Identificativo: Piano dei Fabbisogni v2 dic24

Data: Dicembre 2024

ACCORDO QUADRO PER L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

LOTTO 2 – SERVIZI DI COMPLIANCE E CONTROLLO

PUBBLICHE AMMINISTRAZIONI LOCALI

Piano dei fabbisogni

ARES - Azienda regionale della salute

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Consulting S.r.l. SB

EY Advisory S.p.A.

Teleco S.r.l.

Deloitte. EY teleco

1 INTRODUZIONE

1.1 Ambito

Nel Settembre 2021 CONSIP ha bandito una procedura aperta, suddivisa in due lotti, per "l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni – ID 2296". Il Lotto 2, inerente ai servizi di compliance e controllo, è stato assegnato come primo aggiudicatario al Raggruppamento Temporaneo di Imprese (RTI), la cui mandataria è Deloitte Consulting S.r.l. SB e le società mandanti sono EY Advisory S.p.A. e Teleco S.r.l., per la stipula di contratti esecutivi con le Pubbliche Amministrazioni Locali (PAL).

La durata dell'Accordo Quadro è di 24 mesi, decorrenti dalla data di attivazione. Per durata dell'Accordo Quadro si intende il periodo entro il quale le Amministrazioni potranno affidare, a seguito della approvazione del Piano Operativo, contratti esecutivi agli operatori economici aggiudicatari parti dell'Accordo Quadro per l'approvvigionamento dei servizi oggetto dell'Accordo Quadro. Ciascun Contratto esecutivo avrà una durata massima di 48 mesi decorrenti dalla relativa data di conclusione delle attività di presa in carico.

Il presente documento costituisce il "Piano dei fabbisogni" (o "Ordinativo di fornitura"), contenente i) i requisiti, i servizi, le caratteristiche qualitative, i dimensionamenti; ii) la descrizione del contesto tecnologico ed applicativo e la descrizione delle attività dimensionate, al fine di permettere la identificazione e contestualizzazione dei servizi nonché la eventuale declinazione delle figure professionali e degli strumenti a supporto.

1.2 Richieste dell'Amministrazione contraente

Con la Deliberazione della Giunta Regionale della Regione Autonoma della Sardegna n. 46/27 del 25/11/2021 la Giunta stabilisce di costituire l'ARES a partire dalla data del 1° gennaio 2022.

L'ARES è una azienda sanitaria parte integrante del sistema del Servizio Sanitario della Regione Autonoma della Sardegna e del sistema del Servizio Sanitario Nazionale, è stata istituita per offrire supporto alla produzione di servizi sanitari e socio-sanitari e svolge la propria attività nel rispetto del principio di efficienza, efficacia, razionalità ed economicità.

La mission di ARES, dotata di personalità giuridica di diritto pubblico, di autonomia amministrativa, patrimoniale, organizzativa, tecnica, gestionale e contabile, è quella di supportare le Aziende sanitarie regionali nella produzione di servizi sanitari e sociosanitari. ARES affianca l'Assessorato Regionale alla Sanità e dei Servizi Sociali nella funzione di governance complessiva del Servizio Sanitario Regionale e nel perseguire un'azione omogenea e coordinata tra le Aziende Sanitarie.

All'interno della L.R. 24/2020, la Regione assegna ad ARES importanti compiti di programmazione, monitoraggio e trasformazione digitale, in particolare vengono assegnate ad ARES le seguenti funzioni:

- centrale di committenza per conto delle aziende sanitarie e ospedaliere della Sardegna ai sensi degli articoli 38 e 39 del decreto legislativo 18 aprile 2016, n. 50 (Codice dei contratti pubblici) e successive modifiche e integrazioni, con il coordinamento dell'Assessorato regionale competente in materia di sanità. Nell'esercizio di tale funzione può avvalersi della centrale regionale di committenza di cui all'articolo 9 della legge regionale 29 maggio 2007, n. 2 (legge finanziaria 2007), e successive modifiche e integrazioni. Resta salva la facoltà di tutte le aziende di procedere direttamente all'acquisizione di beni e servizi nei limiti di quanto previsto dall'articolo 37 del decreto legislativo n. 50 del 2016;
- gestione delle procedure di selezione e concorso del personale del Servizio sanitario regionale, sulla base delle esigenze rappresentate dalle singole aziende; può delegare alle aziende sanitarie, sole o aggregate, le procedure concorsuali per l'assunzione di personale dotato di elevata specificità;
- gestione delle competenze economiche e della gestione della situazione contributiva e previdenziale del personale delle aziende sanitarie regionali;

- gestione degli aspetti legati al governo delle presenze nel servizio del personale;
- omogeneizzazione della gestione dei bilanci e della contabilità delle singole aziende;
- omogeneizzazione della gestione del patrimonio;
- supporto tecnico all'attività di formazione del personale del servizio sanitario regionale;
- procedure di accreditamento ECM;
- servizi tecnici per la valutazione delle tecnologie sanitarie (Health Technology Assessment - **HTA**), servizi tecnici per la fisica sanitaria e l'ingegneria clinica;
- **gestione delle infrastrutture di tecnologia informatica, connettività, sistemi informativi e flussi dati in un'ottica di omogeneizzazione e sviluppo del sistema ICT**;
- progressiva razionalizzazione del sistema logistico;
- gestione della committenza inerente all'acquisto di prestazioni sanitarie e socio-sanitarie da privati sulla base dei piani elaborati dalle aziende sanitarie;
- gestione degli aspetti economici e giuridici del personale convenzionato;
- tutte le competenze in materia di controlli di appropriatezza e di congruità dei ricoveri ospedalieri di qualunque tipologia, utilizzando metodiche identiche per tutte le strutture pubbliche e private. Il valore dei ricoveri giudicati inappropriati è scontato dalle spettanze alla struttura interessata al pagamento immediatamente successivo alla notifica del giudizio definitivo di appropriatezza.

Di particolare rilevanza, nell'ambito della L.R. 24/2020, è il contenuto dell'Art.8 – Sanità Digitale – di cii si riportano di seguito i commi più di interesse:

1. La Regione promuove le attività di sanità digitale al fine di garantire una maggiore appropriatezza delle prestazioni sanitarie, di riqualificare la spesa, di promuovere nuove modalità di diagnosi e di cura senza lo spostamento fisico del paziente, di consentire il corretto utilizzo dei progressi della genomica medica, della medicina predittiva e per valutare l'aderenza terapeutica.

2. La Regione si avvale dell'ARES per l'attuazione dell'attività di cui al comma 1 in coerenza con il regolamento (UE) 2016/679 del Parlamento europeo del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), e successive modifiche ed integrazioni.

5. Presso l'ARES è istituita una specifica struttura per la sanità digitale, che si avvale sia del personale del Servizio sanitario regionale che di quello del sistema Regione in applicazione delle norme regionali vigenti e, se necessario, di consulenti all'uopo selezionati, secondo le disposizioni impartite dalla Giunta regionale, da emanarsi entro sessanta giorni dalla data di entrata in vigore della presente legge.

6. L'ARES elabora il piano regionale triennale di sanità digitale, da aggiornarsi annualmente.

Il piano individua una bozza di livelli essenziali della sanità digitale (LEAD) e di nomenclatore tariffario digitale regionale da proporsi all'Assessorato regionale dell'igiene e sanità e dell'assistenza sociale affinché si proceda alla loro approvazione secondo le vigenti disposizioni di legge.

Come ogni altro ente pubblico di medio-grandi dimensioni, l'ARES deve essere pronta a fronteggiare numerosi attacchi informatici, per lo più automatici, ma talora anche mirati e preparati con competenza e risorse dedicate. Per questo da tempo l'Ente ha investito sulla sicurezza del sistema informativo nel suo complesso, in considerazione delle indicazioni dettate dal GDPR e delle misure minime di sicurezza AgID, ed ha l'obiettivo di efficientare il sistema sanitario regionale in linea anche con le finalità ultime del PNRR. Nell'ambito di tali progettualità e considerata la continua evoluzione tecnologica e il costante incremento delle minacce cibernetiche, si rende necessario rivalutare i presidi di sicurezza organizzativi, procedurali e tecnici al fine di identificare le misure di sicurezza più appropriate da adottare per mitigare i rischi.

Nell'ambito del presente Piano dei Fabbisogni si richiede un'attività di analisi dello status quo e di supporto al disegno del piano strategico in ambito Cybersecurity dell'Ente e alle iniziative per rafforzare il livello di maturità della Cybersecurity tenendo in considerazione anche i temi di compliance (es. GDPR, Direttiva NIS) e l'evoluzione tecnologica sempre più spostata verso paradigmi di cloud ibrido. L'intervento mira a rafforzare la relazione tra l'ARES e gli assistiti aumentando la sicurezza e la resilienza del Sistema Informativo dell'Azienda.

1.3 Riferimenti

IDENTIFICATIVO	TITOLO/DESCRIZIONE
ID 2296 - Gara Sicurezza da remoto - Allegato 1 - Capitolato Tecnico Generale	Capitolato Tecnico Generale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Allegato 2B - Capitolato Tecnico Speciale Lotto 2	Capitolato Tecnico Speciale della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Capitolato Oneri	Capitolato d'Oneri della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI
ID 2296 - Gara Sicurezza da remoto - Bando GURI	Bando GURI della GARA A PROCEDURA APERTA PER LA CONCLUSIONE DI UN ACCORDO QUADRO, AI SENSI DEL D.LGS. 50/2016 E S.M.I., SUDDIVISA IN 2 LOTTI E AVENTE AD OGGETTO L'AFFIDAMENTO DI SERVIZI DI SICUREZZA DA REMOTO, DI COMPLIANCE E CONTROLLO PER LE PUBBLICHE AMMINISTRAZIONI

1.4 Acronimi e glossario

DEFINIZIONE/ACRONNIMO	DESCRIZIONE
RTI	Raggruppamento Temporaneo di Impresa
AQ	Accordo Quadro
CE	Contratto Esecutivo
PAL	Pubblica Amministrazione Locale
PA	Pubblica Amministrazione
PAC	Pubblica Amministrazione Centrale
S.I.	Sistema Informativo

2 Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	Azienda Regionale della Salute (ARES)
Indirizzo	Via Piero della Francesca 1
CAP	09047
Comune	Selargius
Provincia	Cagliari
Regione	Sardegna
Codice Fiscale	03990570925
Indirizzo mail	segreteria.direzionegenerale@aressardegna.it
PEC	protocollo@pec.aressardegna.it
Codice PA	P65P3X9X
Comparto di Appartenenza (PAL/PAC)	PAL

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
Nome	Marco
Cognome	Galisai
Telefono	+39 3386570799
Indirizzo mail	marco.galisai@aressardegna.it
PEC	ict.infrastrutture@pec.aressardegna.it

3 Contesto di riferimento

3.1 Contesto dei servizi

Il Sistema Informativo (SI) dell'Ente è un sistema complesso ed articolato che integra la gestione dei procedimenti amministrativi interni all'ente con l'offerta di servizi on line verso cittadini. In questi mesi ARES ha intrapreso una decisa evoluzione delle infrastrutture tecnologiche e applicative volte alla trasformazione digitale del sistema sanitario regionale anche alla luce dei finanziamenti PNRR espressi nel CIS (Contratto Istituzionale di Sviluppo)[1][2].
La configurazione del Sistema Informativo Regionale prevede sia applicazioni gestite su sistemi ospitati nel data center on-premise in fase di potenziamento[3], sia applicazioni gestite in modalità cloud SaaS.
In tale contesto l'Ente si propone di attuare degli interventi finalizzati all'incremento complessivo e progressivo del livello di sicurezza, in coerenza con quanto previsto dalle linee di azione indicate nel Piano Triennale AgID per la PA e finalizzati a contrastare il costante aumento delle minacce informatiche, anche in considerazione degli accadimenti che hanno avuto risvolti sulle PA italiane.

3.2 Contesto tecnico ed operativo

La gestione dei servizi IT è principalmente effettuata con risorse interne, con il contributo di aziende esterne, e l'architettura si basa in gran parte su sistemi basati nei data center on-premise ma anche su ambienti cloud. L'ARES, fornisce servizi alle otto AASSLL (precedentemente aree socio-sanitarie della Azienda per la Tutela della Salute – ATS), alle due Aziende Ospedaliere Universitarie (Cagliari e Sassari), alla Azienda Ospedaliera di Rilievo Nazionale ARNAS – Brotzu e, in maniera minore, alla Azienda per l'Emergenza Urgenza AREUS.

Tali servizi prevedono l'erogazione e gestione dell'impianto applicativo unico tra le Aziende Sanitarie (AS) coordinando, in questa fase iniziale, le Aziende Ospedaliere e AREUS. Dal punto di vista applicativo ed infrastrutturale, nel corso dell'ultimo triennio è stata svolta dapprima un'attività di mappatura e razionalizzazione del parco applicativo ed infrastrutturale delle AS e successivamente è stata identificata la roadmap degli interventi di evoluzione strategica ICT, coerentemente al modello AgID.

Le attività relative al presente Piano di Fabbisogni verranno condotte all'interno di eventuali gruppi di lavoro costituiti dagli interlocutori istituzionali che potranno mettere a disposizione tutte le informazioni ed il proprio know-how durante l'iniziale raccolta delle informazioni nelle prime fasi dei vari stream progettuali oltre al necessario supporto per abilitare il compiersi delle varie iniziative.

3.3 Contesto Economico – Finanziario

Per l'esecuzione dei lavori viene previsto da parte dell'Amministrazione il ricorso, in parte, alle forme di finanziamento acquisite con la partecipazione ai bandi ACN per il piano di implementazione della strategia nazionale di cybersicurezza 2022-2026 (nel seguito Misura 55) e per gli interventi di potenziamento della resilienza cyber delle Pubbliche Amministrazioni (nel seguito Avviso 8), per le quali viene sotto riportata l'allocazione dei fondi negli anni sui servizi del Lotto 2:

Lotto	Servizio	2025				2026				2027				2028			
		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	Bilancio ARES	Avviso 8 AREUS	Misura 55 ACN Capex	Misura 55 ACN Opex
Lotto 2	Security Strategy	x	x			x				x				x			
Lotto 2	Vulnerability assessment	x	x			x				x				x			
Lotto 2	Dynamic Application Security Testing	x				x				x				x			
Lotto 2	Supporto all'analisi e gestione degli incidenti	x				x				x				x			
Lotto 2	Penetration testing	x				x				x				x			
Lotto 2	Compliance normativa	x	x			x				x				x			

[1] C_17_pubblicazioni_3240_14_alleg.pdf (salute.gov.it)
[2] Microsoft Word - D.P.Reg. n. 33 dell'8 giugno 2022 (regione.sardegna.it)
[3] DDG nr. 55 del 13/03/2023 e DDG nr. 56 del 13/03/2023

4 Ambiti funzionali oggetto di intervento

Il processo di trasformazione digitale in corso nella Pubblica Amministrazione, avente la finalità di portare innovazione nei servizi forniti ai cittadini, e la capacità di dover rispondere in maniera rapida ed efficace ai cambiamenti imposti anche dall'ambiente esterno pongono la necessità di una maggior attenzione alle tematiche che riguardano la sicurezza delle informazioni e la protezione dei dati.

Emergono di fatto nuove esigenze di sicurezza delle Informazioni e delle Infrastrutture dovute al mutamento degli scenari di rischio, dalle nuove minacce e dall'estensione delle superfici di attacco esposte, da un punto di vista sia interno (es. performance della modalità di lavoro remoto, gestione della sicurezza degli endpoint, miglioramento delle modalità di accesso da remoto ai sistemi) che esterno (es. evoluzioni di modalità e target degli attacchi). Inoltre, l'ARES intende far fronte alle nuove esigenze di conformità in ambito privacy e sicurezza con particolare riferimento alle più recenti normative in ambito Europeo e Nazionale.

4.1 Obiettivi e benefici da perseguire

L'obiettivo strategico che ARES intende perseguire nell'ambito del presente intervento è relativo allo sviluppo e all'esecuzione di un piano di **security/data protection enforcement e compliance** attinente alle infrastrutture e servizi "digitali" ricadenti nel perimetro:

- della propria organizzazione (ARES);
- del sistema della sanità regionale (ASL e Aziende Ospedaliere);
- di AREUS.

Il piano e le conseguenti attività, tecnologie impiegate e deliverables dovranno essere coerenti e coordinate con il piano, le tecnologie e i deliverables sviluppato nel contesto dell''intervento relativo al lotto 1 del medesimo accordo quadro. Entrambi gli interventi saranno sinergici e finalizzati allo stesso macro obiettivo oltre che ricadenti nell'ambito del medesimo perimetro di attuazione.

In dettaglio il perimetro di intervento riguarda le seguenti organizzazioni:

- ✓ ARES
- ✓ AREUS
- ✓ N.8 ASL regione Sardegna
- ✓ Azienda Ospedaliera Universitaria di Cagliari
- ✓ Azienda Ospedaliera Universitaria di Sassari
- ✓ ARNAS Brotzu

Per maggiore semplicità e chiarezza gli obiettivi operativi del presente lotto sono stati classificati secondo gli obiettivi della "Strategia di Digital Security di ARES":

Obiettivo 2	Protezione degli asset digitali	Tutte le organizzazioni
Obiettivo 5	Protezione dei dati personali degli interessati	Tutte le organizzazioni
Obiettivo 6	Rafforzamento della "safety" dei sistemi critici medicali a garanzia dei pazienti e degli operatori	Tutte le organizzazioni
Obiettivo 7.1	Conformità determina 628/2021, Misure "minime" AGID ex circ. 2/2017, Linee Guida di resilienza Legge 90/2024	Tutte le organizzazioni
Obiettivo 7.2	Conformità GDPR	Tutte le organizzazioni
Obiettivo 7.3	Conformità NIS2/D.Lgs. 138/2024	Solo le organizzazioni in "scope"
Obiettivo 8	Conformità PSNC	AREUS

Obiettivo 9	Certificazione ISO 27001, ISO 27017, ISO 27018	ARES
Obiettivo 10	Qualifica ACN servizi cloud della PA	ARES

A cui si farà riferimento anche nelle tabelle successive.

Gli obiettivi operativi possono essere declinati in modo più dettagliato:

Main ob	**Obiettivi Operativi**	**ID Servizio**
Ob 2 Ob 6 Ob 7.1 Ob 7.3	Sviluppare un "maturity model" finalizzato al supporto della definizione del Piano strategico di security e data protection e della compliance con particolare riferimento alle: • Misure Critical Security Controls v8 del CIS - Center for Internet Security • Misure Minime per la Sicurezza ICT nelle Pubbliche Amministrazioni predisposte da AgID (circolare AgID 2/2027) • Framework Nazionale per la Cybersecurity v2 di cui all'Allegato A e A2 (livelli minimi delle infrastrutture) nel contesto degli obblighi per la Pubblica Amministrazione derivanti dalla Determina AgID 628/2021 • Linee Guida per il rafforzamento della resilienza dei soggetti rientranti nell'ambito di applicazione della Legge 90/2024.	L2.S16 Security Strategy
Ob 2	Effettuare un'attività specifica di cyber-assessment e sviluppo di piani di remediation relativamente alle infrastrutture e servizi digitali delle organizzazioni ricadenti nel perimetro di intervento (approccio proattivo). Tuttavia, qualora nel corso dell'attività di assessment venga riscontrata una evidente misconfiguration dei sistemi di sicurezza o una vulnerabilità grave (cyber issue) che richieda un'azione immediata, si procede con il supporto all'individuazione delle possibili azioni di mitigazione da porre in atto (approccio reattivo).	
Ob 7.3	Effettuare le attività di risk assessment, sviluppo di piani di remediation, sviluppo di compliance documents e monitoraggio continuo richieste dalla Direttiva NIS2 e dal decreto italiano di recepimento (D.Lgs. 138/2024) e successivi DPCM e determine dell'ACN.	
Ob 8	Effettuare le attività di assessment rispetto ai requisiti del Perimetro di Sicurezza Nazionale Cibernetica per AREUS, sviluppare il piano di remediation e predisporre la documentazione di adeguamento necessaria per la compliance e l'accountability delle misure adottate ai sensi del DPCM 81/2021.	
Ob 9	Effettuare un'analisi specifica rispetto allo standard in materia di Sicurezza delle Informazioni, produrre compliance documents, definire policy e processi finalizzati all'ottenimento della certificazione ISO27001:2022 con estensioni ISO27017, ISO27018 nel contesto specifico di ARES.	
Ob 10	Effettuare un'analisi specifica rispetto ai servizi e agli obblighi formali derivanti dalla qualifica ACN servizi cloud PA, produrre i compliance documents e supportare lo sviluppo dei servizi.	
Ob 2	Esecuzione di Test tecnici (Vulnerability Assessment, Penetration Test e Dynamic Application Security Testing) sui servizi identificati come critici. Tali test andranno ripetuti nel corso del dispiegamento delle attività anche per verificare la corretta applicazione di quanto definito nei piani di remediation.	L2.S17 Vulnerability assessment L2.S22 Penetration testing

		L2.S19 Testing Dinamico del Codice
Ob 2 Ob 7.1 Ob 7.2 Ob 7.3 Ob 9 Ob 10	Definire i piani di risposta agli incidenti compreso e i modelli per la ripartenza dei servizi in caso di attacco/incidente informatico conformi alle normative cogenti.	L2.S21 Supporto all'analisi e gestione degli incidenti
Ob 2 Ob 5 Ob 7.2	Nel contesto della digitalizzazione dei servizi rientra, inoltre, la necessità di garantire la corretta attuazione degli adempimenti del GDPR (General Data Protection Regulation - Regolamento UE 2016) applicato all'ambito del perimetro IT e dei servizi digitali di tutte le organizzazioni nel perimetro di intervento.	L2.S23 compliance normativa

4.2 Categorizzazione dell'intervento

4.2.1 Categorizzazione di I livello

AMBITO I LIVELLO (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 al fine di semplificare i servizi ai cittadini
		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**	Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
		Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

4.2.2 Categorizzazione di II livello

I LIVELLO (LAYER)		II LIVELLO
SERVIZI		Servizi al cittadino
		Servizi a imprese e professionisti
		Servizi interni alla propria PA
		Servizi verso altre PA
PIATTAFORME		Sanità digitale (FSE e CUP)
		Identità Digitale
		Pagamenti digitali
		App IO
		ANPR
		NoiPA
		INAD
		Musei
		Siope+
DATI		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport
		Energia
		Ambiente
		Governo e Settore pubblico
	X	Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INTEROPERABILITA		Agricoltura, pesca, silvicoltura e prodotti alimentari
		Economia e finanze
		Istruzione, cultura e sport

		Energia
		Ambiente
		Governo e Settore pubblico
	X	Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INFRASTRUTTURE	X	Data center e Cloud
	X	Connettività
SICUREZZA INFORMATICA	X	Portali istituzionali e CMS
	X	Sensibilizzazione del rischio cyber

4.3 Indicatori di digitalizzazione

4.3.1 Indicatori generali di digitalizzazione

Di seguito si riportano gli indicatori Generali di digitalizzazione previsti per la presente fornitura:

	INDICATORI DI COLLABORAZIONE E RIUSO	VALORE EX ANTE	VALORE EX POST
	Riuso di processi per erogazione servizi digitali	*Nessuna*	*Gestione Uniforme della Sicurezza delle informazioni per i servizi erogati dall'Ente*

Per ciascuno dei soprariportati indicatori, verrà effettuata una valutazione in fase di avvio dei singoli interventi progettuali e a valle, così da misurare il livello di digitalizzazione raggiunto per ciascuno di essi.

5 Servizi richiesti

Di seguito si riporta una sintesi dei servizi e relativa quantificazione:

ID	NOME SERVIZIO	VOCE DI COSTO	Gg/p Team ottimale – N° applicazioni
L2.S16	Security Strategy	L2.S16 – gg/p Team ottimale	**7.350 gg/p**
L2.S17	Vulnerability assessment	L2.S17 – gg/p Team ottimale	**2.048 gg/p**
L2.S19	Dynamic Application Security Testing	L2.S19 – n° applicazioni per profilo	**7 app "bronze"** **4 app "silver"** **3 app "gold"**
L2.S21	Supporto all'analisi e gestione degli incidenti	L2.S21 – gg/p Team ottimale	**936 gg/p**
L2.S22	Penetration testing	L2.S22 – gg/p Team ottimale	**696 gg/p**
L2.S23	Compliance normativa	L2.S23 – gg/p Team ottimale	**4.927 gg/p**

Dettaglio dei servizi richiesti – Delivery plan degli obiettivi operativi

5.1.1 L2.S16 - Security Strategy

5.1.1.1 Descrizione e caratteristiche del servizio

L2.S16 - Security Strategy			Obiettivi	Deliverable	Organizzazioni TARGET
SS.1	Classificazione degli asset	Definizione di un modello per la mappatura e classificazione degli asset e di una procedura per l'identificazione di ruoli e responsabilità, sulla base della classificazione degli asset prodotta dalla piattaforma di asset intelligence e sicurezza selezionata. Definizione del campo di applicazione, contesto e criteri di rischio (rif. ISO 31000).	**Obiettivo 2:** Protezione degli asset digitali	Modello e procedura per la classificazione e e gestione degli asset	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
SS.2	Maturity Model	Definizione di un "maturity model" a partire dal risk assessment prodotto dalla piattaforma di asset intelligence e sicurezza selezionata, finalizzato alla valutazione del rischio, al supporto per la definizione delle misure di trattamento del rischio e al monitoraggio e riesame (rif. ISO 31000).	**Obiettivo 2:** Protezione degli asset digitali	Schema del Maturity Model	
SS.3	Assessment sulla Cybersecurity Posture – CIS v8	Esecuzione di un security assessment su ambiti/perimetri concordati finalizzato all'analisi del livello di maturità delle capacità cyber in termini di organizzazione, processi e tecnologie. L'assessment sarà eseguito sulla base dei controlli del framework CIS - Center for Internet Security - Critical Security Controls V8. Ponderazione del rischio cyber sulla base del livello di maturità dei controlli di sicurezza analizzati. Identificazione dei gap rispetto al framework CIS - Center for Internet Security - Critical Security Controls V8.	**Obiettivo 2:** Protezione degli asset digitali	Maturity Model basato su framework CIS v8 Gap analysis	
SS.4	Azioni di contenimento o di emergenza del rischio cibernetico	Dalle prime risultanze del security assessment emerse, qualora risultassero evidenze esplicite con carattere di urgenza e indifferibilità si individuano nell'immediato le azioni di contenimento del rischio implementabili rapidamente da eseguire in parallelo allo sviluppo del piano definitivo e completo.	**Obiettivo 2:** Protezione degli asset digitali	Elenco e piano di azioni di contenimento di emergenza del rischio cibernetico	
SS.5	Assessment sulla Cybersecurity Posture - FNCS e Misure AGID e Linee Guida Legge 90	Estensione e correlazione dei controlli del Maturity Model rispetto alle Misure Minime per la Sicurezza ICT nelle Pubbliche Amministrazioni predisposte da AgID (circolare AgID 2/2027), al FNCS v2 di cui agli Allegati A e A2 (livelli minimi delle infrastrutture) della Determina AgID 628/2021, alle Linee Guida di resilienza della Legge 90/2024. Identificazione dei gap rispetto alle norme citate e delle relative azioni di rimedio.	**Obiettivo 2:** Protezione degli asset digitali **Obiettivo 7.1:** Conformità determina 628, misure AGID, linee guida Legge 90	Maturity Model esteso al FNCS e alle misure AgID Gap analysis	
SS.6	Gestione dei fornitori e dei rischi associati	Definizione di un modello e di una procedura per la gestione dei rischi di cybersecurity e data protection (nell'ambito della gestione del dato digitale) dei fornitori. Supporto per il censimento dei fornitori rispetto ai servizi di sicurezza esternalizzati e prioritizzazione dei fornitori in termini di cyber risk rating. Definizione del modello e delle checklist per	**Obiettivo 2:** Protezione degli asset digitali **Obiettivo 7.2**: Conformità GDPR	Modello e procedura per la gestione dei rischi cyber dei fornitori Elenco dei	

		la conduzione di verifiche, in modalità self-assessment, sulle misure di sicurezza adottate dai fornitori critici.		fornitori e relativo livello di criticità Checklist per l'esecuzione delle verifiche sui fornitori Aggiornamento Maturity Model	
SS.7	Definizione del modello di gestione e controllo accessi	Esecuzione di un assessment sull'attuale modello di controllo degli accessi logici, rispetto agli asset e servizi IT critici, con focus sull'accesso da parte delle terze parti e delle utenze con accessi privilegiati, al fine di individuarne punti di miglioramento e disegnare il modello to-be da adottare.	**Obiettivo 2:** Protezione degli asset digitali	Predisposizione del Modello di gestione e controllo accessi Aggiornamento Maturity Model	
SS.8	Compliance Direttiva NIS2 / D.Lgs. 138/2024	Aggiornamento del risk assessment e del maturity assessment rispetto alle misure di gestione del rischio previste dalla Direttiva NIS2 e dal decreto italiano di recepimento D.Lgs. 138/2024 e del relativo remediation plan. Redazione dei compliance documents NIS2/D.Lgs. 138/2024. Aggiornamento periodico, annuale, della documentazione predisposta.	**Obiettivo 7.3**: Conformità NIS2/D.Lgs. 138/2024	Maturity assessment, risk assessment e remediation plan aggiornati rispetto alla Direttiva NIS2/D.Lgs. 138/2024 Compliance documents NIS2/D.Lgs. 138/2024	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
SS.9	Compliance PSNC	Svolgimento di un assessment, basato su Framework Nazionale Cyber Security, comprensivo delle disposizioni di cui ai regolamenti vigenti per i soggetti inclusi nel Perimetro di Sicurezza Nazionale in modo da: • Indicare il grado di adeguamento dell'Amministrazione ai livelli standard di sicurezza previsti per il Perimetro di Sicurezza; • Individuare le possibili azioni correttive e soluzioni rispetto agli standard vigenti nell'organizzazione; • Predisporre/aggiornare la documentazione obbligatoria per la compliance e l'accountability delle misure adottate ai sensi del DPCM 81/2021.	**Obiettivo 8:** Conformità PSNC	Maturity Assessment e remediation plan rispetto ai requisiti indicati dal PSNC Documentazione minima obbligatoria richiesta dal PSNC	AREUS
SS.10	Supporto coordinamento alle iniziative di Secure Design in ambito PSN	Supporto e coordinamento per la verifica delle iniziative di Security By Design avviate nel corso delle attività di migrazione verso il PSN (erogate a cura dei professionisti PSN) al fine di garantire la corretta implementazione delle misure by default e by design necessarie.	**Obiettivo 2:** Protezione degli asset digitali	Report di gap analisi delle iniziative avviate dal PSN rispetto alle misure di security	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu

				by design implementate/da implementare	
SS.11	Definizione dei piani di sicurezza e compliance	Individuazione delle azioni di remediation e definizione dei piani di sicurezza e compliance delle organizzazioni nel perimetro di intervento, derivanti dall'applicazione del Maturity Model completo. Sviluppo del piano strategico di ARES.	Tutti gli obiettivi	Piano strategico di security & data protection enforcement	
SS.12	Coordinamento dei piani di sicurezza e compliance	Supporto e coordinamento dell'implementazione dei piani di sicurezza e compliance delle organizzazioni nel perimetro di intervento.	Tutti gli obiettivi	•SAL •Presentazioni management •Reportistica executive •Report di monitoraggio andamento delle implementazioni (es. Lotto1, PSN, altro)	
SS.13	Analisi della conformità ISO 27001 e sue estensioni - ARES	Individuazione dell'ambito di attuazione e verifica della conformità rispetto allo standard ISO27001:2022 e sue estensioni (ISO27017, ISO27018). Identificazione di eventuali gap e definizione delle azioni di rientro, implementazione dei controlli finalizzati a conseguire la certificazione ISO di ARES.	**Obiettivo 9**: Certificazione ISO 27001, ISO 27017, ISO 27018	Piano delle azioni procedurali ed organizzative necessarie a conseguire la certificazione ISO27001 e sue estensioni	ARES
SS.14	Implementazione del SGSI - ARES	Predisposizione della documentazione specifica in ambito ISO/IEC 27001:2022 e sue estensioni (ISO27017, ISO27018) e raccolta delle evidenze dell'implementazione del Sistema di Gestione della Sicurezza delle Informazioni. Erogazione formazione in ambito ISO, supporto nell'esecuzione di audit interni e nel Riesame di Direzione.	**Obiettivo 9**: Certificazione ISO 27001, ISO 27017, ISO 27018	Supporto al processo di certificazione	ARES
SS.15	Qualificazione ACN servizi cloud ARES	Individuazione dei servizi e predisposizione della documentazione e delle azioni indicate nel Decreto direttoriale prot. N. 29 del 02/01/2023 richieste per la qualifica dei servizi.	**Obiettivo 10**: Qualifica ACN servizi cloud della PA	Supporto al processo di qualifica ACN	ARES
SS.16	Miglioramento continuo	Manutenzione periodica del Maturity Model e degli indici di rischio al fine di valutare i miglioramenti della posture di cybersecurity e di aggiornare la prioritizzazione degli interventi residui. Analisi e miglioramento del modello di governo a livello organizzativo e documentale in merito ai principali processi di gestione della cybersecurity e	Tutti gli obiettivi	Modello organizzativo di Security & Data Protection Governance e Assurance	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu

		della data protection.		Framework procedurale di riferimento per la gestione della cybersecurity	
SS.17	Cyber Strategic Risk Management	Valutazione ed analisi del rischio strategico, valutazione dell'intelligence sulle minacce più verticali al contesto in modo strutturato per valutare e mitigare i rischi specifici del contesto di azione con un approccio Data driven.	**Obiettivo 2:** Protezione degli asset digitali	Piano Strategico Cyber con azioni evolutive specifiche	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu

5.1.1.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti in concerto con l'Amministrazione i task e i rispettivi deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Security Solution Architect
- Senior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.1.3 Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

5.1.2 L2.S17 - Vulnerability assessment

5.1.2.1 Descrizione e caratteristiche del servizio

L2.S17 Vulnerability Assessment			**Obiettivi**	**Organizzazioni TARGET**
VA.1	Vulnerability Assessment periodici	Verifiche annuali di sicurezza sul perimetro di sistemi, applicazioni e medical device concordato (infrastruttura di	**Obiettivo 2:** Protezione degli asset digitali	ARES AREUS 8 ASL AOU Cagliari

		base), nell'ordine di 20 applicazioni per anno.		AOU Sassari ARNAS Brotzu
VA.2	Esecuzione delle attività in modalità black-box	Esecuzione delle attività in modalità black-box dall'esterno della rete aziendale e dall'interno sui sistemi locati nei data center on-premise, secondo gli standard della metodologia OWASP, al fine di rilevare vulnerabilità presenti per i target oggetto di analisi mediante tool automatizzati e tecniche manuali.		
VA.3	Prioritizzazione delle vulnerabilità e Remediation Plan.	Prioritizzazione delle vulnerabilità, verifica dei risultati e predisposizione Remediation Plan.		
VA.4	Re-test delle vulnerabilità	Re-test delle vulnerabilità concordando con l'Ente tempistiche e vulnerabilità da analizzare, a seguito del processo di mitigazione delle vulnerabilità effettuato.		

5.1.2.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Penetration tester
- Junior Penetration tester

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.2.3 Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

5.1.3 L2.S19 – Testing Dinamico del Codice

5.1.3.1 Descrizione e caratteristiche del servizio

L2.S19 Testing Dinamico del Codice			**Obiettivi**	**Organizzazioni TARGET**
TD.1	Identificazione del perimetro di applicazioni	Identificazione del perimetro di applicazioni da verificare annualmente, in base alle evoluzioni tecnologiche e nuove implementazioni critiche. Si ipotizza per ogni anno l'esecuzione di testing dinamico del codice su 7 applicazioni con profilo "bronze", 4 con profilo "silver" e 3 con profilo "gold"	**Obiettivo 2:** Protezione degli asset digitali	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
TD.2	Definizione delle modalità operative	Definizione delle modalità operative di esecuzione delle analisi.		
TD.3	Esecuzione del Testing	Esecuzione del Testing del codice sulle applicazioni dell'Ente target, secondo il perimetro concordato.		
TD.4	Analisi risultati e predisposizione reportistica	Analisi risultati e predisposizione reportistica a livello executive e tecnica.		
TD.5	Definizione del remediation plan	Definizione del piano di rimedio da attuare per eliminare le vulnerabilità riscontrate.		
TD.6	Re-test delle applicazioni	Re-test delle applicazioni concordando con l'Ente tempistiche e vulnerabilità da analizzare, a seguito del processo di mitigazione delle vulnerabilità effettuato.		

5.1.3.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "canone (annuale)" e che la metrica di misurazione è "*numero di applicazioni per profilo (Bronze, Silver e Gold)/anno*".

La fatturazione avverrà sulla base dello stato dell'avanzamento dell'esecuzione delle attività di testing dinamico del codice sulle singole applicazioni per tipo di profilo (Bronze, Silver e Gold) e sarà riconosciuta bimestralmente.

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.3.3 Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

5.1.4 L2.S21 - Supporto all'analisi e gestione degli incidenti

5.1.4.1 Descrizione e caratteristiche del servizio

L2.S21 Supporto all'analisi e gestione degli incidenti			**Obiettivi**	**Organizzazioni TARGET**
GI.1	Analisi processi e strumenti per la gestione degli incidenti	Analisi degli attuali processi e strumenti per la gestione degli incidenti nelle organizzazioni in scope, anche con riferimento alle normative applicabili in materia (es. GDPR, Legge 90, Direttiva NIS2, PSNC).	**Obiettivo 2:** Protezione degli asset digitali **Obiettivo 7.1:** Conformità determina 628, misure AGID, linee guida Legge 90 **Obiettivo 7.2**: Conformità GDPR **Obiettivo 7.3**: Conformità NIS2/D.Lgs. 138/2024 **Obiettivo 9**: Certificazione ISO 27001, ISO 27017, ISO 27018 **Obiettivo 10**: Qualifica ACN servizi cloud della PA	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
GI.2	Definizione del modello di gestione degli incidenti	Definizione del modello di gestione degli incidenti in termini di: - People: ruoli e responsabilità per la rilevazione e gestione degli incidenti di sicurezza e per la gestione delle crisi da incidenti informatici; - Process: processi, policy, procedure operative e playbook per la risposta agli incidenti di sicurezza; - Technology: strumenti e soluzioni tecnologiche funzionali alla gestione degli incidenti. Individuazione ed applicazioni delle eventuali azioni da implementare a valle di un incidente grave occorso.		
GI.3	Simulazione annuale di un incidente	Simulazione annuale di un incidente cyber tramite table top exercise, su un perimetro concordato di organizzazioni, e aggiornamento periodico del modello definito.		

5.1.4.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Penetration tester
- Junior Penetration tester
- Forensic Expert

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.4.3 Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

5.1.5 L2.S22 - Penetration testing

5.1.5.1 Descrizione e caratteristiche del servizio

L2.S22 Penetration testing			**Obiettivi**	**Organizzazioni TARGET**
PT.1	Identificazione del perimetro di sistemi	Identificazione del perimetro di sistemi, con rilevazione dei servizi e delle applicazioni critiche da verificare annualmente, in base alle evoluzioni tecnologiche e nuove implementazioni critiche, nell'ordine di 7 per il primo anno e 6 applicazioni per anno per gli anni successivi al primo.	**Obiettivo 2:** Protezione degli asset digitali	ARES AREUS ASL AOU Cagliari AOU Sassari ARNAS Brotzu
PT.2	Definizione delle modalità operative	Definizione delle modalità operative di esecuzione delle analisi.		
PT.3	Esecuzione del Penetration test	Esecuzione del Penetration test sull'infrastruttura e sulle applicazioni dell'Ente target, secondo il perimetro concordato, dall'esterno della rete aziendale e dall'interno sui sistemi locati nei data center on-premise,		

		secondo gli standard della metodologia OWASP.		
PT.4	Analisi risultati e predisposizione reportistica	Analisi risultati e predisposizione reportistica a livello executive e tecnica.		
PT.5	Definizione del remediation plan	Definizione del piano di rimedio da attuare per eliminare le vulnerabilità riscontrate.		
PT.6	Re-test delle applicazioni	Re-test delle applicazioni concordando con l'Ente tempistiche e vulnerabilità da analizzare, a seguito del processo di mitigazione delle vulnerabilità effettuato.		

5.1.5.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona del team ottimale*".

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Security Analyst
- Junior Security Analyst
- Forensic Expert

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es: presso le sedi del RTI).

5.1.5.3 Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

5.1.6 L2.S23 - Compliance normativa

5.1.6.1 Descrizione e caratteristiche del servizio

L2.S23 Compliance Normativa			**Obiettivi**	**Organizzazioni TARGET**
GDPR.1	Assessment della conformità Privacy	Assessment preliminare per la verifica dello stato di compliance as is delle organizzazioni in perimetro, in ambito Privacy, mediante predisposizione di un framework di controllo ed esecuzione di interviste per l'analisi dei processi e delle procedure in ambito e relativa gap analysis rispetto ai requisiti normativi.	**Obiettivo 7.2**: Conformità GDPR	ARES AREUS 8 ASL AOU Cagliari AOU Sassari ARNAS Brotzu
GDPR.2	Aggiornamento del registro dei trattamenti	Tramite il supporto dello strumento opportunamente selezionato, aggiornamento del registro dei trattamenti di ARES e dalle altre AS a partire dalle attuali versioni dei registri dei trattamenti, tramite interviste di approfondimento ed analisi della documentazione rilevante rispetto a nuove progettualità ed esigenze che prevedono trattamenti di dati personali. Manutenzione periodica del registro dei trattamenti in funzione delle iniziative sviluppate da ARES e dalle altre AS che prevedono trattamenti di dati personali.	**Obiettivo 2:** Protezione degli asset digitali **Obiettivo 5:** Protezione dei dati personali degli interessati **Obiettivo 7.2**: Conformità GDPR	
GDPR.3	Esecuzione di analisi dei rischi privacy e DPIA sui trattamenti rilevanti	Tramite il supporto dello strumento opportunamente selezionato, ricognizione dei trattamenti di dati personali svolti da ARES e dalle altre AS che necessitano di specifica analisi dei rischi di impatti privacy. Svolgimento di attività di analisi dei rischi e DPIA, consultazione con i DPO di ARES e delle altre AS e redazione di un documento per ogni trattamento analizzato riportante i risultati emersi, i	**Obiettivo 2:** Protezione degli asset digitali **Obiettivo 5:** Protezione dei dati personali degli interessati **Obiettivo 7.2**: Conformità GDPR	

		rischi connessi e le decisioni intraprese.		
GDPR.4	Consolidamento e governo della Conformità Privacy	Consolidamento del livello di compliance normativa in ambito Privacy mediante revisione ed ottimizzazione dei processi e delle procedure in ambito e piano di rafforzamento delle misure tecniche da adottare per un adeguato livello di sicurezza al trattamento dei dati sui sistemi ICT, tramite una esecuzione periodica dell'assessment basato sul framework predisposto.	**Obiettivo 2:** Protezione degli asset digitali **Obiettivo 5:** Protezione dei dati personali degli interessati **Obiettivo 7.2**: Conformità GDPR	

5.1.6.2 Modalità di erogazione e consuntivazione

Coerentemente a quanto previsto nel "CAPITOLATO TECNICO SPECIALE SERVIZI DI COMPLIANCE E CONTROLLO" si precisa che la modalità di remunerazione di tali servizi è "progettuale (a corpo)" e che la metrica di misurazione è "*giorni/persona"*.

Saranno definiti di concerto con l'Amministrazione dei task e dei deliverable, dimensionati e valorizzati economicamente. La fatturazione avverrà sulla base dello stato dell'avanzamento lavori mensile determinato coerentemente con il piano di lavoro definito e sarà riconosciuta bimestralmente.

Il team di lavoro per la realizzazione delle attività sopraccitate prevede il coinvolgimento delle seguenti figure professionali:

- Security Principal
- Senior Information Security Consultant
- Junior Information Security Consultant
- Senior Security Auditor
- Data Protection Specialist

Le attività saranno erogate presso le sedi dell'Amministrazione Contraente e da remoto (es. presso le sedi del RTI).

5.1.6.3 Attivazione e durata

Si prevede l'avvio del servizio entro Gennaio 2025 per una durata di 48 mesi.

5.2 Organizzazione e figure di riferimento dell'amministrazione

Il principale punto di contatto dell'amministrazione è l'Ing. Marco Galisai del Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica.

L'amministrazione si riserva di poter identificare durante l'esecuzione del contratto ulteriori figure di riferimento con le quali il fornitore potrà interfacciarsi.

5.3 Organizzazione e figure di riferimento del fornitore

Si richiede di indicare nel Piano Operativo le persone incaricate dal Fornitore per la conduzione del progetto e i relativi ruoli/responsabilità.

6 Elementi quantitativi e qualitativi per il dimensionamento servizi

6.1 Elementi quantitativi dei servizi

Si riporta di seguito una caratterizzazione quantitativa di riferimento data dalla complessità dei processi individuati:

ID	NOME SERVIZIO	Gg/p Team ottimale – N° applicazioni	Uffici interessati
L2.S16	Security Strategy	**7.350 gg/p**	**ARES, Enti del SSR**
L2.S17	Vulnerability assessment	**2.048 gg/p**	**ARES, Enti del SSR**
L2.S19	Dynamic Application Security Testing	**7 app "bronze"** **4 app "silver"** **3 app "gold"**	**ARES, Enti del SSR**
L2.S21	Supporto all'analisi e gestione degli incidenti	**936 gg/p**	**ARES, Enti del SSR**
L2.S22	Penetration testing	**696 gg/p**	**ARES, Enti del SSR**
L2.S23	Compliance normativa	**4.927 gg/p**	**ARES, Enti del SSR**

6.2 Elementi qualitativi dei servizi

I servizi dovranno essere svolti tenendo conto delle linee guida tecniche e la normativa vigente o le successive modifiche che verranno individuate.

6.3 Pianificazione dei servizi

La durata ipotizzata per la fornitura è di 48 mesi dalla data di attivazione, compatibilmente con il vincolo definito dall'Accordo quadro, ovvero che i Contratti Esecutivi hanno una durata massima pari alla durata residua, al momento della sua stipula, dell'Accordo Quadro.

Di seguito si riporta la pianificazione di massima del programma con indicazione degli obiettivi in ambito del presente piano dei fabbisogni.

		Anno 1						Anno 2						Anno 3						Anno 4					
		B1	B2	B3	B4	B5	B6	B1	B2	B3	B4	B5	B6	B1	B2	B3	B4	B5	B6	B1	B2	B3	B4	B5	B6
	L2.S16 - Security Strategy																								
SS.1	Classificazione degli asset																								
SS.2	Maturity Model																								
SS.3	*Assessment sulla Cybersecurity Posture – CIS v8*																								
SS.4	*Azioni di contenimento di emergenza del rischio cibernetico*																								
SS.5	*Assessment sulla Cybersecurity Posture - FNCS e Misure AGID e Linee Guida Legge 90*																								
SS.6	*Gestione dei fornitori e dei rischi associati*																								
SS.7	*Definizione del modello di gestione e controllo accessi*																								
SS.8	*Compliance Direttiva NIS2 / D.Lgs. 138/2024*																								
SS.9	*Compliance PSNC*																								
SS.10	*Supporto coordinamento alle iniziative di Secure Design in ambito PSN*																								
SS.11	*Definizione dei piani di sicurezza e compliance*																								
SS.12	*Coordinamento dei piani di sicurezza e compliance*																								
SS.13	*Analisi della conformita ISO 27001 e sue estensioni - ARES*																								
SS.14	*Implementazione del SGSI - ARES*																								
SS.15	*Qualificazione ACN servizi cloud ARES*																								
SS.16	*Miglioramento continuo*																								
SS.17	*Cyber Strategic Risk Management*																								
	L2.S17 Vulnerability Assessment																								
VA.1	Vulnerability Assessment periodici																								
VA.2	Esecuzione delle attività in modalità black-box																								
VA.3	Prioritizzazione delle vulnerabilità e Remediation Plan																								
VA.4	Re-test delle vulnerabilità																								
	L2.S19 Testing Dinamico del Codice																								
TD.1	*Identificazione del perimetro di applicazioni*																								
TD.2	*Definizione delle modalità operative*																								
TD.3	*Esecuzione del Penetration test*																								
TD.4	*Analisi risultati e predisposizione reportistica*																								
TD.5	*Definizione del remediation plan*																								
TD.6	*Re-test delle applicazioni*																								
	L2.S21 Supporto all'analisi e gestione degli incidenti																								
GI.1	Analisi processi e strumenti per la gestione degli incidenti																								
GI.2	Definizione del modello di gestione degli incidenti																								
GI.3	Simulazione annuale di un incidente																								
	L2.S22 Penetration testing																								
PT.1	*Identificazione del perimetro di sistemi*																								
PT.2	*Definizione delle modalità operative*																								
PT.3	*Esecuzione del Testing*																								
PT.4	*Analisi risultati e predisposizione reportistica*																								
PT.5	*Definizione del remediation plan*																								
PT.6	*Re-test delle applicazioni*																								
	L2.S23 Compliance Normativa																								
GDPR.1	*Assessment della conformità Privacy*																								
GDPR.2	*Aggiornamento del registro dei trattamenti*																								
GDPR.3	*Esecuzione di analisi dei rischi privacy e DPIA sui trattamenti rilevanti*																								
GDPR.4	*Consolidamento e governo della Conformità Privacy*																								

GALISAI MARCO

Firmato digitalmente da GALISAI MARCO
Data: 2024.12.11 08:54:29 +01'00'