ARES Sardegna

CONSIP - ID 2213

Accordo Quadro per la Fornitura di Servizi Cloud IaaS e PaaS in un Modello di Erogazione Pubblico

LOTTO 10

PIANO OPERATIVO

Maggio 2024

D·HUB ENGINEERING

ENGINEERING THE DIGITAL TRANSFORMATION COMPANY

LEONARDO

SMI a new youniverse

SOMMARIO

Autore

RTI Engineering D.HUB S.p.A.

Verifica

RTI Engineering D.HUB S.p.A.

Approvazione/i

RTI Engineering D.HUB S.p.A.

Autorizzazione/i

RTI Engineering D.HUB S.p.A.

DATI ANAGRAFICI AMMINISTRAZIONE RICHIEDENTE

DENOMINAZIONE AMMNISTRAZIONE	Azienda Regionale della Salute (ARES)
INDIRIZZO	Via Piero della Francesca 1
CAP	09047
COMUNE	Selargius
PROVINCIA	Cagliari
REGIONE	Sardegna
CODICE FISCALE	03990570925
CODICE IPA	P65P3X9X
INDIRIZZO MAIL	protocollo@aressardegna.it
PEC	ict.siamministrativi@pec.aressardegna.it

REFERENTE AMMINISTRAZIONE	Cesare Delussu
RUOLO	RUP Contratto
TELEFONO	079-2061962
INDIRIZZO MAIL	sc.siamministrativi@aressardegna.it
MAIL PEC	ict.siamministrativi@pec.aressardegna.it

INTRODUZIONE

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.

SCOPO

Il presente piano operativo ha come scopo la migrazione dei sistemi informativi di ARES (SISAR ATTI, SISAR NPC, SISAR PROTOCOLLO, SISAR AMC Contabilità, SISAR AMC Acquisti, SISAR HR, XMPI, ABACO, SAREC ECM) verso l'infrastruttura Oracle Cloud Infrastructure (OCI), in linea con gli obiettivi della prima Mission del PNRR (Digitalizzazione ed Innovazione) e gli "Obiettivi Italia Digitale 2026" – "Obiettivo 3 – Cloud e Infrastrutture Digitali". L'adesione a questa misura prevede l'utilizzo del finanziamento complessivo di 200 milioni di euro, suddiviso equamente tra le Misure 1.1 e 1.2, per supportare la migrazione in Cloud dei dati e sistemi informativi delle Aziende Sanitarie Locali (ASL) e delle Aziende Ospedaliere (AO).

ARES, in qualità di Azienda Regionale della Salute istituita con la Legge Regionale 11 settembre 2020, n. 24, è responsabile della gestione centralizzata delle infrastrutture tecnologiche, dei sistemi informativi e dei flussi dati per il Sistema Sanitario della Regione Sardegna.

Questo piano operativo mira a facilitare il processo di migrazione verso un cloud qualificato, garantendo una gestione omogenea e sicura delle applicazioni richieste dalle amministrazioni locali. La migrazione, pianificata tra la data dell'ordine e con l'obiettivo di chiudere entro il 24/10/2024, si propone di migliorare l'efficienza, la sicurezza e l'innovazione dei servizi digitali sanitari, contribuendo alla realizzazione degli obiettivi di digitalizzazione previsti dal PNRR.

CAMPO DI APPLICAZIONE

Il campo di applicazione del presente Piano Operativo è definito dalla documentazione ricevuta dall'Amministrazione (indicare i riferimenti della PEC ricevuta) ed in particolar modo nelle informazioni contenute nei file denominati ID 2213 - Piano dei Fabbisogni - ARES Multimisura 1.2 v2.docx e

ARES_AssessmentServizi_v5_VERSO CSP - L10.xlsx, nell'ambito dei quali vengono delineate le modalità previste per la migrazione dei sistemi in uso e viene fornito l'elenco dei sistemi da migrare che riportiamo di seguito

- SISAR ATTI
- SISAR NPC
- SISAR PROTOCOLLO
- SISAR AMC Contabilità
- SISAR AMC Acquisti
- SISAR HR
- XMPI
- ABACO
- SAREC ECM

indicando per ciascuno le principali specifiche per ciascuno di essi come "numero di istanze", "spazio su disco", "RAM", core di processo, "dipendenze e interazioni".

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

ACRONIMI E GLOSSARIO

Indicare le definizioni rilevanti per la fornitura e l'ambito di riferimento delle stesse

DEFINIZIONE/ACRONIMO	DESCRIZIONE ESTESA
AQ	Accordo Quadro
CE	Contratto Esecutivo
GG/PP	Giorni Persona
IAAS	Infrastructure As A Service
ICT, IT	Information and Communication Technology, Information Technology
OT	Offerta Tecnica
PA, PPAA	Pubblica Amministrazione, Pubbliche Amministrazioni
PAAS	Platform As A Service
RTI	Raggruppamento Temporaneo di Imprese

RUAC del CE	Responsabile Unico delle attività contrattuali relativo al Contratto Esecutivo

ORGANIZZAZIONE DEL CONTRATTO ESECUTIVO

Per i servizi in ambito al presente Contratto Esecutivo, il RTI adotterà l'organizzazione come esposta nell'Offerta Tecnica, cui si fa riferimento per maggiori dettagli.

IMPORTO CONTRATTUALE E QUANTITÀ PREVISTE PER I SERVIZI OGGETTO DI FORNITURA

In coerenza con gli approfondimenti intercorsi con l'Amministrazione, l'importo contrattuale è pari a 741.521,19 (settecento quarantuno mila cinquecento ventuno/19 euro) IVA esclusa.

Le tabelle seguenti riportano le quantità proposte per i servizi oggetto di fornitura, comprensive delle relative metriche:

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	80
M1.2	**Architettura cloud:** progettare l'architettura logica e fisica delle risorse che verranno utilizzate dai workload.	GG/Persona Team Ottimale	140

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	190
M2.2	**Trasferimento dati:** trasferimento dei dati dai sistemi source ai sistemi target, utilizzando opportune tecniche e strumenti.	GG/Persona Team Ottimale	967

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	700

DELIVERABLE DELLA FORNITURA

L'elenco dei deliverable previsti nella presente fornitura è sintetizzabile come segue:

- Documento di Disegno Workload
- Documento di Architettura Cloud
- Documento di Configurazione Ambienti
- Documento di Trasferimento Dati e Report di Validazione
- Documento di Policy di Sicurezza
- Pianificazione delle Attività e Documenti di Progetto e Architettura di Sicurezza

Si riporta una descrizione sintetica di ciascun deliverable, che in fase di esecuzione della fornitura e di concerto con l'Amministrazione sarà possibile integrare con ulteriori informazioni ritenute utili. Ciascun deliverable è oggetto di approvazione da parte dell'Amministrazione. Tale approvazione è vincolante per le fasi successive.

M1.1 Disegno Workload		
M1.1	**Documento di disegno del workload**	• Nome e descrizione del workload • Requisiti di performance • Complessità del workload • Interazioni con altri workload • Disponibilità del workload su rete privata e/o pubblica
M1.2 Architettura Cloud		
M1.2	**Documento di architettura cloud**	• Diagramma architetturale logico • Diagramma architetturale fisico • Modalità/tecniche di backup • Modalità/tecniche per garantire i requisiti di sicurezza • Modalità/tecniche per garantire i requisiti di alta affidabilità e disaster recovery
M2.1 Configurazione ambienti		
M2.1	**Documento di configurazione ambienti**	• Nome e descrizione del workload di riferimento • Nome e descrizione della risorsa configurata • Configurazioni della risorsa (CPU, RAM, Storage, ...) • Capacità di scalabilità della risorsa • Modalità di phase out per la risorsa • Interazioni e dipendenze da altre risorse
M2.2 Trasferimento Dati		
M2.2	**Documento di trasferimento dati e report di validazione**	• Schemi dei dati sorgenti • Schemi delle basi dati target • Attività sui dati sorgenti prima della migrazione • Modalità/tecniche di migrazione

		• Modalità\tecniche per garantire coerenza ed evitare la corruzione dei dati (esecuzione a carico di Fornitori terzi) • Tecniche e risultati delle attività di validazione • Workload dipendenti dalla base dati migrata

M3.1 Definizione Policy di Sicurezza		
M3.1	**Documento di policy di sicurezza**	• Nome e descrizione dell'applicazione o della base di dati messa in sicurezza • Nome e descrizione della policy implementata • Configurazioni di dettaglio relative alla sicurezza • Luogo di custodia delle chiavi, token, password • Interazioni e dipendenze da altre risorse

Ai deliverable previsti e sintetizzati nell'elenco e nelle tabelle precedenti, si aggiungono inoltre i documenti di gestione del progetto che vengono richiesti espressamente nel piano dei fabbisogni trasmesso dall'Amministrazione.

Più in specifico:

- **Pianificazione di dettaglio**: prodotta e consegnata dal Fornitore all'Amministrazione a **20 giorni lavorativi** dalla data di contrattualizzazione (piano di lavoro generale, come da capitolato tecnico dell'Accordo Quadro di riferimento)
- Documento di **progetto della migrazione e dell'architettura di sicurezza**: prodotta e consegnata dal Fornitore all'Amministrazione a valle della fase M1 secondo pianificazione di dettaglio di cui al punto precedente.
- **Report di completamento della migrazione** (*cutover*): report completo con i dettagli dell'attività di migrazione (già contenuti nei deliverable 2.2), sottoposto all'approvazione da parte dell'Amministrazione all'esito dei test di validazione della migrazione, **entro il 24/10/2024**.

L'insieme dei deliverable documentali proposti garantirà che tutte le fasi della migrazione siano pianificate, eseguite e validate correttamente, assicurando una transizione sicura ed efficiente verso Oracle Cloud Infrastructure.

DATA DI ATTIVAZIONE DEL SERVIZIO DI FORNITURA

Il servizio di fornitura sarà attivato a decorrere dalla data di stipula del Contratto Esecutivo con l'Amministrazione.

INDICAZIONE DEL/I LUOGO/GHI DI ESECUZIONE DELLA FORNITURA

La fornitura verrà erogata principalmente da remoto. Eventuali attività da erogarsi presso la PA verranno concordate con l'Amministrazione in fase di avvio del progetto (riunioni di SAL).

DURATA DEL CONTRATTO ESECUTIVO E DEI SERVIZI

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

Le attività previste dal progetto, concordate nella Pianificazione di dettaglio richiesta dal Piano dei Fabbisogni di concerto con ARES, verranno completate in coerenza con le scadenze del finanziamento ricevuto dagli enti con misura 1.2 del bando multimisura PNRR.

Le prestazioni contrattuali verranno 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.

QUOTA E PRESTAZIONI IN SUBAPPALTO

La quota e le prestazioni in subappalto vengono gestite in conformità all'art. 105 del D. Lgs. 50/2016, vigente ratione temporis e in accordo con l'Amministrazione, fermo restando che potranno essere erogati in subappalto tutti i servizi oggetto del presente Piano Operativo.

RESPONSABILI E FIGURE DI RIFERIMENTO DEL FORNITORE

Di seguito, si riporta l'elenco delle persone incaricate dal Fornitore per la conduzione del progetto indicandone ruoli e responsabilità. Tali figure sono tutte espressione della Azienda Engineering D.HUB S.p.A., Mandataria del presente RTI.

Per i servizi, si fa riferimento ai codici di cui al paragrafo "IMPORTO CONTRATTUALE E QUANTITÀ PREVISTE PER I SERVIZI OGGETTO DI FORNITURA" del presente documento.

Nominativo	Ruolo	Responsabilità (a titolo esemplificativo e non esaustivo)
Sabrina Volpe	**RUAC del CE**	Gestione del CE interfacciandosi, ove necessario con i Responsabili tecnici per l'erogazione dei servizi. Stima, pianificazione e consuntivazione degli obiettivi. Predisposizione e gestione dei Piani di Lavoro, Piano della Qualità generale, ecc… Verifica dei livelli di servizio ed individuazione delle eventuali azioni correttive. Verifica dei risultati sugli indicatori di qualità. Gestione dei team mix effettivi per i singoli servizi e pianificazione delle risorse quantitativamente e qualitativamente adeguate. Adozione di idonei strumenti per facilitare la comunicazione e lo scambio di informazioni tra i vari attori convolti nella fornitura.
Massimiliano Panichi	**Responsabile Tecnico per i Servizi Tecnologici**	Predisposizione dei Piani Operativi e dei Piani di Qualità per le attività ed i progetti; Coordinamento delle risorse impiegate nel servizio negli ambiti assegnati; Verifica sull'erogazione delle attività di tutte le risorse coinvolte nei servizi, conformemente ai requisiti minimi di qualità della fornitura; Partecipazione alle riunioni di avanzamento e/o a riunioni indette dalle Amministrazioni.
Massimiliano Panichi	**Responsabile della Migrazione Cloud**	Definizione e l'implementazione delle pratiche e delle procedure finalizzate a garantire la coerenza delle architetture implementate con la strategia di migrazione; Definizione del sistema di autovalutazione del servizio attraverso l'implementazione, misurazione degli indicatori offerti oltre agli indicatori previsti contrattualmente; Verifica delle attività di analisi qualitativa del prodotto finale, con focus sull'individuazione delle potenziali problematiche con particolare riguardo ad aspetti di security e capacity;

Nominativo	Ruolo	Responsabilità (a titolo esemplificativo e non esaustivo)
		Pianificazione, il coordinamento e la corretta esecuzione del processo di migrazione e la gestione del relativo team, oltre a fornire periodicamente tutte le indicazioni necessarie al miglioramento dei processi di Service management; Stima dell'effort in termini di risorse del team di supporto tecnologico; Identificazione di ottimizzazione dei costi rispetto alla pianificazione con particolare riguardo al monitoraggio dei consumi di risorse rispetto alla pianificazione iniziale; Produzione e la verifica dei seguenti documenti: Documento architetturale, che descrive in generale tutti gli aspetti dell'implementazione (tra cui ad esempio: Architettura, Reti, Storage, policy di sicurezza, procedure di recovery, policy di backup, etc.)

AREE TECNOLOGICHE E SERVIZI

Si riportano di seguito le fasi previste nel Piano dei Fabbisogni e i servizi richiesti che verranno indicati nel Contratto Esecutivo.

FASE M1 - SOLUTION DESIGN E ARCHITECTURE:

Attraverso questa fase che rappresenta il primo passaggio di adozione del paradigma cloud, ARES richiede che vengano progettate ed eseguite attività specifiche quali il disegno architetturale dei propri workload con indicazione delle risorse computazionali necessarie alla corretta esecuzione degli stessi. L'obiettivo generale di tale fase è quello di supportare l'ARES nel definire la mappatura dei workload sulle tecnologie, producendo come output uno specifico documento architetturale con evidenza dei flussi di workload necessari a soddisfare l'architettura complessivamente identificata. Saranno messe 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.

Disegno dei workload (M1.1)

In prima battuta dovrà essere stilata una lista dei workload necessari a soddisfare i requisiti della strategia di migrazione Lift&Shift. Per ogni workload dovranno essere tracciate ed inserite almeno 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.

Il Fornitore si impegna a ricavare direttamente dall'ARES e/o dal suo Fornitore terzo di riferimento, oppure dal produttore e/o fornitore stesso dell'applicativo, o da altre entità pubbliche se coinvolte nella gestione delle infrastrutture e/o delle applicazioni ("società in house", partecipate, enti consorziati, accordi di servizio, …).

A partire dalla strategia di migrazione, per garantire la completezza della fase in oggetto, verrà prodotto un documento riepilogativo denominato Disegno dei workload, **composto da un singolo documento per ciascun workload definito**. Tale documento conterrà almeno la mappatura aggiornata e dettagliata dei servizi e delle applicazioni connessi al workload.

ARES metterà a disposizione del Fornitore il proprio documento di Disegno dei workload, laddove presente, correlato anche dai processi organizzativi e funzionali della struttura. Il Fornitore avrà il compito di verificarne la validità e la consistenza al fine di poterlo utilizzare compiutamente nel processo di migrazione in cloud, ed intraprendere le eventuali azioni di indagine necessarie a completare il documento.

Architettura risorse cloud (M1.2)

Attraverso questo servizio ARES richiede il disegno di dettaglio delle architetture IaaS e PaaS con cui procedere con la migrazione dei workload. Per ogni workload dovrà essere indicata l'architettura di riferimento in termini di risorse cloud tenendo in considerazione tutte le interazioni con altri workload. Per ogni documento di disegno, saranno tracciate 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.

Il Fornitore si impegna a reperire le informazioni necessarie direttamente da ARES e/o dal suo Fornitore terzo 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, …).

A partire dalla strategia di migrazione e dai documenti di disegno dei workload, per garantire la completezza della fase, viene prodotto il documento riepilogativo denominato **Disegno architetturale complessivo** che definisce le risorse cloud necessarie (VM, load balancer, storage, etc) per ciascun workload e le eventuali modalità di interazione.

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. ARES metterà a disposizione del Fornitore il proprio documento di Disegno architetturale, laddove presente, correlato dai processi organizzativi e funzionali della struttura. Il Fornitore avrà il compito di verificarne la validità e la consistenza al fine di poterlo utilizzare compiutamente nel processo di migrazione in cloud. Qualora non sia garantita la consistenza in termini di sicurezza, ARES dovrà preventivamente aggiornare gli applicativi/dati degli ambienti source on-premise. In relazione a questa eventuale attività, si precisa che gli oneri relativi alle attività svolte da fornitori terzi non saranno a carico di Engineering.

FASE M2 – IMPLEMENTAZIONE E MIGRAZIONE

Questa fase rappresenta per ARES un passaggio cruciale nell'adozione del paradigma cloud e prevede vengano implementati gli ambienti necessari ad ospitare i workload nonché trasferiti i dati dagli ambienti on-premise. Nell'implementazione della migrazione verranno assicurati tutti i processi di comunicazione, collaborazione e integrazione tra la componente relativa alle risorse professionali e tecnologiche e la componente dati. Verranno quindi messe 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.

Il servizio prevede la migrazione delle virtual machine e istanze database(s) di ARES dall'attuale collocazione on premise ad Oracle Cloud (OCI), in modalità "lift-and-shift".

Assunzioni

- I tools di migrazione da utilizzare per lo spostamento dei workload (RackWare su OCI, Oracle Data Guard, etc.) verranno messi a disposizione dall'Amministrazione
- Attività svolte tramite accesso da remoto ai sistemi, dalla sede del Fornitore.
- Middleware ed applicazioni: La fornitura del piano di dettaglio delle attività di test applicativi da migrare è in capo alla stazione appaltante/attuali fornitori terzi manutentori dei sistemi oggetto di migrazione
- Gli applicativi/dati degli ambienti source on-premise dovranno essere aggiornati dalla stazione appaltante/attuali fornitori terzi manutentori per garantire la consistenza del processo di migrazione in cloud
- Per minimizzare gli impatti a livello di sistema verranno eseguite le attività di sicurezza a livello perimetrale, mentre le attività di sicurezza applicativa verranno previste a valle della migrazione Lift&Shift, con specifiche progettualità che non rientrano nell'attuale perimetro

Esclusioni

- Middleware ed applicazioni: le attività di test di verifica degli applicativi migrati verranno eseguite dai fornitori terzi che attualmente manutengono gli applicativi stessi con il supporto da parte di Engineering. Sono esclusi dagli oneri Engineering i costi relativi alle attività in capo ai fornitori terzi
- In merito ad un eventuale necessario aggiornamento degli ambienti on-premise, sono esclusi dagli oneri Engineering i costi relativi alle attività in capo ai fornitori terzi

Configurazione Ambienti (M2.1)

In prima battuta verrà stilata una lista delle risorse tecnologiche necessarie a soddisfare i requisiti dei workload. Per ogni risorsa configurata verranno tracciate ed inserite almeno le seguenti informazioni:

- **Nome e descrizione del workload di riferimento**: Ad esempio, SISAR ATTI per la gestione documentale.
- **Nome e descrizione della risorsa**: Dettagli specifici delle risorse cloud (es. VM, storage, ecc.).
- **Configurazioni della risorsa**: Dettagli tecnici quali CPU, RAM, storage, regole di bilanciamento, tunnel VPN, ecc.
- **Capacità di scalabilità della risorsa**: Indicazioni delle API per la gestione automatica dello scaling.
- Referente dell'Amministrazione e/o del Fornitore dell'Amministrazione: Contatto di riferimento per ogni risorsa.
- **Descrizione della modalità di phase out per la risorsa**: Es. configurazione da esportare, dati da esportare, formato dei dati per successiva implementazione.
- **Interazioni e dipendenze da altre risorse**: Dettagli sulle interazioni con altre risorse e dipendenze esistenti.

Il Fornitore si impegna a reperire le informazioni necessarie direttamente da ARES e/o dal suo Fornitore terzo 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, partecipate, enti consorziati, accordi di servizio, ecc.).

Il documento che raccoglie le configurazioni delle risorse costituirà l'assessment delle risorse cloud e rappresenta il deliverable di fornitura del servizio.

Per la corretta stesura del documento, il team di lavoro avrà a disposizione i documenti relativi ai workload e tutte le informazioni presenti nel Piano dei Fabbisogni e nella documentazione fornita da ARES 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. ARES metterà a disposizione del Fornitore il proprio documento di configurazione delle risorse, laddove presente, correlato magari anche dai processi organizzativi e funzionali della struttura. Il Fornitore avrà il compito di verificarne la validità e la consistenza al fine di poterlo utilizzare compiutamente nel processo di migrazione in cloud.

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 e tramite i tool di migrazione messi a disposizione dall'Amministrazione.

Trasferimento Dati (M2.2)

Il processo di migrazione dei dati si articolerà secondo queste fasi:

1. **Preparazione della migrazione**: Inclusi backup e verifica delle connessioni sicure;
2. **Validazione dei dati nel sistema sorgente**: Assicurarsi che i dati siano consistenti e pronti per il trasferimento;
3. **Creazione dello schema dei dati nel sistema destinazione**: Definire come i dati saranno strutturati nel nuovo ambiente;
4. **Mappatura delle strutture dati del sistema sorgente nel sistema destinazione**: Garantire che i dati siano trasferiti correttamente;
5. **Conversione e trasferimento dei dati dal sistema sorgente al sistema destinazione**: Effettuare il trasferimento effettivo dei dati;
6. **Validazione dei dati migrati nel sistema di destinazione**: Verificare che i dati siano stati trasferiti correttamente e che il sistema funzioni come previsto;
7. **Dismissione del sistema sorgente**: Dopo aver confermato che la migrazione è stata completata con successo;

Implementare un corretto processo di migrazione dei dati è di cruciale importanza; verranno quindi seguite best practices per evitare perdita di dati, inconsistenza, lunghi periodi di downtime, corruzione dei dati e interferenze. Le pratiche preparatorie per la migrazione delle basi di dati includeranno:

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

Al termine del trasferimento dei dati negli ambienti target, sarà eseguita la validazione del trasferimento mediante verifica del corretto funzionamento dei workload dipendenti dalla base dati migrata. Verranno altresì effettuate idonee validazioni delle performance, ad esempio attraverso l'esecuzione e la misurazione di query (quali tempo di risposta, throughput e latenza). Saranno inoltre applicate tecniche avanzate di validazione delle basi dati migrate, incluse la riconciliazione per garantire la corrispondenza numerica tra le entità sorgenti e quelle target, e la validazione orizzontale dei valori nel caso in cui la transizione abbia comportato momenti di trasformazione, arricchimento o consolidamento dei dati migrati.

Verrà prodotto un deliverable di fornitura per ogni base dati migrata. Il documento traccerà ed includerà almeno le seguenti informazioni:

- **Schemi dei dati sorgenti**;
- **Schemi per le basi dati target che ospiteranno i dati**;
- **Attività che incidono sui dati sorgente prima della migrazione effettiva**: attività di normalizzazione, modifiche alle tabelle, consolidamenti e arricchimenti;
- **Modalità/tecniche implementate per garantire coerenza ed evitare la corruzione dei dati**;
- **Modalità/tecniche di migrazione**;

- **Workload dipendenti dalla base di dati migrata**;
- **Tecniche e risultati delle attività di validazione**.

Il Fornitore si impegna a reperire le informazioni necessarie direttamente da ARES e/o dal suo Fornitore terzo 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, ecc.).

Per la corretta stesura del documento, il team di lavoro avrà a disposizione i documenti relativi ai workload e tutte le informazioni presenti nel Piano dei Fabbisogni e nella documentazione fornita da ARES 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.

FASE M3 – SECURITY

Garantiamo 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 critici pur con la garanzia di segregazione dei tenant da parte dei CSP. Nel definire le policy di un ambiente cloud si terrà contro dello stato dell'infrastruttura in termini di workload M1.1 e basi dati implementate M2.2 nonché delle configurazioni delle risorse di cui ai deliverable M2.1 così come, infine, dell'intera architettura e interazioni tra risorse M1.2.

Verranno messe 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.

Definizione policy di sicurezza (M3.1)

In prima battuta verrà compiuto un assessment completo sullo stato dell'arte dell'ambiente cloud in termini architetturali e dei workload implementati. Definito lo stato delle risorse, il Fornitore dovrà implementare policy di sicurezza relative agli applicativi oppure relative ai dati.

La scelta e l'eventuale implementazione dei controlli di sicurezza sarà valutata a valle dello studio e dell'analisi dell'attuale soluzione/applicazione di ARES. L'implementazione delle policy di sicurezza perimetrale è inclusa in questa offerta senza ulteriore impegno economico da parte di ARES.

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, edge layer (es. utilizzando una connessione TLS sicura anche nelle comunicazioni con altri applicativi). L'ambiente prevederà l'esposizione delle interfacce applicative su protocollo http TLS attraverso gli strumenti disponibili su OCI;
- 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. Sarà valutata la possibilità di utilizzare ed integrare strumenti per cifrare i dati a riposo oppure per gestire le chiavi di cifratura, sull'ambiente OCI fornito dall'Amministrazione;
- mitigare attacchi DDoS utilizzando il livello di network della piattaforma cloud. Attraverso l'opportuna configurazione dell'ambiente OCI fornito dall'Amministrazione che include funzionalità di rilevazione automatica degli attacchi DDoS e di mitigazione degli attacchi;

- utilizzare una lista di accessi sicuri per reti, applicativi e dati, attraverso l'utilizzo degli strumenti presenti sulla OCI fornita dall'Amministrazione finalizzati a definire gli accessi alle risorse come IAM;
- eseguire un'analisi periodica delle vulnerabilità anche attraverso penetration test;
- utilizzare two factor authentication (2fa) e configurare un meccanismo di single sign on (SSO), Attraverso la configurazione del 2FA per l'accesso utente presente sulla OCI messa a disposizione. Verrà inoltre valutata la possibilità di integrare meccanismi di SSO;
- installare antivirus e anti-malware per i nodi e il networking; sfruttando gli strumenti presenti in OCI per monitorare e mantenere la sicurezza come Cloud Guard.
- abilitare il monitoring ed il logging per il networking, gli applicativi ed i dati, mediante l'opportuna configurazione degli strumenti per monitoring e logging Cloud Infrastructure Logging, presenti sulla OCI;
- connettere ambiente on-premises con ambiente cloud utilizzando sempre un link dedicato ed una VPN sul link pubblico. Sull'ambiente OCI fornito dall'Amministrazione è disponibile la VPN e la connettività verso on premise;

Per ogni base di dati verrà gestita la sicurezza per almeno i seguenti aspetti:

- cifratura dei dati memorizzati nei dischi utilizzando ad esempio AES (Advanced Encryption Standards) 256, attraverso l'utilizzo degli strumenti disponibili in OCI per cifrare i dati a riposo oppure per gestire le chiavi di cifratura;
- utilizzo di uno strumento presente in OCI per la 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 mediante opportuna configurazione ed utilizzo degli strumenti presenti nell'ambiente OCI.;
- proteggere tutti i canali di comunicazione con un certificato SSL, mediante opportuna configurazione ed utilizzo degli strumenti presenti nell'ambiente OCI..

Per le attività di definizione delle policy di sicurezza e per ogni policy, verrà prodotto un deliverable con 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.

Ci impegniamo a reperire le informazioni necessarie direttamente da ARES 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 disponibili i documenti relativi ai workload e tutte le informazioni nei documenti di configurazione risorse e nella documentazione fornita da ARES nella fase preliminare e dovrà tenere conto del contesto istituzionale e funzionale in cui opera.

ARES metterà a disposizione i propri documenti di policy di sicurezza, laddove presenti, correlati magari anche dai processi organizzativi e funzionali della struttura. Verrà infine verificata e validata la consistenza complessiva della conoscenza messa a disposizione al fine di poterli utilizzare compiutamente nel processo di migrazione in cloud.

PREVISIONI PRESCRITTE DAL D.L. 77/2021, CONVERTITO IN L. 108/2021

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 presente Piano Operativo, ciascuna impresa del RTI allega 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.

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.