Il progetto quindi prevede oltre al rafforzamento del Tenant già attivo per la posta Zimbra anche la predisposizione delle risorse necessarie alla migrazione in Cloud del Portale ASL Roma 1 nonchè ampliamento dello storage (Virtual Storage Object) disponibile per entrambe le applicazioni.

I sistemi Zimbra e Portale Aziendale vedranno coinvolte le risorse specialistiche di Laboratori Marconi che sono enabler SPC Cloud e gestiscono dal punto di vista sistemistico entrambe le applicazioni.

4.2.1 IAAS

Il servizio "IaaS - Virtual Data Center" permette alle Amministrazioni di creare e gestire in autonomia le proprie macchine virtuali partendo dalle singole risorse. Le risorse associate al Virtual Data Center possono essere richieste tramite pool base e upgrade di risorse aggiuntive di CPU [vCPU], RAM [GB] e spazio Storage [GB/TB]. Il servizio consente quindi all'Amministrazione di avere a disposizione e riservare risorse computazionali e di organizzarle autonomamente secondo una logica così definita di Virtual Data Center.

L'aggiornamento delle componenti software presenti nella macchina virtuale è a carico dell'Amministrazione che fruisce del servizio.

Il provider garantisce, senza oneri aggiuntivi per l'Amministrazione, di mantenere inalterate le performance e l'operatività del servizio fruito dall'Amministrazione per risorse superiori (gestione overload) fino al 10% del valore nominale del totale delle risorse indicate nei paragrafi successivi, con l'obiettivo di gestire picchi di lavoro estemporanei.

Per il servizio Virtual Data Center, oltre le risorse sopra elencate sono previste una serie di opzioni fatturate sulla percentuale di aumento della performance dello storage (velocità disco) e degli SLA di servizio (tempi di uptime e ripristino) su ora o mese, a consumo o a canone.

In fase di creazione delle VM l'utente ha la possibilità di inserire una propria licenza per il Sistema Operativo.

Nella seguente tabella sono specificate le risorse messe a disposizione:

POSTA ELETTRNICA ZIMBRA

Di seguito la configurazione finale da adottare per il Tenant già attivo, in giallo le risorse che cambiano;

Tenant	Servizio	Elementi	Profilo	Quant	Durata	Totale €
VDCCAN_A	**VDC ZIMBRA (modificato)**	Identificativo per Variazione				
	Virtual Data Center - Canone -	Pool risorse virtuali base - Canone Capacitivo	5 GHz CPU 10 GB RAM 500 GB HD 1 vNetwork (1 IP pubblico + 15 IP privati)	1	7	15.250,2120
		Pool risorse virtuali base - Canone Prestazionale (Dischi di tipo SAS o FC da almeno 15k rpm)	5 GHz CPU 10 GB RAM 500 GB HD 1 vNetwork (1 IP pubblico + 15 IP privati)	-		
		Risorse aggiuntive CPU - Canone	1 GHz	95		
		Risorse aggiuntive RAM - Canone	1 GB	178		
		Virtual Network -Canone	vNetwork base - IP 15 indirizzi IP e 1 indirizzo Pubblico Internet/SPC	4		
		VStorage - Medium - Canone	1 TB	3		
		VStorage - Medium - Canone Storage prestazionale - Canone	1 TB Dischi di tipo SAS o FC da almeno 15k rpm	2		
		VStorage - XLarge - Canone Storage prestazionale - Canone	5 TB Dischi di tipo SAS o FC da almeno 15k rpm	8		
	Unmanaged	Unmanaged	Unmanaged			

VIRTUAL STORAGE

Di seguito la configurazione finale da adottare per lo storage già attivo, in giallo le risorse che cambiano;

Servizio	Elementi	Profilo	Quant	Durata	Totale €
Virtual Storage - Object -	**VStorage - XLarge - Canone**	5 TB	13	7	7.644,0000

TIM DXC.technology	Posteitaliane Postel	Tipo documento: **Progetto dei Fabbisogni**		
Titolo documento: **Progetto dei Fabbisogni Servizi SPC Cloud Lotto 1 : ASL Roma 1**				
Emesso da:	EM-PS.PS/C	Codice documento: 2113664791004005PJFV2	Versione 1	Data di emissione 09/06/2022

PORTALE AZIENDALE

Tenant	Servizio	Elementi	Profilo	Quant	Durata	Totale €
VDCCAN_C	VDC Portale Sito DR	NUOVE RISORSE				
	Virtual Data Center - Canone -	Pool risorse virtuali base - Canone Capacitivo	5 GHz CPU 10 GB RAM 500 GB HD 1 vNetwork (1 IP pubblico + 15 IP privati)	1	7	732,2000
		Pool risorse virtuali base - Canone Prestazionale (Dischi di tipo SAS o FC da almeno 15k rpm)	5 GHz CPU 10 GB RAM 500 GB HD 1 vNetwork (1 IP pubblico + 15 IP privati)	-		
		Risorse aggiuntive RAM - Canone	1 GB	6		
	Unmanaged	Unmanaged	Unmanaged			
VDCCAN_D	VDC Portale Sito Produzione	NUOVE RISORSE				
	Virtual Data Center - Canone -	Pool risorse virtuali base - Canone Capacitivo	5 GHz CPU 10 GB RAM 500 GB HD 1 vNetwork (1 IP pubblico + 15 IP privati)	1	7	732,2000
		Pool risorse virtuali base - Canone Prestazionale (Dischi di tipo SAS o FC da almeno 15k rpm)	5 GHz CPU 10 GB RAM 500 GB HD 1 vNetwork (1 IP pubblico + 15 IP privati)	-		
		Risorse aggiuntive RAM - Canone	1 GB	6		
	Unmanaged	Unmanaged	Unmanaged			

4.3 Impegni servizi professionali

4.3.1 Cloud Enabling

Il servizio "Servizi di Cloud Enabling – Servizi di Virtualizzazione server" permette alle Amministrazioni di usufruire di un servizio fornito in modalità "On Premise" che metta a disposizione delle Amministrazioni servizi di supporto:

- alla virtualizzazione di infrastrutture fisiche nell"ambito dei CED privati delle Pubbliche Amministrazioni (migrazione Phisical-to-Virtual);
- all"introduzione del paradigma cloud nell"ambito della loro infrastruttura tecnologica. In particolare le principali attività sono di seguito elencate:
- analisi costi/benefici e fattibilità
- progettazione di virtual data center/ VM
- configurazione di virtual data center / VM
- supporto per la definizione e configurazione delle policy di backup/restore
- supporto per la progettazione di Virtual Private Cloud e di Virtual Data Center (comprensivo di progettazione di infrastrutture tecnologiche ad uso dei Poli regionali) tutorship

Di seguito il dettaglio delle figure professionali richieste per l'estensione del servizio di posta elettronica e portale aziendale:

Servizio	Elementi	Profilo	Quant
Servizi professionali	**IT Architect senior**	gg/pp	**104**
Servizi professionali	**Sistemista senior**	gg/pp	**186**

4.4 Specifiche di Collaudo

I test di collaudo saranno eseguiti presso la sede del Cliente.

Le seguenti linee guida descrivono lo svolgimento delle prove di collaudo atte a verificare la conformità delle configurazioni particolari richieste dall'<Amministrazione x> per il servizio in oggetto e descritte nel relativo paragrafo del presente documento.

Le modalità di esecuzione ed i relativi documenti di output saranno conformi a quanto già previsto per il collaudo Consip.

I test saranno eseguiti secondo il seguente processo:

1) configurazione del servizio, degli apparati e degli strumenti in base a quanto specificato nella scheda di test;

2) esecuzione del test secondo quanto descritto nella relativa scheda;

3) se l'esito del test è positivo si ritorna al punto 1) procedendo con il test successivo;

4) se l'esito è negativo viene registrata l'anomalia, a cui è associato un livello di gravità (bloccante, grave, accettabile);

5) se l'anomalia è di tipo bloccante si sospende il test in corso proseguendo eventualmente con il test successivo tornando al punto 1).

Le anomalie saranno gestite con le seguenti modalità:

- Classificazione: ogniqualvolta sia rilevata una anomalia essa sarà registrata dall'operatore che esegue il test con la classificazione "grave". Sarà poi cura del team di verifica riclassificare, se necessario, l'anomalia in occasione dei controlli periodici di avanzamento della verifica.
- Notifica di rilevamento: la scheda anomalia compilata dall'operatore ed eventualmente quella con la riclassificazione operata dal team di verifica saranno inviate alle strutture di competenza.
- Notifica di risoluzione: le modalità di risoluzione delle anomalie saranno esaminate dal team di verifica in occasione dei controlli periodici di avanzamento delle verifiche in collaborazione con le strutture di competenza. Sarà quindi ripianificato il processo di verifica per effettuare i nuovi test a valle della risoluzione dell'anomalia.

Nel corso delle attività di verifica saranno condotti opportuni controlli di avanzamento con l'obiettivo di:

1. verificare l'avanzamento della pianificazione temporale;
2. analizzare le anomalie rilevate;
3. analizzare le modalità di risoluzione delle anomalie;
4. progettare i test di regressione per chiusura anomalie;
5. ripianificare le sessioni di test ed aggiornare la pianificazione temporale.

Il Piano di Test è articolato in schede, divise nelle seguenti sezioni:

Campo	Significato
Requisito	Identificativo del requisito oggetto del test
Scopo	Riassume l'obiettivo del test
Modalità di esecuzione	Indica la modalità di esecuzione del test, ad esempio per accesso diretto alla piattaforma, iniziando dall'accesso all'ambiente.
Scenario di riferimento	Descrive lo 'scenario utente' nel quale avviene il test e le condizioni che caratterizzano lo scenario
Macro azioni	Sono i passi operativi che si compiono durante la rappresentazione del test.
Risultato atteso	E' lo scenario utente atteso, a seguito dell'esecuzione del test.
Esito del test	E' l'esito del test, positivo se lo scenario ottenuto a seguito del test coincide con lo scenario atteso, negativo in caso contrario.

5 DESCRIZIONE CENTRO SERVIZI

I Centri Servizi per la fornitura di tutti i Servizi Cloud previsti in convenzione, mettono a disposizione della Pubblica Amministrazione italiana le migliori caratteristiche di **affidabilità, solidità** e **sicurezza** disponibili sul mercato.

Il modello prevede:

- una zona riservata (anche detta "region") dedicata alla Pubblica Amministrazione italiana all'interno di ciascuno dei Centri Servizi primari (Rozzano e Inverno), per l'esercizio dei servizi;
- due region dedicate alla Pubblica Amministrazione italiana all'interno del centro di Disaster Recovery (Roma), in grado di subentrare ad una o ad entrambe le region di esercizio;
- una serie di centri che forniscono funzioni di controllo: Security Operation Center (SOC), Network Operation Center (NOC), Control Room.

La presenza di una doppia infrastruttura di esercizio è intesa ad assicurare maggiore **flessibilità** nella distribuzione del carico computazionale, il che garantisce maggiore **solidità** e **continuità operativa** all'intera fornitura. La soluzione è in linea con i dettami del "Community Cloud" e garantisce tempi di RTO e RPO migliorativi rispetto ai requisiti minimi di gara.

Rispetto al modello precedente, il servizio SaaS di Conservazione Digitale utilizzerà infrastrutture, già accreditate presso AgiD o in fase di accreditamento, attestate presso il centro di Pomezia (primario) e i centri di Torino e Roma (Disaster Recovery).

I siti sono connessi fra loro attraverso la VDCN di Telecom (Virtual Data Center Network), rete di trasmissione dati ad altissima velocità attraverso la quale un Centro Servizi ad essa afferente può erogare i servizi IT verso le reti pubbliche e generare traffico di allineamento dati con gli altri centri del Raggruppamento. Più specificamente, la VDCN è una rete IP/MPLS costituita da un anello ottico realizzato attraverso collegamenti in tecnologia DWDM a multipli di 10Gbps e ricavato sul backbone trasmissivo della Rete di Trasporto Nazionale di Telecom Italia, la dorsale della più grande infrastruttura di connettività disponibile nel nostro paese. L'elevata capacità di forwarding di questa rete, la sua affidabilità e la sua rapida scalabilità le consentono di garantire una totale continuità del servizio. Ciò permette di considerare tutto il modello architetturale come un unico grande centro di erogazione dei servizi.

I Centri Servizi sono collegati sia ad Internet sia alla rete SPC, il che consentirà alle Amministrazioni contraenti di **usufruire dei servizi senza soluzione di continuità**

Il Centro Servizi Telecom di Roma fungerà da Sito di Disaster Recovery. La distanza del sito dai Centri Servizi primari garantisce la continuità operativa a fronte di qualsiasi scenario possibile di indisponibilità:

- infrastruttura hardware fuori uso;
- perdita dei dati elaborati tramite l'infrastruttura;
- evento disastroso che renda il Centro Servizi inagibile e non più funzionante;
- evento disastroso che interessi una area geografica ampia.

La protezione da questi eventi è garantita da un insieme di misure:

- impianti di sicurezza dei Centri Servizi (sistemi anti-incendio, anti-allagamento, anti-intrusione, continuità elettrica);
- tecniche di ridondanza delle infrastrutture IT (connettività, sistemi elaborativi e sistemi di storage duplicati con tecniche di clusterizzazione, mirroring, virtualizzazione, ecc.) che garantiscono un alto --grado di resilienza all'insorgere di guasti;
- backup dei dati delle Amministrazioni sia su infrastrutture di storage poste in ambienti separati dei Centri Servizi con garanzia di elevata protezione fisica, sia su copie di sicurezza trasferite in caveau esterni;
- trasferimento dei dati dai siti di produzione al sito di Disaster Recovery attraverso le funzionalità dei -sistemi di storage, con indici RTO ≤ 4 ore e RPO ≤ 1 ora (vedi anche §5.1);
- trasferimento dei dati dai siti di produzione al sito di Disaster Recovery, con meccanismi tali da -assicurare valori RTO e RPO uguali o inferiori a quattro ore e un'ora rispettivamente

Ogni Centro Servizi ha il suo Piano di Disaster Recovery. Nel momento in cui si verifica un problema e/o un disservizio all'interno del Centro Servizi, viene attivato il **processo di escalation** che include una procedura operativa che ha lo scopo di informare istantaneamente il management di eventi particolarmente significativi.

Mezzi preferenziali per attivare il "team di crisi" sono la chiamata in voce o l'SMS, con modalità che tutelano la tracciabilità di tutte le comunicazioni avvenute. Le informazioni pervenute sono analizzate al fine di stabilire

se il livello di criticità raggiunto è tale da richiedere il coinvolgimento dei livelli superiori: in tal caso, si attiva l'escalation di 2° livello che prevede il coinvolgimento del Responsabile dei Centri Servizi, che ha il compito di attivare il Comitato di Crisi se il problema viene classificato come "disastro"

Il Comitato di Crisi è composto dal Responsabile del Contratto Quadro, dal Responsabile dei Centri Servizi e dai Coordinatori di tutti i siti.

Il comitato ha il compito di:

- analizzare velocemente il problema in corso e dichiarare lo stato di emergenza;
- attivare il Piano di Disaster Recovery;
- reperire personale o apparati di supporto alle attività;
- gestire la comunicazione interna ed esterna;
- seguire l'evolversi della situazione e l'avanzamento delle attività di ripristino e di rientro;
- al termine dell'emergenza, compilare una relazione sulle attività svolte e avviare eventuali iniziative di miglioramento intese ad evitare l'insorgere di eventi analoghi in futuro.

Il modello di servizio viene completato dai *Centri Servizi ausiliari*. Si tratta di unità operative dislocate sul territorio italiano e focalizzate sulla gestione dell'infrastruttura tecnologica, con particolare riferimento alle architetture tecniche, alle piattaforme (storage, server, network) e ai servizi infrastrutturali (backup, monitoraggio, asset management, disaster recovery, ecc.).

La scelta di separare fisicamente i Centri Servizi ausiliari dai Centri Servizi propriamente detti è in primo luogo funzionale alla necessità di **garantire la continuità operativa**.

Infatti:

- in caso di disastro in uno dei Centri Servizi primari gli operatori dei centri ausiliari possono continuare a svolgere le loro attività senza necessità di trasferimenti;
- al tempo stesso, l'attività dei centri ausiliari non richiede particolari infrastrutture in loco (gli operatori accedono ai sistemi attraverso le reti aziendali, con credenziali d'accesso specifiche e riservate): in caso di problemi tecnici nella sede di un centro ausiliario, gli operatori possono spostarsi in una diversa sede aziendale e proseguire la loro attività.

Vediamo quali sono i Centri Servizi ausiliari.

SOC (Security Operation Center) – Si occupano di tutte le attività volte ad assicurare la sicurezza dei sistemi e delle operazioni che rientrano nel perimetro della fornitura, secondo una logica di interoperabilità ed integrabilità. Le attività del SOC si riconducono a questi macro-blocchi:

- Security Risk Management: tutte le iniziative per la definizione e la gestione del rischio informatico declinato in funzione delle esigenze operative;
- Security Intelligence & Incident Response: attività che hanno come fine ultimo l'evoluzione delle discipline di gestione, di risposta e di analisi degli eventi di sicurezza, da attività manuali a processi

automatizzati, che sfruttano la conoscenza del contesto (intelligence) per attivare risposte automatiche agli attacchi informatici;

- Threat & Vulnerability Management: iniziative intese ad individuare il livello di minaccia e identificare/gestire la soluzione nell'ambito delle vulnerabilità di sistema, infrastrutturali e applicative;
- Data Protection & Privacy: individuazione, e gestione del livello di sensibilità delle informazioni in uso, in transito e archiviate, in conformità alle normative vigenti (es., D.Lgs. 196/2003 e s.m.i.);
- Secure Identity & Access: gestione del ciclo di vita delle identità, in termini di riconducibilità a persona fisica degli account di sistema canonici e/o privilegiati, di accesso standard e/o federato alle risorse informatiche, di strong authentication;
- Application Security: supporto all'individuazione, all'analisi e alla gestione delle vulnerabilità del codice applicativo;
- Security Architecture: revisione periodica delle architetture di sicurezza, per colmare le non conformità individuate in sede di valutazione del rischio e le vulnerabilità in genere;
- Digital Investigation & Forensic: analisi delle motivazioni, raccolta delle evidenze di attacco ai fini legali, eventuale stima del danno e raccomandazioni da adottare a valle di un attacco informatico;
- Governance & Compliance: definizione di processi, procedure e politiche per la corretta gestione delle informazioni di sicurezza e l'analisi delle eventuali non conformità verso le best practice, definite dagli standard di mercato (ISO27001, ISAE2434002, PCI DSS, ecc.) e dalle normative di legge.

NOC (Network Operation Center) – Sono le strutture deputate al monitoraggio, alla gestione e alla configurazione dell'infrastruttura di rete del Centro Servizi (LAN di Data Center e delle postazioni di lavoro). Le attività svolte includono la supervisione proattiva/reattiva della rete, la ricezione di reclami e/o richieste di supporto su tematiche di rete, diagnosi di primo livello e di secondo livello, correlazione di allarmi, intervento da remoto, inoltro delle segnalazioni verso altri enti in funzione delle competenze, monitoraggio/supporto fino alla chiusura dell'anomalia.

Control Room – Si occupano di monitorare e gestire le infrastrutture ospitate nei Centri Servizi. Sono costituite da team di specialisti, in possesso delle competenze metodologiche e tecniche necessarie per coprire tutte le attività di analisi e gestione sistemistica delle risorse IT (sistemi operativi, database, middleware). In particolare, al personale delle Control Room sono affidate attività di Capacity Planning, attività di valutazione di impatto (impact analysis) che precedono il change management, attività di monitoraggio e gestione incident, software distribution (es. inserimento di patch di aggiornamento software) – includendo in quest'ultima categoria anche le eventuali attività di test in ambiente di pre-produzione, per la verifica preventiva dei potenziali impatti sul servizio.

I Centri Servizi ausiliari sono ubicati come segue:

- per Telecom: il SOC, il NOC e la Control Room sono attestati a Roma (su sedi distinte);
- per HP: il SOC è attestato a Pomezia, il NOC a Cernusco sul Naviglio; le Control Room sono due, una dedicata alle attività di monitoraggio e attestata a Bari, l'altra alle attività più propriamente di gestione e attestata a Cernusco sul Naviglio;
- per Postel: il NOC e la Control Room sono attestate a Pomezia, il SOC a Roma.
- Nel caso di indisponibilità di uno di questi centri, l'operatività viene spostata rispettivamente su:
- SOC Telecom di Napoli;

- NOC Telecom di Roma (sede diversa da quella del NOC primario);
- Control Room Telecom di Milano;
- SOC/NOC HP di Roma;
- Control Room HP di Cernusco sul Naviglio o di Bari (il sito rimasto attivo eroga tutta l'attività);
- SOC/NOC/Control Room Postel di Genova.
- Per effetto del modello, restano presso i Centri Servizi le sole funzioni responsabili dei servizi di facility (spazi, condizionamento, alimentazione, cablaggio) e dei servizi di prossimità.

6 MODALITA' DI PRESENTAZIONE E APPROVAZIONE STATI AVANZAMENTO MENSILI

Al fine di verificare l'andamento del servizio, sino al superamento del collaudo, lo RTI produrrà dei SAL (Stato Avanzamento Lavori) mensili contenenti le seguenti informazioni:

- avanzamento delle attività relative al piano di realizzazione dell'infrastruttura dedicata al sito;
- evidenze di eventuali scostamenti rispetto al piano temporale di realizzazione;
- eventuali proposte per la nuova pianificazione delle attività;
- evidenze di attività correttive intraprese per la gestione delle criticità rilevate;
- esito di eventuali collaudi parziali e del collaudo finale effettuati;
- varianti e modifiche emerse nel periodo.

I SAL saranno prodotti con cadenza mensile a partire dalla data di approvazione del Progetto stesso ed entro il 15 del mese successivo a quello di riferimento del SAL.

Tutti i SAL saranno soggetti ad approvazione da parte dell'Amministrazione.

7 PIANO DI ATTUAZIONE DEL SERVIZIO

7.1 Piano di Lavoro

I tempi di attivazione previsti sono stimati in 30 gg dalla firma del contratto.

7.2 Piano di Qualità del Servizio.

I fine di assicurare che la fornitura rispetti i requisiti di qualità il Fornitore di ciascun Lotto predispone entro 30 giorni lavorativi dalla stipula del Contratto Quadro un Piano della Qualità Generale. Il Piano della Qualità Generale definisce le caratteristiche qualitative cui deve sottostare l'intera fornitura relativamente alla erogazione dei singoli servizi ed a quanto previsto per l'erogazione degli stessi tramite il Centro Servizi nel presente capitolo 4.

8 TABELLA RIEPILOGATIVA FINALE SERVIZI

Famiglia di Servizi	Durata	UT	Canone annuo	Canone Totale
Cloud Enabling		91.019,70		91.019,70 €
IAAS	7 mesi		41.757,62	24.358,6120
			TOTALE IVA ESCLUSA	**115.378,3120**