforzamento della cultura degli utenti utilizzatori).
L'intervento prevederà inoltre la definizione di un programma formativo rivolto agli utenti dell'Ente che comprenderà anche lo svolgimento di esercitazioni e simulazioni di incidenti; elementi e materiali saranno messi a disposizione delle altre amministrazioni del territorio (attraverso webinar o altre forme di condivisione) al fine di contribuire alla diffusione della cultura Cyber.
Il secondo ambito, attraverso la progettazione e l'implementazione di nuovi servizi, indirizza il rafforzamento della sicurezza perimetrale della rete regionale che eroga servizio, oltre alle stesse sedi Regionali (Palazzo Unico e sedi distribuite sul territorio), a più di 80 amministrazioni locali, circa 550 collegamenti di rete, e che ha il compito di garantire la fruizione dei servizi erogati dal Data Center e dalla Piattaforma Cloud Regionale.

3B. Descrizione delle criticità della postura di sicurezza indirizzate

Max 300 parole

Vulnerabilità infrastrutturali: i servizi infrastrutturali oggetto di analisi sono per loro natura asset e piattaforme condivise dagli utenti e pertanto sono particolarmente critiche dal punto di vista "rischio di compromissione" dei servizi erogati. L'intervento vuole indirizzare la mitigazione dei rischi dovuta a minacce esterne che possano colpire le infrastrutture di accesso ai sistemi IT

dell'Ente con particolare riferimento

- Alle postazioni di lavoro dell'Ente
- Alla rete regionale che offre servizio di accesso
  - alle sedi dell'Ente
  - alle amministrazioni locali piemontesi attestate su di essa.

- Su ambedue gli ambiti va aumentata la capacità di effettuare "*Threat Prevention*" in modo da intercettare prima possibile le minacce e poter limitare il perimetro di diffusione gestendo limitazioni e segmentazioni in modo dinamico all'insorgere di determinate minacce o segnali di compromissione; attività che oggi è limitata a sistemi tradizionali che presuppongono l'intervento umano con interventi reattivi.

- Tempi di rilevazione delle minacce e di reazione alle compromissioni; al fine di mitigare questa criticità si propone di intervenire sia con il potenziamento dei processi sia con l'analisi e la simulazione di situazione di incidenti. Analogamente verrà sviluppato un potenziamento dei servizi erogato dal SOC regionale.

- Potenziali vulnerabilità riconducibili al fattore umano: l'evoluzione delle tecniche di attacco basate sul comportamento dei singoli dipendenti (social engineering, phishing, ecc.) richiedono specifiche azioni formative continuative mirate ad aumentare la consapevolezza dei dipendenti sui rischi e sulle tecniche di attacco informatico. Le conseguenze di un attacco portato a buon fine sull'infrastruttura DaaS dell'Ente potrebbero limitare la piena operatività, quindi, è un'area che va maggiormente presidiata e potenziata.
- La rete regionale condivisa tra gli Enti della PA locale espone tutti gli Enti aderenti al rischio cyber legato all'"anello più debole": è necessario introdurre nella rete strumenti (es. NGFW) per implementare perimetri di protezione e livelli di sicurezza.

3C. Descrizione degli obiettivi dell'intervento e dell'impatto in termini di potenziamento della resilienza cyber, ed in particolare in riferimento:

- adozione di misure e controlli di sicurezza
- supportare il processo di transizione digitale

Max 400 parole

Il tema della sicurezza è uno dei pilastri dell'Agenda digitale del Piemonte in quanto trasversale e funzionale all'erogazione di tutti i servizi digitali. Tale aspetto è stato posto in evidenza con la sottoscrizione dell'Accordo per la crescita e la cittadinanza digitale tra la Regione, AgID e l'Agenzia per la Coesione Territoriale (luglio 2019). Tra le iniziative prioritarie, la razionalizzazione delle risorse ICT con il progetto "Community Cloud Regionale e Razionalizzazione infrastrutture IT degli Enti Locali" che oltre a supportare la migrazione in cloud dei servizi applicativi, prevede il

potenziamento dei servizi di sicurezza cibernetica dedicati a cittadini ed imprese anche attraverso azioni di promozione e sensibilizzazione sui temi della sicurezza informatica.

Rispetto a questi indirizzi, l'azione della Regione Piemonte si è sempre posta nell'ottica della piena adesione e complementarità alle norme nazionali riguardanti il tema della sicurezza IT ed ha quindi investito per rafforzare la propria capacità di monitoraggio, rilevazione e contrasto degli attacchi informatici potenziando sia le tecnologie dedicate alla sicurezza infrastrutturale ed applicativa, sia realizzando strutture operative dedicate al monitoraggio e alla gestione degli attacchi informatici (SOC ed il più recente CSIRT eserciti dalla propria In-house).

L'intervento proposto mira quindi a rafforzare la resilienza cyber degli asset infrastrutturali che consentono l'operatività del sistema informativo regionale ovvero le postazioni di lavoro e la rete regionale passando anche attraverso interventi di potenziamento della consapevolezza dei dipendenti nonché delle procedure operative e delle policy che regolano la gestione degli aspetti legati alla sicurezza; tali aspetti, in particolar modo, saranno definiti in accordo con quanto disposto dalle misure minime di sicurezza AgID nonché dalla normativa di riferimento.

Gli accadimenti degli ultimi mesi confermano infatti che gran parte degli attacchi rivolti alle PA hanno come punto di accesso fattori comportamentali degli utenti e sfruttano le infrastrutture legate ai posti di lavoro come vettore di diffusione.

In tal senso la proposta vuole porre delle solide basi affinché questo rischio possa essere mitigato sfruttando le traiettorie di evoluzione sia del modello di gestione dei posti di lavoro che della rete per le quali la Regione Piemonte ha già indirizzato diversi investimenti.

In linea anche con gli obiettivi del Piano Triennale AgID la proposta mirerà inoltre alla sensibilizzazione e diffusione della consapevolezza del rischio Cyber anche verso la messa a disposizione di materiali e webinar tematici verso altre PA (azione già in corso di svolgimento dal 2021, rif. https://www.csipiemonte.it/it/comunicazione/eventi/webinar).

3D. Descrizione dei contenuti operativi e delle attività previste

Max 300 parole

Analisi postura sicurezza e piano potenziamento: L'analisi verrà condotta sui servizi infrastrutturali di supporto a:

- posti di lavoro
- accessi remoti virtualizzati
- sistemi infrastrutturali a supporto
- gestione identità digitali

ed in generale sulla nuova rete dell'Ente in vista del passaggio al Palazzo Unico, con strutture delocalizzate sull'area metropolitana.

Verranno considerati

- aspetti tecnologici (VA e/o PT)
- procedurali (politiche di accesso, Policy,...)

analizzando quanto in essere e valutando traiettorie di rafforzamento/scoperture da sanare. In funzione delle risultanze verrà redatto un piano di potenziamento individuando rischi ed azioni di contenimento da attuare.

Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity:

verrà effettuata una revisione/Integrazione/potenziamento delle procedure e delle policy e processi legati alla sicurezza dell'Ente, in particolare:

- Disciplinare uso strumenti, procedure operative gestione delle vulnerabilità
- Procedure di gestione e risposta agli incidenti legati ad attacchi ransomware, phishing, ecc.
- Analisi vulnerabilità connesse alla disponibilità servizi legati ai posti di lavoro attraverso effettuazione BIA; definizione
  - strategie tecnico-organizzative
  - realizzazione Business Continuity Plan (ISO22301:2019)
  - processi a supporto

Miglioramento della consapevolezza delle persone:

- Progettazione/implementazione percorso formazione sulla security awareness e data protection. Il materiale prodotto sarà messo a disposizione delle PA del territorio attraverso la piattaforma di formazione online della Regione.
- Progettazione e svolgimento "simulazioni incidenti" per diffondere consapevolezza sulle procedure nonché testarne sul campo efficacia/efficienza
- Disseminazione delle tematiche Cyber e Data Protection sulle PA del territorio attraverso Webinar dedicati

Progettazione e sviluppo nuovi sistemi per mitigazione del rischio:

- Acquisizione, attività progettazione, implementazione/dispiegamento soluzioni Next-Generation-Firewall dedicate alla protezione
  - Ente Regione
  - Enti connessi alla rete Regionale Wi-Pie (elenco PA coinvolte in anagrafica)

- Progettazione/sviluppo soluzioni sicurezza per potenziamento resilienza cyber delle postazioni di lavoro (es. Multifactor Authentication, Securizzazione, Patch Management)
- Potenziamento monitoraggio e capacità reazione minacce Cyber del SOC/CSIRT Regionale

3E. Descrizione delle modalità attuative ovvero delle modalità amministrative per la realizzazione delle attività

Max 300 parole

Regione Piemonte si avvarrà della propria *in-house*, CSI Piemonte, per la realizzazione delle attività.

Come previsto dalla Convenzione Quadro 2022-2026 approvata con D.G.R. n. 21-4474 del 29 dicembre 2021 l'intervento sarà avviato attraverso l'approvazione di specifica Proposta Tecnico Economica formulata da CSI Piemonte e di contestuale determinazione dirigenziale di affidamento del Responsabile del progetto, come definito dalle procedure operative previste dalla Convenzione Quadro, che disciplinano il ciclo completo della fornitura e la rendicontazione per i progetti cofinanziati con fondi europei.

Tutte le attività sopraindicate saranno perfezionate propedeuticamente in modo da consentire l'immediato avvio operativo dei lavori a seguito dell'ammissione formale al finanziamento del progetto e comunque non oltre 15 giorni.

La struttura del responsabile di progetto è composta da:

- funzionari e collaboratori con esperienza di project management e di partecipazione a progetti finanziati con fondi comunitari su diverse programmazioni, con particolare riferimento agli aspetti di rendicontazione, attestazione del raggiungimento di obiettivi e target, partecipazione alle attività di verifica e controllo;

- funzionari di staff specializzati in ambito amministrativo/contabile, che curano iter dall'accertamento alla liquidazione finale.

Verranno individuati in questo contesto un apposito team e un Capo Progetto che lo coordinerà, costituendo il punto di supporto al Dirigente nella completa gestione del progetto e degli adempimenti correlati.

All'interno del team saranno attribuiti ruoli e responsabilità distinti tra i componenti al fine di mitigare i rischi di progetto e prevenire eventuali fenomeni corruttivi.

Nel piano di rafforzamento amministrativo attualmente in corso di attuazione, Regione Piemonte sta valutando di incrementare il numero di risorse da destinare al progetto qui definito.

Sezione 4 – QUADRO FINANZIARIO

In riferimento al paragrafo n. 5.2 “Spese ammissibili” dell’Avviso pubblico recante “Avviso Pubblico per la presentazione di proposte per la realizzazione di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PNRR, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity”M1C1I1.5”, nella presente sezione, deve essere dettagliato il preventivo finanziario.
Si specifica che il Soggetto attuatore dell’intervento potrà presentare esclusivamente costi strettamente connessi allo svolgimento delle attività previste nel Piano di Progetto coerenti e pertinenti con le finalità dell’intervento 1.5, Missione M1C1, e successivamente comprovabili con opportuna documentazione giustificativa. Ai fini dell’ammissibilità delle spese si rimanda alla normativa nazionale ed europea di riferimento vigente e alle indicazioni operative ripotate nel Manuale per i Soggetti Attuatori adottato dall’Agenzia.

Il finanziamento concesso con il presente Avviso è cumulabile con altri finanziamenti a valere su programmi e strumenti dell’Unione europea, a condizione che gli stessi non interessino i medesimi costi in applicazione del principio di addizionalità di cui all’art.9 del Regolamento (UE) 2021/241. Dovrà pertanto essere esplicitato nel preventivo finanziario l’eventuale contributo a carico di altre fonti finanziarie.

Nel caso in cui l’intervento sia stato avviato con una diversa copertura finanziaria a valere sul bilancio dell’Unione, all’atto della sottoscrizione dell’Atto d’Obbligo il Soggetto attuatore dell’intervento dovrà formalmente dimostrare di aver rinunciato al precedente finanziamento, ove questo sia riferito ai medesimi costi per cui si chiede il contributo a valere sul PNRR.

Si fornisce di seguito un dettaglio delle tipologie di spese ammissibili, a titolo esemplificativo e non esaustivo:

- spese per servizi di consulenza per l’implementazione degli interventi progettuali ammissibili secondo indicazioni di cui alla circolare RGS n. 4/2021, incluse attività di formazione specifica;
- spese per la progettazione, lo sviluppo e l’implementazione di software specifici;
- spese per l’acquisto di hardware, software;
- spese per l’acquisizione di servizi per l’implementazione degli interventi progettuali (es: sviluppo software; servizi di connettività; analisi, studi, ecc);
- spese generali e altri costi di esercizio direttamente imputabili all'attività progettuale nella misura pari al 7% di costi diretti ammissibili ai sensi dell’art. 54 lett. a del Reg. (UE) 2021/1060.

4A. Indicazione e descrizione delle **risorse finanziarie** necessarie alla realizzazione del progetto denominato Postazioni di lavoro e rete regionale: l'evoluzione in sicurezza, per ogni macro-attività

COSTO COMPLESSIVO DEL PROGETTO **"Postazioni di lavoro e rete regionale"**: l'evoluzione in sicurezza € 984.400

CONTRIBUTO RICHIESTO € € 984.400 ripartito per le seguenti tipologie di intervento come da prospetto di cui alla *Tabella 1* e il cui dettaglio dei costi preventivati indicato in *Tabella 2*.

Tabella 1 – Contributo richiesto per tipologia di intervento
Compilare con l'importo previsto per ogni intervento comprensivo delle spese generali[1].

TIPOLOGIA INTERVENTO	*TOTALE (al netto di IVA)*	*TOTALE IVA*[2]	IMPORTO FINANZIAMENTO RICHIESTO
Analisi della postura di sicurezza e piano di potenziamento	€ 128.400	-	€ 128.400
Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	€ 117.700	-	€ 117.700
Miglioramento della consapevolezza delle persone	€ 64.200	-	€ 64.200
Progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber	€ 599.300	€ 74.800	€ 674.100

DESCRIZIONE DI ALTRE FONTI DI FINANZIAMENTO UTILIZZATE PER LA REALIZZAZIONE DEL PROGETTO (se previste):

Non sono previste altre fonti di finanziamento

In merito al quadro finanziario indicato, si precisa quanto segue:

Regione Piemonte intende ricorrere alla propria in house nella realizzazione degli interventi della presente proposta; i rapporti in essere sono regolati da un regime di esenzione IVA applicata per le prestazioni di servizio (fatturazione esente IVA) ai sensi dell'art. 10 comma 2 del DPR 633/1972 e dal regime ordinario di IVA nel solo caso di cessioni di beni (fatturazione imponibile oltre IVA 22%);

Nel caso di "acquisizione di servizi" dalla inhouse, essendo la fattura esposta da quest'ultima con l'importo esente IVA (Totale al netto di IVA), l'importo finanziato richiesto corrisponderà al totale della fattura stessa;

Nel caso di "acquisizione di beni" dalla inhouse, essendo la fattura esposta da quest'ultima con l'importo imponibile (Totale al netto di IVA) e con l'importo dell'IVA al 22% (Totale IVA), ed essendo l'IVA sostenuta non recuperabile dal

1 *Le spese generali e altri costi di esercizio direttamente imputabili all'attività progettuale sono riconosciti nella misura pari al 7% dei costi diretti ammissibili (art. 5.2 dell'Avviso)*
2 *Come richiamato dal DPR. 22/2018, art. 15: "Ai sensi dell'articolo 69, paragrafo 3, lettera c), del regolamento (UE) n. 1303/2013, l'imposta sul valore aggiunto (IVA) realmente e definitivamente sostenuta dal beneficiario è una spesa ammissibile solo se questa non sia recuperabile, nel rispetto della normativa nazionale di riferimento […]". Pertanto, questa potrà essere computata nella colonna "importo finanziamento richiesto" esclusivamente al verificarsi di tale fattispecie*.

soggetto beneficiario, l'importo finanziato richiesto corrisponderà al totale della fattura al lordo dell'IVA.

Tabella 2 – Dettaglio dei costi preventivati per ogni attività e tipologia di investimento

Compilare la seguente tabella con il dettaglio dei costi preventivati per ogni attività e tipologia di investimento (rif. Paragrafo 4.1 dell'avviso) prevista per il progetto aggiungendo se necessarie ulteriori righe.

TIPOLOGIA INTERVENTO[3]	ATTIVITA	CATEGORIA DI COSTO[4]	IMPORTO TOTALE	*TOTALE (al netto di IVA)*	*TOTALE IVA[5]*	IMPORTO FINANZIAMENTO RICHIESTO
Analisi della postura di sicurezza e piano di potenziamento	*Assessment Postura di sicurezza su Infrastruttura, Vulnerability Assessment, piano di remediation*	Acquisizione servizi professionali	€ 120.000	€ 120.000	-	€ 120.000
Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	*Revisione di procedure e processi per la gestione del rischio cyber*	Acquisizione servizi professionali	€ 50.000	€ 50.000	-	€ 50.000
	Business Impact Analisys e BC Plan	Acquisizione servizi professionali	€ 60.000	€ 60.000	-	€ 60.000
Miglioramento della consapevolezza delle persone	*Progettazione del percorso formativo, attuazione e simulazioni incidenti*	Acquisizione servizi professionali	€ 60.000	€ 60.000	-	€ 60.000
Progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber	*Potenziamento delle infrastrutture di protezione della Società mediante l'adozione di piattaforme HW e SW:* *NGFW, Securizzazione DaaS e Posti di Lavoro, etc..*	Acquisizione di beni	€ 414.800	€ 340.000	€ 74.800	€ 414.800
	Potenziamento delle infrastrutture di protezione della Società mediante l'adozione di piattaforme HW e SW:	Acquisizione servizi professionali	€ 157.200	€ 157.200	-	€ 157.200

3 *Indicare la tipologia di intervento in coerenza con l'articolo 4.1 dell'Avviso.*

4 *Per categoria di costo indicare ad esempio: acquisizione di beni; acquisizione di servizi; costo personale interno; …)*

5 *Come richiamato dal DPR. 22/2018, art. 15: "Ai sensi dell'articolo 69, paragrafo 3, lettera c), del regolamento (UE) n. 1303/2013, l'imposta sul valore aggiunto (IVA) realmente e definitivamente sostenuta dal beneficiario è una spesa ammissibile solo se questa non sia recuperabile, nel rispetto della normativa nazionale di riferimento […]". Pertanto, questa potrà essere computata nella colonna "importo finanziamento richiesto" esclusivamente al verificarsi di tale fattispecie.*

	Progettazione, sviluppo, attività di implementazione					
	Potenziamento del monitoraggio delle minacce Cyber per SOC e CSIRT regionale	Acquisizione servizi professionali	€ 58.000	€ 58.000	-	€ 58.000
a) TOTALE COSTI DIRETTI						**€ 920.000**
b) SPESE GENERALI 7% DEI COSTI DIRETTI AMMISSIBILI (a*7%)						**€ 64.400**
c) TOTALE RICHIESTO A FINANZIAMENTO (a+b)						**€ 984.400**

Sezione 5 – CRONOPROGRAMMA

5A. Indicazione e descrizione del **cronoprogramma delle attività** di implementazione del progetto
Compilare la tabella sottostante (è possibile aggiungere righe alla tabella)

Tipologie di investimento *(rif. Paragrafo 4.1 dell'avviso)*	Attività (breve descrizione)	Data di inizio prevista (es. Q3 2022)	Data di fine prevista (es. Q4 2022)	Durata espressa in gg
Analisi della postura di sicurezza e piano di potenziamento	*Assessment Postura di sicurezza su Infrastruttura, Vulnerability Assessment, piano di remediation*	Q4 2022	Q4 2023	Effort (300) Durata (350)
Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	*Revisione di procedure e processi per la gestione del rischio cyber*	Q2 2023	Q2 2024	Effort (135) Durata (400)
	Business Impact Analisys e BC Plan	Q2 2023	Q3 2024	Effort (187) Durata (500)
Miglioramento della consapevolezza delle persone	*Progettazione del percorso formativo, attuazione e simulazioni incidenti*	Q4 2022	Q1 2024	Effort (157) Durata (450)
Progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber	*Potenziamento delle infrastrutture di protezione mediante l'adozione di piattaforme HW e SW:* *Securizzazione DaaS e Posti di Lavoro*	Q1 2023	Q4 2023	Effort (127) Durata (300)
	Potenziamento delle infrastrutture di protezione mediante l'adozione di piattaforme HW e SW: *NGFW per Regione ed Enti della rete Regionale*	Q1 2023	Q3 2023	Effort (180) Durata (270)
	Potenziamento degli strumenti di monitoraggio delle minacce Cyber per SOC e CSIRT regionale	Q1 2023	Q1 2024	Effort (154) Durata (420)

Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

REGIONE PIEMONTE

Avviso Pubblico per la presentazione di proposte per la realizzazione di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PNRR, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"

M1C1I1.5

ALLEGATO B – PIANO DI PROGETTO

"Transizione digitale e servizi sicuri"

Sezione 1 – ANAGRAFICA

Titolo del progetto	Transizione digitale e servizi sicuri
CUP	***J14F22001120006***
Interventi ***(in conformità a quanto previsto al par. 4.1 "Caratteristiche degli Interventi di potenziamento" dell'Avviso, indicare una o più tipologie di intervento)***	☒ analisi della postura di sicurezza e piano di potenziamento; ☒ miglioramento dei processi e dell'organizzazione di gestione della cybersecurity; ☒ miglioramento della consapevolezza delle persone; ☒ progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber
Progetto già avviato o in corso di attivazione ***(in conformità a quanto previsto al par. 4 dell'Avviso, purché avviato a decorrere dal 1° febbraio 2020)***	SI ☐ indicare data di stipula_____ e CIG del/dei contratto/i _____ *Oppure* indicare riferimenti (es. determina di aggiudicazione, prot. invio Piano dei Fabbisogni) _____ NO ☒
(in caso di progetto da avviare ex novo) **Tempistiche previste per l'avvio del progetto**	< 15 gg dall'accertamento del decreto di finanziamento
Data di ultimazione dell'intervento prevista	Entro il 30 novembre 2024
Capillarità sul territorio ***(indicare se il progetto proposto coinvolge più Pubbliche Amministrazioni locali riportando la denominazione di ognuna)***	☐ **Coinvolgimento di una P.A**: ☐ **Coinvolgimento da due a cinque P.A.** *(indicare le P.A. coinvolte)*: 1 _____ 2 _____ 3 _____ 4 _____ 5 _____ ☒ **Coinvolgimento di oltre cinque P.A.** (*indicare le P.A. coinvolte, eventualmente aggiungendo righe)*: 1 Città Metropolitana di Torino

	2 Finpiemonte 3 Comune di Biella 4 Comune di Vercelli 5 Consiglio Regionale del Piemonte 6 ARPEA 7 AIPO
Data di ultimazione degli interventi prevista, nel rispetto del target M1C1-19 ***(indicare in GG dalla data di sottoscrizione dell'Atto d'Obbligo)***	Si stimano 730 giorni. La data di ultimazione non andrà comunque oltre il 30/11/2024

1A. Dati identificativi del Soggetto proponente	
Denominazione	Regione Piemonte
CF/P.IVA	80087670016/02843860012
sede legale (*indicare Via/Piazza, n civico e cap.)*	Piazza Castello 165, Torino 10124
posta elettronica certificata (PEC)	gabinettopresidenza-giunta@cert.regione.piemonte.it

1B. Dati identificativi del titolare del potere di impegnare il Soggetto/legale rappresentante	
Nome e Cognome	Alberto Cirio
CF	CRILRT72T06L219J
Nato a	Torino
Residente in (*indicare Via/Piazza, n civico e cap.)*	Piazza Castello 165, Torino 10124

1C. Dati identificativi del Responsabile del Progetto	
Nome e Cognome	Giorgio Consol
CF	CNSGRG65E07E379F
Nato a	Ivrea (TO)
Residente in (*indicare Via/Piazza, n civico e cap.)*	Corso Regina Margherita 174, Torino 10122
Indirizzo e-mail	giorgio.consol@regione.piemonte.it
Numero di telefono	011.4324.001

Sezione 2 – ORGANIZZAZIONE E CAPACITA' AMMINISTRATIVA DEL SOGGETTO ATTUATORE DELL'INTERVENTO

2A. Descrizione e dimensionamento delle strutture coinvolte nella gestione, attuazione e controllo dell'intervento, facendo eventualmente riferimento anche alle attività affidate in outsourcing

Max 150 parole

Regione Piemonte è dotata di due Settori dedicati alla gestione e sviluppo informatico:

- A1910A-Servizi infrastrutturali e tecnologici: 16FTE, di cui 1 unità dirigenziale Gestione dei servizi ICT trasversali alla Regione; programmazione, razionalizzazione e gestione postazioni e strumenti di lavoro della Regione; definizione e gestione delle policy di sicurezza informatica; gestione tecnica dei portali WEB e della intranet regionale; la gestione della connettività sul territorio regionale;
- A1911A-Sistema informativo regionale: 15FTE (1 unità dirigenziale) Programmazione del Sistema Informativo Regionale in coerenza con le norme, le disposizioni e gli indirizzi a livello nazionale e coordinamento del relativo sviluppo; supporto allo svolgimento delle funzioni di RTD; svolgimento delle funzioni di coordinamento e cura degli accordi con soggetti ed organismi esterni

Regione Piemonte è socio fondatore, aderente tramite Convenzione, all'in-house CSI Piemonte, a cui vengono affidate 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.

2B. Descrizione degli elementi utili a garantire la capacità amministrativa del Soggetto attuatore dell'intervento

Max 150 parole

I due settori precedentemente descritti, avvalendosi

- del RTD e del suo staff, che tra i suoi compiti ha anche quello di impulso sui progetti di innovazione tecnologica
- del partner tecnologico CSI Piemonte

ha gestito in ultimo i seguenti progetti cofinanziati con Fondi Europei delle programmazioni 2007–2013 e 2014-2022:

- Accesso ai Servizi con SPID euro 1.620.000
- YUCCA-Smart Data Platform euro 4.100.000
- PiemontePay -PagoPA euro 2.849.851
- Cloud Regionale euro 4.999.968
- Cooperazione territoriale Italia-Francia e Italia-Svizzera

comprensivi delle attività di controllo e audit di primo e secondo livello

Regione Piemonte ha inoltre istituito apposita Struttura temporanea (XST031) dedicata alla Attuazione del PNRR; La convenzione Regione Piemonte-CSI è corredata di uno specifico allegato tecnico che disciplina i progetti cofinanziati con i fondi europei; ciò aggiunto ad una consolidata esperienza pregressa relativa alla gestione di progetti cofinanziati, assicura dei tempi rapidi di affidamento, di messa in esercizio e di rendicontazione dei progetti.

Sezione 3 – DESCRIZIONE DEGLI INTERVENTI

3A. Descrizione dell'ambito di esecuzione dell'intervento (es. descrizione del sistema informatico di riferimento e della struttura organizzativa; specificare la capillarità dell'intervento e quindi la modalità di coinvolgimento e/o impatto su altre amministrazioni.

Max 300 parole

La strategia di transizione digitale della Regione Piemonte, che si concretizza nella sua programmazione a medio termine (Programma pluriennale ICT 2021-23 approvato con DGR 58-4509 del 29/12/2021), si articola nella doppia direzione di rafforzare il sistema informativo dell'Ente (SIRe) per adeguarlo alle necessità interne e alla evoluzione dei servizi e di creare le condizioni di un ecosistema digitale pubblico dell'intera PA regionale.

Il SIRe è costituito dall'insieme di risorse e componenti tecnologiche, risorse umane e competenze, regole, standard, sicurezza, procedure, organizzate per fornire agli utenti i servizi informativi richiesti.
Dal punto di vista logico, con lo scopo di offrire una vista sintetica e generale, l'architettura del SIRe è articolata secondo i seguenti livelli:

- applicativi tematici per l'erogazione dei servizi rivolti a Cittadini, Imprese e PA;
- basi dati che costituiscono il patrimonio informativo della Regione Piemonte;
- middleware applicativo che consente l'integrazione e l'interoperabilità tra i diversi applicativi;
- infrastrutture, suddivise in tre sottocomponenti: il Data Center, la Rete, le Postazioni di Lavoro (PC e altri device di accesso);
- software strumentali per attività di Sviluppo e Test.

La sicurezza informatica, nel significato ampio di protezione delle risorse da incidenti o attacchi malevoli, riservatezza delle informazioni, continuità del servizio, rappresenta una componente trasversale e determinante sia in termini di presidio costante sia in termini di evoluzione del sistema informativo su temi quali la **Cybersecurity,** la **BIA,** la **gestione dell'identità digitale**.

Tali temi saranno affrontati nel progetto proposto coinvolgendo in modo trasversale le diverse direzioni regionali, sia in termini di consapevolezza della cultura della sicurezza, sia in termini di raggiungimento dei risultati.

Gli enti del territorio potranno altresì beneficiare degli strumenti, dei processi, della formazione e dell'esperienza che saranno realizzati dal progetto con particolare riferimento alle piattaforme condivise tra Regione e una pluralità di enti sul territorio (PiemontePay, SPID, Cloud).

3B. Descrizione delle criticità della postura di sicurezza indirizzate

Max 300 parole

Il presente progetto ha come obiettivo l'indirizzo delle seguenti criticità:

- **Presenza di potenziali vulnerabilità nello sviluppo del software**: lo sviluppo di soluzioni applicative determina statisticamente l'introduzione di vulnerabilità determinate dalla scrittura del codice sorgente. L'intervento è mirato all'individuazione delle potenziali vulnerabilità attraverso un processo/servizio di revisione del codice (code review).

- **Insufficiente livello di competenze nell'ambito dello sviluppo del software:** la conoscenza di tecniche e strumenti per lo sviluppo di "codice sicuro" costituisce un aspetto fondamentale per garantire la sicurezza delle applicazioni. L'intervento è mirato ad aumentare il livello di competenza nella sicurezza applicativa e data protection con particolare riferimento alla filiera di sviluppo che utilizza il Cloud Regionale

- **Processi di risposta agli incidenti ed alla gestione delle crisi scarsamente strutturati** che devono essere migliorati e potenziati ma soprattutto resi maggiormente noti all'organizzazione e consolidati ai fini di una tempestiva reazione.

- **Disservizi alla PA e ai cittadini** a fronte di indisponibilità totale o parziale delle infrastrutture su cui i servizi vengono erogati, che comportano una conseguente discontinuità operativa, con impatti sul funzionamento interno dell'Ente pubblico e sui procedimenti a rilevanza esterna.
- **Incompletezza nei controlli di sicurezza e vulnerabilità in fase di test e collaudo del software** a causa del limitato supporto di strumenti automatici nell'esecuzione delle verifiche o della mancata adozione di una metodologia consolidata

- **Controllo limitato e parziale capacità di audit sul ciclo di vita delle identità digitali**, il loro aggiornamento e deprovisioning e i profili assegnati

- **Vulnerabilità introdotte nell'utilizzo dei servizi e nei comportamenti** da parte degli utilizzatori per effetto di una mancanza di consapevolezza e di cultura

3C. Descrizione degli obiettivi dell'intervento e dell'impatto in termini di potenziamento della resilienza cyber, ed in particolare in riferimento:

- adozione di misure e controlli di sicurezza
- supportare il processo di transizione digitale

Max 400 parole

Alcuni degli obiettivi di seguito descritti si inseriscono all'interno di un percorso di evoluzione che la Regione Piemonte ha intrapreso negli ultimi 5 anni volto all'automazione dei processi di delivery della propria filiera produttiva successivamente estesa, anche in coerenza con il ruolo di aggregatore territoriale sul digitale, agli altri Enti locali che condividono soluzioni e servizi erogati dalla propria in-house.

O1. **Potenziare gli strumenti per la mitigazione del rischio cyber** nell'ambito dell'analisi delle vulnerabilità delle applicazioni destinate alla filiera di delivery introducendo un approccio che sfrutti maggiormente l'automazione. Oggi il processo di analisi delle vulnerabilità esiste ma è

gestito in ottica tradizionale.

O2. **Evolvere il processo operativo e la metodologia** per l'individuazione e la risoluzione delle vulnerabilità, individuate sia per le applicazioni dispiegate sul cloud regionale, sia per quelle ospitate su altre infrastrutture, supportando i processi di transizione al digitale con strumenti di controllo e verifica "automatizzati" all'interno della filiera di produzione del software, rendendo così più resilienti e periodici i controlli.

O3. **Effettuare la redazione del piano di potenziamento delle capacità cyber** in conseguenza anche all'analisi di postura, effettuata su un perimetro di servizi ritenuto architetturalmente aggiornato e stabile nei prossimi 3/5 anni. Di conseguenza il modello sarà applicato su altri ambiti.

O4. **Miglioramento e potenziamento dei processi di gestione del rischio cyber** attualmente in uso, sia nella risposta agli attacchi sia nel potenziamento dei processi e delle metodologie di sviluppo sicuro dei servizi in ottica security by-design

O5. **Potenziamento dei processi di business impact analysis** a supporto della continuità operativa e con annessa impostazione/revisione del Piano di Business Continuity

O6. **Potenziamento della security awareness**, ovvero la percezione del livello di consapevolezza dei rischi di sicurezza cui sono esposti i servizi ed i dati della PA tramite il rafforzamento delle competenze ma anche attraverso la conoscenza dei concetti di security e privacy by design calati maggiormente nell'ecosistema dei servizi erogati dall'Ente.

O7. **Evoluzione e governo dei sistemi per la gestione dell'Identità digitale** nell'ottica di fornire una gestione del ciclo di vita più strutturata e con maggiori funzionalità di controllo e monitoraggio

3D. Descrizione dei contenuti operativi e delle attività previste

Max 300 parole

Postura della sicurezza (obiettivi O1, O2, O3, O4)

Analisi postura di sicurezza applicazioni individuate in un "**insieme predefinito"**, ovvero:

- 11 nel Cloud Regionale consolidate, che non prevedono nel medio periodo un piano di revisione/sostituzione: 2 Formazione Professionale, 1 Lavoro, 3 Ambiente, 1 Cultura, 1 Procurement, 1 Sanità, 2 Territorio
- 1 non ancora in cloud, ambito Lavoro/Energia, come riferimento in termini di vulnerabilità, impatti e tipologia di interventi su famiglie equiparabili.

Security Awareness (obiettivo O6)
Predisposizione/erogazione percorsi formativi ai dipendenti su data protection, security-by-design, gestione/risposta incidenti.
Revisione/Integrazione delle procedure legate alla sicurezza dei servizi dell'Ente (obiettivi O3, O4, O5):

- Revisione e potenziamento policy e processi relativi allo sviluppo sicuro by-design in

funzione dell'introduzione della componente trasversale di verifica automatizzata vulnerabilità

- Definizione/potenziamento processi operativi di risposta agli attacchi, incidenti e crisis management
- Revisione/potenziamento processi a supporto continuità operativa: analisi vulnerabilità connesse alla disponibilità servizi attraverso BIA; definizione strategie tecnico-organizzative e realizzazione BC-plan (ISO22301:2019)

Realizzazione strumenti analisi vulnerabilità e interventi di mitigazione (obiettivi O1, O2, O3, O4)

- Progettazione e sviluppo componente trasversale di verifica automatizzata vulnerabilità nel processo di delivery sull "**insieme predefinito di applicazioni"**
- Interventi mitigazione delle vulnerabilità gravi individuate e messa in sicurezza applicazioni in esito **all'analisi postura**
  - Funzionale al nuovo processo di delivery controllato, utilizzabile da tutti i nuovi sviluppi secondo il modello "continuous vulnerability management" di cui beneficeranno gli Enti indicati in anagrafica
  - Trasversale ai servizi erogati sul Cloud regionale

Evoluzione piattaforma identità digitale(Obiettivo O7)

- Dismissione attuale sistema di erogazione delle identità utilizzato dai dipendenti per accesso ai servizi basato su certificati P12 verso adozione nuova piattaforma integrata di gestione ciclo-vita delle credenziali (analisi e progettazione):
- Indipendenza da
  - piattaforma hardware utilizzata
  - luogo di accesso
- Logiche controllate di self-provisioning
- Cruscotto gestione/monitoraggio ciclo di vita

3E. Descrizione delle modalità attuative ovvero delle modalità amministrative per la realizzazione delle attività

Max 300 parole

Regione Piemonte si avvarrà della propria *in-house*, CSI Piemonte, per la realizzazione delle attività.

Come previsto dalla Convenzione Quadro 2022-2026 approvata con D.G.R. n. 21-4474 del 29 dicembre 2021 l'intervento sarà avviato attraverso l'approvazione di specifica Proposta Tecnico Economica formulata da CSI Piemonte e di contestuale determinazione dirigenziale di affidamento del Responsabile del progetto, come definito dalle procedure operative previste dalla Convenzione Quadro, che disciplinano il ciclo completo della fornitura e la rendicontazione per i progetti cofinanziati con fondi europei.

Tutte le attività sopraindicate saranno perfezionate propedeuticamente in modo da consentire l'immediato avvio operativo dei lavori a seguito dell'ammissione formale al finanziamento del

progetto e comunque non oltre 15 giorni.

La struttura del responsabile di progetto è composta da:

- funzionari e collaboratori con esperienza di project management e di partecipazione a progetti finanziati con fondi comunitari su diverse programmazioni, con particolare riferimento agli aspetti di rendicontazione, attestazione del raggiungimento di obiettivi e target, partecipazione alle attività di verifica e controllo;
- funzionari di staff specializzati in ambito amministrativo/contabile, che curano iter dall'accertamento alla liquidazione finale.

Verranno individuati in questo contesto un apposito team e un Capo Progetto che lo coordinerà, costituendo il punto di supporto al Dirigente nella completa gestione del progetto e degli adempimenti correlati.

All'interno del team saranno attribuiti ruoli e responsabilità distinti tra i componenti al fine di mitigare i rischi di progetto e prevenire eventuali fenomeni corruttivi.

Nel piano di rafforzamento amministrativo attualmente in corso di attuazione, Regione Piemonte sta valutando di incrementare il numero di risorse da destinare al progetto qui definito.

Sezione 4 – QUADRO FINANZIARIO

In riferimento al paragrafo n. 5.2 "Spese ammissibili" dell'Avviso pubblico recante "Avviso Pubblico per la presentazione di proposte per la realizzazione di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PNRR, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity"M1C1I1.5", nella presente sezione, deve essere dettagliato il preventivo finanziario.
Si specifica che il Soggetto attuatore dell'intervento potrà presentare esclusivamente costi strettamente connessi allo svolgimento delle attività previste nel Piano di Progetto coerenti e pertinenti con le finalità dell'intervento 1.5, Missione M1C1, e successivamente comprovabili con opportuna documentazione giustificativa. Ai fini dell'ammissibilità delle spese si rimanda alla normativa nazionale ed europea di riferimento vigente e alle indicazioni operative ripotate nel Manuale per i Soggetti Attuatori adottato dall'Agenzia.

Il finanziamento concesso con il presente Avviso è cumulabile con altri finanziamenti a valere su programmi e strumenti dell'Unione europea, a condizione che gli stessi non interessino i medesimi costi in applicazione del principio di addizionalità di cui all'art.9 del Regolamento (UE) 2021/241. Dovrà pertanto essere esplicitato nel preventivo finanziario l'eventuale contributo a carico di altre fonti finanziarie.

Nel caso in cui l'intervento sia stato avviato con una diversa copertura finanziaria a valere sul bilancio dell'Unione, all'atto della sottoscrizione dell'Atto d'Obbligo il Soggetto attuatore dell'intervento dovrà formalmente dimostrare di aver rinunciato al precedente finanziamento, ove questo sia riferito ai medesimi costi per cui si chiede il contributo a valere sul PNRR.

Si fornisce di seguito un dettaglio delle tipologie di spese ammissibili, a titolo esemplificativo e non esaustivo:

- spese per servizi di consulenza per l'implementazione degli interventi progettuali ammissibili secondo indicazioni di cui alla circolare RGS n. 4/2021, incluse attività di formazione specifica;
- spese per la progettazione, lo sviluppo e l'implementazione di software specifici;
- spese per l'acquisto di hardware, software;
- spese per l'acquisizione di servizi per l'implementazione degli interventi progettuali (es: sviluppo software; servizi di connettività; analisi, studi, ecc);
- spese generali e altri costi di esercizio direttamente imputabili all'attività progettuale nella misura pari al 7% di costi diretti ammissibili ai sensi dell'art. 54 lett. a del Reg. (UE) 2021/1060.

4A. Indicazione e descrizione delle **risorse finanziarie** necessarie alla realizzazione del progetto denominato Transizione digitale e servizi sicuri, per ogni macro-attività

COSTO COMPLESSIVO DEL PROGETTO "***Transizione digitale e servizi sicuri*** *":* € 995.100

CONTRIBUTO RICHIESTO € 995.100 ripartito per le seguenti tipologie di intervento come da prospetto di cui alla *Tabella 1* e il cui dettaglio dei costi preventivati indicato in *Tabella 2*.

Tabella 1 – Contributo richiesto per tipologia di intervento
Compilare con l'importo previsto per ogni intervento comprensivo delle spese generali[1].

TIPOLOGIA INTERVENTO	*TOTALE (al netto di IVA)*	*TOTALE IVA*[2]	IMPORTO FINANZIAMENTO RICHIESTO
Analisi della postura di sicurezza e piano di potenziamento	€ 288.900	0	€ 288.900
Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	€ 278.200	0	€ 278.200
Miglioramento della consapevolezza delle persone	€ 64.200	0	€ 64.200
Progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber	€ 363.800	0	€ 363.800

DESCRIZIONE DI ALTRE FONTI DI FINANZIAMENTO UTILIZZATE PER LA REALIZZAZIONE DEL PROGETTO (se previste):

1 *Le spese generali e altri costi di esercizio direttamente imputabili all'attività progettuale sono riconosciti nella misura pari al 7% dei costi diretti ammissibili (art. 5.2 dell'Avviso)*
2 *Come richiamato dal DPR. 22/2018, art. 15: "Ai sensi dell'articolo 69, paragrafo 3, lettera c), del regolamento (UE) n. 1303/2013, l'imposta sul valore aggiunto (IVA) realmente e definitivamente sostenuta dal beneficiario è una spesa ammissibile solo se questa non sia recuperabile, nel rispetto della normativa nazionale di riferimento […]". Pertanto, questa potrà essere computata nella colonna "importo finanziamento richiesto" esclusivamente al verificarsi di tale fattispecie*.

Finanziato dall'Unione europea NextGenerationEU · DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE · ACN · REGIONE PIEMONTE

Non sono previste altre fonti di finanziamento

In merito al quadro finanziario indicato, si precisa quanto segue:

Regione Piemonte intende ricorrere [illegible] inhouse nella realizzazione degli interventi della [illegible] proposta; i rapporti in essere sono regolati da un regime di esenzione IVA applicata per le prestazioni di servizio (fatturazione esente IVA) ai sensi dell'art. 10 comma 2 del DPR 633/1972 e dal regime ordinario di IVA nel solo caso di cessioni di beni (fatturazione imponibile oltre IVA 22%);

Nel caso di "acquisizione di servizi" dalla inhouse, essendo la fattura esposta da quest'ultima con l'importo esente IVA (Totale al netto di IVA), l'importo finanziato richiesto corrisponderà al totale della fattura stessa;

Nel caso di "acquisizione di beni" dalla inhouse, essendo la fattura esposta da quest'ultima con l'importo imponibile (Totale al netto di IVA) e con l'importo dell'IVA al 22% (Totale IVA) ed essendo l'IVA sostenuta non recuperabile dal soggetto beneficiario, l'importo finanziato richiesto corrisponderà al totale della fattura al lordo dell'IVA.

Tabella 2 – Dettaglio dei costi preventivati per ogni attività e tipologia di investimento

Compilare la seguente tabella con il dettaglio dei costi preventivati per ogni attività e tipologia di investimento (rif. Paragrafo 4.1 dell'avviso) prevista per il progetto aggiungendo se necessarie ulteriori righe.

TIPOLOGIA INTERVENTO[3]	ATTIVITA	CATEGORIA DI COSTO[4]	IMPORTO TOTALE	*TOTALE (al netto di IVA)*	*TOTALE IVA[5]*	IMPORTO FINANZIAMENTO RICHIESTO
Analisi della postura di sicurezza e piano di potenziamento	**Postura della sicurezza applicativi perimetro regionale**	Acquisizione servizi professionali	130.000	130.000	0	130.000
Analisi della postura di sicurezza e piano di potenziamento	**individuazione e analisi vulnerabilità su perimetro applicativi prefissato e piano di remediation**	Acquisizione servizi professionali	140.000	140.000	0	140.000
Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	**Revisione/ Integrazione delle procedure e policy**	Acquisizione servizi professionali	150.000	150.000	0	150.000
Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	**Business Impact Analysis a supporto della continuità operativa**	Acquisizione servizi professionali	110.000	110.000	0	110.000

3 *Indicare la tipologia di intervento in coerenza con l'articolo 4.1 dell'Avviso.*

4 *Per categoria di costo indicare ad esempio: acquisizione di beni; acquisizione di servizi; costo personale interno; …)*

5 *Come richiamato dal DPR. 22/2018, art. 15: "Ai sensi dell'articolo 69, paragrafo 3, lettera c), del regolamento (UE) n. 1303/2013, l'imposta sul valore aggiunto (IVA) realmente e definitivamente sostenuta dal beneficiario è una spesa ammissibile solo se questa non sia recuperabile, nel rispetto della normativa nazionale di riferimento […]". Pertanto, questa potrà essere computata nella colonna "importo finanziamento richiesto" esclusivamente al verificarsi di tale fattispecie.*

Miglioramento della consapevolezza delle persone	**Security Awareness e formazione**	Acquisizione servizi professionali	60.000	60.000	0	60.000
Progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber	**Realizzazione strumenti analisi vulnerabilità filiera automation ed interventi di mitigazione**	Acquisizione servizi professionali	230.000	230.000	0	230.000
Progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber	**Evoluzione piattaforma di identità digitale**	Acquisizione servizi professionali	110.000	110.000	0	110.000
a) TOTALE COSTI DIRETTI						**€ 930.000**
b) SPESE GENERALI 7% DEI COSTI DIRETTI AMMISSIBILI (a*7%)						**€ 65.100**
c) TOTALE RICHIESTO A FINANZIAMENTO (a+b)						**€ 995.100**

Sezione 5 – CRONOPROGRAMMA

5A. Indicazione e descrizione del **cronoprogramma delle attività** di implementazione del progetto
Compilare la tabella sottostante (è possibile aggiungere righe alla tabella)

Tipologie di investimento *(rif. Paragrafo 4.1 dell'avviso)*	Attività (breve descrizione)	Data di inizio prevista (es. Q3 2022)	Data di fine prevista (es. Q4 2022)	Durata espressa in gg
Analisi della postura di sicurezza e piano di potenziamento	**Postura della sicurezza applicativi perimetro regionale**	Q1 2023	Q3 2023	Effort (401) Durata (270)
Analisi della postura di sicurezza e piano di potenziamento	**individuazione e analisi vulnerabilità su perimetro applicativi prefissato e piano di remediation**	Q3 2023	Q3 2024	Effort (432) Durata (430)
Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	**Revisione/Integrazione delle procedure e policy**	Q1 2023	Q2 2024	Effort (463) Durata (600)
Miglioramento dei processi e dell'organizzazione di gestione della cybersecurity	**Business Impact Analysis a supporto della continuità operativa**	Q1 2023	Q3 2024	Effort (340) Durata (600)
Miglioramento della consapevolezza delle persone	**Security Awareness e formazione**	Q4 2022	Q2 2024	Effort (157) Durata (530)
Progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber	**Realizzazione strumenti analisi vulnerabilità filiera automation ed interventi di mitigazione**	Q1 2023	Q2 2024	Effort (710) Durata (500)
Progettazione e	**Evoluzione piattaforma**	Q1 2023	Q2 2024	Effort (362)

sviluppo di nuovi sistemi per la mitigazione del rischio cyber	**di identità digitale**			Durata (360)