

APPENDICE 1 – SERVIZI CLOUD NIVOLA
AL CAPITOLATO TECNICO DI GARA

ASL VC - ACCORDO QUADRO RILANCIO COMPETITIVO PER L'ACQUISIZIONE DI UN SISTEMA DI
CARTELLA CLINICA ELETTRONICA

INDICE

1	INSTALLAZIONE E CONFIGURAZIONE INIZIALE	3
2	GESTIONE OPERATIVA	3
3	GESTIONE DEL SOFTWARE DI BASE E D'AMBIENTE E DELLE RELATIVE CONFIGURAZIONI	4
4	PROCEDURE DI BACKUP	4
5	RUOLI E RESPONSABILITA'	5
6	PIATTAFORMA NIVOLA	5
6.1	DEFINIZIONI E ACRONIMI	6
6.2	LA PIATTAFORMA NIVOLA	7
6.3	LE AVAILABILITY ZONES	8
6.4	LA STRUTTURA ORGANIZZATIVA	9
6.5	UTENTI, RUOLI ED ACCOUNT	9
6.6	CERTIFICAZIONI E COMPLIANCE	10
6.7	TIPOLOGIA DI UTENTI DELLA PIATTAFORMA	11
6.8	FASE DI PROVISIONING-ATTIVAZIONE SERVIZI	11
6.9	EROGAZIONE DEI SERVIZI	11
6.10	TIPOLOGIA DEI DATI TRATTATI	11
6.11	SERVIZI E INTERFACCE VISIBILI ALL'APPALTATORE	12
6.11.1	RISORSE ELABORATIVE	12
6.11.2	STORAGE AAS	13
6.11.3	BACKUP AAS	14
6.11.4	IL SERVICE PORTAL	14
6.11.5	ACCESSO TRAMITE CLI	14
6.11.6	TOOLS	14
6.12	MODALITÀ DI CONDUZIONE DEI SERVIZI	14
6.12.1	ATTIVITÀ IN CARICO ALL'APPALTATORE	14
6.12.2	ATTIVITÀ IN CARICO AL CSI-PIEMONTE	16
6.12.3	CONDIZIONI GENERALI	17
6.13	MANUALE UTENTE	17

1 INSTALLAZIONE E CONFIGURAZIONE INIZIALE

La Soluzione proposta dovrà essere predisposta su due istanze dedicate (test e produzione), raggiungibili tramite URL pubbliche dedicate. L'Appaltatore avrà accesso ai tre/due ambienti secondo le modalità indicate nel presente Allegato e nel Capitolato Tecnico. L'ambiente di test sarà utilizzato anche per effettuare le prove delle nuove versioni della Soluzione e le verifiche di corretto funzionamento delle componenti di integrazione e delle procedure di migrazione dati. L'Appaltatore dovrà pertanto garantirne l'aggiornamento e il mantenimento per tutta la durata del contratto.

La base dati dell'ambiente di test dovrà essere inizializzata a cura dell'Appaltatore con i dati oggetto di migrazione previamente validati dalla stazione appaltante, opportunamente anonimizzati, sui quali sarà erogata l'attività di formazione per ciascuna ASL.

L'elenco dei ruoli e delle responsabilità del Fornitore è inserito nell'Allegato 1A "Tabella RACI", ma a titolo esemplificativo e non esaustivo, dovrà effettuare le seguenti attività:

- predisposizione degli ambienti infrastrutturali (*virtual machines*, sistemi operativi, *middleware*, *data base*, ecc.);
- predisposizione degli ambienti applicativi di test e produzione;
- installazione della Piattaforma applicativa in tutti gli ambienti;
- installazione delle eventuali componenti di integrazione in tutti gli ambienti;
- inizializzazione della base dati di test sia con i dati di cui al punto precedente, sia con dati di prova esaustivi, tali da consentire la successiva verifica sul corretto funzionamento delle componenti e per poter procedere all'accettazione della Soluzione;
- verifica del corretto funzionamento di tutte le componenti;

Le attività di installazione e configurazione, necessarie alla messa in funzione e alla verifica di accettazione della Soluzione, dovranno essere adeguatamente descritte e documentate dal Fornitore nel Piano di Progetto.

2 GESTIONE OPERATIVA

Il servizio di gestione operativa è l'insieme delle attività necessarie a garantire la disponibilità della Piattaforma applicativa, delle componenti di integrazione e della firma digitale, nonché del software di base e d'ambiente necessario al corretto funzionamento della Soluzione. Dovrà essere erogato in una finestra temporale h24x365gg.

Il Servizio prevede almeno le seguenti attività a titolo esemplificativo:

- gestione del software di base e d'ambiente e delle relative configurazioni;
- gestione delle procedure di backup;
- monitoraggio e verifica delle procedure batch;
- trattamento dati;
- controllo, misurazione e analisi delle prestazioni e monitoraggio del corretto funzionamento di tutte le component della Soluzione fornita.

3 GESTIONE DEL SOFTWARE DI BASE E D'AMBIENTE E DELLE RELATIVE CONFIGURAZIONI

Prevede la verifica continuativa del corretto funzionamento, la distribuzione e l'installazione di eventuali correzioni o aggiornamenti (*patches, fix, ecc.*), nonché la configurazione dei software di base e d'ambiente. Prevede, inoltre, il ripristino di tutte le componenti software nella loro piena funzionalità in caso di guasti o malfunzionamenti del software.

Eventuali attività che potranno comportare un fermo del servizio saranno preventivamente concordate con la stazione appaltante.

4 PROCEDURE DI BACKUP

L'aggiudicatario dovrà dare indicazioni precise circa le procedure di backup al fine di garantire il completo salvataggio di tutte le componenti applicative e di tutti i dati. Gli strumenti di backup che saranno messi a disposizione dalla stazione appaltante tramite la piattaforma cloud regionale saranno implementati e configurati secondo le indicazioni dell'aggiudicatario.

Si precisa che non è in alcun modo consentito all'Appaltatore eseguire operazioni di backup o, in generale, di duplicazione anche solo parziale dei dati presso strutture o sistemi non individuati dalla stazione appaltante ed esterni allo stesso.

Gestione Procedure di Disaster Recovery

Al fine di proteggere l'erogazione dei servizi dovranno essere progettate e predisposte dall'Appaltatore le opportune procedure di replica in coerenza con i livelli minimi richiesti di RPO (Recovery Point Objective) e RTO (Recovery Time Objective).

Poiché l'Appaltatore potrebbe utilizzare servizi as a Service (managed), sarà a cura del CSI-Piemonte implementare le opportune procedure di replica e messa a disposizione dei servizi anche in condizioni di evento disastroso in funzione delle specifiche indicazioni ricevute dall'Appaltatore in fase di implementazione.

Inoltre, per l'implementazione di servizi di Disaster Recovery sono messe a disposizione 3 *availability zone* indipendenti e separate presso il Datacenter di Torino e Vercelli, per l'installazione della Soluzione.

LIVELLI DI SERVIZIO RELATIVI ALLA GESTIONE OPERATIVA DELLA SOLUZIONE

Di seguito i livelli di servizio previsti per la corretta erogazione del servizio che devono essere garantiti in funzione dei livelli di severità e dei valori soglia per gli indicatori di qualità indicati.

Utilizzo delle risorse

Indicatore	Descrizione	IQ	Soglia minima per IQ
Disponibilità	In fase di erogazione il Fornitore potrà richiedere un Incremento delle risorse rispetto al valore dichiarato nel Progetto infrastrutturale (o sue successive attualizzazioni) e riferito all'ambiente di produzione. Una richiesta superiore a tale soglia sarà a completo carico del Fornitore.	IC	<=20%

Disaster recovery

Indicatore	Descrizione	IQ	Soglia minima per IQ
RTO Applicativo	I tempi di RTO (Recovery Time Objective)	DRT	<=4h

Alta affidabilità – Business Continuity

Indicatore	Descrizione	IQ	Soglia minima per IQ
RTO Applicativo	I tempi di RTO (Recovery Time Objective)	BC1	<=1h
RPO	I tempi di RPO (Recovery Point Objective)	BC2	<=1h

5 RUOLI E RESPONSABILITA'

Sono indicati nell'Allegato 1A "Tabella RACI" i ruoli e le responsabilità previste per l'esecuzione dell'appalto in relazione alla piattaforma cloud e ai servizi cloud erogati.

6 PIATTAFORMA NIVOLA

Come già indicato nel Capitolato Tecnico, la Soluzione deve essere ospitata su piattaforma cloud regionale presso il CSI-Piemonte, che mette a disposizione servizi dispiegati su 3 *availability zone* dislocate nei Datacenter di Torino e Vercelli. I servizi sono erogati dalla piattaforma regionale Cloud Nivola.

Nei successivi paragrafi viene fornita una panoramica della piattaforma Nivola messa a disposizione da CSI-Piemonte, nonché un quadro esaustivo dei servizi infrastrutturali messi a disposizione dalla medesima.

Sono riportati:

- gli elementi principali relativi alla piattaforma Nivola ed a ciascun servizio infrastrutturale erogato;
- le tipologie di utenti della piattaforma;
- le modalità di attivazione dei servizi (prima attivazione);
- descrizione dei servizi di business messi a disposizione;
- descrizione del portale Nivola (*Service Portal*);
- descrizione delle modalità di accesso tramite CLI (*Command Line Interface*).

Nel Capitolo “Modalità di conduzione dei servizi” vengono descritte le caratteristiche dei servizi in carico all’Appaltatore ed i servizi in carico al Team di supporto Nivola. Nel caso specifico l’Appaltatore avrà in carico la gestione delle *virtual machine* sia lato sistema operativo, sia lato componenti applicative.

Nella tabella seguente si riportano le definizioni dei riferimenti ricorrenti utilizzati, allo scopo di facilitarne la comprensione e l'applicazione.

6.1 Definizioni e acronimi

Definizione	Significato
Nivola	Ci si riferisce al complesso di tutte le componenti della piattaforma: Service Portal, CMP, back-end.
Service Portal	È il portale di servizio a cui consumer e provider accedono per il governo dei servizi esposti da Nivola. L’interfaccia è in grado cooperare con le API di business esposte dalla CMP. Il Service Portal espone inoltre funzioni proprie come l’accesso alla documentazione, ai video tutorial, alla chat e al Servizio di assistenza tramite il Team di Supporto Nivola per supportare l’utente in caso di problemi, malfunzionamenti o semplici how-to-use.
Compute Services	Categoria di servizi che permette di fruire di risorse elaborative (espresse in CPU, RAM e spazio disco) in differenti flavour e template, corredate da servizi di networking e security. Sulla base del perimetro delle risorse presenti, gli utilizzatori saranno in grado di realizzare i propri tenant, istanziare le macchine virtuali selezionandole da un ampio catalogo di template e di gestirle in modo autonomo e integrato con gli altri servizi disponibili.
DBaaS	“Data Base as a Service” sono servizi gestiti costituiti da ambienti virtuali dedicati in differenti configurazioni e tecnologie, con differenti livelli di affidabilità e ridondanza in funzione delle esigenze del Cliente. Sono inclusi i servizi di backup, restore, monitoraggio, aggiornamento e patching.
STaaS	Il servizio prevede la fornitura di spazio disco prestazionale raggiungibile via rete con protocolli NFS e CIFS esclusivamente dalle macchine virtuali Nivola. La messa a disposizione dei servizi di storage avviene su infrastrutture ridondate e configurate in alta affidabilità.

BCKaaS	Il servizio di backup as a service è attivabile dall'utente per il backup delle macchine virtuali attivate in Nivola. È possibile scegliere se attivare il backup sulle risorse selezionate e scegliere i livelli di retention più appropriati per il proprio servizio. Il servizio viene erogato attraverso piattaforme che permettono una notevole affidabilità infrastrutturale, e attraverso la funzione di "deduplica dei dati", per il raggiungimento di una elevata efficienza. I backup sono depositati su apparati storage differenti da quelli che ospitano dati e servizi.
CMP	Cloud Management Platform - piattaforma di integrazione ed automazione che espone tutti i servizi di business attraverso API (Application programming Interface) richiamabili dall'utente o attraverso l'uso del Service Portal. Include i servizi di accounting, profilazione, security.
API	Application Programming Interface (in italiano traducibile come Interfaccia di programmazione di un'applicazione), le API sono strumenti di programmazione messi a disposizione degli sviluppatori per facilitare il loro compito nella realizzazione di applicazioni integrate.
NSC	Nivola Support Center - Single Point of Contact per tutti i servizi cloud (Nivola, NMSF, POSC)
CLI	Command Line Interface - nel progetto Nivola trattasi di command interface dedicata alla gestione di tutte le risorse della CMP. L'utilizzo è possibile per tutti gli utenti accreditati.
APP Engine	Template preconfigurato composto da risorse elaborative, database, storage, reti e sicurezza che implementa una particolare funzione
Region	Aggregato di una o più Availability Zone
Availability Zone	Aggregato di uno o più Site. L'AZ è caratterizzata da una sua completa autonomia infrastrutturale e indipendenza
Site	Aggregato di uno o più POD
POD	Point Of Delivery - aggregato di infrastrutture elaborative, storage, rete e sicurezza autoconsistenti
Utente/User	Persona fisica accreditata all'accesso ai servizi Nivola
Account	Contenitore di istanze di servizio
PII	personally identifiable information - informazioni personali.
VM	Virtual Machine
CMP	Cloud Management Platform - piattaforma di integrazione del progetto Nivola.
TSN	Team di Supporto Nivola.

6.2 La Piattaforma Nivola

Nivola è una piattaforma di servizi *cloud* completamente *open source* nata per semplificarne la fruizione da parte della Pubblica Amministrazione. Mette a disposizione potenza di calcolo, *storage*, rete e database oltre a numerosi altri servizi e *utility*. Il risultato è quello di permettere la completa autonomia nella creazione del proprio sistema informativo e laddove necessario nella migrazione delle proprie applicazioni in assoluta sicurezza rendendo trasparenti le tecnologie sottostanti. Nivola è in grado di mappare ruoli, compiti e responsabilità, in una struttura gerarchica che permette di governare autonomamente gli aspetti tecnici e di operatività del servizio, garantendo la necessaria sicurezza e suddivisione dei ruoli. I server virtuali sono in esecuzione sia su piattaforma *OpenStack* che su piattaforma *vSphere* in funzione dei template prescelti.

Tutti i dischi/file system dei server virtuali sono salvati su *datastore* messi a disposizione dalla *Storage Area Network*. Si tratta di un'area composta da più *server Storage* centrali collegate alle differenti infrastrutture virtuali tramite fibra ottica. Ogni *datastore*, definito su infrastruttura virtuale, ha più *path*, in modo da evitare *single point of failure* in caso di guasto di una fibra ottica, porta switch o porta server fisico. I dischi su *storage* sono configurati in RAID con *hot spare* in modo che, in caso di guasto di un disco, questo passi automaticamente in stato di *fault* e sia sostituito da altro disco senza alcun disservizio o perdita di dati.

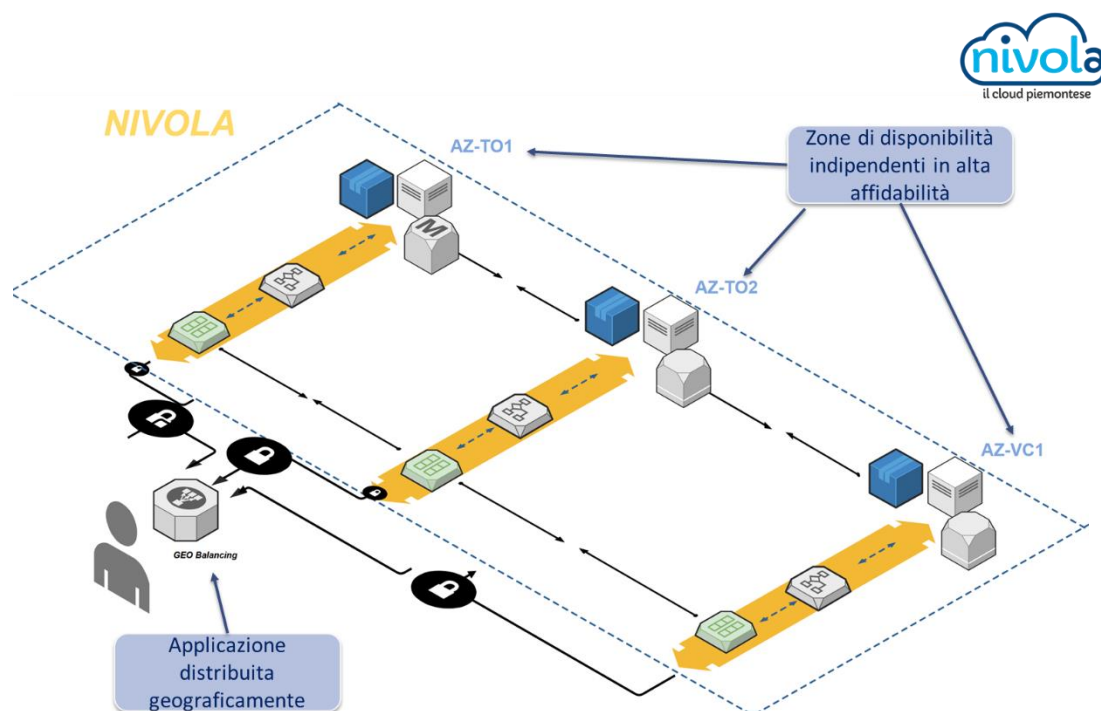
I sistemi operativi di riferimento sono:

- RedHat 6.x e successive
- CentOS 6.x e successive
- Oracle linux 5.x e successive
- Microsoft Windows 2008 server e successive

6.3 Le availability zones

Le tre *Availability Zones* (A.Z.) a disposizione di Nivola sono tra di loro indipendenti, prevedono infrastrutture elaborative e tecnologie dedicate e sono dispiegate nei due Datacenter del Consorzio e, in particolare, due all'interno del Datacenter di Torino e una nel Datacenter di Vercelli.

Le risorse infrastrutturali di ciascuna *availability zone* sono collocate all'interno di sale CED compartimentate e attestate su rack dedicati. Dal punto di vista dell'alimentazione elettrica, dei sistemi di condizionamento e antincendio le *availability zones* sono tra di loro indipendenti. In fase di creazione dei propri servizi è possibile scegliere l'*Availability zone* in base a specifiche esigenze di distribuzione geografica mantenendo inalterata l'alta affidabilità.



6.4 La struttura organizzativa

All'interno di Nivola sarà possibile modellare una struttura organizzativa su tre livelli in modo da permettere di attribuire responsabilità e gestione dei servizi secondo una gerarchia precisa. Nell'Account sarà istanziata l'infrastruttura in modo da soddisfare il fabbisogno tecnologico e di sicurezza necessario. Alla Divisione è demandato il compito di controllo del consumo delle risorse degli Account che potrà creare in assoluta autonomia. Il vertice della struttura è costituito dall'Organizzazione che avrà la visione completa dell'utilizzo della piattaforma con la possibilità di declinarla in base alle Divisioni e agli Account.

La struttura organizzativa è la suddivisione gerarchica che permette di personalizzare i servizi, l'accesso o le impostazioni per diversi gruppi di utenti o dispositivi. Nella piattaforma Nivola la struttura organizzativa si articola su 3 livelli:

Organizzazione: è gerarchicamente l'entità organizzativa più elevata e può coincidere con il nome del cliente. Nella piattaforma le risorse sono a disposizione di varie organizzazioni, che sono però dal punto di vista logico completamente separate e indipendenti;

- Divisione: è il secondo livello organizzativo. Una organizzazione può avere più divisioni. Il concetto di Divisione rappresenta quindi una suddivisione logica dell'Organizzazione, e può riflettere dunque una divisione di tipo territoriale, organizzativa o di tipo di business; inoltre ciascuna Divisione controlla le risorse e i consumi di ciascun Account all'interno della Divisione»;
- Account: è l'ultimo livello organizzativo e dipende dalla Divisione. Una Divisione contiene uno o più Account. L'Account è il livello organizzativo all'interno del quale l'Utente potrà creare, controllare e gestire i propri servizi. È possibile creare molteplici Account con lo scopo di separare progetti differenti, oppure distinguere ambienti di sviluppo da quelli di produzione oppure allo scopo di suddividere la rendicontazione dei consumi.

Tutte le risorse e i servizi sono associabili solo a livello di Account. Non è possibile associare i servizi alle Divisioni o alle Organizzazioni. L'Account rappresenta quindi il contenitore in cui vengono implementati e resi disponibili tutti i servizi utente. La gestione delle risorse utente avverrà quindi a livello di Account con dei ruoli abilitati ad operare a questo livello.

6.5 Utenti, ruoli ed Account

Si possono distinguere più ruoli all'interno della piattaforma, che si correlano alla struttura organizzativa definita. Ad ogni ruolo può corrispondere almeno un utente, e quindi almeno una persona fisica che svolge quella funzione. Una persona registrata sul sistema può essere associata a più ruoli anche su strutture organizzative differenti. Ad esempio un utente può avere ruoli differenti su account anche di divisioni distinte.

Ad oggi all'interno del sistema sono implementati i seguenti ruoli utente.

Master di Organizzazione: questo ruolo rappresenta gli utenti che possono svolgere funzioni amministrative all'interno dell'Organizzazione quali la creazione, sempre all'interno dell'organizzazione di pertinenza, delle divisioni e degli account; può inoltre profilare gli utenti per renderli operativi all'interno della propria struttura ed eventualmente registrare utenti non ancora

presenti sulla piattaforma. Il Master di Organizzazione può monitorare i costi e lo stato delle risorse a tutti i livelli della propria struttura organizzativa (divisioni e account) e visualizzarne i relativi report. Non ha però accesso alle funzioni di gestione (creazione/modifica/cancellazione) delle risorse associate agli account della propria organizzazione.

Master di Divisione: questo ruolo rappresenta gli utenti che possono svolgere funzioni amministrative all'interno della Divisione quali la creazione, sempre all'interno della divisione di pertinenza, degli account; può inoltre profilare gli utenti per renderli operativi all'interno della propria struttura ed eventualmente ha la possibilità di registrare utenti non ancora presenti sulla piattaforma. Il Master di Organizzazione può monitorare i costi e lo stato delle risorse a tutti i livelli della propria struttura organizzativa (account) e visualizzarne i relativi report. Non ha però accesso alle funzioni di gestione (creazione/modifica/cancellazione) delle risorse associate agli account della propria divisione.

Amministratore di Back Office: utente che all'interno del sistema ha privilegi sulle funzioni di BackOffice (registrazione nuovi Utenti, Accreditamento, creazione livelli organizzativi) e monitoraggio costi e stato della piattaforma. L'Amministratore di BackOffice può profilare utenti con ruoli a qualsiasi livello della struttura organizzativa. Può inoltre accedere ai report dei costi e consumi aggregati a qualsiasi livello. Il ruolo è solitamente associato a utenti dei gruppi di gestione e supporto Csi Piemonte.

Master di Account: utente che all'interno dell'Account può gestire tutte le risorse, sulle quali ha quindi il massimo dei privilegi. Il Master di Account può quindi creare/cancellare/modificare le risorse, può anche gestire le risorse create da altri utenti nell'account. Il Master di Account può visualizzare e accedere ai report dei costi e dei consumi relativamente al proprio account. Il master di account non può registrare nuovi utenti all'interno della propria piattaforma e non può profilare altri utenti ad accedervi.

La fase di introduzione di un nuovo utente si articola in questo modo: un master, nel limite dei privilegi del suo livello gerarchico, può accreditare un utente registrato sulla piattaforma assegnandogli un ruolo, in questo modo gli concede dei permessi per svolgere determinate funzioni che faranno ricadere il nuovo utente in un determinato gruppo.

La stessa operazione può essere effettuata e delegata all'operatore di Backoffice.

Riassumendo:

- Un Master di Organizzazione può accreditare o revocare utenti all'interno delle proprie divisioni o account
- Un Master di Divisione può accreditare o revocare utenti all'interno dei propri account.
- L'Amministratore di Backoffice può accreditare o revocare ruoli agli utenti a qualsiasi livello della struttura gerarchica.

6.6 Certificazioni e compliance

I servizi cloud erogati dal CSI Piemonte sono certificati ISO 27001:2013 e conforme ai controlli previsti dalle norme ISO 27017:2015 e ISO 27018:2014, ISO 20000-1 e ISO 22301. Il CSI Piemonte è inoltre qualificato come CSP (Cloud Service Provider) accreditato da AGID e le proprie infrastrutture

sono state riconosciute da AGID come candidabili ad essere utilizzate dal Polo Strategico Nazionale. Inoltre è certificato Tier III secondo lo standard ANSI TIA 942.

6.7 Tipologia di utenti della piattaforma

Le tipologie di utenze sono identificate in:

- personale interno CSI-Piemonte, in quanto primo utilizzatore dei servizi che vengono implementati sulla piattaforma per la costruzione e sviluppo di nuovi servizi applicativi;
- risorse messe a disposizione dall'Appaltatore.

6.8 Fase di provisioning-attivazione servizi

Ricevuta la documentazione prevista dell'Appaltatore, il CSI-Piemonte avvia l'attivazione dei servizi cloud. La persona indicata come riferimento tecnico dell'Appaltatore viene contattata dal servizio di assistenza del CSI-Piemonte per i dettagli tecnici.

In questa fase l'Appaltatore deve dichiarare se il riferimento tecnico sia anche la persona da contattare in caso di *incident* di sicurezza oppure se preferisca specificare un nominativo diverso, in ottemperanza alle norme in ambito di *data breach*.

6.9 Erogazione dei Servizi

L'Appaltatore riceverà il link e le credenziali per accedere al Service Portal, alla CLI e ad altri tools eventualmente necessari, attraverso i quali:

- accede alla piattaforma Nivola;
- visualizza l'elenco dei servizi messi a disposizione;
- scarica la documentazione relativa ai manuali utente;
- visualizza l'andamento dei consumi per ogni servizio;
- modifica le caratteristiche dei servizi in uso;
- sottopone le richieste di assistenza e supporto rispetto ai servizi messi a disposizione.

All'atto del *kick off* saranno condivise anche le policy di controllo dell'accesso al sistema da parte dell'Appaltatore.

6.10 Tipologia dei dati trattati

La piattaforma Nivola per il suo normale funzionamento non tratta dati di tipo PII dell'Appaltatore, gli unici dati contenuti sono le informazioni di profilazione delle utenze.

I dati contenuti nelle aree di archiviazione (storage, database e backup) vengono manipolati esclusivamente dal personale autorizzato del CSI-Piemonte (Team di Supporto Nivola o Datacenter) e gestiti secondo le *best practices* relative ai dati PII.

Resta inteso che per l'ambiente di test predisposto dall'Appaltatore sulla piattaforma Nivola non saranno in alcun modo utilizzati dati provenienti da fonti (STaaS, DBaaS e backup) dell'Appaltatore e quindi che potrebbero contenere dati di tipo PII.

6.11 Servizi e Interfacce visibili all'Appaltatore

6.11.1 Risorse elaborative

Il servizio permette, attraverso la piattaforma Nivola, di assegnare le risorse elaborative (esprese in CPU, RAM e spazio disco) necessarie ed indicate dall'Appaltatore all'interno della relazione tecnica. L'Appaltatore sarà in grado di realizzare macchine virtuali e di gestirle in modo autonomo e coeso con gli altri servizi disponibili sulla piattaforma come per esempio le risorse di rete, il bilanciamento, data base, backup, ecc.

In fase di creazione iniziale, come evidenziato dalla tabella RACI dei capitoli precedenti, l'Appaltatore fornirà al CSI Piemonte le indicazioni precise relativi agli ambienti e alle risorse necessarie tramite la compilazione della Scheda di Provisioning in linea con quanto dichiarato in fase di Gara e contenuto all'interno dello Schema di Deployment.

Tagli delle risorse

L'Appaltatore nella sua Relazione Tecnica dovrà indicare il fabbisogno di risorse in base alle seguenti disponibilità:

Flavour	Risorse		
	Core	RAM (GB)	Disco (GB)
m1.small	1	2	20
m1.medium	2	4	40
m1.large	4	8	80
r4.2xlarge	2	8	80
m1.2xlarge	8	24	140
r4.4xlarge	2	16	100
i3.4xlarge	8	32	140
i3.8xlarge	8	48	140
d2.8xlarge	16	64	140

Nel caso in cui le risorse messe a disposizione non fossero sufficienti a soddisfare le necessità della soluzione applicativa proposta, l'Appaltatore dovrà evidenziare i volumi necessari indicando nel dettaglio le risorse necessarie per ciascuno dei seguenti servizi:

- virtual machine (CPU, RAM, HD);
- backup: spazio necessario per il backup con una retention indicative di 30 giorni;
- DBAAS: tecnologia (tra quelle disponibili), dimensioni (RAM, CPU, HD), eventuali tools necessari per la normale amministrazione.

Il CSI-Piemonte tramite la piattaforma Nivola metterà a disposizione dell'Appaltatore i seguenti servizi:

- Compute Services;

- Reti: private, RUPAR, Internet Assegnazione indirizzamento RUPAR e/o Internet;
- STAAS: storage a blocchi montabile sulle singole VM tramite protocollo nfs o cifs;
- applicazione eventuale policy di affinità/anti-affinità;
- configurazione policy di sicurezza sui firewall fisici;
- configurazione policy di sicurezza tramite la definizione di appositi Security Group virtuali (micro-segmentazione);
- servizio di monitoraggio della piattaforma cloud e dei servizi di DBAAS e STAAS;
- servizio di Backup as a Service;
- servizi di VPN.

L'appaltatore in caso di utilizzo di RDBMS che richiedano licenze d'uso (a titolo di esemplificativo e non esaustivo Oracle Database, Microsoft Sql Server) dovrà prevedere l'uso di licenze proprie, Bring Your Own License (BYOL, uso di licenze proprie): con questo modello di licenza, è possibile eseguire le implementazioni di Database usando la licenza di proprietà dell'Appaltatore. Per eseguire un'istanza database con il modello BYOL, occorre disporre dell'opportuna licenza (con licenza e supporto per aggiornamento del software) per la classe di istanze database e l'edizione di Database che si desidera eseguire. Rimane a carico dell'appaltatore il rispetto delle policy di licenza di Database per software, nell'ambiente di cloud computing.

Supporto, nella configurazione BYOL l'appaltatore potrà continuare a usare l'account attivo di supporto e contattare direttamente il produttore per le richieste specifiche relative al servizio Database.

Scalabilità, si potrà scalare le istanze database in conformità con i termini della licenza (o delle licenze) di Database.

Upgrade di versione, Con il modello BYOL è possibile migrare dalle edizioni Standard del software a Enterprise Edition, purché si disponga di una licenza idonea non utilizzata per l'edizione e la classe di istanza database che si desidera impiegare. Per modificare l'edizione conservando i dati, è necessario acquisire uno snapshot dell'istanza database in esecuzione e utilizzarlo per creare una nuova istanza database con l'edizione desiderata. L'istanza database precedente deve poi essere eliminata, a meno che non si disponga della relativa licenza e si desideri mantenerla in esecuzione.

Multizona, per impiegare le istanze database di standby potrà essere necessario il doppio delle licenze per le implementazioni Multi-AZ rispetto alle implementazioni Single-AZ corrispondenti. Tuttavia, prima di tutto dovrai consultare il contratto di licenza del software e verificare la conformità con le policy di licenza del produttore.

6.11.2 Storage aaS

Il servizio messo a disposizione per l'Appaltatore è composto da spazio disco prestazionale o *lowrange* raggiungibile via rete (NFS o CIFS). La messa a disposizione dei servizi di storage avviene su infrastrutture ridondate e configurate in alta affidabilità.

6.11.3 Backup aaS

Il servizio messo a disposizione per l'Appaltatore è composto da servizi *managed* configurati in funzione delle indicazioni fornite dall'Appaltatore e contenuti nel Progetto Infrastrutturale. Il servizio prevede la funzione di *snapshot* giornaliero delle VM indicate dall'Appaltatore.

6.11.4 Il Service Portal

Il Service Portal (portale di servizio) permette all'Appaltatore di interagire con la piattaforma NIVOLA. Attraverso l'utilizzo di un browser è possibile operare sui servizi e sulle risorse messe a disposizione dalla piattaforma stessa.

6.11.5 Accesso tramite CLI

All'Appaltatore è inoltre fornito anche un accesso tramite CLI (*Command Line Interface*) in cui sono disponibili tutte le funzionalità di business presenti sul *Service Portal* con un livello di granularità e di dettaglio maggiore.

L'accesso a tale strumento, disponibile per ogni *availability zone*, è soggetto ad autenticazione e profilazione coerente con quella del *Service Portal* e delle API, in modo che l'operatività sia consentita solo nelle aree di competenza associate con il profilo utente. Attraverso la CLI è inoltre possibile aprire sessioni SSH verso le VM applicative di test e di produzione create per ospitare il servizio applicativo messo a disposizione dall'Appaltatore.

6.11.6 Tools

La piattaforma Nivola mette a disposizione ulteriori *tools* che permetteranno all'Appaltatore di svolgere le attività correlate alla Conduzione dei Servizi in totale autonomia (interfacce per amministrazione DB con profili applicativi, servizi proxy per abilitazione servizi di trasferimento file verso le VM applicative, front-end Guacamole ecc.).

6.12 Modalità di conduzione dei servizi

6.12.1 Attività in carico all'Appaltatore

Per i servizi oggetto del Capitolato l'Appaltatore assumerà la conduzione operativa di tutte le componenti di sistema presenti all'interno della piattaforma Nivola e necessarie al funzionamento della Soluzione.

Nell'Allegato 1A "Tabella RACI" sono elencati nel dettaglio i ruoli e le responsabilità. A titolo esemplificativo saranno a carico dell'Appaltatore:

- la gestione sistemistica delle VM applicative;
- l'esecuzione di attività di installazione e configurazione delle componenti del sistema operativo delle VM eventualmente non presenti nelle immagini standard;
- l'aggiornamento del sistema operativo e dei software eventualmente installati sulle VM a cura dell'Appaltatore;

- l'installazione delle patch e degli aggiornamenti di sicurezza nell'ambito della versione e della release del sistema operativo installato;
- l'identificazione degli impatti e la ricerca della loro causa, attraverso un processo correttivo (*troubleshooting*), a fronte del presentarsi di malfunzionamenti;
- la fornitura, l'installazione, la gestione e l'aggiornamento del sistema locale antivirus dei server Microsoft eventualmente necessari all'Appaltatore;
- il mantenimento, nello svolgimento delle attività, del controllo degli accessi finalizzato a proteggere e limitare gli interventi sui server solo agli utenti autorizzati, in accordo con le indicazioni fornite dal CSI-Piemonte;
- la costante messa in sicurezza del sistema, al fine di ridurre la superficie di attacco del sistema operativo delle VM, attraverso l'applicazione delle best-practice relative all'*hardening* dei sistemi, con l'eventuale rimozione o disabilitazione di software, di utenze o di servizi non necessari;
- l'ottimizzazione continua delle risorse a sua disposizione al fine di migliorare le prestazioni di sistema, eventualmente bilanciando le risorse tra le AZ, adeguando le aree di storage e parametrizzando il software di base;
- la fornitura, l'installazione, la configurazione e la gestione delle componenti aggiuntive del sistema operativo eventualmente necessarie per il funzionamento della Soluzione (Es.: Application server, Web Server, ecc.);
- la predisposizione della struttura dello spazio disco utente;
- il mantenimento della sicurezza di rete logica delle VM applicative su cui è in esecuzione la Soluzione;
- il *troubleshooting* applicativo-sistemistico per la Soluzione;
- il monitoraggio sistemistico e applicativo delle VM e delle componenti applicative di cui è composta la Soluzione;
- backup e restore: sono a carico dell'Appaltatore l'indicazione delle specifiche tecniche di backup per quanto riguarda il servizio di Backup as a Service, la creazione di opportune procedure di export ed importo dei dati, la responsabilità della consistenza logica dei dati contenuti nel backup, in particolar modo in caso di procedure di export dei Database. L'Appaltatore ha a disposizione gli strumenti che gli consentono di essere autonomo ed indipendente nella fase di *restore*. Si precisa che l'Appaltatore non dovrà effettuare *restore* dei dati presenti nell'ambiente di produzione verso gli ambienti di formazione e test;

- la gestione delle *policy* (definite da CSI-Piemonte) di protezione dei dati degli ambienti RDBMS dedicati al servizio.

6.12.2 Attività in carico al CSI-Piemonte

A titolo esemplificativo in relazione ai servizi cloud messi a disposizione del Fornitore saranno a carico del CSI-Piemonte:

- la gestione della piattaforma cloud Nivola per l'erogazione dei servizi messi a disposizione dell'Appaltatore, facendosi carico sia della gestione della sicurezza fisica e logica, sia dell'aggiornamento tecnologico dell'infrastruttura che ospita i servizi della Piattaforma Cloud Nivola;
- l'accoglienza e l'assistenza di primo livello per problematiche legate alla piattaforma Nivola, accompagnando l'Appaltatore sulle tematiche di utilizzo della piattaforma, sulle informazioni riguardanti funzionalità presenti sulla stessa e sull'assistenza tecnico/sistemistica per le problematiche che necessitano di tale competenza;
- il corretto funzionamento delle infrastrutture Cloud su cui è ospitata la Soluzione, in forma integrata per assicurare la regolare conduzione in piena operatività dei sistemi (server, apparati di rete, storage, bilanciamento geografico) e software (Service Portal, Cloud management Platform e servizi Cloud erogati), utilizzati per la quotidiana erogazione dei servizi e prodotti costituenti la piattaforma Nivola;
- il monitoraggio operativo H24 7x7 delle componenti della Piattaforma Nivola;
- la risoluzione degli incidenti infrastrutturali e/o la richiesta di *change* con l'obiettivo di perseguire, per tali interventi, un incremento di efficacia ed efficienza;
- il supporto all'uso;
- la gestione della piattaforma e delle sue componenti per poter intervenire a fronte di potenziali criticità, malfunzionamenti o *change*;
- la raccolta e messa a disposizione dei log di sicurezza della piattaforma. Il CSI-Piemonte è punto di riferimento per l'Appaltatore per la messa a disposizione delle informazioni di competenza;
- l'attività di *Incident Management* e *Data Breach*: si occupa della raccolta e messa a disposizione dei dati relativi agli incidenti della piattaforma Nivola. Il CSI-Piemonte è punto di riferimento per l'Appaltatore per la messa a disposizione delle informazioni di competenza;
- la gestione dell'infrastruttura dei servizi di backup. Il CSI-Piemonte è responsabile della fase di *restore* fisico su indicazione dell'Appaltatore;

- la messa a disposizione del servizio di *Tenant* di rete, che prevede la predisposizione di una zona di rete riservata in cui l'Appaltatore può operare in completa autonomia; le configurazioni comprendono indirizzi IP su reti esterne attestate su rete RUPAR o su rete INTERNET, proxy, firewall, DNS.

L'Allegato 1A "Tabella RACI" riporta in maniera dettagliata ruoli e responsabilità in capo al Fornitore aggiudicatario, alla Stazione Appaltante e al CSI Piemonte.

6.12.3 Condizioni Generali

Sarà richiesta all'Appaltatore l'adesione alle Condizioni Generali d'uso della piattaforma cloud NIVOLA al fine di poter procedere alla consegna delle credenziali di accesso al servizio.

6.13 Manuale utente

All'atto del *kick off* sarà messo a disposizione dell'Appaltatore il Manuale d'uso in formato elettronico aggiornato all'ultima versione. Successivamente, secondo quanto previsto nel Piano delle Consegne, saranno rese disponibili le credenziali di accesso al servizio.