ACCORDO QUADRO PER LA FORNITURA DI **SERVIZI CLOUD IAAS E PAAS** IN UN MODELLO DI EROGAZIONE PUBBLICO NONCHÉ PER LA PRESTAZIONE DI SERVIZI CONNESSI, SERVIZI PROFESSIONALI DI SUPPORTO ALL'ADOZIONE DEL CLOUD, SERVIZI PROFESSIONALI TECNICI PER LE PUBBLICHE AMMINISTRAZIONI

ID 2213 - LOTTO 10

PIANO DEI FABBISOGNI
ARES MULTIMISURA 1.2

INDICE

1. CONTESTO

In coerenza con gli obiettivi della prima delle sei "Mission" del PNRR (Digitalizzazione ed Innovazione), e nello specifico degli "Obiettivi Italia Digitale 2026" – "Obiettivo 3 – Cloud e Infrastrutture Digitali", è stato pubblicato, sulla piattaforma "PA digitale 2026", l'Avviso del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri, dedicato sia alla Misura 1.1 "Infrastrutture digitali" che alla Misura 1.2 "Abilitazione al cloud per le PA locali".

L'Avviso ha una dotazione finanziaria complessiva pari a 200 milioni di euro, suddivisa in parti uguali tra le due misure. Il bando multimisura 1.1 e 1.2 "Infrastrutture digitali e abilitazione al cloud" prevede quindi fondi per supportare la migrazione in Cloud dei dati e sistemi informativi delle Aziende Sanitarie Locali (ASL) e delle Aziende Ospedaliere (AO). Con riferimento al contesto organizzativo del Sistema Sanitario della Regione Sardagna, le aziende ospedaliere convolte sono due di fascia 500-1000 posti letto, una di fascia 0-500 posti letto. Le ASL coinvolte sono sette nella fascia 0-500.000 assistiti, una nella fascia 500.000-1.000.000 assistiti. L'Azienda Regionale Emergenza Urgenza Sardegna (AREUS) rientra nella fascia di oltre un milione di assistiti.

Azienda	ASL 01	ASL 02	ASL 03	ASL 04	ASL 05	ASL 06	ASL 07	ASL 08	AOU SS	AOU CA	ARNAS	AREUS
PL\Assistiti	31.450	161.192	154.873	56.938	160.031	97.809	125.430	560.453	507	467	585	1.648.176

In questo contesto, ARES, l'Azienda Regionale della Salute istituita con la Legge Regionale 11 settembre 2020, n. 24 la quale legge le attribuisce in maniera centralizzata la gestione delle infrastrutture di tecnologia informatica, connettività, sistemi informativi e flussi dati in un'ottica di omogeneizzazione e sviluppo del sistema ICT, sta coordinando la contrattualizzazione dei servizi di migrazione ambito delle richieste delle amministrazioni.

Tale adesione prevede la migrazione verso cloud qualificato di servizi richiesti dalle amministrazioni e delle applicazioni ad essi collegate, secondo la misura 1.2.

2. OGGETTO E IMPORTO

Nel presente paragrafo è indicato**l'elenco dei singoli servizi**che l'Amministrazione intende acquisire**, sulla base di quelli indicati nell'Accordo Quadro**:

- **FASE M1: SOLUTION DESIGN E ARCHITECTURE**
  1) **Disegno workload (M1.1):** definire, a partire dalla lista degli applicativi, i relativi workload che andranno implementati in cloud.
  2) **Architettura cloud (M.1.2):** progettare l'architettura logica e fisica delle risorse che verranno utilizzate dai workload.
- **FASE M2: IMPLEMENTAZIONE MIGRAZIONE**
  3) **Configurazione ambienti (M2.1):** configurare le risorse cloud considerando aspetti quali la scalabilità e le policy di sicurezza.
  4) **Trasferimento dati (M2.2)**: trasferimento dei dati dai sistemi source ai sistemi target, utilizzando opportune tecniche e strumenti. Si intende incluso il trasferimento o la riconfigurazione delle componenti infrastrutturali, architetturali e\o applicative necessarie, oltre che il collaudo dei servizi sugli ambienti target.
- **FASE M3: SECURITY**
  5) **Definizione policy di sicurezza (M3.1):** implementazione di policy di sicurezza al fine di prevenire data leakage , un controllo debole degli accessi, attacchi DDoS, data breaches , la perdita di dati e garantire una corretta gestione delle identità e della privacy.

Le motivazioni contrattuali e/o organizzative che sottendono tale scelta sono le seguenti:

L'Amministrazione, con l'obiettivo di mettere in sicurezza i propri servizi e rinnovare l'infrastruttura, ritiene necessario procedere alla migrazione di servizi su cloud, sfruttando i servizi IaaS offerti da OCI come piattaforma più adeguata per le esigenze dell'Amministrazione. Considerate le stringenti tempistiche dettate dal bando multimisura, l'Amministrazione ritiene opportuno il coinvolgimento del Fornitore per la progettazione e l'esecuzione della migrazione verso OCI, come rafforzamento delle risorse e delle competenze necessarie per garantire il successo del progetto nei tempi previsti.

Si ritiene inoltre necessario, dato il cambio di paradigma da on premise a cloud, la revisione e il rafforzamento della postura di sicurezza sul nuovo tenant, per il quale si richiede supporto al Fornitore come esperto di materia.

Non si ritiene necessaria invece, in questa fase, l'acquisizione di servizi di monitoraggio, capacity planning, gestione incident e training, ritenendo sufficienti le competenze e risorse interne all'Amministrazione in prima fase della migrazione.

A fronte, quindi, dei servizi scelti, è riportato nel seguito indicazione del fabbisogno stimato (tipologia, quantità e caratteristiche dei singoli servizi)**:**

FASE: M1	**SOLUTION DESIGN E ARCHITECTURE**		
Servizio	**Descrizione**	**Metrica**	**Quantità**
M1.1	**Disegno Workload**: definire, a partire dalla lista degli applicativi, i relativi workload che andranno implementati in cloud.	GG/Persona Team Ottimale	60
M1.2	**Architettura cloud:** progettare l'architettura logica e fisica delle risorse che verranno utilizzate dai workload.	GG/Persona Team Ottimale	120

FASE: M2	IMPLEMENTAZIONE MIGRAZIONE		
Servizio	**Descrizione**	**Metrica**	**Quantità**
M2.1	**Configurazione ambienti:** configurare le risorse cloud considerando aspetti quali la scalabilità e le policy di sicurezza	GG/Persona Team Ottimale	200
M2.2	**Trasferimento dati:** trasferimento dei dati dai sistemi source ai sistemi target, utilizzando opportune tecniche e strumenti. Si intende incluso il trasferimento o la riconfigurazione delle componenti infrastrutturali, architetturali e\o applicative necessarie, oltre che il collaudo dei servizi sugli ambienti target.	GG/Persona Team Ottimale	1300

FASE: M3	SECURITY		
Servizio	**Descrizione**	**Metrica**	**Quantità**
M3.1	**Definizione policy di sicurezza**: implementazione di policy di sicurezza al fine di prevenire data leakage, un controllo debole degli accessi, attacchi DDoS, data breaches, la perdita di dati e garantire una corretta gestione delle identità e della privacy.	GG/Persona Team Ottimale	400

Per la realizzazione del presente intervento, l'importo contrattuale complessivo è di**settecentoquarantunomila cinquecento quaranta setteeuro e venti centesimi di euro (741.547,20€)IVA esclusa.**

3. ATTIVAZIONE, DURATAE LUOGO DEL SERVIZIO

L'attivazione del servizio prevista indicativamente per il **01/06/2024**.

Il Contratto Esecutivo avrà una durata di **12 mesi** decorrenti dalla data di attivazione del servizio.

Le attività dovranno essere completate entro il 24/10/2024 in coerenza con le scadenze del finanziamento ricevuto dagli enti con misura 1.2 del bando multimisura PNRR.

Le prestazioni contrattuali dovranno essere svolte presso la sede del Fornitore e/o presso le specifiche sedi dell'Amministrazione. Le sedi effettive e puntuali per l'erogazione di ciascun servizio/attività saranno indicate dall'Amministrazione a seconda della modalità di erogazione dei servizi.

4. DESCRIZIONE DEI SINGOLI SERVIZI

I servizi oggetto del presente piano dei fabbisogni sono utilizzati dagli enti come raffigurato nella tabella seguente:

SERVIZIO	APPLICATIVI	ASL 01	ASL 02	ASL 03	ASL 04	ASL 05	ASL 06	ASL 07	ASL 08	AOU CA	AOU SS	ARNAS	AREUS
ANAGRAFE NAZIONALE ASSISTIBILI	XMPI	X	X	X	X	X	X	X	X				
EDUCAZIONE CONTINUA IN MEDICINA	SAREC ECM	X	X	X	X	X	X	X	X	X	X	X	X
SORVEGLIANZA, PREVENZIONE E TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	SISAR SPRESAL NPC	X	X	X	X	X	X	X	X				
PROTOCOLLO	SISAR PROTOCOLLO	X	X	X	X	X	X	X	X	X	X	X	X
GESTIONE DOCUMENTALE	SISAR ATTI	X	X	X	X	X	X	X	X	X	X	X	X
PERSONALE	SISAR HR	X	X	X	X	X	X	X	X	X	X	X	X
CONTABILITA , BILANCIO E CONTROLLO	SISAR AMC	X	X	X	X	X	X	X	X	X	X	X	X
CONTABILITA , BILANCIO E CONTROLLO	ABACO	X	X	X	X	X	X	X	X				

ACQUISTI	SISAR AMC	x	x	x	x	x	x	x	x	x	x	x	x

Per tali servizi è richiesta la migrazione da parte del Fornitore verso infrastruttura Oracle Cloud, già contrattualizzato tramite AQ Public Cloud Iaas-Paas Lotto 1. Tutte le applicazioni, anche se eroganti servizi a diversi enti, hanno architettura centralizzata, e sono localizzate nel Data Center di Regione Sardegna (CRESSAN). Si prevede la migrazione di tutte le applicazioni su di un unico tenant e la configurazione dei permessi e delle visibilità a livello applicativo.

L'Amministrazione gestirà le attività di Project Management tramite proprie risorse e fornitori già contrattualizzati. Si richiede al Fornitore la disponibilità alla predisposizione della pianificazione delle attivitàdi propria competenza, da approvare da parte dell'Amministrazione e da integrare alla pianificazione già predisposta da parte dell'Amministrazione.

Si consideri che qualunque elemento di pianificazione proposto dal Fornitore dovrà rispettare le seguenti milestone in corrispondenza delle scadenze dettate dal bando multimisura, in particolare:

- Consegna della pianificazione di dettaglio a 10 gg solari dalla data di contrattualizzazione, e approvazione di questa da parte dell'Amministrazione;
- Consegna del documento di progetto della migrazione e dell'architettura di sicurezza entro 1 mese solare dalla data di contrattualizzazione, e approvazione di questi da parte dell'Amministrazione;
- Completamento della migrazione (cutover) entro il 24/10/2024, con approvazione da parte dell'Amministrazione all'esito dei test di validazione della migrazione.

Si specifica che l'Amministrazione potrà richiedere al Fornitore di erogare i servizi di sicurezza anche relativamente ad applicazioni da migrare verso OCI non espressamente incluse nell'elenco (ad esempio in sostituzione, esclusione, aggiunta alle applicazioni indicate sopra), a condizione che, dietro valutazione congiunta dell'Amministrazione e del Fornitore, tale modifica al perimetro sia a parità di effort o comunque inclusa nella quantità di giornate previste.

4.1 FASE M1: SOLUTION DESIGN E ARCHITECTURE

Questa fase rappresenta il primo passaggio di adozione del paradigma cloud e prevede che il Fornitore progetti ed esegua attività specifiche quali il disegno architetturale dei workload con indicazione delle risorse computazionali necessarie alla corretta esecuzione degli stessi.

L'obiettivo generale del Fornitore è quello di supportare l'Amministrazione nel definire la mappatura dei workload sulle tecnologie cloud identificando il miglior modo di migrare gli applicativi, le aree applicative o un intero sistema informativo. Inoltre, il Fornitore dovrà produrre come output uno specifico documento architetturale con evidenza dei flussi dei workload che può soddisfare l'architettura.

Il Fornitore dovrà quindi mettere a disposizione specifiche metodologie e strumenti tecnologici per l'analisi della situazione in essere (AS-IS), la fase di verifica con l'Amministrazione, la produzione dei deliverable di fase, costituita dal disegno dei workload e dall'architettura target.

4.1.1 Disegno dei workload (M1.1)

In prima battuta dovrà essere stilata una lista dei workload necessari a soddisfare i requisiti della strategia di migrazione. Per ogni workload dovrannoessere tracciate le seguenti informazioni:

- il nome ed una breve descrizione del workload con indicati il requisito soddisfatto della strategia di migrazione prevedendo l'indicazione dell'applicazione source ed il sistema informativo di appartenenza (ad es.: sottosistema/area/ambiente funzionale/ isola/…);
- le risorse target di riferimento (VM, piattaforme, DMBS, …) ed i relativi requisiti di performance
- la complessità del workload: numero di utenti, interazioni DB, …
- il referente dell'Amministrazione e/o del Fornitore dell'Amministrazione;
- le interazioni con altri workload;
- la disponibilità del workload su rete privata e\o pubblica.

L'Amministrazione ha già effettuato una prima attività di assessment infrastrutturale e applicativo che ha portato alla definizione del dimensionamento infrastrutturale.Il Fornitore dovrà quindi valutare la validità e la consistenza del documento al fine di poterlo utilizzare compiutamente nel processo di migrazione in cloud, in accordo con l'Amministrazione, ed intraprendere le eventuali azioni di indagine necessarie a completare il documento, dove necesario.

Il documento sarà oggetto di approvazione da parte dell'Amministrazione, vincolante per le fasi successive.

4.1.2 Architettura risorse cloud (M1.2)

Il seguente servizio è finalizzato al disegno di dettaglio delle architetture IaaS e PaaS con cui procedere con la migrazione dei workload.Il Fornitore dovrà identificare per ogni workload l'architettura di riferimento in termini di risorse cloud tenendo in considerazione tutte le interazioni con altri workload.

Per ogni documento di disegno, il Fornitore dovrà tracciare ed inserire almeno le seguenti informazioni:

- Il diagramma architetturale logico;
- Il diagramma architetturale fisico;
- Le modalità/tecniche di backup della piattaforma;
- Le modalità/tecniche per garantire i requisiti di sicurezza;
- Le modalità/tecniche per garantire i requisiti di alta affidabilità e disaster recovery, dove richiesti.

Il Fornitore è obbligato a reperire le informazioni necessarie per la definizione di quanto sopra direttamente dall'Amministrazione e/o dal suo Fornitore di riferimento, oppure dal produttore e/o fornitore stesso dell'applicativo e/o da altre entità pubbliche se coinvolte nella gestione delle infrastrutture e/o delle applicazioni ("società in house", società partecipate, enti consorziati, accordi di servizio, …).

L'Amministrazione anticipa che la strategia di migrazione desiderata è di tipo "re-host / lift & shift" dove il Fornitore lo riterrà tecnicamente applicabile.

A partire dalla strategia di migrazione e dai documenti di disegno dei workload, il Fornitore dovrà, per garantire la completezza della fase, produrre un documento riepilogativo denominato Disegno architetturale complessivo che definisca le risorse cloud necessarie (VM, load balancer, storage, etc) per ciascun workload e le eventuali modalità di interazione. Il documento costituirà una componente fondamentale dell'attuazione del processo di migrazione e dovrà essere elaborato anche a partire dalle informazioni presenti nel Piano dei Fabbisogni e nella documentazione fornita dall'Amministrazione nella fase preliminare e dovrà tenere conto del contesto istituzionale e funzionale in cui si opera.

Il documento dovrà essere elaborato dal Fornitore all'interno del servizio in oggetto e la rendicontazione delle attività connesse è da intendersi ricompresa all'interno del dimensionamento del servizio stesso, senza oneri aggiuntivi per l'Amministrazione. Inoltre, esso dovrà essere mantenuto aggiornato durante tutta l'esecuzione contrattuale, senza

alcun onere aggiuntivo per l'Amministrazione.

Il Fornitore avrà il compito di verificare la validità e la consistenza del documento al fine di poterlo utilizzare compiutamente nel processo di migrazione in cloud, in accordo con l'Amministrazione.

Il documento sarà oggetto di approvazione da parte dell'Amministrazione, vincolante per le fasi successive.

4.2 FASE M2: IMPLEMENTAZIONE MIGRAZIONE

In questo paragrafo viene illustrata la fase migrazione ad ambienti cloud definiti nelle fasi preliminari del processo complessivo idoneo a soddisfare i requisiti dell'Amministrazione. Questa fase rappresenta un passaggio cruciale nell'adozione del paradigma cloud e prevede che il Fornitore implementi gli ambienti necessari ad ospitare i workload e si occupi del trasferimento dei dati dagli ambienti on-premise. Il Fornitore, a prescindere delle modalità di erogazione del servizio, è obbligato a garantire la composizione ottimale del team di lavoro, prevedendo skill di natura eterogenea per garantire la presenza di tutte le competenze tecnologiche necessarie per la migrazione. Nell'implementazione della migrazione il Fornitore dovrà assicurare tutti i processi di comunicazione, collaborazione e integrazione tra la componente relativa alle risorse professionali e tecnologiche e la componente dati. -

Il Fornitore dovrà quindi mettere a disposizione specifiche metodologie e strumenti tecnologici per tracciare l'avanzamento delle attività e raccogliere i deliverable di fase che saranno rispettivamente documenti relativi alle configurazioni di dettaglio delle risorse per la fase M2.1 e documenti sulle configurazioni di dettaglio delle basi di dati M2.2.

4.2.1 Configurazione ambienti (M2.1)

In prima battuta il Fornitore dovrà stilare una lista delle risorse tecnologiche necessarie a soddisfare i requisiti dei workload.

Per ogni risorsa configurata il Fornitore dovrà tracciare ed inserire almeno le seguenti informazioni:

- il nome ed una breve descrizione del workload di riferimento;
- il nome ed una breve descrizione della risorsa
- le configurazioni della risorsa (CPU, RAM, Storage, regole di bilanciamento, tunnel vpn, etc)
- La capacità di scalabilità della risorsa con indicazioni delle API per la gestione automatica dello scaling
- il referente dell'Amministrazione e/o del Fornitore dell'Amministrazione;
- Descrizione della modalità di phase out per la risorsa (es. configurazione da esportare, dati da esportare, formato dei dati per successiva implementazione, etc);
- le interazioni e le dipendenze da altre risorse.

Il Fornitore è obbligato a reperire le informazioni necessarie per la definizione di quanto sopra direttamente dall'Amministrazione e/o dal suo Fornitore di riferimento, oppure dal produttore e/o fornitore stesso dell'applicativo e/o da altre entità pubbliche se coinvolte nella gestione delle infrastrutture e/o delle applicazioni ("società in house", società partecipate, enti consorziati, accordi di servizio, …).La costruzione di questo elenco potrà seguire un approccio iterativo ed incrementale, in cui si collezionano inizialmente le risorse di cui si ha maggiore evidenza e si integra successivamente la lista con le risorse per le quali sono necessari prerequisiti in termini di risorse dipendenti.

Il documento che raccoglie le configurazioni delle risorse costituirà l'assessment delle risorse cloud e costituisce il deliverable di fornitura del servizio. Per la corretta stesura del documento il team di lavoro avrà disponibile i documentirelativi ai workload e tutte le informazioni presenti nel Piano dei Fabbisogni e nella documentazione fornita dall'Amministrazione nella fase preliminare e dovrà tenere conto del contesto istituzionale e funzionale in cui si opera.

Il documento dovrà essere elaborato dal Fornitore all'interno del servizio in oggetto e la rendicontazione delle attività connesse è da intendersi ricompresa all'interno del dimensionamento del servizio stesso, senza oneri aggiuntivi per l'Amministrazione. Inoltre, esso dovrà essere mantenuto aggiornato durante tutta l'esecuzione contrattuale, senza alcun onere aggiuntivo per l'Amministrazione.

Il Fornitore ha quindi in carico, a valle dell'approvazione del documento di configurazione da parte dell'Amministrazione, l'effettiva predisposizione degli ambienti, la configurazione di tutte le risorse e delle loro interazioni, il testing delle configurazioni ed eventuali successive modifiche alla configurazione resesi necessarie nella fase di collaudo dei servizi, sull'ambiente fornito tramite opportune credenziali fornite dall'Amministrazione.

4.2.2 Trasferimento dati (M2.2)

Il Fornitore a valle della configurazione delle risorse, o congiuntamente in base alla modalità prevista di migrazione, ha in carico la migrazione di tutte le componenti necessarie al funzionamento del servizio, siano esse applicative, database, di sicurezza, infrastrutturali o architetturali. La eventuale configurazione o upgrade è a carico del Fornitore dove necessaria per garantire il funzionamento dei servizi sul nuovo ambiente. Si consideri l'attività di migrazione a pari perimetro di funzionalità dei servizi, dove tecnicamente possibile adottando framework "re-host / lift & shift".

Eventuali configurazioni successive delle applicazioni migrate anche con modalità lift & shift sono a carico del Fornitore (es: riconfigurazione dei flussi applicativi, modifica IP\URL configurate, etc)

Il processo di migrazione dei dati si articola tipicamente secondo queste fasi, a carico del Fornitore:

1. preparazione della migrazione
2. validazione dei dati nel sistema sorgente
3. creazione dello schema dei dati nel sistema destinazione
4. mappatura delle strutture dati del sistema sorgente nel sistema destinazione
5. conversione e trasferimento dei dati dal sistema sorgente al sistema destinazione
6. validazione dei dati migrati nel sistema di destinazione
7. dismissione del sistema sorgente.

È di cruciale importanza implementare un corretto processo di migrazione dei dati, per cui è opportuno che il Fornitore segua delle best practices per evitare che si verifichino perdita dei dati, inconsistenza dei dati, lunghi periodi di downtime, corruzione dei dati e interferenze. Per tali motivi il Fornitore nelle fasi preparatorie della migrazione delle basi di dati seguirà specifiche pratiche tra cui:

- Esecuzione di un backup completo del database;
- Utilizzo, dove possibile, di connessione diretta al cloud, per il trasferimento dei dati;
- Utilizzare livelli di connessioni e metodi di autenticazione sicura agli ambienti sorgente e target;
- Proteggere i dati sorgente da scritture accidentali durante il processo di migrazione;

Terminato il trasferimento dei dati sugli ambienti target, il fornitore dovrà validare il trasferimento verificando il corretto funzionamento dei workload dipendenti dalla base dati migrata, ed effettuando opportune validazioni di performance, ad esempio effettuando e misurando query. Il Fornitore dovrà effettuare anche tecniche avanzate di validazione delle basi dati migrate tra cui la riconciliazione al fine di assicurare che il numero di entità sorgenti sia uguale al numero di entità target, oppure la validazione orizzontale dei valori, nel caso in cui la transizione abbia previsto dei momenti di trasformazione, arricchimento o consolidamento dei dati migrati.

Il Fornitore dovrà produrre per ogni base dati migrata un deliverable di fornitura, il documento dovrà tracciare ed

inserire almeno le seguenti informazioni:

- gli schemi dei dati sorgenti;
- gli schemi per le basi dati target che ospiteranno i dati;
- le attività che incidono sui dati sorgente prima della migrazione effettiva, tra cui attività di normalizzazione, modifiche alle tabelle, consolidamenti e arricchimenti;
- le modalità/tecniche implementate per garantire coerenza ed evitare la corruzione dei dati;
- le modalità/tecniche di migrazione;
- i workload dipendenti dalla base di dati migrata;
- tecniche e risultati delle attività di validazione.

Il Fornitore è obbligato a reperirele informazioni necessarie per la definizione di quanto sopra direttamente dall'Amministrazione e/o dal suo Fornitore di riferimento, oppure dal produttore e/o fornitore stesso dell'applicativo e/o da altre entità pubbliche se coinvolte nella gestione delle infrastrutture e/o delle applicazioni ("società in house", società partecipate, enti consorziati, accordi di servizio, …).Per la corretta stesura del documento il team di lavoro avrà disponibile i documenti relativi ai workload e tutte le informazioni presenti nel Piano dei Fabbisogni e nella documentazione fornita dall'Amministrazione nella fase preliminare e dovrà tenere conto del contesto istituzionale e funzionale in cui opera.

Il documento dovrà essere elaborato dal Fornitore all'interno del servizio in oggetto e la rendicontazione delle attività connesse è da intendersi ricompresa all'interno del dimensionamento del servizio stesso, senza oneri aggiuntivi per l'Amministrazione. Inoltre, esso dovrà essere mantenuto aggiornato durante tutta l'esecuzione contrattuale, senza alcun onere aggiuntivo per l'Amministrazione.

Nel caso in cui l'Amministrazione abbia provveduto in autonomia a migrare i dati ed abbia prodotto opportuni documenti di deliverable, il Fornitore, su richiesta dell'Amministrazione, avrà il compito di verificarne la validità e la consistenza.

4.3 FASE M3: SECURITY

In questo paragrafo vengono illustrate le modalità con cui il Fornitore dovrà garantire l'adozione delle più opportune policy di sicurezza per gli ambienti cloud implementati. Gli aspetti di sicurezza, in uno scenario di condivisione delle risorse fisiche, risultano molto critiche pur con la garanzia di segregazione dei tenant da parte dei CSP. Problematiche come data leakage, controllo debole degli accessi, attacchi DDoS, data breaches, perdita di dati, la gestione delle identità e della privacy devono essere tenute in forte considerazione. Per mitigare questi rischi, le piattaforme cloud forniscono un insieme di policy, controlli e regole che assieme proteggono l'infrastruttura con misure specificatamente destinate alla sicurezza.

Il fornitore nel definire le policy di un ambiente cloud dovrà tener contro dello stato dell'infrastruttura in termini di workload M1.1 e basi dati implementate M2.2 e dovrà avere conoscenza delle configurazioni delle risorse di cui ai deliverable M2.1 nonché dell'intera architettura e interazioni tra risorse M1.2.

Il Fornitore dovrà quindi mettere a disposizione specifiche metodologie e strumenti tecnologici per tracciare le attività svolte e raccogliere i deliverable di fase che saranno rispettivamente documenti relativi alle policy di sicurezza implementate.

4.3.1 Definizione policy di sicurezza (M3.1)

In prima battuta il Fornitore dovrà analizzare lo stato dell'ambiente cloud in termini architetturali e dei workload implementati. Definito lo stato delle risorse, il Fornitore può essere ingaggiato per implementare policy di sicurezza

relative agli applicativi oppure relative ai dati.

Per ogni applicativo il Fornitore dovrà gestire la sicurezza per almeno i seguenti aspetti:

- mettere in sicurezza tutte le risorse, non solo quelle esposte verso l'esterno, edgelayer (es. utilizzando una connessione TLS sicura anche nelle comunicazioni con altri applicativi)
- proteggere i dati memorizzati, data in rest, in qualsiasi forma digitale (es. database, data warehouse, spreadsheet, archivi, nastri, backup, dispositivi mobile, ecc.) attraverso la cifratura
- mitigare attacchi DDoS utilizzando il livello di network della piattaforma cloud;
- utilizzare una lista di accessi sicuri per reti, applicativi e dati
- eseguire un'analisi periodica delle vulnerabilità anche attraverso penetration test
- utilizzare twofactor authentication (2fa) e configurare un meccanismo di single sign on (SSO)
- installare antivirus e anti-malware per i nodi e il networking
- abilitare il monitoring ed il logging per il networking, gli applicativi ed i dati
- connettere ambiente on-premises con ambiente cloud utilizzando sempre un link dedicato ed una VPN sul link pubblico.

Per ogni base di dati il Fornitore dovrà gestire la sicurezza per almeno i seguenti aspetti:

- cifratura dei dati memorizzati nei dischi utilizzando ad esempio AES (Advanced Encryption Standards) 256
- utilizzo di uno strumento di gestione delle chiavi per la memorizzazione dei dati sensibili come credenziali, token per le API, certificati SSL, chiavi private
- controllare gli accessi sulla base del ruolo degli utenti
- proteggere tutti i canali di comunicazione con un certificato SSL

Per le attività di definizione delle policy di sicurezza e per ogni policy, il Fornitore dovrà produrre un deliverable che riporti almeno le seguenti informazioni:

- il nome ed una breve descrizione dell'applicazione o della base di dati messa in sicurezza;
- il nome ed una breve descrizione della policy implementata;
- le configurazioni di dettaglio in relazione a quanto espresso in precedenza;
- il luogo di custodia delle chiavi, token, password o altri parametri relativi alla policy;
- il referente dell'Amministrazione e/o del Fornitore dell'Amministrazione;
- le interazioni e le dipendenze da altre risorse.

Nel caso in cui l'Amministrazione abbia usufruito dei Servizi di Supporto di cui ai Lotti 2-6, potranno essere utilizzate tutte le informazioni inserite e derivanti dai relativi deliverable di fornitura di tali servizi. In caso contrario o in aggiunta se necessario, il Fornitore è obbligato a reperirle direttamente dall'Amministrazione e/o dal suo Fornitore di riferimento, oppure dal produttore e/o fornitore stesso dell'applicativo e/o da altre entità pubbliche se coinvolte nella gestione delle infrastrutture e/o delle applicazioni ("società in house", società partecipate, enti consorziati, accordi di servizio, …).

I documenti che raccolgono le configurazioni delle policy di sicurezza costituiranno l'assessment di security. Per la corretta stesura dei documenti il team di lavoro avrà disponibile i documenti relativi ai workload e tutte le informazioni nei documenti di configurazione risorse e nella documentazione fornita dall'Amministrazione nella fase preliminare e dovrà tenere conto del contesto istituzionale e funzionale in cui opera.

I documenti dovranno essere elaborati dal Fornitore all'interno del servizio in oggetto e la rendicontazione delle attività connesse è da intendersi ricompresa all'interno del dimensionamento del servizio stesso, senza oneri aggiuntivi per l'Amministrazione. Inoltre, esso dovrà essere mantenuto aggiornato durante tutta l'esecuzione contrattuale, senza alcun onere aggiuntivo per l'Amministrazione.

Nel caso in cui l'Amministrazione disponga già di documenti di policy di sicurezza, il Fornitore, su richiesta dell'Amministrazione, avrà il compito di verificarne la validità e la consistenza al fine di poterlo utilizzare compiutamente nel processo di migrazione in cloud, in accordo con l'Amministrazione.

Il Fornitore ha quindi in carico, dopo l'approvazione della documentazione da parte dell'Amministrazione, l'implementazione delle policy di sicurezza che saranno oggetto di controllo e validazione da parte dell'Amministrazione.

5. SUBAPPALTO

Il Fornitoreche si sia riservato la possibilità di ricorrere al subappalto deve indicare, nel **Piano Operativo**, la quota e le prestazioni da subappaltare. A tal fine si rammenta che Il subappalto è ammesso in conformità all'art. 105 del D. Lgs. 50/2016, vigente *ratione temporis*.

6. PNRR

PRESCRIZIONI SPECIFICHE PER AFFIDAMENTI AFFERENTI GLI INVESTIMENTI PUBBLICI FINANZIATI, IN TUTTO O IN PARTE, 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

Tenuto conto anche della natura bifasica dell'Accordo Quadro e delle condizioni stabilite nell'ambito di quest'ultimo, sulla base delle quali sono state formulate le offerte di prima fase, ai sensi dell'art. 47, comma 7, del D.L. 77/2021, convertito in L. 108/2021, non troveranno applicazione, nell'ambito del presente affidamento, le previsioni di cui al comma 4 del medesimo articolo.

Unitamente al Piano Operativo, ciascuna impresa del RTI dovrà produrre apposita dichiarazione, attestante quanto segue:

1. che la propria azienda occupa oltre 50 dipendenti, allegando:
   a) copia dell'ultimo rapporto sulla situazione del personale maschile e femminile redatto ai sensi dell'articolo 46 del d.lgs. n. 198/2006, con attestazione della sua conformità a quello eventualmente già trasmesso alle rappresentanze sindacali aziendali e ai consiglieri regionali di parità ovvero, in mancanza, con attestazione della sua contestuale trasmissione alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità. Tale attestazione dovrà essere sottoscritta dal legale rappresentante (o persona munita di comprovati poteri di firma);
   b) in aggiunta, nel caso in cui non abbia provveduto alla trasmissione del rapporto nei termini indicati dall'articolo 46 del decreto legislativo n. 198/2006
   l'attestazione dell'avvenuta trasmissione dello stesso alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità, in data anteriore a quella di presentazione del Piano Operativo;
   In caso di RTI/Consorzi ordinari o di Consorzi di cui alle lettere b) e c) del Codice, la copia del rapporto e la relativa attestazione dovranno essere prodotte da ciascuna impresa del

RTI/Consorzio o da ciascuna consorziata esecutrice, tenuta alla redazione del rapporto ai sensi dell'art. 46 del D.lgs. 198/2006.

c) dichiarazione sull'aver assolto agli obblighi di cui alla legge 68/1999
d) di impegnarsi, in caso di aggiudicazione, a consegnare alla stazione appaltante, entro 6 mesi dalla stipula del contratto la relazione relativa all'assolvimento degli obblighi di cui alla medesima legge n. 68/1999 e alle eventuali sanzioni e provvedimenti disposti a loro carico nel triennio antecedente la data di presentazione del Piano Operativo. La relazione dovrà essere trasmessa entro il medesimo termine anche alle rappresentanze sindacali aziendali.

Ovvero in alternativa

2. che la propria azienda occupa un numero di dipendenti pari o superiore a 15 e inferiore a 50:
   a) di impegnarsi a predisporre una relazione di genere sulla situazione del personale maschile e femminile in ognuna delle professioni ed in relazione allo stato di assunzioni, della formazione, della promozione professionale, dei livelli, dei passaggi di categoria o di qualifica, di altri fenomeni di mobilità, dell'intervento della Cassa integrazione guadagni, dei licenziamenti, dei prepensionamenti e pensionamenti, della retribuzione effettivamente corrisposta che dovrà essere consegnata, in caso di aggiudicazione, alla stazione appaltante, nonché alle rappresentanze sindacali aziendali, alla consigliera e al consigliere regionale di parità, entro 6 mesi dalla stipula del contratto;
   b) che, nei dodici mesi antecedenti alla presentazione del Piano Operativo, non ha violato l'obbligo di cui all'art. 47, comma 3, del D.L. 77/2021, convertito in L. n. 108/2021;
   c) di impegnarsi, in caso di aggiudicazione, a consegnare alla stazione appaltante, entro 6 mesi dalla stipula del contratto la relazione relativa all'assolvimento degli obblighi di cui alla medesima legge n. 68/1999 e alle eventuali sanzioni e provvedimenti disposti a loro carico nel triennio antecedente la data di presentazione del Piano Operativo. La relazione dovrà essere trasmessa entro il medesimo termine anche alle rappresentanze sindacali aziendali.
   d) di aver assolto agli obblighi di cui alla legge n. 68/1999;

ovvero, in alternativa

3. che la propria azienda ha un numero di dipendenti inferiore a 15 e non è, pertanto, tenuta al rispetto di quanto prescritto dall'art.47, comma 2, 3 e 3-bis, del DL. n. 77/2021, convertito in L. 108/2021.

L'Amministrazione, ai sensi di quanto previsto dall'art. 47, comma 9 del D.L. n. 77/2021, convertito in l. 108/2021, pubblica sul profilo di committente, nella sezione "Amministrazione Trasparente", i rapporti e le relazioni di cui ai commi 2, 3 e 3-bis del medesimo articolo, ai sensi dell'articolo 29 del Codice. L'Amministrazione procederà anche con gli ulteriori adempimenti di cui al citato articolo 47 comma 9, D.L. 77/2021, convertito in l. 108/2021.