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

REGIONE MARCHE

ARS Marche

Costituito

Raggruppamento Temporaneo di Imprese

composto da:

Deloitte Risk Advisory S.r.l.

EY Advisory S.p.A.

Teleco S.r.l.

Firma

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 Risk Advisory S.r.l. 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

ARS Marche (Agenzia Regionale Sanitaria Regione Marche), con sede in Via Gentile da Fabriano 3, svolge un ruolo cruciale all'interno del sistema sanitario regionale. L'Agenzia fornisce assistenza tecnica e scientifica al Servizio Sanità, al Servizio Politiche Sociali e agli enti del sistema sanitario regionale, fungendo da strumento operativo per tali servizi. Inoltre, ARS Marche supporta la pianificazione sanitaria in linea con la programmazione regionale.

In relazione alla continua evoluzione tecnologica e al sempre più crescente ruolo che l'ICT svolge a supporto dei servizi offerti ai cittadini ed alle imprese, la gestione della sicurezza delle informazioni e la conformità alla normativa a tutela dei dati personali sono quindi diventati aspetti fondamentali per qualsiasi organizzazione.

Il presente piano dei fabbisogni si prefigge l'obiettivo di consolidare ed espandere, nei limiti delle risorse disponibili, alcune azioni strategiche già intraprese nell'ambito delle strategie generali descritte in precedenza.

Il servizio prevede:

(i) lo sviluppo di una metodologia di **classificazione degli asset e di definizione dei sistemi critici**;

(ii) la definizione delle linee di indirizzo di un **Piano strategico di security & compliance per la sanità digitale;**

(iii) la definizione delle linee guida per la **progettazione e verifica delle procedure per la gestione della sicurezza e resilienza dei sistemi critici nonché per la gestione di identità e accessi dei sistemi critici**.

Il perimetro di analisi e sviluppo riguarda esclusivamente i dispositivi, i sistemi applicativi e servizi presenti nel contesto del data center regionale "Sanzio" e i servizi erogati dall'ARS Marche.

Nell'ambito del contratto quadro per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni e per la realizzazione del progetto finanziato (CUP H31B24000020001) tramite fondi PNRR in risposta all'avviso 8/2024 di ACN, l'Amministrazione richiede, ai fini dello sviluppo del Progetto di Sicurezza, l'esecuzione dei servizi afferenti al Lotto 2- Servizi di Compliance e controllo:

- **Servizio di Security Strategy (L2.S16) - Classificazione degli asset e definizione dei sistemi critici;**

- **Servizio di Security Strategy (L2.S16) - Piano strategico;**
- **Servizio di Security strategy (L2.S16) - Procedure per la gestione della sicurezza e resilienza dei sistemi critici;**
- **Servizio di Security Strategy (L2.S16) - Procedure per la gestione di identità e accessi dei sistemi critici.**

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
AGID	Agenzia per l'Italia Digitale
ICT	Information and Communications Technology
PA	Pubblica Amministrazione
ACN	Agenzia per la Cybersicurezza Nazionale

2 Anagrafica dell'amministrazione

DATI ANAGRAFICI DELL'AMMINISTRAZIONE	
Ragione sociale Amministrazione	ARS Marche
Indirizzo	Via Gentile da Fabriano 3
CAP	60125
Comune	Ancona
Provincia	Ancona
Regione	Marche
P.IVA	01486510421
Indirizzo mail	regione.marche.ars@emarche.it
PEC	regione.marche.ars@emarche.it
Codice PA	
Comparto di Appartenenza (PAL/PAC)	

DATI ANAGRAFICI REFERENTE DELL'AMMINISTRAZIONE	
(1 referente) Nome	Flavia
Cognome	Carle
Indirizzo mail	flavia.carle.regione.marche.it
(2 referente) Nome	Alessandro
Cognome	Giommi
Indirizzo mail	alessandro.giommi@regiona.marche.it
(3 referente) Nome	Marco
Cognome	Pompili
Indirizzo mail	Marco.pompili@regione.marche.it
PEC	regione.marche.ars@emarche.it

3 Contesto di riferimento

3.1 Contesto dei servizi

L'ARS Marche, in linea con la sua missione istituzionale, ha recentemente avviato un'iniziativa per definire un modello regionale di sanità digitale basato su cinque principi:

- Governance;
- Integrazione;
- Conformità normativa;
- Sicurezza;
- Resilienza delle infrastrutture e dei servizi.

Le azioni strategiche contemplate dall'iniziativa sono:

1. Sviluppo di un piano generale e di successive e conseguenti iniziative operative, in linea con le strategie nazionali e regionali in tema di sicurezza digitale che comprenda tutti gli Enti del SSR, il Dipartimento salute e l'ARS;
2. Implementazione di misure organizzative e tecniche anche attraverso l'utilizzo di metodologie e tecnologie integrate di sicurezza informatica, che coinvolgano tutti gli Enti del SSR, in grado di assicurare pratiche di governance, conformità normativa, sicurezza e resilienza dei servizi di sanità digitale;
3. mettere a disposizione del SSR un team di risposta agli incidenti (SOC) che supporti i sistemi IT, IoT, OT e medicali coordinato con il CSIRT e il SOC della Regione Marche;
4. sostenere una visione armonizzata della sanità digitale attraverso la supervisione, il monitoraggio e il supporto alla realizzazione del complesso delle azioni relative alla sanità digitale

Il progetto dell'ARS ha l'obiettivo di gestire il nuovo e complesso contesto della sicurezza digitale dei servizi sanitari all'interno dell'intero ecosistema tecnologico sanitario regionale e secondo le necessità dei progetti PNRR avviati e in corso di attivazione nel settore della sanità digitale e di assicurare, in questo contesto, la conformità normativa alle norme cogenti di tutti gli Enti sanitari della Regione Marche.

Il Progetto di Sicurezza di ARS Marche si pone l'obiettivo di rafforzare il governo e la maturità di Sicurezza e Data Protection di tutto l'ecosistema della sanità digitale regionale, ossia garantire Riservatezza, Integrità e Disponibilità e Resilienza del dei servizi e del patrimonio informativo.

Questo modello richiede e prevede l'adozione di un approccio nuovo che contempli elementi di novità rispetto al passato così da rispondere alle mutate esigenze di contesto (normativo in primis), garantendo al contempo la continuità di quanto avviato.
Inoltre, le sfide a cui si è chiamati a rispondere richiedono l'adozione di una visione strategica di lungo periodo e la definizione di piani tattici con risultati nel medio-breve.

3.2 Contesto tecnico ed operativo

Per tale fornitura non sono individuati specifici vincoli di tipo tecnico ed operativo.
In termini di requisiti specifici per l'esecuzione delle attività oggetto dei servizi richiesti si rimanda ai requisiti trasversali previsti per l'Accordo Quadro.
Le attività verranno condotte all'interno di eventuali gruppi di lavoro costituiti dagli interlocutori istituzionali nell'ambito di ARS Marche.

3.3 Contesto Economico – Finanziario

L'Amministrazione potrebbe ricorrere in tutto o in parte, a forme di finanziamento con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC.

4 Ambiti funzionali oggetto di intervento

4.1 Obiettivi e benefici da perseguire

In linea con quanto descritto in precedenza, è stato individuato, nell'ambito del Lotto 2- Servizi di Compliance e controllo dell'Accordo Quadro, avente ad oggetto per l'affidamento di servizi di sicurezza da remoto, di compliance e controllo per le Pubbliche Amministrazioni, il seguente obiettivo di sintesi, che ricade nel più ampio programma di attuazione delle iniziative in ambito Progetto di Sicurezza:

- Obiettivo: individuare le linee strategiche in materia di sicurezza ICT, definire e monitorare le relative azioni strategiche adottate, al fine di realizzare un "progetto di sicurezza" unitario e coerente all'interno dell'ecosistema di ARS Marche (L2.S16)

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
	NAD
	Musei
	Siope+
DATI	Agricoltura, pesca, silvicoltura e prodotti alimentari
	Economia e finanze
	Istruzione, cultura e sport
	Energia
	Ambiente
	Governo e Settore pubblico

		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
		Salute
		Tematiche internazionali
		Giustizia e sicurezza pubblica
		Regioni e città
		Popolazione e società
		Scienza e tecnologia
		Trasporti
INFRASTRUTTURE		Data center e Cloud
		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 all'interno del sistema Comunale*

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:

SERVIZI RICHIESTI				
ID	**NOME SERVIZIO**	**VOCE DI COSTO**	**QUANTITA'**	**IMPORTO**
L2.S16	Security Strategy (L2.S16)	L2.S16 - gg/p Team ottimale	860	**215.000 €**
			TOTALE	**215.000 €**

5.1 Dettaglio dei servizi richiesti

5.1.1 L2.S16 - Security Strategy

5.1.1.1 Descrizione e caratteristiche del servizio

Macro-Attività	Attività	Deliverable
Classificazione degli asset e definizione dei sistemi critici	Analisi e classificazione degli asset IT e Medical Device attraverso la definizione di un modello strutturato basato sul livello di criticità rappresentato dalla potenziale perturbazione del servizio a cui l'asset si riferisce. A tal fine verranno sfruttate le risultanze dell'azione di "discovery" del collector Armis installato nel perimetro del Data Center Sanzio. Individuazione della relazione degli asset con i sistemi applicativi e relazione di quest'ultimi ai servizi di sanità digitale. Implementazione di un framework di valutazione della criticità, che tenga conto del servizio, del sistema applicativi e del ruolo dell'asset nel sistema applicativo finalizzato a supportare una gestione efficace dei rischi e delle priorità di intervento su base servizio. La criticità di un dispositivo sarà valutata in base al livello di perturbazione del servizio e agli impatti che esso può determinare a livello di potenziali danni al paziente, a livello economico, e di erogazione dei servizi (liste di attesa)	Documento di Tassonomia degli asset IT e Medical Device. Framework dei Criteri per la valutazione della criticità.
Piano strategico	Analisi della postura di sicurezza dei servizi basata sui rischi rilevati nei sistemi applicativi, a sua volta valutati secondo la classificazione del rischio cyber dei dispositivi che costituiscono il sistema applicativo. La definizione del perimetro degli asset e l'individuazione dei dispositivi sarà realizzata utilizzando il collector Armis presente nel Data Center Sanzio.	Toolkit di supporto alla Roadmap strategica.

Procedure per la gestione della sicurezza e resilienza dei sistemi critici	Miglioramento dei processi e dell'organizzazione attraverso attività di formalizzazione di un processo per la gestione della sicurezza e resilienza dei sistemi critici in funzione delle risultanze e delle vulnerabilità emerse dalle attività del Piano Strategico.	Documenti di processo di gestione della sicurezza e resilienza dei sistemi critici.
Procedure per la gestione di identità e accessi dei sistemi critici	Miglioramento dei processi e dell'organizzazione attraverso attività di formalizzazione di un processo per la gestione delle identità digitali, in particolare sulla gestione degli accessi amministrativi e sulla relativa revisione degli accessi.	Documenti di processo di gestione delle identità digitali e ciclo di vita degli accessi dei sistemi critici.

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

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 marzo 2025 per una durata massima di 9 mesi.

5.2 Organizzazione e figure di riferimento dell'amministrazione

Si riportano di seguito il personale principale di riferimento dell'Amministrazione con i relativi ruoli/responsabilità.

STRUTTURA	FIGURE DI RIFERIMENTO
Direttore dell'Agenzia Regionale Sanidaria (ARS) delle Marche	Flavia Carle
Settore HTA, tecnologie biomediche e sistemi informativi (ARS Merche)	Alessandro Giommi
Settore LFussi Informativi e Monitoraggio SSR (ARS Marche)	Marco Pompili

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	Uffici interessati	Ambiti di servizio	Numero Key user coinvolti	Numero Volumi
L2.S16	Security Strategy (L2.S16) - Classificazione degli asset e definizione dei sistemi critici	100	**>5**	**>5**	**>15**	**N/A**
L2.S16	Security Strategy (L2.S16) - Piano strategico	460	**>5**	**>5**	**>15**	**N/A**
L2.S16	Security strategy (L2.S16) - Procedure per la gestione della sicurezza e resilienza dei sistemi critici	140	**>5**	**>5**	**>15**	**N/A**
L2.S16	Security Strategy (L2.S16) - Procedure per la gestione di identità e accessi dei sistemi critici	160	**>5**	**>5**	**>15**	**N/A**

6.2 Elementi qualitativi dei servizi

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

Si riportano di seguito i principali riferimenti alla normativa regionale, nazionale ed internazionale in ambito Sicurezza e Privacy con riferimento al perimetro del presente Piano dei fabbisogni:

- Regolamento Europeo in materia di protezione dei dati personali ("GDPR") e Decreto Legislativo 10 agosto 2018, n. 101, che hanno completamente cambiato il paradigma di conformità alla normativa privacy e che pertanto richiedono un grosso lavoro di analisi e di adeguamento;
- Misure di Sicurezza AgID che prevedono l'esecuzione di un'analisi dell'infrastruttura informatica al fine di garantire la conformità ai livelli previsti dall'AgID;
- Strategia Cloud Italia che prevede nuovi livelli di adeguamento per le infrastrutture digitali e per i servizi Cloud per la pubblica amministrazione, fino al completamento della migrazione dei servizi presso il PSN (Polo Strategico Nazionale) o altro Cloud Provider qualificato entro il 30 G.

6.3 Pianificazione dei servizi

La durata ipotizzata per la fornitura è di 9 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 sui mesi previsti, con indicazione dei servizi attivati per gli obiettivi in ambito del presente piano dei fabbisogni.

	Marzo 25	Aprile 25	Maggio 25	Giugno 25	Luglio 25	Agosto 25	Settembre 25	Ottobre 25	Novembre 25	Dicembre 25

• Servizi L2.S16 per la definizione di:
  • Classificazione degli asset e definizione dei sistemi critici
  • Piano strategico
  • Procedure per la gestione della sicurezza e resilienza dei sistemi critici
  • Procedure per la gestione di identità e accessi dei sistemi critici										