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

NOTA BENE:

Durante l'esecuzione contrattuale è possibile che il progresso tecnologico innovi i servizi di base con l'introduzione di nuove funzionalità e/o nuovi servizi in ogni caso complementari/supplementari ai servizi previsti in gara mediante procedura negoziata ai sensi dell'art. 63 co. 3 lett b), d.lgs. n. 50/2016 oppure mediante una modifica ai sensi dell'art. 106 co.1 lett. b) d.lgs. n. 50/2016.

L'organismo tecnico di Coordinamento e Controllo, raccolta la necessità di introduzione di un nuovo servizio, esclusivamente se lo stesso risulta nella disponibilità dell'aggiudicatario dell'Accordo Quadro, richiederà allo stesso, sulla base di un apposito documento di "specifiche tecniche" (con annessi i requisiti da garantire), la quotazione di un servizio da inserire nei servizi oggetto di fornitura. Tale nuovo servizio sarà dunque inserito in perimetro tra i servizi acquistabili.

INDICE

1. DATI ANAGRAFICI DELL'AMMINISTRAZIONE

Ragione sociale Amministrazione:	Azienda Regionale della Salute della Sardegna (ARES)
Indirizzo	Via Piero della Francesca 1 – 09047 Selargius (CA)
CAP	09047
Comune	Selargius
Provincia	CA
Regione	Sardegna
Codice Fiscale	03990570925
Codice IPA	03990570925
Indirizzo mail	segreteria.direzionegenerale@aressardegna.it
PEC	protocollo@pec.aressardegna.it

Referente Amministrazione	Ing. Marco Galisai
Ruolo	SC Infrastrutture e Rete Dati
Telefono	+39 338 6570799
Indirizzo mail	marco.galisai@aressardegna.it
PEC	Ict.infrastrutture@pec.aressardegna.it

2. CONTESTO

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

ARES (Azienda Regionale della Salute della Sardegna) opera con l'obiettivo di supportare le altre Aziende sanitarie regionali nella produzione di servizi sanitari e socio-sanitari. In particolare, la Regione si avvale di ARES per la realizzazione delle attività di sanità digitale con lo scopo di garantire una evoluzione delle prestazioni sanitarie, l'integrazione tra le reti sanitarie, promuovere nuove modalità di diagnosi e cura e riqualificare la spesa, contenendo e gestendo i rischi derivanti dalle attività precipue di ARES (pazienti, operatori, continuità dei servizi e sanzioni).

- ***DESCRIZIONE DEI FONDI***

Per questo progetto ARES Sardegna ha intenzione di utilizzare i fondi disponibili qui di seguito descritti:

- Fondi a bilancio di ARES Sardegna: durata 48 mesi
- Fondi del finanziamento ottenuto in relazione all'Avviso 8 di ACN (Agenzia per la Cybersicurezza Nazionale) per AREUS relativi ad attività da completare entro dicembre 2025
- Fondi di finanziamento ottenuto in relazione alla Misura 55 di ACN relativi ad attività da completare entro dicembre 2026.

Si chiede all'RTI di tenere conto dei vincoli imposti dai finanziamenti su elencati nella redazione del PO e nella pianificazione delle attività, al fine di garantire un'esecuzione e conseguente consuntivazione in linea con i tempi dichiarati per l'ottenimento dei fondi di cui sopra.

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

ARES Sardegna si configura come Azienda Sanitaria che ha il compito di gestire le piattaforme tecnologiche di tutti gli enti sanitari regionali.

In particolare, ARES la responsabilità diretta/indiretta di gestione, controllo e monitoraggio di:

- Sistemi Informativi sanitari e amministrativi
- Infrastruttura rete dati
- Data Center e Cloud
- Sistemi Medicali IoMT
- Dispositivi IoT/OT connessi in rete dati

per tutti gli enti sanitari regionali inclusa AREUS (Azienda Regionale dell'Emergenza e Urgenza della Sardegna) che eroga il servizio 112 e che ha una serie di peculiarità e vincoli rispetto agli altri enti.

Sono stati individuati **5 obiettivi strategici** che ARES, intende perseguire usufruendo di convenzioni apposite, come la presente e mantenendo relazioni con partner tecnologici che aiuteranno l'Amministrazione nella messa a terra delle iniziative:

1. **Proteggere** i dati dei pazienti, degli operatori nonché i dati aziendali
2. **Assicurare** la **continuità** dei servizi sanitari, tecnici e amministrativi
3. **Rafforzare** la **«safety»** ed assicurare la sicurezza dei sistemi critici
4. **Offrire servizi sicuri** per la constituency
5. **Rafforzare** la **conformità a leggi** e regolamenti di sicurezza

Il Dipartimento Sanità Digitale e Innovazione Tecnologica di ARES attraverso le proprie strutture, assicura la gestione delle tecnologie biomediche, delle infrastrutture tecnologiche e dei sistemi di sanità digitale di tutte le Aziende del Servizio Sanitario Regionale in termini di efficienza, efficacia e sicurezza. In linea con la strategia della Sanità Digitale a livello nazionale, ARES Sardegna ha l'obiettivo di mettere a disposizione di tutte le aziende sia i sistemi di gestione dei **Dossier Sanitari Elettronici** che i singoli verticali offrendoli in modalità SaaS a tutti gli enti sanitari del territorio e garantire l'alimentazione del **Fascicolo Sanitario Elettronico** della Regione Sardegna.

L'ecosistema *Sanità* si costruisce su un numero di attori così elevato che la protezione delle organizzazioni sanitarie dai cyberattacchi richiede necessariamente una visione end-to-end degli obiettivi di alto valore in tutto l'ecosistema.

Per affrontare e comprendere al meglio il perimetro di intervento delle iniziative di sicurezza, sono state eseguite delle attività finalizzate alla comprensione dello stato attuale degli enti sanitari e di AREUS.

Le informazioni ottenute, tramite interviste a analisi documentale, hanno permesso di comprendere la numerosità di dispositivi presenti all'interno degli enti. La tabella seguente presenta i risultati dell'analisi e riporta la numerosità dei device per tipologia.

Ente	ICT				Ing. Clinica	IoT/OT	Posti letto
	PdL	Server	Network	Stampanti	IoMT		
ASL 1 Sassari	1800	150	250	740	2200	120	352
ASL 2 Gallura	1400	100	200	450	2230	80	391
ASL 3 Nuoro	1400	120	200	450	1500	80	420
ASL 4 Ogliastra	600	80	70	270	460	50	117
ASL 5 Oristano	1400	80	200	425	1850	80	400
ASL 6 Medio Campidano	800	80	100	220	830	50	186
ASL 7 Sulcis	1300	80	200	480	1350	60	287
ASL 8 Cagliari	3000	150	300	1010	3030	150	505
ARNAS Brotzu + Businco	2200	150	250	450	3850	100	770
AOU CA Policlinico Monserrato	1200	100	150	300	2330	60	466
AOU SS Santissima Annunziata	2700	450	350	450	5330	150	1065
AREUS (2 sedi)	400	50	80	80	300	20	-
ARES	500	30	50	110	-	15	-
TOTALI	18500	1620	2400	5435	25260	1015	4959

Per ciò che concerne l'indicazione del patrimonio installato dei medical device (Ing. Clinica - IoMT) si specifica che il dato indicato in tabella individua il numero massimo degli asset tecnologici che compongono i vari sistemi medicali connessi in rete (Es. un ecotomografo è composto mediamente da 6 asset, un'apparecchiatura radiologica è composta da circa 10 asset e così via). Pertanto, i sistemi medicali connessi in rete e da monitorare sono in misura relativamente inferiore agli asset indicati.

L'analisi eseguita ha permesso inoltre di definire le iniziative di sicurezza da coordinare, tenendo conto della successiva definizione degli Enti prioritari da cui partire tra quelli in perimetro:

- ✓ ARES
- ✓ AREUS
- ✓ N.8 AASSLL
- ✓ Azienda Ospedaliera Universitaria di Cagliari
- ✓ Azienda Ospedaliera Universitaria di Sassari

- ✓ ARNAS Brotzu

L'analisi sulla postura di sicurezza, condotta nei mesi precedenti al presente Piano dei Fabbisogni, è stata effettuata sulla base del *Framework Nazionale di Cyber Security,* in cui sono state analizzate e valutate le categorie e le funzioni in esso previste. E' stata eseguita una valutazione qualitativa del livello di maturità attuale rispetto al valore futuro ottenibile a valle della realizzazione delle iniziative di security pianificate:

Categoria	Funzione	AS-IS	TO-BE
Identify	Asset Management	Bassa	Alta
Identify	Business Environment	Bassa	Bassa
Identify	Governance	Bassa	Media
Identify	Risk Assessment	Bassa	Media
Identify	Risk Management Strategy	Bassa	Bassa
Identify	Supply Chain Risk Management	Bassa	Media
Protect	Identity Management and Access Control	Bassa	Media
Protect	Awareness and Training	Bassa	Media
Protect	Data Security	Bassa	Media
Protect	Information Protection Processes and Procedures	Bassa	Media
Protect	Maintenance	Bassa	Bassa
Protect	Protective Technology	Media	Alta
Detect	Anomalies and Events	Bassa	Alta
Detect	Security Continuous Monitoring	Bassa	Alta
Detect	Detection Processes	Bassa	Alta
Respond	Response Planning	Bassa	Alta
Respond	Communications	Bassa	Alta
Respond	Analysis	Bassa	Alta
Respond	Mitigation	Bassa	Alta
Respond	Improvements	Bassa	Alta
Recover	Recovery Planning	Bassa	Bassa
Recover	Improvements	Bassa	Bassa
Recover	Communications	Bassa	Bassa

▪ DESCRIZIONE DELL'ESIGENZA

Negli ultimi anni la minaccia cibernetica è notevolmente cresciuta in quantità e qualità e le tipologie di attacchi con finalità estorsive hanno trovato nuove e più invasive forme. ARES, come ogni Ente di medio-grandi dimensioni, si trova a fronteggiare ogni giorno decine di migliaia di attacchi informatici, per lo più automatici, ma talora anche mirati e preparati con competenza e risorse dedicate. Il contesto sanitario territoriale della Sardegna, delle aziende sanitarie ospedaliere, delle ASL e di AREUS che si avvalgono di ARES, richiede una gestione della sicurezza applicata non solo al contesto IT, ma anche a quello dei dispositivi medici e dei sistemi medicali, al fine di garantire la sicurezza informatica dell'Amministrazione e degli altri enti del SSR mediante la prevenzione e la gestione delle minacce, ed un governo efficace ed efficiente dei rischi di sicurezza.

Vista la criticità dei servizi gestiti da AREUS, è fondamentale procedere per questo ente in maniera prioritaria e con interventi specifici, volti a migliorare la postura di sicurezza, censire e proteggere in maniera continuativa gli asset IT e

IoMT critici (ad es. gli asset presenti a bordo delle ambulanze), garantirne il corretto funzionamento e la protezione dei dati trasmessi, oltre che incrementare il livello di sicurezza delle Centrali Operative e dei sistemi ad esse legati. Inoltre è necessario adottare misure di sicurezza rigorose e che tengano in considerazioni gli standard militari al fine della protezione delle infrastrutture critiche e dei dati sensibili gestiti da AREUS.

Il presente capitolo ha lo scopo di descrivere le esigenze di ARES 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 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 che saranno esplicitati nei paragrafi successivi:

L1.S1 - Security Operation Center (SOC)

L1.S2 - Next Generation Firewall

L1.S3 - Web Application Firewall

L1.S4 - Gestione Continua delle Vulnerabilità di Sicurezza

L1.S5 - Threat Intelligence & Vulnerability Data Feed

L1.S9 - Formazione e Security Awareness

L1.S15 - Servizi Specialistici

ID	Linea di Servizio AQ2296 Lotto1	Obiettivi	Organizzazioni Target
L1.S1 SOC	L1.S1 Security Operation Center (SOC) Servizio di monitoraggio continuativo degli eventi attraverso uno scambio informativo bidirezionale con i servizi L1.S2, L1.S3, L1.S4, L1.S5, L1.S7 al fine di individuare nel minor tempo possibile gli attacchi ai danni dell'Integrità, Confidenzialità e/o Disponibilità del patrimonio informativo ed attivare la risposta in maniera tempestiva.	Proteggere i dati dei pazienti Assicurare la continuità dei servizi clinici e sanitari Rafforzare la «safety» ed assicurare la sicurezza dei sistemi critici Rafforzare la conformità a leggi e regolamenti di sicurezza	ARES; AREUS; n. 8 ASL Regione Sardegna; AOU Cagliari; AOU Sassari; ARNAS Brotzu

ID	Linea di Servizio AQ2296 Lotto1	Obiettivi	Organizzazioni Target
L1.S2 NGFW	L1.S2 - Next Generation Firewall – servizio che consente di implementare i controlli di sicurezza essenziali alla protezione di rete, applicando restrizioni alle comunicazioni esterne o interne, limitando gli accessi delle singole risorse ai soli flussi di traffico definiti come leciti.	Proteggere i dati dei pazienti Assicurare la continuità dei servizi clinici e sanitari Rafforzare la «safety» ed assicurare la sicurezza dei sistemi critici	ARES; AREUS; n. 8 ASL Regione Sardegna; AOU Sassari;
L1.S3 WAF	L1.S3 - Web Application Firewall – servizio finalizzato alla protezione degli Enti in perimetro, da attacchi veicolati ai dati delle applicazioni web, agendo da filtro del traffico di rete dello strato applicativo.	Proteggere i dati dei pazienti Assicurare la continuità dei servizi clinici e sanitari Rafforzare la «safety» ed assicurare la sicurezza dei sistemi critici	ARES; AREUS; n. 8 ASL Regione Sardegna; AOU Cagliari; AOU Sassari; ARNAS Brotzu
L1.S4 VM	L1.S4 - Gestione continua delle vulnerabilità di sicurezza (Vulnerability Management) – il servizio ha lo scopo di rilevare, monitorare e ridurre la superfice d'attacco esposta dell'Amministrazione	Proteggere i dati dei pazienti Assicurare la continuità dei servizi clinici e sanitari Rafforzare la «safety» ed assicurare la sicurezza dei sistemi critici Rafforzare la conformità a leggi e regolamenti di sicurezza	ARES; AREUS; n. 8 ASL Regione Sardegna; AOU Cagliari; AOU Sassari; ARNAS Brotzu
L1.S5 TI	L1.S5 - Threat Intelligence & Vulnerability Data Feed - la piattaforma fornisce informative complete e continuative (feed) relative alle minacce e vulnerabilità di sicurezza, specificamente adattate alle Pubbliche Amministrazioni, grazie alla possibilità di utilizzare un'ampia quantità di fonti informative OSINT (Open Source Intelligence ad accesso libero) e CLOSINT (Closed Source Intelligence non liberamente disponibili).	Proteggere i dati dei pazienti Assicurare la continuità dei servizi clinici e sanitari Rafforzare la «safety» ed assicurare la sicurezza dei sistemi critici Rafforzare la conformità a leggi e regolamenti di sicurezza	ARES; AREUS; n. 8 ASL Regione Sardegna; AOU Cagliari; AOU Sassari; ARNAS Brotzu
L1.S9 Formazione	L1.S9 - Formazione e Security Awareness – il servizio ha lo scopo di sviluppare negli utenti le competenze essenziali, le tecniche e i metodi fondamentali per prevenire il più possibile gli incidenti di sicurezza e reagire al meglio a fronte di eventuali problemi.	Proteggere i dati dei pazienti Assicurare la continuità dei servizi clinici e sanitari Rafforzare la «safety» ed assicurare la sicurezza dei sistemi critici Rafforzare la conformità a leggi e regolamenti di sicurezza	ARES; AREUS; n. 8 ASL Regione Sardegna; AOU Cagliari; AOU Sassari; ARNAS Brotzu
L1.S15 Servizi Specialistici	L1.S15 - Servizi Specialistici – tali servizi sono stati pensati per supportare l'operatività delle single linee di servizio e per fornire agli Enti in perimetro un approccio alla strategia di Sicurezza completa ed integrato.	Proteggere i dati dei pazienti Assicurare la continuità dei servizi clinici e sanitari Rafforzare la «safety» ed assicurare la sicurezza dei sistemi critici Offrire servizi in cloud sicuri per la constituency Rafforzare la conformità a leggi e regolamenti di sicurezza	ARES; AREUS; n. 8 ASL Regione Sardegna; AOU Cagliari; AOU Sassari; ARNAS Brotzu

Servizio SOC

La raccolta ed il monitoraggio degli eventi di sicurezza è una delle attività principali per avere sotto controllo lo stato di salute delle infrastrutture dell'Amministrazione. Nello specifico, il servizio sarà declinato su due aree: quella prettamente ICT (Pdl, server, device IT) quella IoT/OT e quella IoMT relativa ai dispositivi medici. Fatto salvo quanto esplicitato nel precedente paragrafo, per i dispositivi medici sono stati individuati 5000 asset a criticità elevata, che saranno oggetto di monitoraggio. Analogamente i device ICT considerati critici sono stimati in 4000 (di cui 1500 switch e 2500 stampanti) e i sistemi IoT critici (esclusi i Medical Device) sono stimati nel numero di 600.

Gli Enti che beneficeranno del servizio sono: ARES, AREUS, le 8 AASSLL e le 3 Aziende Ospedaliere presenti sul territorio.

In particolare, si richiede un servizio SOC gestito H24 in grado di segnalare tempestivamente vulnerabilità e attacchi informatici, integrato con le applicazioni/piattaforme presenti nell'Amministrazione per il blocco degli attacchi. L'obiettivo è quello di avere un sistema ed 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 raccomandazioni relative alle azioni di contenimento e ripristino e prevenzione futura.

Inoltre, per consentire un monitoraggio a 360 gradi degli asset tecnologici di competenza di ARES, si richiede che il servizio SOC includa nel perimetro anche gli asset IoMT in modo da garantire adeguate misure di prevenzione e monitoraggio nel parco delle tecnologie biomediche di pertinenza ingegneria clinica.

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 48 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				
				> 6.000 Eps	45.836	45.836	45.836	45.836

Next Generation Firewall

In ambito sicurezza perimetrale, il servizio relativo ai Next Generation Firewall consente all'Amministrazione di filtrare tutto il traffico che i dispositivi di rete scambiano sia internamente che esternamente rispetto a un determinato perimetro, limitando o bloccando eventi quali accessi non autorizzati, malware o servizi non consentiti.

L'Amministrazione richiede n. 10 cluster di Firewall con una banda fino a 15 Gbps, configurati in alta affidabilità, a protezione delle 8 ASL, dell'Azienda Ospedaliera di Sassari, AREUS e ARES.

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 48 mesi.

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	20	20	20	20
				> 15 Gbps				

Web Application Firewall

L'eterogeneità e la numerosità delle applicazioni in capo ad ARES, rende necessario un servizio a protezione dei dati e delle applicazioni attraverso una soluzione di Web Application Firewall (WAF) a protezione degli enti in perimetro. Si richiede quindi una dotazione di 1 cluster in alta affidabilità (i.e. 2 web application firewall), a servizio di tutti gli enti inclusi nel perimetro, con una banda fino a 5 Gbps.

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 48 mesi.

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	2	2	2	2
				> 5 Gbps				

Gestione Continua delle Vulnerabilità di Sicurezza

La gestione dell'intero ciclo di vita delle vulnerabilità presuppone una vista ed un controllo completo degli asset da monitorare, per questo si rende necessaria l'implementazione di un servizio di asset intelligence ed asset management che sia in grado di censire, classificare e manutenere, attraverso strumenti automatici, gli asset IT e medicali dell'Amministrazione. Unitamente a tale servizio si richiede di implementare, attraverso adeguati strumenti tecnologici, un servizio che consenta all'Amministrazione - tramite un processo automatico di assessment delle vulnerabilità - di ottenere una fotografia precisa del livello e gravità del rischio a cui, in quel momento, sono esposti i sistemi informatici oggetto del servizio.

Il servizio dovrà essere implementato secondo le caratteristiche definite per ciascun Ente Sanitario e in accordo con i referenti di ARES. Si prevede un volume di circa 29.500 device/IP.

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 48 mesi.

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	29574	29574	29574	29574

Threat Intelligence & Vulnerability Data Feed

Il servizio richiesto dovrà consentire di ricevere un flusso continuo o, almeno, periodico a scadenze concordate di informazioni relative a minacce e vulnerabilità di sicurezza del sistema informativo di ARES o che coinvolga in qualche modo asset, account e/o credenziali afferenti a tutti gli Enti in perimetro. Devono essere disponibili le informazioni più recenti, permettendo così di prevedere/prevenire le minacce prima che entrino in azione migliorando gli attuali controlli e le funzionalità di protezione già presenti.

Tali servizi sono riassunti nella seguente tabella che descrive le numerosità richieste per la loro erogazione (71 feed). Si richiede che il piano di lavoro abbia una durata complessiva di 48 mesi.

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	71	71	71	71

Formazione e Security Awareness

Parallelamente alle iniziative di carattere più tecnologico, ARES intende avviare una serie di attività strutturate, per accrescere la consapevolezza sulla sicurezza informatica e sui rischi che ARES affronta nel quotidiano. Nello specifico si richiedono iniziative di security awareness e formazione per i dipendenti di ARES e dei 12 Enti afferenti, per accrescerne le competenze, tramite l'esecuzione di:

1. Formazione specifica per le strutture tecniche degli enti: due sessioni formative per personale tecnico IT (per 15 discenti a sessione per AREUS, AOU Sassari, AOU Cagliari e AO Brotzu e 150 discenti per ARES) aventi oggetto tematiche di cyber Security da concordare con le Amministrazioni e da erogare nel primo anno di vita contrattuale;
2. Formazione per la popolazione aziendale: attività formativa annuale (per un totale di 4 anni) per accrescere la consapevolezza degli utenti/dipendenti di ARES e dei 12 Enti in perimetro (circa 11.000 utenti).
3. Formazione per il top management: attività formativa annuale (per un totale di 4 anni) specifica per Top Management (circa 8 discenti ad Ente), finalizzata al miglioramento della cultura della sicurezza informatica e con lo scopo di fornire ai dirigenti le conoscenze necessarie per comprendere i rischi informatici, valutare le minacce e adottare le misure di sicurezza più efficaci.

L'attività di awareness deve essere eseguita con periodicità annuale tramite la fornitura di sessioni formative specifiche per la tipologia di audience erogate in aula e tramite webinar.

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 48 mesi.

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	1754	1506	1647	1647

Servizi Specialistici

A completamento delle linee di servizio sopra citate, si richiedono dei servizi specialistici al fine di completare l'offerta dei servizi standard, in considerazione delle esigenze specifiche e peculiari di questa Amministrazione.

Qui di seguito l'elenco delle attività da includere nei servizi specialistici richiesti:

L1.S1 - SOC

- Esecuzione incontri e interviste con i referenti dei dodici enti al fine di raccogliere le informazioni necessarie all'avvio del servizio, supportare il cliente per le attività necessarie alla predisposizione e configurazione dei propri apparati per l'integrazione con le tecnologie a supporto dei servizi previsti
- Attività di supporto specialistico erogata come presidio On Site dedicato alle strutture dell'organizzazione, garantendo una protezione avanzata e personalizzata delle infrastrutture IT;

L1.S2 - NGFW

- Attività a supporto del servizio NGFW per la progettazione di un servizio di accesso sicuro in MFA per gli utenti. Attività di monitoraggio e supporto per la protezione basata su DNS, al fine di bloccare gli accessi a siti malevoli.

L1.S3 – WAF

- Attività a supporto del servizio WAF finalizzate alla messa in esercizio degli apparati

L1.S4 - Gestione continua delle vulnerabilità

- Supporto per la messa in esercizio di una piattaforma di vulnerability management evoluta che consenta la gestione della sicurezza degli asset ed il relativo ciclo di vita;
- Assessment per rilevazione delle informazioni propedeutiche all'implementazione del SOC IT e degli apparati elettromedicali;
- Supporto alle attività di analisi delle vulnerabilità che emergono durante l'erogazione dei servizi e mitigazione degli impatti relativi agli applicativi coinvolti;
- Supporto per la redazione dei piani di remediation a seguito rilevazione delle vulnerabilità;

L1.S5 – Threat Intelligence

- Servizi aggiuntivi di Threat Intelligence avanzata a supporto del governo e del monitoraggio delle terze parti e delle risorse esposte degli Enti in perimetro.

L1.S15 - Ulteriori attività

- Supporto nella revisione dell'impianto documentale di sicurezza che viene impattato dalla messa in esercizio dei servizi gestiti (procedure di gestione degli incidenti, patch management, asset management, ecc., ecc.);
- Attività di project management e program management; generazione dei report personalizzati rispetto ai report e relazioni standard forniti dai servizi a Catalogo (output).

Inoltre, si richiede di prevedere un'adeguata quantità di ore per ingaggiare specialistici di cybersecurity per dare supporto, gestire, configurare su indicazioni di ARES quanto già dettagliato nei paragrafi precedenti relativi ai vari servizi per renderli allineati alle esigenze di sicurezza e controllo.

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 48 mesi.

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	11921,0	6513,0	5472,0	5472,0

I servizi specialistici dovranno essere così ripartiti:

Codice servizio collegato	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 SOC	On-boarding Enti e integrazione con infrastrutture Enti	A task	A corpo	gg/p Team ottimale	4550,0	1640,0	1640,0	1640,0
L1.S1 SOC	EPP con Sophos	A task	A corpo		2440,0	2000,0	2000,0	2000,0
L1.S2 NGFW	SetUp NGFW e Integrazione con infrastrutture Enti	A task	A corpo	gg/p Team ottimale	74,0			
L1.S2 NGFW	Secure Access	A task	A corpo	gg/p Team ottimale	1350,0	418,0	418,0	418,0
L1.S2 NGFW	Protezione DNS	A task	A corpo	gg/p Team ottimale	0,0	1041,0	0,0	0,0
L1.S3 WAF	SetUp WAF	A task	A corpo	gg/p Team ottimale	200,0	100,0	100,0	100,0
L1.S4 VM	Progetto Asset Intelligence	A task	A corpo	gg/p Team ottimale	1967,0			
L1.S5	TI moduli aggiuntivi	A task	A corpo		467,0	441,0	441,0	441,0
L1.S15 SS	Servizi di Governance e PMO	A task	A corpo	gg/p Team ottimale	873,0	873,0	873,0	873,0

Mappatura tra servizi e fonti di budget da utilizzare

Qui di seguito è raffigurata la mappatura dei fondi disponibili, come indicato nella sezione 2. Contesto, rispetto ai servizi richiesti da questo Piano dei Fabbisogni e considerando anche la loro distribuzione negli anni.

Lotto	Servizio	2025				2026				2027				2028			
		Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex (NEW)	Misura 55 ACN Opex (NEW)	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex
Lotto 1	Security Operation Center (SOC)		x	-	x	x			x	x				x			
Lotto 1	Next Generation Firewall (NGFW)		x	-	x	x			x	x				x			
Lotto 1	Web Application Firewall (WAF)		x	-	x	x			x	x				x			
Lotto 1	Gestione continua delle vulnerabilità di sicurezza (Vulnerability Management)		x	-	x	x			x	x				x			
Lotto 1	Threat Intelligence & Vulnerability Data Feed (TI)		x	-	x	-			x	x				x			
Lotto 1	Formazione e Security Awareness		x	x	x	x			-	x				x			
Lotto 1	Servizi specialistici per SOC			x	x	x		x		x				x			
Lotto 1	Servizi specialistici per NGFW			x	-	x		x		x				x			
Lotto 1	Servizi specialistici per WAF			x	-	x		x		x				x			
Lotto 1	Servizi specialistici per VM			x	-	-		-		-				-			
Lotto 1	Servizi specialistici per TI			-	-	x				x				x			
Lotto 1	Servizi specialistici di Governance e PMO			-	x	x			x	x				x			

- ***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 dell'Amministrazione ove specificato dall'Amministrazione stessa; in alternativa presso la Sede del Fornitore.

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		

GALISAI MARCO
Firmato digitalmente da GALISAI MARCO
Data: 2024.12.16 17:23:23 +01'00'