PIANO OPERATIVO PER L'AFFIDAMENTO DI PRODOTTI PER LA SICUREZZA PERIMETRALE, PROTEZIONE DEGLI ENDPOINT E ANTI-APT

LOTTO 3

AZIENDA OSPEDALIERA SANTOBONO PAUSILIPON
NAPOLI

Tabella Revisioni

Revisione	Descrizione modifiche	Data
1.0	Prima emissione	03/10/2023

Indice

1. INTRODUZIONE

1.1 PREMESSA

Il presente documento descrive il Piano Operativo TIM, relativamente alla richiesta di fornitura di prodotti per la sicurezza perimetrale per la Pubblica Amministrazione **AZIENDA OSPEDALIERA SANTOBONO PAUSILIPON**, in conformità alle richieste espresse dall'Amministrazione durante gli incontri informali intercorsi.

L'Azienda Ospedaliera Santobono Pausilipon svolge la funzione di tutela e promozione della salute degli individui e della collettività, attraverso attività di prevenzione, cura degli stati di malattia e di recupero della salute, garantendo i Livelli Essenziali di Assistenza - (LEA) e consolidando l'integrazione tra assistenza territoriale e ospedaliera, al fine di mantenere il più alto livello possibile di qualità della vita dei cittadini, fornendo servizi erogati direttamente nel rispetto della persona ed in condizioni di sicurezza e di riservatezza. In ambito territoriale coincide con il territorio di Napoli.
Il progetto prevede la fornitura di prodotti per la sicurezza perimetrale e l'erogazione di servizi connessi.

1.2 SCOPO

Lo scopo del documento è quello di formulare una proposta tecnico/economica secondo le modalità tecniche ed i listini previsti nell'Accordo Quadro.

1.3 RIFERIMENTI

Identificativo
Piano dei Fabbisogni - Allegato 1.PIANO DEI FABBISOGNI PIANO DEI FABBISOGNI.PDF
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Speciale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato Tecnico Generale
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT – Lotti 1,2,3 - Capitolato d'oneri
ID 2367 AQ - Prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT –- Offerta Tecnica Lotto Lotti 1,2,3

1.4 ACRONIMI E GLOSSARIO

Definizione / Acronimo	Descrizione
AgID	Agenzia per l'Italia Digitale
Consip	Consip S.p.a.
RTI	Raggruppamento Temporaneo d'Impresa
SPC	Sistema Pubblico di Connettività

2. ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

Per il coordinamento delle attività contrattuali previste il RTI impiegherà i referenti di seguito indicati:

- **Responsabile Unico della Attività Contrattuali dell'Accordo Quadro (RUAC-AQ)**

Nome Cognome: Massimiliano Materazzi
e-mail: massimiliano.materazzi@telecomitalia.it

che dovrà riferire, per quanto di competenza, a Consip/Organismo Tecnico di Coordinamento e Controllo, ove richiesto, su tutte le tematiche contrattuali relative all'Accordo Quadro.

Nel Piano Operativo dovrà inoltre essere indicato il modello organizzativo impiegato per l'esecuzione delle attività ed in particolare le persone di riferimento che saranno coinvolte nel processo, che comprendono almeno:

- il "*Responsabile dell'Amministrazione*" (già identificato nel "*Piano dei Fabbisogni*");
- il "*Responsabile del Fornitore*" (cfr. par. 2.4.1.2 del Capitolato Tecnico Generale).

- **Responsabile del Fornitore**

Nome Cognome: **Nicola Memeo**
telefono/cellulare: **+393486052419**
e-mail: **Nicola.Memeo@maticmind.it**

che dovrà riferire, per quanto di competenza, all'Amministrazione su tutte le tematiche contrattuali relative al Contratto Esecutivo.

- **Referente Tecnico per l'erogazione dei servizi**

Nome Cognome: **Daniela Lazzaro**
telefono/cellulare: **+393665635371**
e-mail: **Daniela.Lazzaro@maticmind.it**

(PM di delivery di riferimento del progetto)

che dovranno garantire il corretto svolgimento delle attività e dei servizi ed il relativo livello di qualità di erogazione nel rispetto dei KPI previsti dal Capitolato Tecnico – Parte speciale (cfr. capitolo 5).

2.1 CATEGORIZZAZIONE DEGLI INTERVENTI

In relazione al Piano Triennale per l'Informatica delle Pubbliche Amministrazioni, di seguito si riporta "l'inquadramento o categorizzazione" degli interventi che l'Amministrazione intende realizzare.

Ambito (layer)	Obiettivi Piano Triennale
Servizi	Servizi al cittadino
	Servizi a imprese e professionisti
	Servizi interni alla propria PA
	Servizi verso altre PA
Dati	Favorire la condivisione e il riutilizzo dei dati tra le PA e il riutilizzo da parte di cittadini e imprese
	Aumentare la qualità dei dati e dei metadati
	Aumentare la consapevolezza sulle politiche di valorizzazione del patrimonio informativo pubblico e su una moderna economia dei dati
Piattaforme	Favorire l'evoluzione delle piattaforme esistenti per migliorare i servizi offerti a cittadini ed imprese semplificando l'azione amministrativa
	Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle PA
	Incrementare e razionalizzare il numero di piattaforme per le amministrazioni
Infrastrutture	Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni locali favorendone l'aggregazione e la migrazione sul territorio (Riduzione Data Center sul territorio)
	Migliorare la qualità e la sicurezza dei servizi digitali erogati dalle amministrazioni centrali favorendone l'aggregazione e la migrazione su infrastrutture sicure ed affidabili (Migrazione infrastrutture interne verso il paradigma cloud)
	Migliorare la fruizione dei servizi digitali per cittadini ed imprese tramite il potenziamento della connettività per le PA

Interoperabilità	Favorire l'applicazione della Linea guida sul Modello di Interoperabilità da parte degli erogatori di API
	Adottare API conformi al Modello di Interoperabilità
X Sicurezza Informatica	X Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
	X Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

3. PROGETTO DI ATTUAZIONE

Nel "Piano Operativo" il Fornitore dovrà riportare, a titolo esemplificativo e non esaustivo, almeno i seguenti aspetti, in coerenza con quanto espresso dall'Amministrazione nel suo "Piano dei fabbisogni":

• l'importo contrattuale complessivo e per ciascuna voce oggetto di quotazione economica, con il dettaglio dei prodotti e dei servizi oggetto del contratto esecutivo, anche in base alle indicazioni riportate nei rispettivi paragrafi relativi ai prodotti e ai servizi previsti

Tipologia Prodotto	Codice Articolo	Descrizione Articolo	Produttore	Quantità	Prezzo Totale
Fornitura	CISCO-FPR4115-F5C	Fornitura in opera NGFW-F5-CI-CISCO-FPR4115-F5C	CISCO	6	€ 386.657,28
Servizi	SP-STA	Servizio di supporto specialistico - Security Principal - fascia standard		22	€ 6.820,00
Servizi	SSAR-STA	Servizio di supporto specialistico - Senior Security Architect - fascia standard		38	€ 10.260,00
Servizi	SSAN-STA	Servizio di supporto specialistico - Senior Security Analyst - fascia standard		45	€ 12.195,00
Servizi	SST-STA	Servizio di supporto specialistico - Senior Security Tester - fascia standard		95	€ 25.935,00
Servizi	JSAN-STA	Servizio di supporto specialistico - Junior Security Analyst - fascia standard		15	€ 3.412,50
Manutenzione 24 mesi	MANLP-NGFW-F5-CI	Manutenzione mensile LP Next Generation Firewall Fascia 5		1	già compreso all'interno della fornitura degli apparati alla Riga 1
Importo Complessivo					€ 445.279,78

la durata del Contratto Esecutivo è **24 Mesi**

Informazioni tecniche riguardanti hardware e software oggetto di fornitura sono riportate nel Capitolo 4 "Prodotti offerti".
Le forniture e i servizi verranno effettuati presso:

INDIRIZZO	NUM. CIV.	COMUNE	CAP	Referente	Recapito telefonico	Mail
VIA TERESA RAVASCHIERI, GIÀ VIA DELLA CROCE ROSSA, 8, 80122		NAPOLI (NA)	80127	GENNARO SIRICO	+39 0812205393	G.SIRICO@SANTOBONOPAUSILIPON.IT

Di seguito vengono riassunte le previsioni di impiego in giorni persona per il servizio di fornitura:

Servizio	Figura professionale	Giornate
Realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso	Security Principal	22
	Senior Security Architect	38
	Senior Security Analyst	45
	Senior Security Tester	95
	Junior Security Analyst	15

I prodotti e i servizi proposti, in relazione alle esigenze espresse dall'Amministrazione nel Piano dei Fabbisogni si compongono degli elementi descritti in dettaglio nel seguito del Capitolo.

4. PRODOTTI OFFERTI

Next Generation Firewall	
DENOMINAZIONE BRAND	**FASCIA 5 (cfr. definizione CTSpeciale)**
Cisco	*Modello* ***CISCO- FPR4115-F5C*** *Codice Prodotto* ***CISCO-FPR4115-F5C*** *1xFPR4115-NGFW-K9* *+ 2xFPR4K-NM-8X1G-F* *+ 1xL-FPR4115T-TMC= (24 mesi)* *+ 1xSF-FMC-KVM-10-K9*

4.1 NGFW

Next Generation Firewall

4.1.1 Brand 2 - Cisco

Cisco Firepower 4115 è una piattaforma di Next Generation Firewall (NGFW) utilizzata come strumento di sicurezza e difesa contro le minacce. Presenta un'architettura fortemente innovativa per abilitare funzionalità come firewall, crittografia e ispezione delle minacce, più altre funzionalità di sicurezza avanzate per fornire protezione contro attacchi più sofisticati, garantendo ottime prestazioni.
La piattaforma è il prodotto offerto di fascia 5 relativo all'Accordo Quadro (throughput fino a 19.5 Gbps). La configurazione mette a disposizione 16x porte 1000 Base-T e 8x porte 10G SFP+. E' possibile configurare gli apparati in modalità clustering fino ad un numero massimo di 6 Cisco Firepower 4115.
Inoltre, la piattaforma supporta la configurazione in modalità "multi-instance", ossia la capacità di creare diversi container virtuali che forniscono meccanismi di sicurezza in maniera indipendente tra loro, utilizzando un sottoinsieme di risorse hardware dell'appliance opportunamente dedicate e beneficiando di una gestione separata. Il numero massimo di istanze virtuali possibili è 7.
Oltre al supporto di funzionalità tradizionali come firewalling, packet routing, VPN, NAT ed altre, supporta funzionalità di sicurezza avanzate tra cui:

- **Application Visibility and Control** per il riconoscimento e la definizione di policy su base applicazione
- **Next-Generation Intrusion Prevention System** per funzionalità di rilevamento e prevenzione delle intrusioni (IDS, IPS) basate sul motore Snort, per il blocco delle minacce (NGIPS).
- **Advanced Malware Protection** per l'identificazione, il blocco, il tracciamento, l'analisi e il contenimento di malware, anche in modalità retrospettiva, con la possibilità di analisi tramite sandbox

L'immagine di cui sopra rappresenta una possibile configurazione del modello descritto, ottenibile anche con moduli non necessariamente disponibili in Accordo Quadro
Cisco Firepower si differenzia per le sue funzionalità di NGIPS le quali non sono basate solamente su signature ma anche su informazioni di contesto aggiuntive (tramite "passive discovery") relative all'ambiente specifico (sistemi operativi, files, applicazioni, utenti e altro), permettendo dunque l'attivazione di regole IPS/IDS dedicate ed ottimizzate per lo scenario specifico. Inoltre, altra caratteristica differenziante di Cisco Firepower è la capacità di fornire funzionalità di *Network File Trajectory and Retrospection* per i file intercettati, ossia di costruire una mappa relativa ai movimenti dello stesso file all'interno della rete, indicando quali host ha attraversato e fornendo informazioni su eventuali cambiamenti della reputazione del file nel tempo.
La gestione della piattaforma avviene attraverso Cisco Firewall Management Center, appliance virtuale installabile in diversi ambienti virtualizzati, che permette il monitoraggio e la visibilità, nonchè la gestione delle policy e delle configurazioni fino a 10 piattaforme. Inoltre, il prodotto presente in Accordo Quadro include la possibilità di utilizzare Cisco Secure X, soluzione cloud-based di Extended Detection Response (XDR) che fornisce ulteriori funzionalità in termini di *Threat Hunting*, *Incident Response* e *Automation/Orchestration*.
La configurazione del modello disponibile in Accordo Quadro può essere completata con l'aggiunta di ottiche SFP/SFP+ di tipo 1/10G fibra acquistabili fuori Accordo Quadro.
Il prodotto Cisco Firepower e le sue funzionalità fornite si inseriscono all'interno di una soluzione di sicurezza integrata con altri prodotti, disponibili fuori Accordo Quadro, come:

- Accesso Remoto in VPN: Cisco Firepower + Cisco Anyconnect
- Contenimento Rapido delle Minacce: Cisco Firepower + Cisco ISE
- *Complete File Trajectory*: Cisco Firepower + Cisco Secure Endpoint
- Autenticazione a più Fattori per Accesso Remote VPN: Cisco Firepower + Cisco DUO
- Accesso a funzionalità di Sandboxing Avanzate: Cisco Firepower + Cisco Threat Grid
- Funzionalità di Protezione DNS avanzate e centralizzate: Cisco Firepower + Cisco Umbrella

Le informazioni fornite nel documento sono a puro titolo informativo e descrittivo. Per ogni riferimento e approfondimento consultare la documentazione ufficiale al seguente link:
https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datasheet-c78-742474.html

4.2 SERVIZIO DI SUPPORTO SPECIALISTICO

Il servizio di Supporto Specialistico consente alle Amministrazioni Contraenti di richiedere del personale specializzato con l'obiettivo di essere supportata in varie attività inerenti sia la fornitura specifica acquistata in AQ sia, in maniera più generale, la propria infrastruttura di sicurezza informatica. Il servizio riguarderà esclusivamente le attività riportate nel seguito:

a) la realizzazione di specifiche integrazioni tra i prodotti acquistati e prodotti già presenti presso l'Amministrazione al fine di massimizzare l'efficacia dei prodotti acquisiti e garantire la sicurezza del sistema nel suo complesso

b) l'effettuazione, nelle fasi successive all'implementazione dei prodotti, di attività di analisi specifiche che consentano di stabilire le policy di sicurezza maggiormente adeguate da implementare nel complesso dei sistemi dell'Amministrazione

c) il supporto operativo al personale dell'Amministrazione nella gestione della sua infrastruttura, fornendo competenze specifiche in ambito di sicurezza informatica. Tale supporto potrà essere sia in modalità "a chiamata" sia in modalità "presidio" laddove l'Amministrazione, in ragione della complessità della propria infrastruttura, ravveda la necessità di avere del personale del Fornitore presso la propria sede in maniera continuativa

d) il supporto operativo al personale dell'Amministrazione nella gestione del suo centro operativo dedicato alla sicurezza (SOC), fornendo competenze specifiche in tale ambito. Per l'effettuazione del complesso di attività previste per il supporto specialistico il Fornitore dovrà prevedere le figure professionali riportate nel seguito. Si precisa che, fatto salvo il possesso del diploma di scuola media superiore, i requisiti accademici richiesti per ogni figura (titoli di studio) possono essere utilmente soddisfatti attraverso il possesso di una cultura equivalente, maturata attraverso lo svolgimento di esperienze lavorativo-professionali, pari a:

☐ **5 (cinque) anni aggiuntivi nel settore ICT** nel caso di laurea specialistica

☐ **3 (tre) anni aggiuntivi nel settore ICT** nel caso di laurea triennale.

4.3 Servizio di Manutenzione

La manutenzione comprende le attività volte a garantire una pronta correzione dei malfunzionamenti e il ripristino delle funzionalità, anche attraverso attività di supporto on-site. L'Amministrazione Contraente ha richiesto a pagamento il servizio di manutenzione in base al profilo di qualità per i servizi erogati: *Low Profile* (*Business Day*).
Il servizio di manutenzione è offerto per 24 mesi.
In accordo con l'Amministrazione, si predisporrà un accesso remoto sicuro utilizzando account VPN personali configurati e abilitati opportunamente, con tracciatura degli accessi per eventuali successivi audit, accessi che comunque dovranno essere limitati al tempo strettamente necessario all'esecuzione dell'attività, ad esempio mediante utenze token create all'occorrenza a supporto delle stesse (ad. es. effettuazione di diagnosi attraverso i propri sistemi di gestione e di management per analisi di problematiche e malfunzionamenti segnalati dall'Amministrazione).

Le attività di manutenzione possono riassumersi in:

- ricezione della chiamata di assistenza da parte dell'Amministrazione e assegnazione del Severity Code
- risoluzione del problema tramite supporto telefonico all'utente (ove possibile) e/o eventuale intervento/i remoto/i;
- risoluzione della causa del guasto tramite, ove necessario:
- intervento presso la sede/luogo interessato
- ripristino del servizio/funzionalità sui livelli preesistenti al guasto/anomalia, secondo gli SLA contrattualizzati, anche attraverso sostituzioni di elementi danneggiati o verifica funzionale del sistema per assicurare l'eliminazione della causa del guasto.

5 PIANO DI LAVORO

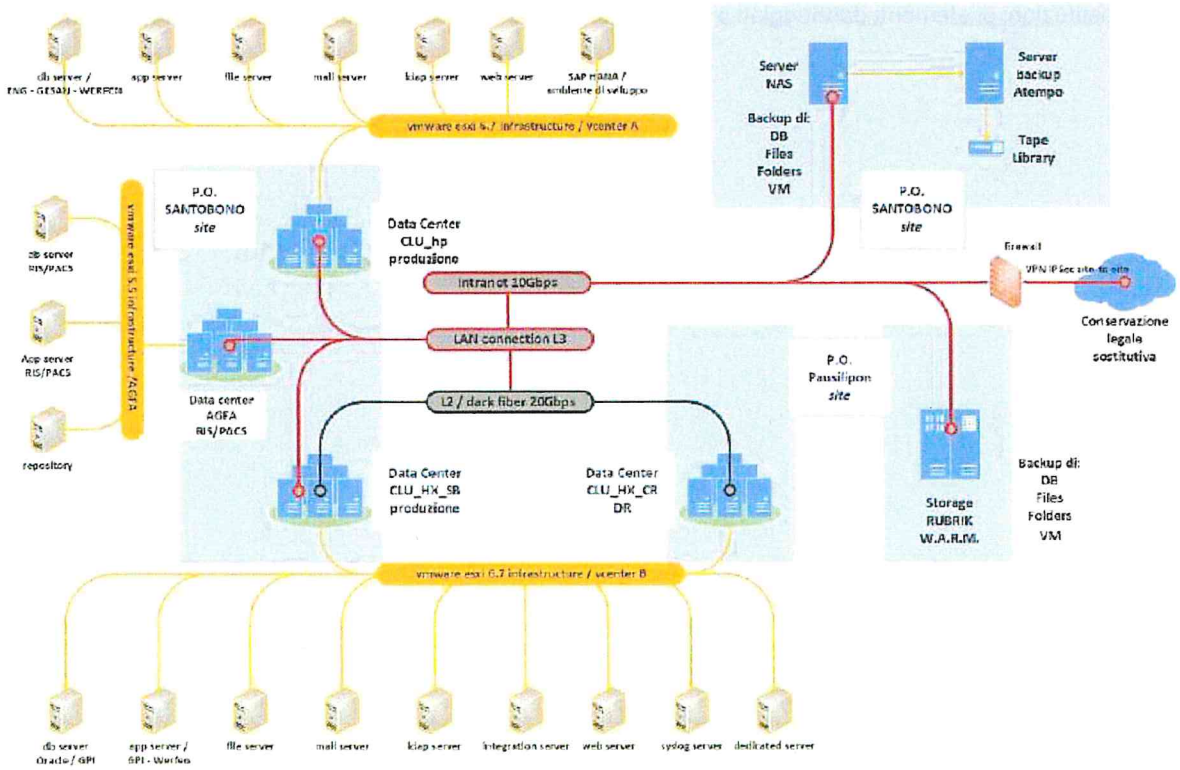
5.1 SPECIFICHE DI PROGETTO

Si precisa che tutte le eventuali attività propedeutiche all'installazione degli apparati sono a carico dell'Amministrazione Contraente (predisposizione delle linee di alimentazione, linee dati, rack, supporti etc...)

Nella seguente tabella vengono sintetizzate le configurazioni previste:

Vendor	Device	Configuration	Note	External Reference
Cisco	*FPR4115*	Basic Setup	Software Upgrade	
			Interfacce di Rete	
			Routing Info	
			High Availability	
			Licensing	
			MGMT VPN	
			VDOMS	
			VRF	
			NAT	
		NGFW Setup	Firewall	
			AntiVirus	
			Application Control	
			IPS	
			VPN IPSec	

Lo schema logico dell'architettura è:



I tempi di consegna della fornitura e relativa documentazione indicati dal vendor sono stimati in 30 giorni lavorativi.

5.2 PIANO DELLE ATTIVITÀ

Di seguito uno schema di GANTT relativo alle attività da svolgere:

(*) Per quanto riguarda le attività di supporto specialistico, saranno previste diverse figure professionali che lavoreranno contemporaneamente nel periodo di tempo indicato ed entro e non oltre il 15/12/2023.

5.3 PIANO DI PRESA IN CARICO

Di seguito si riportano le principali attività:

- predisposizione e configurazione dei servizi proposti;
- creazione dell'account del referente dell'Amministrazione per l'accesso al Portale della Fornitura e configurazione dell'Area Privata;
- acquisizione degli standard, modalità operative, linee guida e metodologie in uso presso l'Amministrazione, ove presenti.

Non sarà possibile stabilire preventivamente le Release software necessarie. Le stesse saranno concordate successivamente con i Referenti Tecnici del cliente

Entro 30 giorni dalla stipula del Contratto esecutivo verrà svolta la prima riunione di lavoro con il referente tecnico del Fornitore ed i referenti tecnici dell'Amministrazione.

A seguito di tale riunione la presa in carico prevederà:

- Appena i dispositivi saranno visibili in rete (post Prima Configurazione), verrà redatto un verbale attestante la conclusione dello stato di installazione dei dispositivi propedeutico alla fatturazione della componente hardware
- Identificare il team di progetto: verrà designato un team di progetto che lavorerà sulla presa in carico del servizio IT e verrà definito un responsabile del progetto.
- Acquisizione di standard e metodologie: Rivedere gli standard, le modalità operative, le linee guida e le metodologie in uso presso l'Amministrazione per integrare le migliori pratiche in uso e conformarsi ai requisiti dell'Amministrazione.
- Test del servizio: il servizio sarà testato con i rappresentanti dell'Amministrazione per valutare l'efficacia dell'implementazione e identificare eventuali problemi o aree di miglioramento.
- Conduzione del servizio IT: la conduzione del servizio avverrà effettuando monitoraggi sulle performance per valutare l'efficacia dell'implementazione, identificando eventuali aree di miglioramento.
- Redazione di verbale per la conclusione delle attività

L'attività di presa in carico dovrà essere completata entro il termine massimo di un mese solare dalla data di stipula del Contratto esecutivo. In caso contrario, l'Amministrazione si riserva il diritto di richiedere l'applicazione della relativa penale prevista nel contratto.

5.4 SPECIFICHE DI COLLAUDO

Il piano dei test previsto per i Firewall sarà composto dai seguenti punti:

- Verifica delle policy applicate
- Test HA
- Report dei risultati: infine, si creerà un report dei risultati dei test, che include un riassunto delle attività, degli obiettivi e dei test case utilizzati. Il report potrà contenere anche eventuali raccomandazioni per migliorare il Firewall o per futuri test.