SAN GIUSEPPE MOSCATI - AVELLINO
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALITÀ

C.da Amoretta 83100 Avellino – P.IVA 01948180649

ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI – ID 2296 – **LOTTO 1**

PIANO DEI FABBISOGNI

INDICE

1. DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione:	Azienda Ospedaliera San Giuseppe Moscati
Indirizzo	Contrada Amoretta
CAP	83100
Comune	Avellino
Provincia	AV
Regione	Campania
Codice Fiscale	01948180649
Codice IPA	ao_sgma
Indirizzo mail	info@aornmoscati.it
PEC	protocollo.generale@pec.aornmoscati.it

Referente Amministrazione	Giuseppe Versace
Ruolo	Direttore U.O.C. Sistemi Informativi
Telefono	0825 203039
Indirizzo mail	sistemi.informativi@aornmoscati.it
PEC	sistemi.informativi@pec.aornmoscati.it

2. CONTESTO

- ***DESCRIZIONE DELL'AMMINISTRAZIONE CONTRAENTE***

L'Azienda Ospedaliera Moscati si avvale di un'infrastruttura digitale complessa attraverso la quale eroga servizi a un'ampia area metropolitana. L'adozione di nuovi paradigmi di costruzione ed erogazione dei servizi digitali (cloud computing, mobile workplace), la crescita costante di attacchi cyber sempre più sofisticati, l'adeguamento del quadro normativo alle nuove esigenze di privacy e protezione delle infrastrutture critiche, rendono necessaria una profonda rivalutazione degli aspetti concettuali, tecnici e organizzativi legati alla cybersicurezza, soprattutto in relazione alla estrema dinamicità e complessità delle sue manifestazioni.

Il progetto interessa i dipendenti dell'Amministrazione per gli aspetti relativi alla formazione e prevede interventi in aree diverse che contribuiscono a comporre una visione organica della cybersicurezza necessaria a garantire la continuità dei servizi digitali e la salvaguardia del patrimonio informativo detenuto dall'Amministrazione.

- ***DESCRIZIONE DEL CONTESTO TECNOLOGICO, APPLICATIVO E PROCEDURALE***

La transizione digitale gioca un ruolo chiave nell'evoluzione dei modelli organizzativi della PA, soprattutto in un contesto come quello odierno che necessita di un'intensa collaborazione tra gli attori della pubblica amministrazione per offrire servizi utili, efficienti e innovativi ai cittadini. La necessità di garantire la collaborazione tra diversi attori istituzionali e la spinta normativa del GDPR che sancisce l'obbligo di attuare le misure tecniche e organizzative per mitigare il rischio connesso ai trattamenti dei dati privati, attribuiscono alla cyber sicurezza un ruolo cruciale per la realizzazione di nuovi servizi digitali.
Le pratiche del lavoro agile e il cloud computing nelle diverse declinazioni adottato dall'Amministrazione, hanno determinato il superamento del tradizionale modello di difesa basato sul presidio di un perimetro aziendale definito entro il quale contenere risorse e utenze aziendali e attraverso il quale relazionarsi al mondo esterno. L'Amministrazione è quindi nella condizione di dover adottare un modello di borderless security focalizzata sulle entità che erogano, abilitano o fruiscono i servizi digitali, sulla verifica delle identità che le qualificano, sul monitoraggio pervasivo di eventi e comportamenti. Il monitoraggio continuo della superfice di attacco e la formazione di cybersicurezza sono aspetti coerenti ed essenziali di questa visione. Con questo progetto, l'AO Moscati si pone pertanto l'obiettivo del potenziamento delle misure di sicurezza in alcune funzioni chiave del suo ecosistema digitale, con l'obiettivo di conseguire un deciso incremento della resilienza cyber anche attraverso l'adozione di buone pratiche da parte degli utenti che saranno oggetto di formazione specifica.

DESCRIZIONE DELL'ESIGENZA

Il presente capitolo ha lo scopo di descrivere le esigenze dell'Azienda Ospedaliera Moscati nell'ambito dei servizi offerti dall'Accordo quadro AQ 2296 – Lotto 1 per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, stipulato da Consip S.p.A. (Consip) e dal Raggruppamento Temporaneo di Imprese (RTI) composto da:

- Accenture S.p.A.
- Fastweb S.p.A.
- Fincantieri NexTech S.p.A.
- Difesa e Analisi Sistemi S.p.A.

L'Amministrazione rileva un forte deficit di competenze e strumenti per la gestione efficace del rischio cyber determinato da minacce sofisticate e in continua evoluzione. La casistica recente degli incidenti relativa ad amministrazioni pubbliche che attuano una gestione della sicurezza digitale analoga a quella dell'Azienda Ospedaliera Moscati, evidenzia la necessità

di dotarsi quanto prima possibile delle competenze e degli strumenti necessari a riportare il rischio cyber a un livello accettabile e compatibile con la missione dell'Amministrazione.

Le criticità rilevate riguardano i seguenti aspetti:

- monitoraggio delle vulnerabilità e delle minacce
- formazione dei dipendenti sulla natura del rischio cyber e addestramento alla sua gestione

Gli interventi previsti indirizzano in maniera diretta le criticità elencate, e si calano in un contesto organizzativo che prevede un deciso potenziamento delle Security Operation con l'obiettivo di conseguire una gestione efficace del rischio cyber in tutti i suoi aspetti.

Il Comune di Napoli si impegna ad effettuare l'opportuna segnalazione al Centro di Valutazione e Certificazione Nazionale (CVCN) qualora i servizi richiesti siano inseriti nel Perimetro di sicurezza nazionale cibernetica.

- ***SINTESI DEI SERVIZI RICHIESTI***

Le richieste del presente Piano dei Fabbisogni riguardano l'erogazione dei seguenti servizi:

-**L1.S1. Servizio SOC Security Operation Center**

Si richiede di implementare, un servizio di monitoraggio e alerting degli eventi/minacce di sicurezza al fine di consentire una gestione degli incidenti di sicurezza dalla fase di identificazione e notifica dell'evento, fino alle azioni di contenimento, ripristino e prevenzione futura in stretta collaborazione tra l'outsourcer e le strutture dell'Amministrazione preposte alla gestione sistemistica. Tra le funzioni richieste ci si aspetta quindi raccolta centralizzata dei log e degli eventi; correlazione tra eventi diversi raccolti; disponibilità di un cruscotto (dashboard) che fornisca agli analisti, in tempo reale, una rappresentazione della situazione in essere; capacità di identificazione, gestione, mitigazione e risoluzione degli attacchi; produzione di report periodici di sintesi, di incident report di dettaglio ed istruzioni operative. Si richiede, infine, di ricevere ed analizzare la reportistica e i log dando anche la giusta priorità ai processi di risoluzione e/o mitigazione delle minacce.

-**L1.S9. Formazione e Security Awareness**

Si richiede di implementare un servizio che mira a sensibilizzare l'Amministrazione sui vari aspetti della sicurezza delle informazioni, aumentando il livello di consapevolezza dei dipendenti e quindi elevando il livello di sicurezza del Comune di Napoli. L'obiettivo è sviluppare negli utenti le competenze, le tecniche ed i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza.

-**L1.S15. Servizi Specialistici**

Si richiede di prevedere un'adeguata quantità di giornate di servizi specialistici e team di cybersecurity per dare supporto, gestire, trattare o comunque coprire quanto già dettagliato nei precedenti servizi e nei paragrafi di descrizione del contesto di interesse.

Tali servizi sono riassunti nella seguente tabella che descrive le numerosità richieste per la loro erogazione. Si richiede, altresì che il piano di lavoro abbia una durata complessiva di 24 mesi.

L1.S1 – SECURITY OPERATION CENTER								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S1	Security Operation Center	As a service (Device equivalenti)	A canone (annuale)	Fino a 300 Eps				
				Fino a 600 Eps				
				Fino a 1.200 Eps				
				Fino a 6.000 Eps	250	250		
				> 6.000 Eps				

L1.S2 – NEXT GENERATION FIREWALL								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S2	Next Generation Firewall	As a service	A canone (annuale)	Fino a 250 Mbps				
				Fino a 2 Gbps				
				Fino a 4 Gbps				
				Fino a 7 Gbps				
				Fino a 15 Gbps				
				> 15 Gbps				

L1.S3 – WEB APPLICATION FIREWALL								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S3	Web Application Firewall	As a service	A canone (annuale)	Fino a 500 Mbps				
				Fino a 5 Gbps				
				> 5 Gbps				

L1.S4 – GESTIONE CONTINUA DELLE VULNERABILITÀ								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S4	Gestione continua delle vulnerabilità	As a service	A canone (canone annuale per indirizzo IP)	Fino a 50 IP				
				Fino a 200 IP				
				> 200 IP				
L1.S5 – THREAT INTELLIGENCE & VULNERABILITY DATA FEED								

Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno
L1.S5	Threat intelligence & Vulnerability data feed	As a service	A canone (canone annuale per datafeed)	Fino a 10 datafeed				
				Fino a 50 datafeed				
				> 50 datafeed				

L1.S6 – PROTEZIONE NAV. INTERNET E POSTA ELETTRONICA								
Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno
L1.S6	Protezione navigazione internet e posta elettronica	As a service	A canone (canone annuale per utente)	Fino a 1.000 utenti				
				Fino a 5.000 utenti				
				Fino a 10.000 utenti				
				Fino a 20.000 utenti				
				> 20.000 utenti				

L1.S7 – PROTEZIONE END POINT								
Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno
L1.S7	Protezione End Point	As a service	A canone (canone annuale per numero di nodi)	Fino a 500 nodi				
				Fino a 1.000 nodi				
				Fino a 5.000 nodi				
				> 5.000 nodi				

L1.S8 – CERTIFICATI SSL								
Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno
L1.S8	Certificati SSL	As a service	A corpo (costo per certificato)	SSL OV				
				SSL OV Wildcard				
				SSL EV				
				SSL DV				
				SSL Code signing				
				SSL Client Auth				

L1.S9 – FORMAZIONE E SECURITY AWARENESS

Codice	Descrizione	Tipologia d'erogazione	Valutazione economica	Fasce	Q.tà I Anno	Q.tà II Anno	Q.tà III Anno	Q.tà IV Anno
L1.S9	Formazione e Security Awareness	A task	A corpo	gg/p Team ottimale	155	155		

L1.S10 – GESTIONE IDENTITÀ E ACCESSO UTENTE								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S10	Gestione identità e accesso utente	As a service	A canone (canone annuale per utente)	Fino a 10.000 utenti				
				Fino a 100.000 utenti				
				Fino a 500.000 utenti				
				> 500.000 utenti				

L1.S11 – FIRMA DIGITALE REMOTA								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S11	Firma digitale remota	As a service	A canone (canone annuale per utente)	50 e fino a 200 utenti				
				200 e fino a 500 utenti				
				500 e fino a 1.000 utenti				
				> 1.000 utenti				
				Garantita - N. 1 firma				
				Garantita - N. 5 firme aggiuntive				

L1.S12 – SIGILLO ELETTRONICO								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S12	Sigillo elettronico	As a service	A canone (canone annuale per numero di firma)	Garantita - N. 1 firma				
				Garantita - N. 5 firme aggiuntive				

L1.S13 – TIMBRO ELETTRONICO								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S13	Timbro elettronico	As a service		Fino a 1.000 timbrature				

			A consumo (costo per timbratura)	Fino a 10.000 timbrature				
				Fino a 100.000 timbrature				
				Fino a 1.000.000 timbrature				
				Fino a 10.000.000 timbrature				
				> 10.000.000 timbrature				

L1.S14 – VALIDAZIONE TEMPORALE ELETTRONICA QUALIFICATA								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S14	Validazione temporale elettronica qualificata	As a service	A canone (canone annuale per marca)	Fino a 1.000 Marcature				
				Fino a 10.000 Marcature				
				Fino a 100.000 Marcature				
				Fino a 1.000.000 Marcature				
				Fino a 10.000.000 Marcature				
				> 10.000.000 Marcature				
				Garantita - N. 1 marcatura				
				Garantita - N. 1 marcatura aggiuntiva				

L1.S15 – SERVIZI SPECIALISTICI								
Codice	**Descrizione**	**Tipologia d'erogazione**	**Valutazione economica**	**Fasce**	**Q.tà I Anno**	**Q.tà II Anno**	**Q.tà III Anno**	**Q.tà IV Anno**
L1.S15	Servizi specialistici	A task	A corpo	gg/p Team ottimale	100	80		

- ***LUOGO DI EROGAZIONE***

In base alla modalità di esecuzione dei servizi le prestazioni contrattuali dovranno essere svolte come di seguito indicato:

- per i servizi erogati *da remoto*: presso i Centri Servizi del Fornitore;
- per i servizi on-site: presso le sedi.

INDICATORE DI PROGRESSO

Per ogni classe di controlli ABSC (Agid Basic Security Control) previsti dalle misure minime di sicurezza AGID, ove successivamente modificate ed integrate, sarà calcolato il valore del relativo Indicatore di Progresso (Ip) dell'intervento ottenuto attraverso la realizzazione dell'Ordinativo di Fornitura (acquisto di servizi previsti nell'Ordinativo), che sarà determinato come da schema seguente:

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

Il Direttore U.O.C. Sistemi Informativi
Dott. Giuseppe Versace