POR CAMPANIA FESR 2014-2020

ASSE 2 "ICT E AGENDA DIGITALE"

OBIETTIVO SPECIFICO 2.2 "DIGITALIZZAZIONE DEI PROCESSI AMMINISTRATIVI E DIFFUSIONE DI SERVIZI DIGITALI PIENAMENTE INTEROPERABILI"

AZIONE 2.2.1 "SOLUZIONI TECNOLOGICHE PER LA DIGITALIZZAZIONE E L'INNOVAZIONE DEI PROCESSI INTERNI DEI VARI AMBITI DELLA PUBBLICA AMMINISTRAZIONE NEL QUADRO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ"

SCHEDA PROGETTO

PROGETTO DA AVVIARE ☒
PROGETTO IN CORSO ☐

SOGGETTO PROPONENTE	ASL NAPOLI 3 SUD	
CODICE FISCALE	06322711216	
PEC	sistemi.informatici@pec.aslnapoli3sud.it	
REFERENTE PROGETTO	Dr. Maurizio Imperatrice	Mail: sistemi.informatici@aslnapoli3sud.it

TITOLO DEL PROGETTO
AslNa3_Progetto di digitalizzazione dei processi amministrativi e implementazione di un sistema di cybersecurity per la gestione dei rischi informatici

DESCRIZIONE DEL PROGETTO, CON EVIDENZA DEGLI ELEMENTI DI COERENZA CON LA DGR N. 354 DEL 19/06/2023 E CON L'AZIONE 2.2.1 DEL POR CAMPANIA FESR 2014-2020

(Partendo dall'analisi dei fabbisogni, illustrare, in maniera dettagliata, gli interventi proposti e le spese consequenziali, riportando, in maniera puntuale, le spese relative a:

a) Servizi di digitalizzazione della documentazione sanitaria a supporto degli assistiti e degli operatori sanitari (specificare la tipologia di documenti da digitalizzare ed il numero di documenti per ciascuna tipologia);

b) Attrezzature per la digitalizzazione dei risultati diagnostici (indicare le singole attrezzature ed il relativo numero, nonchè eventuali software di funzionamento);

c) *Sistemi di Cyber Security (specificare componenti hardware, componenti software ed eventuali spese necessarie ai fini dell'installazione).*

a)L'Azienda Sanitaria Locale Napoli3 Sud ha già avviato da tempo un processo di dematerializzazione dei propri archivi cartacei e trasformazione in digitale dei propri processi aziendali. Nel solco di questa strategia e in linea con quanto indicato nella DGR 354 del 19/6/2023, questa Amministrazione intende proseguire con la *digitalizzazione delle Cartelle Cliniche cartacee degli anni pregressi e dell'anno corrente, e con la dematerializzazione e gestione digitale dei Consensi che raccoglie dai cittadini durante l'erogazione di prestazioni sanitarie.*
L'azione progettuale, così articolata, riscontra quanto richiesto dalla DGR 354 del 19/6/23, in quanto espressamente orientata all'erogazione di servizi finalizzati alla dematerializzazione di documentazione sanitaria e a supportare l'azienda nei processi di sorveglianza sanitaria.

Di seguito si descrivono le singole fasi progettuali:

Digitalizzazione Cartelle Cliniche

Il processo di digitalizzazione delle Cartelle Cliniche viene svolto mediante esecuzione di specifiche fasi lavorative quali:

- La presa in carico della documentazione cartacea dalle sedi indicate e il trasferimento presso il centro esterno di lavorazione
- La dematerializzazione delle singole Cartelle e relativa metadatazione con produzione di file in formato pdf e successiva metadatazione dei campi che saranno utilizzati come filtri di ricerca
- La ricomposizione del fascicolo e la raccolta in contenitori per la custodia
- La custodia provvisoria del cartaceo in depositi attrezzati ad ospitarli
- La lavorazione della documentazione cartacea produrrà un archivio digitale delle Cartelle Cliniche che sarà messo a disposizione di assistiti e operatori sanitari dell'ASL.

Per la realizzazione delle suddette attività è stato definito il piano dei fabbisogni con la descrizione dettagliata dei singoli interventi e relativi costi.

c) La sicurezza in sanità è un tema molto rilevante perché i nostri dati esigono protezione rispetto ai rischi di accesso indebito, alterazione e manipolazione, a seguito di attacchi cibernetici ai sistemi informativi sanitari. Anche alla luce dei recenti attacchi hacker subito dalle Aziende Sanitarie non si può negare che le violazioni causate dagli attacchi citati stanno aumentando in misura esponenziale ed è altrettanto evidente come non ci si possa più permettere di sottovalutare la problematica.
È quindi fondamentale proteggere i dati da accessi non autorizzati e tentativi malevoli di esfiltrazione perché una loro violazione potrebbe avere conseguenze molto gravi, tra cui ad esempio il furto di identità e discriminazione. La sanità digitale va realizzata all'interno di un progetto organico e lungimirante di governance sanitaria, che minimizzi i rischi cibernetici e promuova una condivisione selettiva dei dati. Per garantire la sicurezza è pertanto necessario implementare alcune misure tecniche atte a garantire:

- La gestione delle informazioni sensibili e personali
- Il controllo dell'accesso e la sua limitazione al solo personale autorizzato
- La conformità alle normative come il Regolamento Generale sulla Protezione dei Dati (GDPR) per evitare sanzioni e rischi per la reputazione
- Il controllo e la gestione in sicurezza delle apparecchiature medicali disponibili in Azienda.

Dopo l'attacco ricevuto nel Gennaio del 2022 l'Azienda Napoli 3 ha messo in campo un notevole sforzo per migliorare lo stato della sicurezza delle proprie risorse in rete. In particolare si sta passando da una rete piatta ad una rete oppotunamente segmentata in diverse reti locali organizzate in modo tematico.
Parallelamente si sta procedendo ad ultimare la messa in dominio delle postazioni di lavoro aziendali nell'ottica di un controllo più granulare della sicurezza.
È anche in corso il progetto di implementazione della SDWan (Software defined Wan) che attraverso l'uso di firewall di nuova generazione garantirà la sicurezza e la resilienza della rete dell'ASL.
Per aumentare i livelli di sicurezza aziendale si è deciso di adottare gli strumenti offerti dal mercato attraverso il true-up del contratto Consip EA6 attualmente in essere, con l'acquisto di licenze capex.

L'installazione e configurazione dell'ambiente di cui sopra, sarà realizzato con il supporto di specialisti Microsoft attraverso l'attivazione del contratto Microsoft Enterprise Services di supporto tecnico specialistico.

Riepilogo dei Servizi	Corrispettivo EUR
Unified Enterprise Support	90.186,75
Unified Proactive Services Add on	25.456,00
Designated Support Engineering |	48.500,00
Subtotale	162.142,75
Flex Allowance	(23.342,75)
Vantaggi di Software Assurance *	(61.096,00)
Corrispettivi Totali (imposte escluse)	**79.704,00**

Attraverso la convenzione Consip Cybersecurity2 si procede all'acquisto di:

- n.2 NAC (sistemi per controllo accessi) - Fascia alta
- n.2 Next Generation Firewall NGFW - Fascia alta

acquistinretepa

Cybersecurity 2 - prodotti e servizi connessi

Corrispettivi e tariffe

RTI Telecom

Prodotto/servizio	Prezzo
NGFW - Fascia 1 Fortinet [Euro ad unità]	1.211,18 €
NGFW - Fascia 1 Cisco [Euro ad unità]	1.213,71 €
NGFW - Fascia 1 Palo Alto [Euro ad unità]	1.059,24 €
NGFW - Fascia 1 Forcepoint [Euro ad unità]	933,22 €
NGFW - Fascia 2 Fortinet [Euro ad unità]	6.672,19 €
NGFW - Fascia 2 Cisco [Euro ad unità]	5.039,51 €
NGFW - Fascia 2 Palo Alto [Euro ad unità]	8.951,15 €
NGFW - Fascia 2 Forcepoint [Euro ad unità]	9.586,10 €
NGFW - Fascia 3 Fortinet [Euro ad unità]	12.502,60 €
NGFW - Fascia 3 Cisco [Euro ad unità]	12.018,48 €
NGFW - Fascia 3 Palo Alto [Euro ad unità]	15.062,48 €
NGFW - Fascia 3 Forcepoint [Euro ad unità]	11.262,52 €
NGFW - Fascia 4 Fortinet [Euro ad unità]	33.216,09 €
NGFW - Fascia 4 Cisco [Euro ad unità]	38.839,58 €
NGFW - Fascia 4 Palo Alto [Euro ad unità]	24.019,90 €
NGFW - Fascia 4 Forcepoint [Euro ad unità]	21.230,77 €
NGFW - Fascia 5 Fortinet [Euro ad unità]	50.386,49 €
NGFW - Fascia 5 Cisco [Euro ad unità]	64.442,88 €
NGFW - Fascia 5 Palo Alto [Euro ad unità]	41.050,87 €
NGFW - Fascia 5 Forcepoint [Euro ad unità]	37.683,32 €
NGFW - Fascia 6 Fortinet [Euro ad unità]	99.845,39 €
NGFW - Fascia 6 Cisco [Euro ad unità]	148.255,36 €
NGFW - Fascia 6 Palo Alto [Euro ad unità]	66.798,74 €
NGFW - Fascia 6 Forcepoint [Euro ad unità]	51.217,88 €
NAC - Fascia 1 HPE Aruba [Euro ad unità]	5.981,41 €
NAC - Fascia 1 Fortinet [Euro ad unità]	10.057,32 €
NAC - Fascia 2 HPE Aruba [Euro ad unità]	10.073,47 €
NAC - Fascia 2 Fortinet [Euro ad unità]	11.445,96 €
NAC - Fascia 3 HPE Aruba [Euro ad unità]	13.444,83 €
NAC- Fascia 3 Fortinet [Euro ad unità]	13.521,59 €
NAC - Fascia 4 HPE Aruba [Euro ad unità]	56.704,76 €
NAC - Fascia 4 Fortinet [Euro ad unità]	66.577,91 €
NAC - Fascia 5 HPE Aruba [Euro ad unità]	122.319,75 €
NAC - Fascia 5 Fortinet [Euro ad unità]	144.737,90 €

In riferimento alla soluzione di sicurezza, nella presente integrazione al progetto inizialmente presentato, questa Amministrazione si è trovata a garantire la continuità dei propri servizi di sicurezza scaduti nel mese di Luglio. Nel frattempo, con propri fondi, ha proceduto ad aderire alla Convenzione Consip Cybersecurity da Remoto, al fine di attivare alcuni servizi di sicurezza (SOC, SIEM, SOAR, ed altro) per il monitoraggio continuo all'interno della propria rete aziendale e con l'obiettivo di raccogliere, ordinare, classificare e analizzare le varie tipologie di attività, utilizzando servizi di threat intelligence per elaborare le informazioni fornite dai sistemi di protezione e mettere in atto le azioni di response a salvaguardia dell'integrità delle risorse aziendali. Pertanto, in base a quanto precisato, il costo di alcune componenti inizialmente previste è stato stralciato pervenendo ad un costo inferiore rispetto alla prima versione di scheda di progetto.

OBIETTIVI DEL PROGETTO E RISULTATI ATTESI

In considerazione delle potenzialità in termini conoscitivi che rappresenta il patrimonio documentale delle cartelle cliniche, appare di importanza strategica mettere in atto tutte le misure finalizzate a creare una banca dati in cui raccogliere, centralizzare e condividere i fascicoli in formato elettronico sicuro nel pieno rispetto delle recenti normative in materia di sicurezza e privacy dei dati sanitari. Ciò consentirà all'azienda sanitaria di promuovere il raggiungimento di obiettivi quali: l'ottimizzazione della spesa pubblica, l'introduzione di nuove tecnologie digitali innovative e orientate all'interoperabilità e alla condivisone delle informazioni tra tutti gli stakeholder in ambito sanitario, il supporto all'analisi delle informazioni sanitarie per migliorare i processi di monitoraggio e sorveglianza sanitaria.

Per quanto riguarda i sistemi di cybersecurity l'obiettivo del progetto è implementare le seguenti tecnologie:

- soluzione di sicurezza degli endpoint, server, dispositivi dell'azienda, workload in cloud e rete per permette di rilevare più velocemente le minacce e migliorare i tempi di indagine e risposta attraverso l'analisi della sicurezza (protezione da ransomware, malware, phishing e altre minacce)
- ampliamento servizi di sicurezza a copertura dell'utenza aziendale (Identity Access Management)
- Next Generation Firewall (NGFW) che integrano e aggiornano una serie di funzionalità per la protezione dalle minacce informatiche avanzate
- NAC per la sicurezza fisica di rete e abilitare l'accesso a quegli utenti e dispositivi riconosciti e che rispettano le policy aziendali/negare l'accesso agli utenti/dispositivi non conformi alle politiche di sicurezza aziendali