UNIVERSITÀ DEGLI STUDI DEL MOLISE

CAMPOBASSO

PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) MISSIONE 4, COMPONENTE 2, INVESTIMENTO 3.1 “Fondo per la realizzazione di un sistema integrato di infrastrutture di ricerca e innovazione”

PROGETTO “Strengthening of the Italian RI for Metrology and Open Access Data in support to the Agrifood” - CUP I83C22001040006.

CAPITOLATO TECNICO (ALL. B)

PROCEDURA APERTA SOPRA SOGLIA COMUNITARIA IN MODALITÀ TELEMATICA PER L’AFFIDAMENTO DELLA REALIZZAZIONE DI UN’INFRASTRUTTURA PER LA GESTIONE DEI DATI AUTENTICATI SU BLOCKCHAIN PUBBLICHE E PRIVATE.

CODICE IDENTIFICATIVO GARA: 992233490A

Sommario

1. Introduzione

Il progetto di cui al presente capitolato riguarda la realizzazione di un'infrastruttura per la gestione dei dati autenticati su blockchain pubbliche e private all'interno di un esistente complesso edilizio, posto nel II Edificio Polifunzionale in Via De Sanctis snc, Campobasso. Inoltre, il progetto mira anche ad allestire due laboratori di informatica in due sedi dell'Università degli Studi del Molise, ossia nella sede di Pesche e nella sede di Termoli.

2. Il progetto METROFOOD-IT

L'Università degli Studi del Molise, come finalità del progetto METROFOOD-IT, intende realizzare un Data Center che farà da infrastruttura per la gestione dei dati autenticati su blockchain pubbliche e private. Inoltre, l'Università degli Studi del Molise mira ad allestire due laboratori di informatica sia presso la sede di Pesche che presso la sede di Termoli.

Il progetto METROFOOD-IT mira a realizzare la piena implementazione dell'infrastruttura e strutturando la strategia, le procedure e il sistema di supporto per l'erogazione di servizi attraverso Accesso Transnazionale (sia fisico che remoto) e l'accesso virtuale, raggiungendo così la piena operatività. I servizi offerti permetteranno all'infrastruttura di fare da interfaccia tra ricerca e innovazione, ma anche tra degli specifici attori (come, ad esempio, attori industriali e consumatori). Inoltre, con questi specifici servizi, è possibile definire e sperimentare diversi processi e scenari per lo sviluppo di sistemi agroalimentari sostenibili e innovativi, la sicurezza alimentare, diete sane e soluzioni per una bioeconomia circolare.

Il Data Center di METROFOOD-IT è creato per la cooperazione di quattro principali categorie di utenti: ricercatori, policy makers (o agenzie di ispezione e controllo), operatori del settore alimentare e consumatori (o associazioni di consumatori). Per iniziative di co-creazione ci sono anche le aziende che cooperano con i cittadini, le agenzie di ispezione e controllo, i decisori politici e le autorità locali.

L'infrastruttura di METROFOOD-IT mira a creare due tipi di infrastruttura: un'infrastruttura fisica (Physical-RI, P-RI) ed un'infrastruttura elettronica (e-infrastructure, e-RI).

L'infrastruttura fisica (P-RI) completa una rete esistente di facilities all'avanguardia che si distingue in due aree, "Metro" e "Food". Nell'area "Metro" sono presenti laboratori per la caratterizzazione chimica, chimico-fisica e microbiologica degli alimenti e di qualsiasi matrice di interesse per il settore agroalimentare, come ad esempio matrici ambientali dell'agroecosistema di produzione, mangimi, materiali a contatto con gli alimenti, e così via. Nell'area "Food" sono presenti campi/fattorie

sperimentali per la produzione agricola e l'allevamento, impianti su piccola scala per la trasformazione e la conservazione degli alimenti, cucine-laboratorio per la preparazione degli alimenti e siti "demo" per il coinvolgimento diretto degli stakeholder e per la gestione di Living labs. Invece, l'infrastruttura elettronica (e-RI) consiste in un'architettura orientata ai servizi che fornisce una piattaforma accessibile per la condivisione e l'integrazione dei dati, conoscenze e informazioni sugli strumenti metrologici per l'analisi degli alimenti e per facilitare la condivisione e l'utilizzo di dati da parte della comunità di utenti. L'e-RI aggiunge i risultati della componente fisica dell'infrastruttura ai dati esistenti. Inoltre, essa espande la sua interoperabilità e si integra con i dati derivanti da altre reti e infrastrutture.

L'infrastruttura deve essere in linea con i principi della Responsible Research and Innovation (RRI). Quindi, deve fornire servizi distribuiti, garantendo l'affidabilità e l'armonizzazione delle procedure. Inoltre, si mira ad adottare un approccio FAIR sui dati e sui servizi digitali a supporto dell'agroalimentare.

Grazie all'installazione di questa infrastruttura, l'Università degli Studi del Molise può avere una forte caratterizzazione sul punto di vista della ricerca e dello sviluppo. Quindi, il Data Center del progetto METROFOOD-IT dell'Università degli Studi del Molise mira ad investire su tecnologie molto innovative, come la tecnologia Blockchain e il Cloud computing. Con questa infrastruttura si intende integrare il settore agroalimentare con nuove tecnologie garantendo privacy e sicurezza. Inoltre, l'Università degli Studi del Molise intende modernizzare il proprio apparato informatico, valorizzando il proprio patrimonio informativo. Per queste ragioni, si è anche pensato all'allestimento di due laboratori di informatica all'avanguardia sia per la sede di Pesche che per la sede di Termoli.

Il Data Center di METROFOOD-IT, oltre a valorizzare il progetto omonimo e l'Università degli Studi del Molise, valorizza anche la Regione Molise attraverso le tecnologie che offre l'infrastruttura. Pertanto, l'Università degli Studi del Molise deve dotarsi di una struttura innovativa che possa raccogliere, analizzare, conservare e trasmettere i dati raccolti. L'infrastruttura deve essere caratterizzata dai seguenti aspetti principali:

1. deve avere tecnologie principalmente Open Source eseguibile su piattaforme interamente Open-source, quali Linux;
2. è progettata per migliorare l'interoperabilità verso altre apparecchiature scientifiche;
3. deve essere altamente scalabile, multiprotocollo ad alte prestazioni per file e object storage;
4. deve essere affidabile e sicura, basata su multithreading, multi-core microprocessore;

5. deve essere flessibile sull'allocazione e il controllo delle risorse dedicate alla conservazione all'interno dell'infrastruttura basata su Blockchain-as-a-Service;
6. deve adottare specifiche di sicurezza che garantiscono i requisiti posti dalla gestione dei dati;
7. deve garantire una continuità di servizio anche in caso di interruzioni della rete elettrica.

Il presente capitolato tecnico disciplina gli aspetti tecnici della fornitura di hardware e software. Inoltre, esso descrive l'installazione, la manutenzione e l'assistenza tecnica specialistica per la realizzazione del Data Center.

3. Infrastruttura Blockchain-as-a-Service

L'infrastruttura per METROFOOD-IT dovrà includere tutte le parti hardware e le licenze software necessarie e dimensionate per garantire la piena funzionalità del sistema secondo quanto richiesto, secondo quanto offerto dal Fornitore e secondo quanto raccomandato dal produttore in condizioni di massimo carico e massima occupazione di spazio. Si specifica che non sarà necessario fornire tutti i cavi patch (patch cable) necessarie ai collegamenti con la rete LAN mentre sarà necessario fornire tutte le componenti del cablaggio per l'interconnessione delle componenti del sistema.

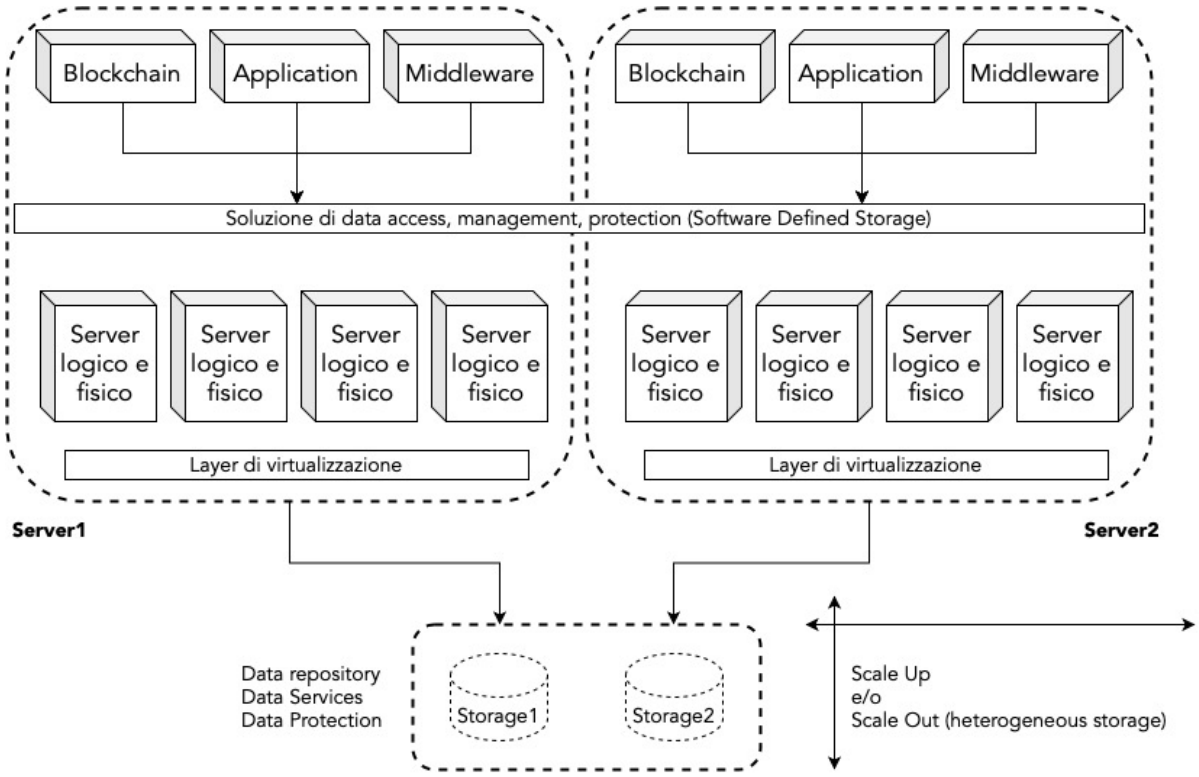


Figura 1. Schema logico per un'architettura di riferimento

La soluzione rappresenta il centro di raccolta di tutti i dati che devono essere conservati e tracciati con sicurezza. Le seguenti caratteristiche vogliono massimizzare la realizzazione dei progetti presenti e futuri di Ateneo:

- l'eterogeneità dei protocolli di comunicazione per interagire con dati provenienti da fonti diverse presenti e future;
- l'affidabilità e la sicurezza;
- la scalabilità modulare;
- la semplicità di configurazione e gestione;
- la possibilità di diversificare i volumi storage in base a requisiti di performance;
- la facile interazione con ambienti Big Data;
- la facile interazione con ambienti Cloud.

Dal punto di vista infrastrutturale la soluzione dovrà essere composta da tre macro-elementi:

- componente software per la gestione e accesso condiviso ai dati (Software Defined Storage);
- componente repository dati (Storage);
- componente computazionale (Server).

La soluzione offerta dovrà essere nuova e non potranno essere offerti apparecchiature e strumenti usati, né in condizioni "ricondizionate" o provenienti da precedenti sessioni demo. Quanto offerto dovrà essere esente da qualsiasi difetto per quanto riguarda la progettazione, il materiale, l'esecuzione e la lavorazione dello stesso, deve essere perfettamente funzionante nonché esente da vincoli, cauzioni o oneri, ipoteche, gravami e diritti di terzi di qualsiasi genere e da controversie imputabili a violazione di brevetti.

Inoltre, dovrà essere fornito il manuale utente aggiornato per l'utilizzo delle apparecchiature e delle schede di installazione.

La soluzione dovrà essere conforme a tutti gli obblighi che incombono sui fabbricanti/importatori in merito ai loro prodotti (o a quelli immessi sul mercato sotto la propria responsabilità) in virtù delle Direttive Comunitarie.

3.1 Sostenibilità

Il Fornitore dovrà obbligatoriamente presentare adeguate certificazioni a sostegno della soluzione proposta in ottica "green", come ad esempio, EnergyStar, 80 Plus, e così via.

3.2 Componente software storage per la gestione e l'accesso condiviso ai dati

La soluzione hardware e software richiesta dovrà prevedere uno scale-out file system parallelo ad alte prestazioni, elemento centrale della soluzione proposta con caratteristiche funzionali, prestazionali e di elevata affidabilità. La soluzione dovrà essere preferibilmente di tipo Software Defined Storage (SDS) per fornire tutte le funzioni richieste dall'Università degli studi del Molise.

I nodi, o building block (BB), proposti dovranno essere paritetici e fornire una componente server (fisica/virtuale) avente servizi di gestione ed accesso alla componente storage fisica, servizi di replicazione remota, accesso ai client NFS, SMB and Object. Inoltre, sul repository storage fisico in SAN o NAS ci devono essere funzioni di memorizzazione, archiviazione, data protection e con opportune caratteristiche di alta affidabilità.

Il sistema deve garantire l'esecuzione di operazioni di upgrade sia in scale-out (aggiungendo altri nodi ed ampliando il file system) che in scale-up (aggiungendo altra capacità di memorizzazione e/o di throughput) all'interno del singolo nodo.

Tutti i nodi che formano i sistemi offerti hanno caratteristiche hardware e software tali da offrire e garantire la stessa tipologia di servizi come richiesto dal presente capitolato di gara. In questo modo sarà possibile consentire la realizzazione di un'architettura flessibile composta da nodi paritetici ed indipendenti, governati dall'unico Software Defined Storage, capaci di operare come un unico sistema distribuito che ripartisca il carico di lavoro tra servizi, sessioni, I/O, dati e carico computazionale su tutti i nodi o, mediante policy configurabili in modalità concorrente su un loro sottoinsieme.

La soluzione proposta con i suoi nodi è quindi replicabile e scalabile sia orizzontalmente che verticalmente risultando pienamente aderente alle definizioni di sistema Scale-Out.

La soluzione proposta deve essere basata su:

- un file system parallelo ad alte prestazioni estremamente scalabile e flessibile di tipo scale-out che consente di disaccoppiare le crescite hardware indipendentemente dalla componente software per operare scelte ottimizzanti in virtù delle esigenze sia delle specifiche istanze di calcolo sia di gestione di dati;
- un'architettura scale-out e scale-up per aumentare lo spazio disco (anche di tier e qualità differenti) attraverso incrementi di capacità.

Inoltre, i nodi del cluster devono essere paritetici, ossia devono avere la stessa configurazione hardware server e storage, devono essere adeguati alle specifiche esigenze e devono ospitare le medesime componenti software. L'uniformità tecnologica della soluzione proposta verrà garantita

dall'architettura Software Defined Storage (SDS) proposta, soluzione flessibile che si adattano alle esigenze dell'Università degli Studi del Molise e di METROFOOD-IT.

Un elemento fondante sarà la possibilità di poter creare cluster scale-out locali che si scambiano dati a seconda delle esigenze oppure cluster su distanze geografiche maggiori. La mancanza di lock-in tecnologici è un valore aggiunto senza limitazioni alle possibili modifiche e alle crescite per l'acquisizione di nuovo hardware.

La soluzione deve rispondere pienamente alle seguenti caratteristiche:

- **longevità**: garanzie e roadmap per i traguardi dei prossimi 5 anni;
- **flessibilità dell'architettura**: da garantire attraverso la soluzione SDS per avere flessibilità nelle modifiche necessarie nel corso del periodo di validità del contratto, potendo anche ridisegnare e destinare parte delle sue componenti a finalità non ancora emerse al momento della definizione dell'infrastruttura iniziale;
- **upgrade**: l'upgrade dei sistemi può essere eseguito in modalità scale-out e/o scale-up, ma sempre in modalità concorrente;
- **cambio d'uso**: deve essere possibile configurare l'infrastruttura (o una sua parte) in modo da destinarla alle rinnovate esigenze operative ed applicative senza compromettere l'architettura e le funzionalità offerte. Inoltre, deve essere possibile collegare ed integrare lo storage anche con ambienti cloud, containerizzati e Kubernetes;
- **estensibilità con sistemi di archiviazione**: per integrare successivamente l'infrastruttura con soluzioni di data protection, backup e archiviazione.

3.2.1 Aderenza architetturale

L'architettura della soluzione prevista nel II Edificio Polifunzionale dell'Università degli Studi del Molise deve poter operare come singolo sistema, essere modulare e supportare l'espansione della stessa in modalità scale-out. L'architettura, logicamente composta da nodi indipendenti capaci di operare come un unico sistema distribuito, dovrà ripartire il carico di lavoro tra servizi, sessioni, I/O, dati e carico computazionale su tutti i nodi o, mediante politiche configurabili a caldo, su un loro sottoinsieme.

3.2.2 Descrizione delle componenti hardware

La soluzione proposta dovrà poter prevedere la possibilità di integrare al suo interno componenti di caratteristiche e prestazioni differenti, almeno relativamente a:

- supporti di memorizzazione di tipologie, prestazioni e dimensioni differenti;

- tipologie e prestazioni delle componenti di I/O di front-end;
- modelli e prestazioni delle CPU;
- tipologie e prestazione della memoria cache.

Tutte le componenti, sebbene diverse per caratteristiche, dovranno essere completamente integrate tra loro, permettendo di sfruttare a pieno le capacità di ognuna. Il Fornitore deve descrivere dettagliatamente tutte le componenti hardware e software incluse in offerta.

3.2.3 Nodi del sistema

I nodi presenti nel sistema devono essere dei nodi ridondanti di tipologia active/active la cui sostituzione anche a caldo non deve avere alcun impatto sulle funzionalità ed operatività del sistema proposto.

3.2.4 Power e Ridondanza

La rimozione/sostituzione anche a caldo di un alimentatore non deve avere nessun impatto sulle funzionalità ed operatività del sistema. Il sistema di alimentazione fornito deve essere dimensionato in modo tale da supportare il consumo a pieno carico con ridondanza su due linee di alimentazione, in cui la mancanza di alimentazione su una delle due linee non deve avere alcun impatto sulle funzionalità ed operatività del sistema.

3.2.5 Cooling, raffreddamento e ventilazione

Il sistema di raffreddamento e ventilazione deve essere tale da supportare il funzionamento a pieno carico. Il sistema deve prevedere la sostituzione di ventole, componenti a caldo, senza richiedere il fermo del sistema. Inoltre, devono essere forniti i dati di targa a pieno carico di ingombro, peso, consumi elettrici e raffreddamento.

3.2.6 Autenticazione e management

Il sistema deve prevedere l'autenticazione alle sessioni di amministrazione tramite Microsoft Active Directory ad un Domain Functional Level almeno Windows 2012 R2 e 2016, con sistemi standard LDAP e LDAPS, oltre a consentire la creazione di utenti locali.

3.2.7 Tool di management

Il sistema deve prendere un software di gestione con GUI basata su accesso tramite WEB, protocollo SSH, con messaggi di notifica stato tramite e-mail, SNMP e Syslog. Il sistema storage dovrà prevedere

un unico punto di gestione che dovrà essere accessibile sempre con le medesime modalità e caratteristiche a prescindere dalla disponibilità delle risorse del sistema. Dal management unificato dovranno essere gestibili tutte le caratteristiche e le funzionalità del sistema.

Il sistema è stato pensato per avere una logica distribuita e quindi esso dovrà essere pensato con un management unificato. In pratica, il sistema storage dovrà avere un singolo punto di gestione, che dovrà essere accessibile sempre con le stesse modalità e caratteristiche a prescindere dalla disponibilità delle risorse del sistema.

3.2.8 Supporto e gestione delle quote

Il sistema deve prevedere la gestione delle quote. In pratica, il sistema deve poter definire livelli di quota per ogni directory, utente e, gruppo di utenti.

3.2.9 Supporto snapshot

Il sistema deve permettere la gestione degli snapshot dei singoli filesystem/directory, creabili sia in modalità manuale che programmata/automatica, almeno 200 per singolo file system. Inoltre, deve essere possibile eliminare manualmente ed automaticamente su base temporale degli snapshot.

3.2.10 Replica

Il sistema deve supportare la funzionalità di replica sincrona e/o asincrona dei dati almeno tra i sistemi della stessa classe e tipologia. La replica deve essere ottenuta tramite proprie funzionalità native e non tramite apparati o applicativi esterni allo stesso. L'algoritmo utilizzato per la replica deve essere ottimizzato per l'utilizzo su reti geografiche prevedendo il tracciamento e il trasferimento delle sole porzioni di dati modificate in modalità incrementale. Le modalità con cui la replica deve avvenire, almeno in termini di sistema sorgente e destinazione, set di dati sorgente/destinazione, frequenza (RPO), devono essere modificabili dall'amministratore secondo modalità differenti per ciascun set di dati.

I sistemi devono poter fornire la funzionalità per assegnare a specifici dati priorità di performance in modo che questi possano risiedere sulla tipologia di nodi/dischi più adeguati a garantire le migliori prestazioni.

3.2.11 Data reduction

Il sistema dovrà permettere di applicare tecniche di data reduction, almeno due tra thin-provisioning, compressione e de-duplica, che potranno essere eseguite online, ed essere configurabili indipendente su più sottoinsiemi tramite policy granulari.

3.2.12 Integrità dei dati (WORM)

Il sistema dovrà proteggere i dati con protezione WORM (Write Once Read Many) per impedire modifiche o cancellazioni accidentali o volontarie dei dati. Esso deve soddisfare i requisiti richiesti dalle normative vigenti, incluse le rigide norme americane SEC 17a-4. Inoltre, il sistema deve consentire l'adozione di politiche di management al termine del periodo di protezione.

3.2.13 Data Protection

Il sistema dovrà prevedere un set completo di livelli di protezione del dato inserito nel sistema. Il sistema deve configurare differenti livelli di protezione e deve impostare la tolleranza al numero di nodi che possono essere indisponibili senza che il sistema ne venga influenzato.

Per rispettare il vincolo di assenza di SPOF, la caduta di una risorsa non deve mai rappresentare motivo di degrado delle funzioni del sistema o di possibili perdite di dati. Le modalità e i livelli di protezione devono essere dinamici, impostabili a caldo e configurabili a vari livelli sulle risorse del sistema fino ad arrivare al singolo file (granularità massima).

3.2.14 Software di Search and Indexing

La soluzione proposta deve poter prevedere come ulteriore opzione aggiuntiva la certificazione con almeno uno strumento di analisi dei dati e dei metadati associati ai file system. In particolare:

- Gestione dell'indicizzazione dei contenuti e possibilità di interrogare il sistema per monitorare lo spazio utilizzato anche con filtri sulle caratteristiche dei file quali la tipologia dei file, la dimensione, criteri temporali fornendo rappresentazione tabellare e grafica dei risultati, anche aggregati.
- Gestione dei tag custom sui dati: possibilità per l'utente finale di associare dei metadati testuali (tag) ai propri file (data curation). I metadati devono poter essere organizzati in insiemi definiti dall'amministratore del sistema ed eventualmente personalizzabili dall'utente. Questi metadati custom vanno ad affiancare i metadata standard normalmente associati ai file ed alle cartelle (dimensione, data di creazione, modifica, accesso, permessi, tipo del file, eventuali attributi aggiuntivi dipendenti dal file system, ecc.).
- Movimentazione dei dati: possibilità di scatenare azioni di movimentazione dei file stessi, definibili dagli utenti amministratori del sistema (ad esempio, archiviazione su una determinata area del sistema di tutti i dati della directory X più vecchi di Y giorni). In particolare, devono essere supportati la copia e lo spostamento di file tra sistemi di diverse

locazioni geografiche, la copia e lo spostamento di dati tra aree storage con diverse prestazioni.

3.2.15 Cifratura delle sessioni di management

Le sessioni di management devono essere effettuate con le sole versioni di protocollo cifrato, ad es. HTTPS, SSH, SNMPv3 in luogo di HTTP, Telnet, SNMP v1/2 i quali, se presenti, dovranno poter essere disabilitati.

3.2.16 Audit management

Tutte le operazioni di amministrazione devono essere tracciate e registrate all'interno del sistema.

3.2.17 Gestione guasti

Il guasto di uno dei componenti o nodi che lo compongono non dovrà compromettere assolutamente la funzionalità e la disponibilità del sistema. Al ripristino del componente o del nodo guasto dovrà seguire in maniera automatica il ripristino della consistenza dei dati eventualmente necessario. Deve essere fornito uno strumento di controllo e gestione anche degli eventuali guasti.

Il sistema deve avere anche un meccanismo per l'invio automatico delle segnalazioni di guasto ad apposito sistema di raccolta e diagnostica fornito dal produttore del sistema.

3.2.18 Online upgrade

Il sistema deve avere la possibilità di installare gli aggiornamenti per tutti i componenti del sistema senza interruzione di servizio. Viene ammessa l'interruzione momentanea del servizio su una parte dei nodi durante l'aggiornamento a condizione che questo non impedisca l'erogazione dei servizi, qualora questo sia richiesto dalle procedure di upgrade certificate dal produttore del sistema.

3.2.19 Protezione dei dati e ridondanza sui dati

Il sistema deve avere un sistema di protezione dei dati basato su una codifica di tipo RAID6 oppure Erasure code che rilevi e corregga automaticamente almeno due guasti in contemporanea ai supporti di memorizzazione, senza compromettere l'integrità e la disponibilità dei dati.

3.2.20 Hot spare

Il sistema deve possedere la funzionalità di hot-spare distribuito o tecnologia superiore, in modo da garantire tempi di ripristino inferiori rispetto alla normale operazione di rebuild all'interno di un equivalente sistema RAID con hot-spare standard.

3.2.21 Tiering

Il sistema deve permettere funzioni di spostamento automatico dei dati (file e/o block data) su aree di memorizzazione più o meno performanti in base all'utilizzo degli stessi (tiering automatico).

3.2.22 Protocolli client

Il sistema deve poter utilizzare i seguenti protocolli: NFS v3 e v4, SMBv2 e v3, e S3. I protocolli accessibili dai client devono prevedere la possibilità di operare con traffico crittografato.

3.2.23 Autenticazione client

Il sistema deve essere certificato compatibile Microsoft Active Directory ad un Domain Functional Level almeno Windows 2012 R2 e 2016, con sistemi standard LDAP ed LDAPS.

3.2.24 Namespace unico

I dati presenti nel sistema devono poter essere accessibili tramite un unico namespace condiviso su tutto il sistema. Il sistema deve poter indirizzare tutti i dati presenti sul sistema tramite l'unico namespace secondo politiche configurabili dinamicamente dall'amministratore del sistema.

3.2.25 Bilanciamento

Il sistema deve supportare la funzionalità di bilanciamento del carico tra nodi componenti il sistema installati nella stessa località geografica, e che questo avvenga in modo del tutto trasparente e senza la necessità di modifica alle applicazioni client che utilizzano le risorse del sistema.

3.2.26 Crittografia dati at rest

I dati devono essere salvati in modalità cifrata, conformemente allo standard FIPS-140-2.

3.3 Componente repository dati (Storage)

La soluzione richiesta è così composta:

- due storage repository ciascuno con le caratteristiche riportate in Tabella 1;
- due switch SAN ciascuno con le caratteristiche riportate in Tabella 1.

3.3.1 Tabella Requisiti Minimi Repository Storage e Switch

Tabella 1. Tabella requisiti minimi repository storage e switch

Requisiti minimi STORAGE repository	
Dimensione totale utile	Minimo 42.5 TB utili netti effettivi decimali prima dell'utilizzo di fattori di data reduction per la coppia di array
Area Performante (no HDD)	100% dello spazio totale
Lettura/scrittura random Area performante	Minimo 50.000 IOPS considerando rapporto R/W 50/50 e blocksize 8KB
Lettura/scrittura sequenziale Area performante	Minimo 3GB/s considerando rapporto R/W 50/50 e blocksize 256KB
Consumi	Massimo 8KW totali
Dimensione in rack unit del sistema	Massimo 5U per l'intero sistema storage
Cache	Minimo 64 GB per controller
Dimensione totale	Minimo 42.5 TB utili (base 10)
Connessione singolo nodo	Minimo 2 porte 10 Gbps per nodo e 4 porte FC 32 Gbit in SAN
Connessione front-end interno del sistema	Minimo 4 porte Ethernet 10Gbps SFP + con ottiche SR
Protezione dei dati	Il sistema deve garantire l'integrità e la disponibilità dei dati e la completa funzionalità anche a fronte del guasto contemporaneo di almeno un nodo ed almeno 2 dischi dei nodi rimanenti. La capacità utilizzata per i dati ridondanti (al fine di protezione) dev'essere di almeno il 10% dello spazio totale effettivo
WORM	Si richiede il supporto per la funzionalità di retention WORM preimpostabile che deve essere applicabile sia a livello di directory che a livello di singolo file.
Connettività per il management	Deve essere fornita almeno 1 porta RJ45 100/1000 Mbps dedicata alle funzionalità di management per ogni nodo
Switch SAN	24 porte da 32 Gbps di cui attive e licenziate 16 16 cavi LC/LC OM3 da 5 metri

3.4 Componente computazionale (Server)

L'infrastruttura server per METROFOOD-IT dovrà includere tutte le parti hardware e le licenze software necessarie e dimensionate per garantire la piena funzionalità del sistema secondo quanto richiesto, secondo quanto offerto dal fornitore e secondo quanto raccomandato dal produttore di massimo carico.

3.4.1 Tabella Requisiti minimi Server

L'infrastruttura server, proposta e descritta nel dettaglio, dovrà essere costituita da due server fisici uguali ed ogni server dovrà avere i seguenti requisiti minimi:

Tabella 2. Tabella requisiti minimi server

Requisiti minimi	
Caratteristiche HW	Minimo 2 socket e minimo 24 core attivi con clock fino a 4.0 GHz, con la potenzialità di crescita all'interno dello stesso server del 100% senza aggiungere HW
	Supporto 192 thread simultanei
	1TB di memoria RAM raddoppiabile
	N. 2 Schede HBA dual port 32 GB Optical Fibre Channel PCIe4
	N. 4 Schede LAN dual port 10/25 Gb NIC&ROCE PCIe3
	N. 4 x 25 GbE Optical Transceiver SFP + SR
	N. 4 x 800GB SSD PCIe4 NVMe U.2 module di tipo hot-swap
	N. 10 slot PCIe4/e5 e/o form factor OCP disponibili sul singolo server
	N. 1 rack standard da 42Unit
	N. 1 console di management
	Occupazione massima di 6 Rack-unit inclusa la console di management ed il relativo monitor
	Consumo energetico del server al 100% di utilizzo inferiore a 2250 Watts
Virtualizzazione Firmware	Virtualizzazione che permetta la creazione di Virtual Machine (partizioni logiche).

	Supporto fino a 1000 Virtual Machine (partizioni logiche) per sistema. Supporto fino a 20 Virtual Machine (partizioni logiche) per core.
Sistema operativo	Possibilità di installare sulle VM vari distribuzioni del sistema operativo Linux (RedHat, Suse, CentOS)
	Licenze Red Hat Enterprise Linux

3.5 Infrastruttura di rete

I nodi di calcolo e lo storage devono essere connessi tramite la rete di produzione almeno a 10Gbps. La fornitura dovrà comprendere i relativi apparati attivi e passivi di interconnessione e cablaggio.

3.5.1 Switch

Di seguito sono riportati i requisiti minimi che dovranno obbligatoriamente essere rispettati e supportati nella soluzione proposta. Devono essere compresi nella soluzione almeno due switch di tipo Layer 3, ognuno dei quali deve avere le seguenti caratteristiche:

- almeno 20 porte Ethernet a 10 Gb, 4 uplink 10G/25G SFP28 e 2x 40G QSFP+ (può essere diviso in 4x 10G SFP+) e supportare in ogni porta lo stacking fisico;
- n. 16 transceiver SFP+ 10GE BASE-SR;
- n. 8 transceiver SFP+ 1GE BASE-T (RJ45) o n.1 switch dedicato al management Out-Of-Band (OOB);
- n. 2 transceiver QSFP+ 40GE per interconnessione switch.

3.5.1.1 IPv4/IPv6 Dual Stack Multi-Layer Switching

Nel Data Center, deve essere supportato lo switching multistrato dual-stack IPv4/IPv6, i protocolli di routing tra cui Routing Information Protocol (RIP), Open Shortest Path First version 2 (OSPFv2), Intermediate System to Intermediate System version 4 (IS-ISv4), and Border Gateway Protocol version 4 (BGP4). Inoltre, deve supportare i protocolli di routing IPv6, tra cui il routing statico, RIPng (Routing Information Protocol next generation), OSPFv3, IS-ISv6 e BGP4+.

3.5.1.2 Stacking

Lo switch proposto deve supportare lo stacking, in cui più dispositivi fisici, collegati tramite collegamenti aggregati e virtualizzati in un unico dispositivo logico.

3.5.1.3 Politiche di protezione della sicurezza

L'apparato proposto deve difendere e controllare efficacemente la diffusione di virus e attacchi utilizzando molteplici meccanismi intrinseci come la protezione anti-DoS, scansione IP, controllo della validità dei pacchetti ARP sulle porte e policy ACL.

Deve supportare gli ACL IPv6 basati su hardware, che possono facilmente controllare l'accesso degli utenti IPv6. Gli switch devono consentire la coesistenza di utenti IPv4 e IPv6 e possono controllare le autorizzazioni di accesso degli utenti IPv6, ad esempio limitare l'accesso a risorse sensibili sulla rete.

Devono poter essere implementate delle CPU protection policy in cui il traffico inviato alla CPU viene classificato ed elaborato in base alla priorità della coda e la velocità della larghezza di banda è limitata come richiesto.

Deve essere garantito anche il DHCP snooping, connessione tramite Secure Shell (SSH), Simple Network Management Protocol version 3 (SNMPv3) e Network Foundation Protection Policy.

3.5.1.4 Alta affidabilità

Lo switch deve essere dotato di moduli di alimentazione ridondanti integrati e gruppi di ventole modulari, che possono essere sostituiti a caldo e non influire sul normale funzionamento del dispositivo. Deve essere supportato il rilevamento dei guasti e le funzioni di allarme per i moduli di alimentazione e ventola. La velocità della ventola deve poter essere regolata automaticamente per adattarsi meglio all'ambiente circostante.

Oltre le precedenti indicazioni, devono essere supportati i protocolli Spanning Tree Protocols (STPs) – 802.1d, 802.1w e 802.1s, Virtual Router Redundancy Protocol (VRRP), Ethernet Ring Protection Switching (ERPS), Rapid Link Detection Protocol (RLDP), Rapid Ethernet Uplink Protection Protocol e il protocollo Bidirectional Forwardin Detection (BFD).

3.5.1.5 Caratteristiche tecniche

Di seguito le caratteristiche minime della configurazione dello switch:

PORTE	
10G SFP+	20
25G SFP28	4
40G QSFP+	2
Densità di porte 1G	20
Densità di porte 10G	24
Densità di porte 25G	4

Densità di porte 40G	2
Densità di porte 10G con cavo breakout	32
Densità di porte 25G con cavo breakout	4
Densità di porte 40G con cavo breakout	2
Numero di porte di gestione	1
Numero di porte console	1
Numero di porte USB	1

Di seguito le caratteristiche minime per memoria e processore:

Chip	BCM56170
CPU	ARM A9 Single-Core CPU, 1.25GHz
DRAM	1GB
SDRAM	1GB
Memoria flash	1GB
Latenza	1.11µs
Buffer di pacchetti	4MB

Di seguito le caratteristiche minime per alimentazione ventole:

Alimentazione	Dual 1+1 redundant power supply
Numero di ventole	2x Hot-swappable Fans
Flusso d'aria	Front-to-back
Rumore	<78dB
Velocità massima della ventola	18000rpm
Consumo massimo di energia	85W
Potenza massima nominale	150W
Efficienza dell'alimentazione	85% (220Vac 50% load)
Valori di uscita	Main output: 12V 12.5A

Di seguito le caratteristiche minime di performance:

Capacità di switching	760 Gbps
Velocità di inoltro	565 Mpps
Tipo di layer	Layer 3
Numero totale di indirizzi MAC	32000
Numero totale di routes IPv4 (routes indirette)	16000
Numero totale di percorsi host IPv4 (direct routes e ARP)	16000
Numero totale di routes IPv6 (routes indirette)	4094
Numero totale di percorsi host IPv6 (routes dirette e NDP)	4000
Numero totale di routes multicast IPv4	4000

Numero totale di routes multicast IPv6	2000
QoS ACL scale	2500
Security ACL scale	2500
VLAN IDs	4000
Porte virtuali STP (port* VLANs) per MST	64
Totale interfacce virtuali switchate (SVIs)	4094
Jumbo frame	9216 bytes

3.5.1.6 Quality of Service

Lo switch deve supportare la classificazione e il controllo dei vari flussi, inclusi i flussi MAC, flussi IP e flussi applicativi, per implementare il controllo fine della larghezza di banda, la priorità di inoltro e altre policy di flusso.

Deve essere garantita la codifica 802.1p, IP ToS, filtraggio del traffico da livello 2 a livello 7, SP, WRR e altri criteri QoS.

3.5.1.7 Gestione

Lo switch deve supportare il protocollo SNMP (Simple Network Management), RMON (Remote Network Monitoring), poter implementare il backup del registro e configurazione tramite unità flash USB e Syslog per la diagnosi e la manutenzione di rete. Gli amministratori devono poter utilizzare CLI, gestione basata sul Web e Telnet per gestire il dispositivo.

3.5.2 Firewall

Di seguito sono riportati i requisiti minimi che dovranno obbligatoriamente essere rispettati e supportati nella soluzione proposta.

3.5.2.1 Architettura hardware

Tutte le funzionalità richieste devono essere presenti su ognuno degli apparati proposti. Tali apparati dovranno essere basati su macchine fisiche con hardware dedicato.

Ognuno degli apparati oggetto della fornitura dovrà essere dotato delle seguenti interfacce di rete:

Quantità	**Tipologia**
1	USB Port
1	Console Port
2	GE RJ45 HA/MGMT Ports
16	GE RJ45 Ports

2	10 GE SFP+ FortiLink Slots
8	GE SFP Slots
2	10 GE SFP+

Nella fornitura devono essere compresi almeno 2 SFP+ SR 10000 Mbit/s 850 nm.
Gli apparati devono avere alimentazione e ventole di raffreddamento con alimentatori 80Plus Compliant. Gli apparati dovranno avere la larghezza adatta a rack standard 19".

3.5.2.2 Funzionalità di base

Il Sistema Operativo degli apparati oggetto della fornitura dovrà essere basato su un'architettura software proprietaria.
Gli apparati dovranno garantire contemporaneamente le funzionalità base di Routing, Firewalling, IPSec VPN e SSL VPN.

3.5.2.3 Alta affidabilità

L'architettura deve prevedere la ridondanza dei servizi su due o più apparati per assicurare l'alta affidabilità dei servizi stessi. I servizi non devono essere impattati nel caso di guasto di un singolo apparato o di un aggiornamento dell'architettura stessa.

- Modalità operative tra gli apparati: Active/Passive, Active/Active, Clustering;
- Sincronizzazione delle configurazioni;
- Sincronizzazione delle sessioni;
- Failover del traffico tra gli apparati senza perdita di servizio;
- Supporto del Link Aggregation Control Protocol (LACP), IEEE (802.3ad) su singolo apparato.

3.5.2.4 Virtualizzazione

È richiesto che l'architettura supporti la separazione logica di ogni apparato in almeno 10 contesti virtuali: deve essere possibile partizionare ogni apparato in differenti apparati virtuali che agiscano in maniera indipendente.

Gli apparati devono supportare le interfacce logiche con la separazione del traffico tramite 802.1q.

3.5.2.5 Routing

Gli apparati dovranno essere in grado di supportare funzionalità di routing statico e routing dinamico (RIP, OSPF, BGP) e SD-Wan Routing.

Gli apparati dovranno garantire la funzionalità di inoltro del traffico in base a specifiche regole indipendentemente dai percorsi riportati in tabella di routing (funzionalità nota come Policy Based Routing). Il traffico deve essere selezionato sulla base di regole di livello 3 e livello 4.

3.5.2.6 Virtual Private Network

Gli apparati dovranno supportare funzionalità di IPSec VPN, in modalità Gateway-to-Gateway e in modalità Client-to-Gateway, e di SSL VPN. Inoltre, devono supportare gli algoritmi riportati di seguito:

- Retrocompatibilità con algoritmi non raccomandati (fonte NSA e NIST)
    - Algoritmi di cifratura DES e 3DES;
    - Algoritmi di autenticazione MD5, SHA-1;
    - IKEv1;
    - Perfect forward secrecy (DH groups) – 1,2.
- Altri algoritmi:
    - Algoritmi di cifratura AES-128 e AES-256;
    - Algoritmi di autenticazione SHA-256;
    - Manual key, IKEv2, PKI (X.509);
    - Perfect forward secrecy (DH) – 5 (1536 bits), 14 (2048 bits);
    - Perfect forward secrecy (ECDH) – 19 (256-bit elliptic curve), 20 (384-bit elliptic curve).

3.5.2.7 Funzionalità evolute

Gli apparati oggetto della fornitura dovranno poter integrare le funzionalità di base con le seguenti funzionalità avanzate:

- Quality of Service;
- SSL Inspection;
- Intrusion Prevention System;
- Anti Malware;
- Application Control;
- Web Security – URL and web content, Video and Secure DNS Filtering;
- Anti-Spam;
- IoT Detection Service.

3.5.2.8 Quality of service

È richiesto che l'architettura supporti le seguenti funzioni di QoS per la prioritizzazione del traffico:

- Configurazione di banda massima per indirizzo IP (Sorgente e destinazione) e servizio (Livello 4);
- RFC 2474 IP DiffServ in IPv4;
- Configurazione di filtri per determinare la Class of Service (CoS);
- Classificazione del traffico.

3.5.2.9 SSL Inspection

Gli apparati dovranno poter decifrare le sessioni SSL, in ingresso e uscita, per poter applicare le politiche e i controlli di sicurezza sul contenuto del traffico in transito.

3.5.3 Anti Malware

Gli apparati dovranno supportare funzionalità di Anti Malware in modo da poter identificare minacce all'interno dei contenuti del traffico che attraversa gli apparati stessi. Gli apparati devono supportare la funzionalità sui seguenti protocolli: HTTPS, HTTP, FTP, SMTP e SMB. Essi dovranno essere in grado di analizzare il contenuto del traffico (es. file scaricati, file spediti, ecc.), identificare eventuali elementi malevoli e in caso positivo generare un alert e/o bloccare gli stessi contenuti malevoli in maniera automatizzata.
Dovrà essere possibile permettere, bloccare e controllare in maniera flessibile i tipi di file che vengono trasportati, attraverso la rete, tramite applicazioni. L'aggiornamento delle signature deve avvenire sia in modalità automatiche che manuale.

3.5.3.1 Intrusion Prevention System

Gli apparati dovranno supportare funzionalità di IPS in modo da poter identificare minacce all'interno dei flussi di traffico che attraversano gli apparati stessi:

- **Stateful protocol signatures:** il traffico viene confrontato esclusivamente con le signature compatibili con il contesto del protocollo.
- **Meccanismo di rilevazione degli attacchi:** stateful signatures, protocol anomaly detection e application identification;
- **Meccanismi di risposta agli attacchi:** drop connection, close connection, session packet log;
- **Meccanismi di risposta agli attacchi:** drop connection, close connection, session packet log;
- **Meccanismi di notifica agli attacchi:** syslog;
- **Protezione Worm:** signature che rilevano il traffico generato dai sistemi compromessi da Worm o il loro transito sulla rete;
- **Protezione dai Trojan:** rilevazione del traffico generato dai sistemi compressi da Trojan o il loro transito sulla rete;

- **Protezione da Spyware, Adware e Keylogger:** rilevazione del traffico generato dai software elencati o rilevazione del loro transito sulla rete;
- Possibilità di realizzare signature personalizzate;
- Possibilità di configurare soglie di traffico per protocollo;
- Frequenza degli aggiornamenti giornalieri in caso di emergenza per la diffusione di una nuova minaccia.

L'aggiornamento delle signature deve avvenire sia in modalità automatica che manuale.

3.5.3.2 Application Control

Gli apparati devono permettere il controllo sui flussi applicativi per permettere o negare il traffico di una o di un gruppo di applicazione mediante policy di sicurezza.

3.5.3.3 Web Security

Il servizio di filtraggio degli URL deve fornire una protezione completa contro le minacce, tra cui ransomware, furto di credenziali, phishing e altri attacchi trasmessi dal Web. Deve garantire l'analisi e la correlazione del comportamento attraverso l'uso dell'intelligenza artificiale per bloccare gli URL dannosi sconosciuti.

3.5.3.4 Anti-spam

Gli apparati devono avere un approccio completo e multilivello per rilevare e filtrare lo spam. La tecnologia di rilevamento deve ridurre drasticamente il volume dello spam perimetrale, offrendoti un controllo su attacchi e infezioni e-mail.

3.5.3.5 IoT Detection Service

Gli apparati dovranno includere una libreria locale (installata) di dispositivi IoT che viene regolarmente ampliata e aggiornata per rilevare e bloccare potenziali minacce informatiche che prendono di mira i dispositivi IoT.

3.5.3.6 Performance

Ogni singolo apparato dovrà raggiungere almeno i seguenti livelli di performance:

- Gli apparati dovranno supportare singolarmente un throughput di almeno 10Gbps. Tale dato di throughput dovrà essere considerato per traffico UDP (64 Byte Frames) con la sola funzionalità di firewall abilitata.

- Gli apparati devono avere una latenza massima di 4.97µs. Tale misurazione dovrà essere effettuata per traffico UDP (64 Byte Frames) con la sola funzionalità di firewall abilitata.
- Gli apparati dovranno supportare singolarmente un throughput di almeno 2.6Gbps. Tale dato di throughput dovrà essere considerato con tutte le funzionalità abilitate (Application Control, NGFW and Threat Protection).
- Gli apparati dovranno supportare singolarmente almeno 56.000 nuove sessioni TCP per secondo e 1.5 Milioni di sessioni contemporanee complessive.
- Gli apparati devono supportare almeno 16000 tunnel IPSec VPN.
- Gli apparati dovranno supportare singolarmente un throughput di almeno 12Gbps per la funzionalità di IPSec VPN con la seguente configurazione:
    - IPSec site-to-site;
    - IKEv2;
    - Pre-shared key;
    - IKE & ESP encryption – AES-128;
    - IKE & ESP integrity – SHA256;
    - IKE Diffie-Hellman – Group 5;
    - Traffico TCP a 1024 bytes;
- Gli apparati dovranno supportare singolarmente almeno 40 contesti virtuali.

3.5.3.7 Autenticazione

Si chiede che sia obbligatoria l'autenticazione locale per la gestione degli apparati, tale autenticazione deve permettere la distinzione tra un profilo amministratore e un profilo utente (sola lettura). Gli apparati firewall dovranno supportare l'autenticazione degli utenti mediante integrazione con server LDAP e RADIUS. Il riconoscimento dell'utente dovrà essere utilizzato dall'apparato per selezionare il tipo di profilo e i permessi di accesso.

3.6 Armadio rack

L'armadio rack deve avere le seguenti caratteristiche minimali:

- armadio standard 19" con altezza massima 42U(60cm larghezza, 1,07 m di profondità, 186,46 m) e profondità massima 120 cm;
- conforme alla certificazione EIA-310-D;
- telaio saldato;
- complete di ruote;

- coperture e pannelli laterali, porte anteriori e posteriori con superfice forata per almeno il 65%;
- dispositivo antiribaltamento o piedi stabilizzanti;
- possibilità di ospitare dispositivi profondi fino a 90 cm.

3.7 UPS

Il gruppo di continuità deve essere dotato delle seguenti principali caratteristiche:

- Potenza nominale 6.000 Va – 6000W;
- Tecnologia PWM ad alta frequenza;
- Neutro passante;
- Equipaggiato con batterie d'accumulatori al piombo-acido di tipo ermetico regolate da valvola, contenute all'interno del UPS in un apposito vano o in uno o più armadi esterni, dimensionate per garantire un'autonomia minima pari a **4 minuti** all'80% del carico.

Dovrà essere previsto un UPS per singolo server e un UPS per lo storage.

3.7.1 Caratteristiche generali

3.7.1.1 Principio di funzionamento VFI

La tipologia di funzionamento dell'UPS è VFI (Voltage and Frequency Independent secondo classificazione EN- IEC62040-3) che garantisce una tensione di uscita, verso le utenze, filtrata e stabilizzata, non dipendente dalla rete di alimentazione. Ciò significa che la tensione fornita in uscita viene ricavata da quella di ingresso attraverso due stadi in cascata. Il primo provvede ad effettuare una prima conversione da alternata a continua, mentre il secondo, attraverso un procedimento inverso, rigenera la sinusoide alternata di uscita a partire dalla continua.
Questo doppio stadio permette di filtrare completamente eventuali disturbi o anomalie della rete. La tensione continua presente all'ingresso del secondo stadio denominato "inverter" può essere fornita, tramite un opportuno stadio survoltore, anche dalle batterie dell'UPS. È così possibile, in caso di mancanza o anomalie sulla tensione di ingresso, avere comunque la corretta tensione di uscita senza alcuna discontinuità. Nel caso poi di sovraccarichi o guasti, l'intervento immediato del by-pass statico garantisce comunque l'alimentazione ininterrotta al carico.

3.7.1.2 Architettura

L'architettura dovrà essere di tipo **parallelo distribuito**, ovvero il carico dovrà essere ripartito tra tutti i moduli di potenza presenti sulla singola fase (**load sharing**), in modo tale che nessuno dei moduli di

potenza rimanga inattivo o in stand-by. Con configurazione ridondante e in caso di guasto risulta così possibile continuare ad alimentare il carico collegato senza discontinuità nell'erogazione dell'energia.

In caso di guasto ad uno o più moduli, la potenza garantita da quelli ancora funzionanti sarà la seguente: $P_{out} = P_{nom} \frac{(n-x)}{n}$.

3.7.1.3 Modulo di potenza

Ciascun modulo di potenza dovrà essere composto dai seguenti blocchi funzionali:

- Raddrizzatore/PFC;
- Bypass automatico.

Il raddrizzatore dell'UPOS dovrà essere costituito da un circuito di controllo e regolazione (PFC), che oltre alle funzioni di normale raddrizzatore dovrà provvedere a:

- correggere automaticamente il fattore di potenza del carico per riportarlo ad un valore >0,99 già con un valore di carico in uscita pari al 20% del carico nominale;
- alimentare l'inverter senza richiedere energia alle batterie anche in presenza di tensione di rete molto bassa;
- assicurare una distorsione armonica totale della corrente d'ingresso THDIin < 3% senza l'aggiunta di filtri o componenti supplementari.

Invece, il bypass dovrà essere progettato e realizzato conformemente a quanto di seguito descritto:

- Interruttore statico con tempo di intervento nullo, con in parallelo un interruttore elettromeccanico che si attiva in ritardo ma che garantisce dissipazione nulla nel tempo.
- Logica di comando e di controllo gestita da microprocessore che provvederà a:
    - trasferire automaticamente il carico direttamente sulla rete primaria senza interruzione dell'alimentazione, al verificarsi delle condizioni di sovraccarico, sovratemperatura, tensione continua fuori delle tolleranze ed anomalia inverter;
    - ritrasferire automaticamente il carico da rete primaria a linea inverter, senza interruzione dell'alimentazione, al ripristino delle condizioni normali del carico;
    - se la rete primaria e l'inverter non sono sincronizzati il bypass dovrà essere disabilitato.

3.7.1.4 Segnalazioni e allarmi

L'UPS deve essere gestito da un microprocessore e deve essere in grado di visualizzare tramite un pannello di controllo e display LCD, allarmi e modalità di funzionamento come di seguito descritto:

- funzionamento normale;
- frequenza d'uscita non sincronizzata con l'ingresso;

- funzionamento a batteria;
- funzionamento in bypass;
- modulo di potenza guasto;
- sovraccarico;
- anomalia generica;
- errato collegamento neutro;
- riserva di autonomia;
- fine autonomia.

3.7.1.5 Normative

Le scelte, gli sviluppi ingegneristici, la scelta del materiale e dei componenti, la realizzazione delle apparecchiature dovranno essere in accordo con Direttive Europee e Norme vigenti in materia. Il Sistema Statico di Continuità dovrà possedere la marcatura CE in accordo con le Direttive 2014/35, 2104/30. L'UPS dovrà essere progettato e realizzato in conformità alle seguenti norme:

- EN 62040-1 "Prescrizioni generali e di sicurezza per UPS utilizzati in aree accessibili all'operatore";
- EN 62040-2 "Prescrizioni di compatibilità elettromagnetica (EMC)";
- EN 62040-3 "Prescrizioni di prestazione e metodi di prova".

3.8 Software

Il sistema deve essere corredato di tutte le componenti software necessarie al System Management per la gestione dell'intero cluster dalle seguenti funzionalità:

- **tool grafici web-based per la gestione dinamica dei file system e dei volumi:** possibilità di aumentare e diminuire le dimensioni di un file system e di un volume mentre il file system ed il volume sono on-line e disponibili al sistema operativo ed alle applicazioni;
- **tool grafici web-based per il monitoraggio delle prestazioni:** i tool devono fornire, tramite interfaccia grafica web-based, informazioni in real-time sugli indicatori più rilevanti delle prestazioni del sistema (CPU, memoria, accessi a disco, utilizzo della LAN);
- **tool grafici web-based per l'installazione e l'amministrazione del sistema**;
- **tool grafico web-based per la creazione, la modifica, la cancellazione delle risorse associate al sistema:** le funzioni di servizio come accensione, spegnimento, monitoraggio e varie funzioni di system management come l'aggiornamento dei livelli di firmware o il controllo di eventi;
- **tool grafico web-based necessario alla gestione del firmware in modalità remota**.

3.9 Personal Computer e Laptop

La fornitura dovrà prevedere anche Personal Computer e Laptop come di seguito descritti.

3.9.1 Personal Computer Desktop (All-in-One)

Si richiede la fornitura di 30 Personal Computer Desktop (All-in-One) che devono avere le caratteristiche previste di seguito:

Unità Centrale di Elaborazione	CPU Intel Core i7 di dodicesima generazione
Memoria RAM	Memoria DDR4 da 16 GB
Memoria di Massa	SSD M.2 PCIe NVMe da 512 GB Class 35
Sistema operativo e certificazioni	Precaricamento Microsoft Windows 10 Pro/11 Pro “nuovo di fabbrica”
Display	Monitor 24”
Controller grafico	Controller grafico integrato
	Supportare almeno una risoluzione 1920x1080 con 16,7 milioni di colori e grafica 3D
Dispositivi e porte di connessione	N° 3 porte USB 3.2 Gen 1 Type-A Ports con Smart Power On
	N° 2 porte USB 3.2 Gen 2 Type-A Ports
	N° 1 porta HDMI 2.0-out
	N. 1 DisplayPort++ 1.4/HDCP 2.3 Port
	N. 1 USB 3.2 Gen 2x2 Type-C Port
	Modulo wireless 6E 2x2 e Bluetooth
	Webcam full HD retrattile con riduzione temporale della distorsione
Tastiera	Italiana estesa, Qwerty con tasti funzione per Windows, con tastierino numerico separato e con il tasto Euro
Mouse	Ottico, a due o tre pulsanti con rotella per lo scrolling
Aggiornamenti driver	Il produttore del Personal Computer deve mettere a disposizione il proprio sito web eventuali nuovi versioni dei driver o dei software di supporto al prodotto offerto

3.9.2 Personal Computer

Di seguito l'elenco dettagliato delle caratteristiche minime di due tipologie di PC:

Tipologia 1	
Unità Centrale di Elaborazione	CPU Intel Core i7 di dodicesima generazione
Memoria RAM	Memoria DDR4 da 32 GB a 3.200 Mhz
Memoria di Massa	SSD M.2 PCIe NVMe da 512 GB
Sistema operativo e certificazioni	Precaricamento Microsoft Windows 10 Pro/11 Pro "nuovo di fabbrica"
Display	Monitor 14"
Controller grafico	Controller grafico integrato
	Supportare almeno una risoluzione 1920x1080 con 16,7 milioni di colori e grafica 3D
Dispositivi e porte di connessione	N° 2 porte USB 3.2 Gen 1 SuperSpeed (5 Gbps)
	N° 2 porte Thunderbold 4 con modalità alternativa DisplayPort/USB4/erogazione alimentazione
	Wi-Fi 6E (802.11ax)
	Webcam full HD 1080p
	Tastiera retroilluminata
	Rilevamento impronta digitale
Aggiornamenti driver	Il produttore del Personal Computer deve mettere a disposizione il proprio sito web eventuali nuovi versioni dei driver o dei software di supporto al prodotto offerto

Tipologia 2	
Unità Centrale di Elaborazione	CPU Intel Core i7 di dodicesima generazione
Memoria RAM	Memoria DDR4 da 32 GB a 3.200 Mhz
Memoria di Massa	SSD M.2 PCIe NVMe da 1000 GB
Sistema operativo e certificazioni	Precaricamento Microsoft Windows 10 Pro/11 Pro "nuovo di fabbrica"
Display	Monitor 16" - Retroilluminazione a LED – FHD+ (1920x1200) – Luminosità: 250 nit – Contrasto 1000:1 –

	Tempo di risposta: 35 ms
Controller grafico	Controller grafico integrato
	Memoria RAM dedicata 2 GB
Dispositivi e porte di connessione	N° 2 porte USB 3.2 Gen 1 SuperSpeed (5 Gbps) Type-A
	N° 1 porte USB 3.2 Gen 2x2 SuperSpeed (20 Gbps) Type-C
	Wi-Fi 6E (802.11ax)
	Webcam full HD
	Tastiera retroilluminata
	Rilevamento impronta digitale
Aggiornamenti driver	Il produttore del Personal Computer deve mettere a disposizione il proprio sito web eventuali nuovi versioni dei driver o dei software di supporto al prodotto offerto

4. Servizi professionali di installazione, configurazione e formazione

Il Fornitore dovrà provvedere all'installazione di tutti i dispositivi ed alla completa verifica delle funzionalità di tutte le componenti. È da intendersi, altresì, a carico del fornitore, il trasporto e lo smaltimento del materiale costituente l'imballaggio delle componenti consegnate nonché il ritiro e lo smaltimento degli apparati dismessi qualora presenti.

I servizi di consegna, installazione, configurazione e attivazione degli Apparati dovranno essere effettuati presso il II Edificio Polifunzionale dell'Università degli Studi del Molise, situato in Campobasso in Via Francesco De Sanctis, 1.

Il trasporto e la consegna delle apparecchiature sono a carico del Fornitore. I rischi di perdita e danni alle apparecchiature sono a carico del Fornitore fino alla consegna delle stesse presso i locali dell'Università degli Studi del Molise.

Il Fornitore dovrà possedere la certificazione di qualità ISO 9001 per i processi di realizzazione ed erogazione del servizio di vendita e/o noleggio e/o di assistenza e/o di manutenzione di Apparati Server, Storage e Apparati per Storage Area Network.

In particolare, la consegna fisica degli apparati dovrà essere effettuata entro i 25 (venticinque) giorni lavorativi successivi alla data di stipula del contratto e comprende ogni onere relativo ad imballaggio, trasporto, consegna "al piano", posa in opera, asporto dell'imballaggio e qualsiasi altra attività ad essa strumentale.

Ove l'accesso ai locali dell'Università degli Studi del Molise comporti qualsivoglia attività, comprese opere e mezzi di sollevamento, dette attività dovranno essere effettuate dal Fornitore, con oneri e carico del Fornitore stesso. Le attività di consegna includeranno ogni onere relativo ad imballaggio, trasporto, facchinaggio, consegna "al piano", posa in opera, installazione delle apparecchiature e delle opzioni, prima accensione e verifica delle funzionalità, asporto dell'imballaggio e qualsiasi altra attività ad esse strumentale.

L'Università degli Studi del Molise metterà a disposizione, presso il CED, un locale per ospitare i sistemi pronti per la consegna ed alimentazione monofase.

Le apparecchiature dovranno essere rese funzionanti e consegnate insieme alla manualistica tecnica d'uso e su di esse sarà effettuata la verifica di funzionalità, intesa come verifica dell'accensione e del funzionamento dell'apparecchiatura (completa di tutti i componenti), che darà luogo, congiuntamente all'identificazione di quantità e tipologia tutte le componenti previste dalla configurazione richiesta dall'Università degli Studi del Molise, alla redazione di un **verbale di consegna**.

Dovranno quindi essere identificati in quantità e tipologia tutte le componenti previste dalla configurazione richiesta dal committente, indicando esplicitamente la precisa rispondenza delle caratteristiche tecniche delle apparecchiature e delle componenti fornite con le caratteristiche tecniche previste contrattualmente dalla fornitura.

Sarà cura della struttura di coordinamento e pianificazione del Fornitore avvertire preventivamente il responsabile di Università del Molise delle imminenti attività.

Qualora la fornitura, o parte di essa, non venga eseguita nei termini fissati, il Fornitore resterà assoggettato al pagamento delle penalità indicate nel contratto.

Resta comunque inteso che tutte le apparecchiature acquisite dall'Università degli Studi del Molise nell'ambito della presente fornitura sono nuove di fabbrica, in tutte le loro componenti.

Le attività di installazione e configurazione hardware avverranno nel normale orario di lavoro (tutti i giorni lavorativi tra le 8:00 e le 18:00). In particolare, il Fornitore dovrà provvedere ad avviare le attività di:

- verifiche propedeutiche all'installazione dei nuovi sistemi;
- installazione degli apparati e dei componenti aggiuntivi oggetto della fornitura e l'aggiornamento software laddove necessario;
- connessione degli apparati forniti, incluso il cablaggio degli apparti come i patch-panel presenti in base alle configurazioni stabilite;

- configurazione ed inizializzazione delle apparecchiature e del relativo software, secondo le specifiche fornite da Università degli Studi del Molise, e verifica del loro corretto funzionamento;
- verifica del perfetto funzionamento delle apparecchiature, del collegamento delle stesse e della loro configurazione;
- esecuzione di prove di funzionamento relative all'hardware;
- fornitura ed installazione degli accessori che si dovessero rendere necessari in sede di installazione.

Il Fornitore Aggiudicatario al termine delle attività sopra descritte dovrà consegnare alla Committente il documento relativo alle "Specifiche di installazione" aggiornato, recante almeno le seguenti indicazioni:

- tipo, modello e numero seriale di ciascun apparato;
- identificativo del software installato.

Per quanto riguarda il personale tecnico dell'Ateneo, esso dovrà essere formato relativamente al funzionamento e all'utilizzo delle apparecchiature e del software installato. La formazione potrà essere erogata on-site e/o a distanza. Essa dovrà avere una durata minima di 50 ore e dovrà essere rilasciata la certificazione sull'attività svolta al personale individuato dall'Ateneo.

5. Manutenzione e servizio di assistenza tecnica

I prodotti devono essere nuovi, originali, non contraffatti, non rigenerati o di provenienza illegale e l'Università degli Studi del Molise deve figurare come primo registrante. Il sistema deve avere un rilevamento automatizzato dei problemi e raccolta delle informazioni sullo stato del sistema per creare e notificare i casi in modo automatizzato con canale di comunicazione con crittografia. L'impresa che si aggiudicherà la vendita deve garantire il buon funzionamento delle apparecchiature, dei loro componenti e degli impianti.

Inoltre, esse deve garantire l'obbligo di sostituirli o ripararli, senza ulteriori costi aggiuntivi, in loco (on-site).

Dovrà essere previsto un servizio di manutenzione con validità non inferiore ai 36 mesi a decorrere dalla data di accettazione del contratto su tutti prodotti, sia hardware che software. I sistemi devono essere coperti 24 ore e 7 giorni su 7 per segnalazione di guasti ed anomalie da effettuare su sistema multipiattaforma, come ad esempio, per telefono, e-mail e segnalazione web. I livelli di servizio sono descritti di seguito.

Il servizio di manutenzione sarà erogato dai costruttori/produttori delle componenti hardware e software con i quali il personale tecnico dell'Università degli Studi del Molise interagirà direttamente senza intermediazione del fornitore. Il servizio di manutenzione deve comprendere la sostituzione delle parti non funzionanti con ricambi identici all'originale; se ci saranno parti sostituite o rimosse, essere saranno ritirate.

La fruizione senza limitazioni o costi aggiuntivi di qualsiasi attività di aggiornamento firmware e software necessario sia per eliminare o risolvere anomalie, sia per implementare nuove funzionalità per tutta la durata del ciclo di vita del prodotto. Le eventuali attività di carattere tecnico manutentivo-correttivo e/o manutentivo-preventivo che si rendono necessarie dopo la scadenza dei contratti o eventuali rinnovi di manutentivo-preventivo che si rendessero necessarie dopo la scadenza dei contratti o eventuali rinnovi di manutenzione, verranno valorizzate al momento della richiesta.

Il servizio sopradescritto dovrà ritenersi applicabile a qualsiasi componente della soluzione.

L'impresa fornitrice deve fornire uno o più numeri telefonici e orari di reperibilità telefonica attivi nell'orario di ufficio dalle 8.00 alle 20.00 per tutti i giorni lavorativi dell'anno (dal lunedì al venerdì compresi).

Deve essere previsto che non ci sia nessun onere aggiuntivo per eventuali sostituzioni per UNIMOL in caso di costi di manodopera, di spedizione, o di qualsiasi altra natura. In caso di malfunzionamento, il fornitore deve prendere in carico il ticket entro un tempo massimo di 4 ore dalla segnalazione alla quale sarà associato il relativo numero di ticket.

L'intervento per la risoluzione di malfunzionamenti hardware e/o software deve rispettare la tabella sottostante:

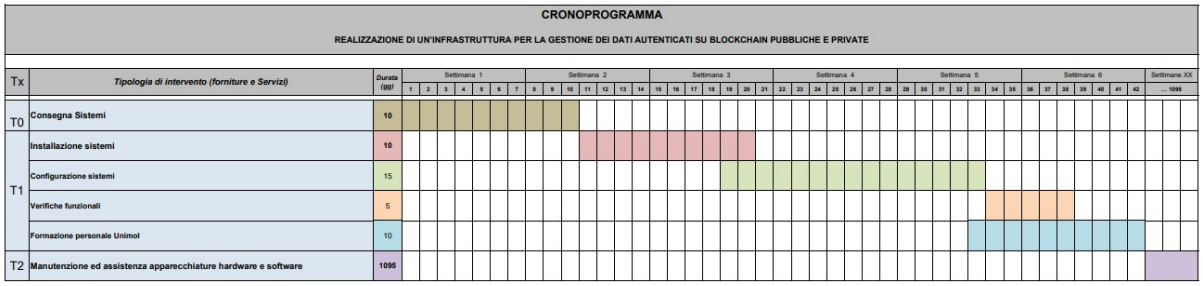
Livello di gravità	**Tempi di risposta**	**Tempi di risoluzione**
Livello 1 - Alto impatto Con riferimento ai sistemi oggetto della fornitura, si verifica la parziale indisponibilità di almeno uno di essi	Entro 4 ore dalla segnalazione	Entro il tempo massimo di 24 ore solari
Livello 2 - Medio impatto Con riferimento ai sistemi oggetto della fornitura, si verifica la parziale indisponibilità di almeno uno di essi	Entro 4 ore dalla segnalazione	Entro il tempo massimo di 48 ore solari
Livello 3 - Basso impatto Si verifica un fault, su uno qualsiasi dei sistemi oggetto della fornitura, che non ne pregiudica il corretto funzionamento	Entro 4 ore dalla segnalazione	Non superiore a 72 ore solari

Le attività necessarie alla risoluzione del malfunzionamento, a discrezione di UNIMOL, potranno proseguire ad oltranza anche nelle giornate di sabato, domenica e/o in giorni festivi. Il malfunzionamento terminerà con la risoluzione del problema.

6. Cronoprogramma

Si allega il Cronoprogramma di riferimento:

- T0 = Avvio di consegna delle Forniture;
- T1= T0 + 32 (trentadue) giorni naturali e consecutivi i: Installazione, Configurazione, verifiche funzionali dei sistemi e formazione;
- T2 = T1 + 1095 (millenovantacinque) giorni naturali e consecutivi: Manutenzione ed assistenza apparecchiature hardware e software.



Firmato digitalmente da: GIACOMO GIUSEPPE VERDE
Organizzazione: UNIVERSITA' DEGLI STUDI DEL MOLISE/92008370709
Data: 29/06/2023 11:56:10

Firmato digitalmente da: Valerio Barbieri
Organizzazione: UNIVERSITA' DEL MOLISE/92008370709
Data: 29/06/2023 11:55:07

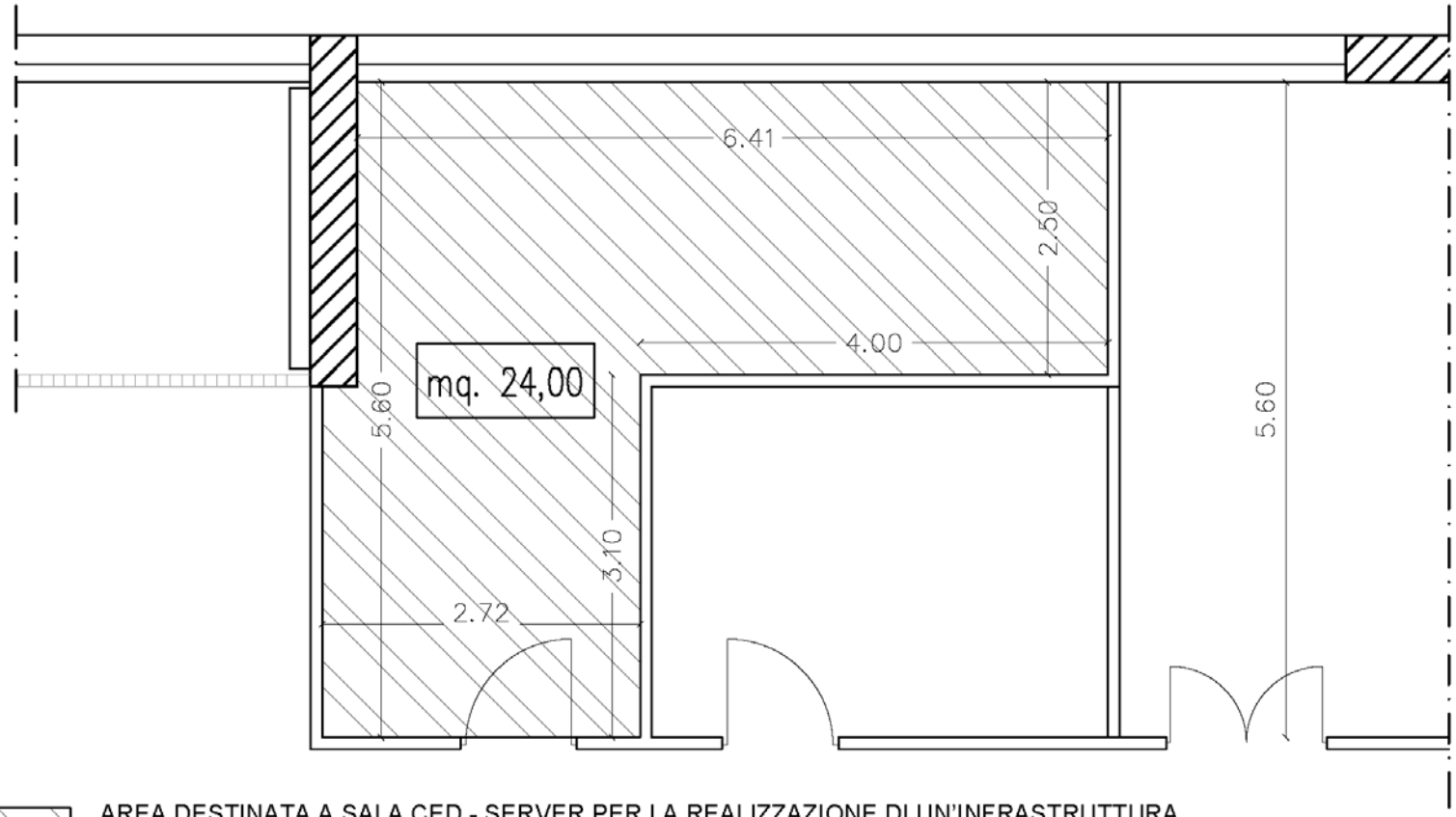
CRONOPROGRAMMA

REALIZZAZIONE DI UN'INFRASTRUTTURA PER LA GESTIONE DEI DATI AUTENTICATI SU BLOCKCHAIN PUBBLICHE E PRIVATE

Tx	*Tipologia di intervento (forniture e Servizi)*	*Durata (gg)*	Settimana 1							Settimana 2							Settimana 3							Settimana 4							Settimana 5							Settimana 6							Settimane XX
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	... 1096
T0	Consegna Sistemi	10																																											
T1	Installazione sistemi	10																																											
	Configurazione sistemi	15																																											
	Verifiche funzionali	5																																											
	Formazione personale Unimol	10																																										
T2	Manutenzione ed assistenza apparecchiature hardware e software	1095																																										

EDIFICIO II POLIFUNZIONALE
LOCALE TECNICO: SALA CED - SERVER
STRALCIO PIANTA PIANO TERRA - QUOTA 653.50

Scala 1:50



AREA DESTINATA A SALA CED - SERVER PER LA REALIZZAZIONE DI UN'INFRASTRUTTURA PER LA GESTIONE DEI DATI AUTENTICATI SU BLOCKCHAIN PUBBLICHE E PRIVATE