PROCEDURA APERTA SOPRA SOGLIA COMUNITARIA AI SENSI DELL'ART. 71 DEL D. LGS. N. 36/2023, PER L'AFFIDAMENTO DEL SERVIZIO DI SVILUPPO, INSTALLAZIONE, TEST E MANUTENZIONE DI UNA PIATTAFORMA CLOUD DISTRIBUITA E DI SERVIZI APPLICATIVI CON IL CRITERIO DELL'OFFERTA ECONOMICAMENTE PIÙ VANTAGGIOSA SULLA BASE DEL MIGLIOR RAPPORTO QUALITÀ/PREZZO NELL'AMBITO DEL PIANO NAZIONALE RIPRESA E RESILIENZA (PNRR) MISSIONE 4 "ISTRUZIONE E RICERCA" COMPONENTE 2 "DALLA RICERCA ALL'IMPRESA" – LINEA DI INVESTIMENTO 3.1 "FONDO PER LA REALIZZAZIONE DI UN SISTEMA INTEGRATO DI INFRASTRUTTURE DI RICERCA E INNOVAZIONE" - PROGETTO "FOSSR" - CUP B83C22003950001 CIG A03B49C208

CAPITOLATO TECNICO

Sommario

1. PREMESSE

La Stazione Appaltante, Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche (CNR-ICAR), intende procedere mediante procedura di gara per l'assegnazione di un servizio di sviluppo, installazione, test e manutenzione di:

- una infrastruttura software e applicativi software di integrazione atti alla costruzione di una piattaforma cloud distribuita su più nodi, con l'obiettivo di fornire un ambiente flessibile e scalabile per la gestione di risorse, dati e servizi;
- un portale web multilingua che funga sia da unico punto di accesso ai servizi offerti dalla piattaforma cloud tramite autenticazione di tipo Single Sign-On (SSO) sia da catalogo dati e servizi attraverso un marketplace.

Tutte le componenti software dovranno essere distribuite su attrezzature hardware in fase di acquisizione e dispiegamento dalla Stazione Appaltante e da altri Istituti del CNR, presso quattro data center dislocati sul territorio nazionale. La piattaforma cloud risultante fungerà da sistema per la gestione e condivisione di dati e applicativi per la ricerca nell'ambito del progetto "FOSSR – Fostering Open Science in Social Science Research", il cui obiettivo è la creazione di un'infrastruttura di ricerca distribuita atta a offrire strumenti e servizi di supporto alla comunità scientifica nell'ambito delle scienze sociali. L'infrastruttura di ricerca da realizzare sarà collegata ad altre infrastrutture di ricerca esistenti, quali CESSDA, RISIS e SHARE, oltre a usufruire di dati statistici. Per raggiungere tale scopo, è in fase di progettazione un Cloud Italiano per l'Open Science, seguendo le linee guida del progetto "European Open Science Cloud" (EOSC), in cui integrare servizi innovativi relativi alla raccolta dati, all'analisi dei dati e alla data curation, seguendo i principi FAIR. L'intera piattaforma cloud dovrà essere sviluppata e configurata utilizzando server, storage e networking in fase di acquisizione, che saranno installate in quattro data center del CNR. In particolare, sono stati definiti due tipi di data center (nodi): i nodi di primo livello avranno hardware più potente in termini di calcolo e archiviazione rispetto a quelli di secondo livello. I nodi di primo livello sono in fase di installazione presso le sedi dell'Istituto ICAR di Napoli e di Palermo. I nodi di secondo livello saranno realizzati presso le sedi dell'Istituto ISTC di Catania e dell'Istituto IrCRES di Torino. Inoltre, sarà presente un quinto nodo basato su un cluster con funzionalità dedicate ad un applicativo denominato Virtual Research Environment (VRE) presso la sede dell'Istituto ISTI di Pisa. Tutti i nodi saranno comunque dotati di server all'avanguardia dotati di CPU e GPU di ultima generazione. I server saranno provvisti di tue tipologie differenti di storage (block e object), per consentire la gestione flessibile e scalabile dei dati all'interno dell'infrastruttura:

- lo storage di tipo block sarà gestito tramite BeeGFS, un sistema di file distribuito ad alte prestazioni, open-source e altamente scalabile;
- lo storage di tipo object verrà gestito attraverso nodi di tipo Ceph, un sistema di storage distribuito open-source progettato per fornire storage affidabile, scalabile e ad alte prestazioni e particolarmente adatto a sistemi cloud.

Saranno garantiti collegamenti in rete a banda larga e bassa latenza mediante tecnologia Rockport. Ciascun nodo di primo livello dovrà essere configurato per ospitare applicativi OpenStack per la creazione di una piattaforma cloud. Tutti i nodi dovranno essere configurati dall'operatore economico per la creazione e la gestione di macchine virtuali e container orchestrator tramite software appropriati come Kubernetes. Inoltre, dovrà essere fornita alla Stazione Appaltante la possibilità di

gestire dinamicamente la creazione e cancellazione di container e macchine virtuali per ospitare nuovi applicativi sviluppati dalla Stazione Appaltante o da altri partner del progetto per la gestione e l'analisi dei dati e metadati che saranno trattati. I nodi di primo livello, basati su OpenStack e container orchestrator, e i nodi di secondo livello, basati su framework per la gestione ed orchestrazione di macchine virtuali e di container, dovranno essere provvisti di servizi applicativi sviluppati dall'operatore economico per favorire la costruzione di un'unica piattaforma virtuale integrata. I nodi di primo livello saranno responsabili di fornire i servizi di front-end, i quali avranno la capacità di accogliere tutte le richieste di accesso ai servizi e dati provenienti da utenti esterni. Tali richieste saranno poi instradate verso i servizi di back-end disponibili presso i quattro data center, seguendo politiche configurabili (ad esempio, basate sul bilanciamento del carico).
Gli applicativi software sviluppati dall'operatore economico dovranno offrire la capacità di pubblicare dati, metadati, strumenti e servizi. Questi elementi saranno successivamente accessibili agli utenti tramite interrogazioni, organizzati in un catalogo suddiviso in diverse aree tematiche. Il catalogo sarà reso accessibile tramite un marketplace accessibile direttamente dal portale web.
L'operatore economico avrà la responsabilità principale di effettuare l'installazione e la configurazione dei software di base necessari per abilitare il cloud e gestire le macchine virtuali e i container. Successivamente, dovrà sviluppare un portale web che consentirà l'accesso alle funzionalità dell'intera piattaforma. Il portale sarà progettato con l'implementazione delle più recenti politiche di sicurezza. Inoltre, sarà incluso un sistema di accesso basato su Single Sign-On (SSO) per semplificare e migliorare l'esperienza di accesso degli utenti. Gli utenti avranno la possibilità di richiedere capacità di calcolo e spazio di archiviazione per i propri applicativi. Questi applicativi potranno essere eseguiti all'interno di macchine virtuali e/o container resi disponibili dagli amministratori di sistema. Pertanto, la piattaforma dovrà garantire la possibilità continua di aggiungere e rimuovere macchine virtuali e container. Questi conterranno gli strumenti e i servizi sviluppati dagli utenti che richiederanno tali risorse.
Sarà possibile accedere in remoto all'attrezzatura hardware. A questo riguardo, la Stazione Appaltante fornirà le modalità di accesso necessarie.
Qualora dovessero sorgere ostacoli di natura tecnica, organizzativa o amministrativa durante la fase di implementazione dei data center, si dovrà prendere in considerazione l'opzione di installare l'infrastruttura nei data center disponibili. Tale decisione sarà il risultato di una valutazione attenta delle circostanze e delle esigenze operative, mirando a garantire un'efficace ed efficiente realizzazione dei data center, tenendo conto delle sfide incontrate.
Dato che esiste una disparità nelle prestazioni dei vari nodi, è possibile determinare il valore percentuale dell'impatto economico sul progetto per ciascun nodo. Questo valore sarà stabilito al 40% per i nodi di primo livello (Napoli e Palermo) e al 10% per i nodi di secondo livello (Torino e Catania). Si richiede che l'operatore economico tenga conto di queste percentuali nel caso in cui, a causa di problemi tecnici, uno dei nodi dovesse essere escluso dal progetto. In tal caso, la percentuale dell'impatto economico sarà sottratta dall'importo concordato per il pagamento totale.
Inoltre, la stazione appaltante, al fine di garantire la trasparenza, l'integrità e l'efficienza della procedura di gara, si riserva il diritto di revocare l'intera gara nel caso in cui si verifichino eventi imprevedibili o circostanze eccezionali che rendano impossibile o non più conveniente procedere con la selezione dell'appaltatore. Questa riserva è una misura precauzionale volta a gestire situazioni eccezionali che potrebbero influenzare negativamente il corretto svolgimento della gara stessa. La stazione appaltante si impegna a valutare attentamente ogni situazione e a informare tempestivamente tutti i partecipanti in caso di revoca, fornendo le ragioni e i dettagli rilevanti.
Le prossime sezioni illustrano le caratteristiche hardware del sistema e le specifiche tecniche richieste relativamente allo sviluppo, all'installazione e alla configurazione software.

1.1. Specifiche hardware della strumentazione prevista nei data center

Al fine di fornire una panoramica generale delle attrezzature hardware che saranno installate presso i 4 data center, sulle quale dovrà essere installato e configurato il software necessario, vengono in questa sezione descritte le specifiche hardware del nodo di primo livello situato presso la sede di Napoli della Stazione Appaltante, per quanto riguarda i server e l'infrastruttura di rete. Seppur non contenente le informazioni relative a tutti i nodi, tale descrizione potrà essere utilizzata come guida di riferimento per la costruzione della piattaforma cloud.

1.1.1. Nodo di primo livello CNR-ICAR NAPOLI

Per la sede di Napoli sono state identificate le seguenti tipologie di nodo:

- Compute & Cloud: tali nodi andranno a coprire le esigenze di calcolo del sistema sia in termini di cloud che di algoritmi basati su approcci di Intelligenza Artificiale (IA).
- Nodi Management & Login: sono nodi atti a gestire l'infrastruttura e le funzionalità di accesso alla stessa.
- Nodi BeeGFS: questi nodi copriranno le necessità relative al block storage.
- Nodi Ceph: nodi necessari a garantire le funzionalità Cloud.
- Nodi GPU: tali nodi ospiteranno le schede grafiche necessarie per l'esecuzione di complessi algoritmi di deep learning.

Le tabelle proposte nel seguito descrivono le caratteristiche hardware per ogni tipologia di nodo.

Nodi Compute and Nodi Cloud		
Tipologia	**Modello**	**Quantità**
Server	PowerEdge R7525 Server (General Purpose)	100
Processore per server	AMD7413 2.65GHz,24C/48T,128M,180W,3200CK	2
RAM per server	32GB - 2Rx4 DDR4 RDIMM 3200MHz	32
Storage per server	3.84TB SSD SAS ISE RI 12Gbps	4
	960GB SSD SAS ISE RI 12Gbps	2

Nodi per Management, Nodi per lo Storage and nodi BeeGFS		
Tipologia	**Modello**	**Quantità**
Server	PowerEdge R7525 Server (nVME)	6
Processore per server	AMD7413 2.65GHz,24C/48T,128M,180W,3200CK	2
RAM per server	32GB - 2Rx4 DDR4 RDIMM 3200MHz	32
Storage per server	3.84TB SSD SAS ISE RI 12Gbps	14

	960GB SSD SAS ISE RI 12Gbps	2
	1.6TB Enterprise NVMe Mixed Use Drive U.2	8

Nodi di tipo Ceph per la gestione del Cloud		
Tipologia	**Modello**	**Quantità**
Server	PowerEdge R7525 Server (vSAN Ready 1 TB RAM)	11
Processore per server	AMD7413 2.65GHz,24C/48T,128M,180W,3200CK	2
RAM per server	32GB - 2Rx4 DDR4 RDIMM 3200MHz	32
Storage per server	3.84TB SSD SAS ISE RI 12Gbps	16
	1.6TB Enterprise NVMe Mixed Use Drive U.2	8

Nodi GPU Ready		
Tipologia	**Modello**	**Quantità**
Server	PowerEdge R7525 Server (GPU Double-Wide Ready)	10
Processore per server	AMD EPYC 7313 3.0GHz, 16C/32T, 128M Cache (155W) DDR4-3200	2
RAM per server	32GB - 2Rx4 DDR4 RDIMM 3200MHz	32
Storage per server	3.84TB SSD SAS ISE RI 12Gbps	7
	960GB SSD SAS ISE RI 12Gbps	2

Per quanto concerne le schede grafiche, saranno presenti 24 GPU Nvidia H100.
Gli apparati di rete necessari includono gli switch, le ottiche e le relative licenze accessorie per l'implementazione dell'infrastruttura. Per poter interconnettere correttamente le componenti, saranno implementate tre distinte tipologie di rete:

- **Rete di Management In-Band (IBN)**: attraverso questa rete viaggerà il traffico utile alla gestione dell'infrastruttura ed alla interconnessione ad alta velocità dei nodi storage Ceph della partizione Cloud. Tale rete sarà implementata in topologia spine-leaf interamente ridondata con velocità di accesso dei nodi pari ad almeno 25 Gbps. L'interconnessione tra i livelli spine e leaf avverrà con link ridondati aventi velocità di almeno 100 Gbps ed in modo che il rapporto di oversubscription sia non superiore a 3:1. Per una corretta gestione dei cablaggi, sarà predisposta una coppia di switch leaf per ogni rack aventi un sufficiente numero di porte a 25 Gbps, per l'interconnessione con i nodi, e di porte a 100 Gbps per l'interconnessione con gli switch spine. Oltre alle porte necessarie alle interconnessioni, è

prevista un'ulteriore quota di porte pari ad almeno il 10% delle porte occupate per garantire la scalabilità futura dell'infrastruttura. Saranno presenti due switch spine, ognuno dotato di un numero di porte a 100GbE sufficiente ad interconnettere in maniera ridondata tutti gli switch leaf rispettando il livello di oversubscription prescritto, tutti i nodi Ceph mediante 2 connessioni a 100GbSR4 MPO per nodo e a realizzare l'interconnessione alla rete d'Istituto mediante almeno 4 link a 25Gb SR. Gli switch spine e leaf saranno nativamente in grado di realizzare una topologia priva di SPOF mediante l'implementazione di meccanismi MC-LAG in grado di rendere trasparente ai nodi, a meno di un'eventuale riduzione della larghezza di banda delle connessioni, un eventuale guasto o riavvio di un qualunque apparato appartenente alla rete. L'interconnessione verso i nodi avverrà mediante link in fibra ottica a 25Gb SR.

- **Rete di Management Out-Of-Band (OOBN)**: tale rete interconnetterà baseboard management controller di tutti i nodi e le interfacce di management OOB di tutte le altre componenti dell'infrastruttura (sistemi storage, apparati di rete, PDU, etc). Tale rete sarà implementata in topologia spine-leaf e ridondata a livello di spine. La velocità di accesso sarà a 1Gbps in tecnologia Base-T (rame). Le interconnessioni tra spine e leaf dovranno invece essere implementate in modalità ridondata mediante link in fibra ottica con velocità non inferiore a 10Gbps. Sarà pertanto fornito per ogni rack del nuovo Data Center almeno uno switch 1/10 Gbps (per un totale di 8 switch), dotato di un numero di porte a 1Gbps sufficiente ad interconnettere tutti i nodi presenti nel rack, più una ulteriore quota di porte libere pari ad almeno il 10% delle porte occupate. Sarà inoltre fornita una coppia di switch spine, ognuno dotato di un numero di porte a 10Gbps sufficiente ad interconnettere in maniera ridondata tutti gli switch leaf ed a realizzare l'interconnessione alla rete d'Istituto mediante almeno 2 connessioni a 10 GbSR.
- **Rete di interconnessione a bassa latenza (LLN)**: tale rete interconnetterà tutti i nodi di calcolo della partizione HPC, realizzata con tecnologia e hardware RockPort.

2. CARATTERISTICHE TECNICHE/FUNZIONALITÀ E DOTAZIONI MINIME DEL SERVIZIO

In questa sezione, è presentata un'ampia panoramica dei requisiti software essenziali per l'implementazione del servizio di *Infrastructure as a Service* (IaaS) e del portale web, che costituiscono l'elemento centrale del presente capitolato. La tabella successiva offre una visione ad alto livello dei software necessari per garantire il funzionamento complessivo dell'infrastruttura e dei servizi previsti dal progetto. Ogni voce nella tabella fornisce informazioni rilevanti su ciascun software, comprensive del suo nome, una breve descrizione delle sue funzionalità e del ruolo chiave che svolge nell'ambito del progetto. Inoltre, vengono fornite eventuali note o dettagli pertinenti per una comprensione generale delle esigenze software.
Al fine di mantenere una visione generale delle necessità software, la tabella categorizza i software in base al livello in cui saranno ospitati all'interno dell'infrastruttura (nodi di primo livello o di secondo livello) e al loro tipo (intra data center o inter data center). Questa classificazione aiuta a delineare chiaramente il ruolo generale di ciascun software e la sua responsabilità nella gestione delle risorse e dei servizi all'interno o tra i data center. La tabella sottostante presenta una sintesi concisa dei software fondamentali richiesti per la realizzazione del progetto, fornendo brevi dettagli relativi alle loro funzionalità e al contributo essenziale che apportano all'ambito dei data center.

Tabella 1 - Software Richiesti

Software	Descrizione	Note	Livello	Tipo
Piattaforma Cloud	Software abilitanti al modello di infrastruttura come servizio (cloud IaaS) implementati presso i nodi di primo livello. Gestione di macchine virtuali e bilanciamento del carico.	Tecnologia richiesta OpenStack	1° livello	Inter data center
Servizi di integrazione, di gestione e di infrastruttura	Servizi applicativi ospitati in VM sui nodi di primo livello in grado di gestire le interazioni tra i servizi ospitati da tutti i nodi in maniera trasparente.	Fare riferimento alla tabella 2, del paragrafo 2.2	1° livello	Inter data center
Gestore Container	Software per la gestione dei container.	Tecnologia richiesta Kubernetes	1° livello 2° livello	Intra data center
Sistema di logging	Software atto alla raccolta dei log di accesso e delle attività degli utenti.	Open Source o sviluppato dall'operatore economico.	1° livello 2° livello	Intra data center
Sistema di autenticazione e autorizzazione	Sistema di autenticazione di tipo Single Sign On e sistema di autorizzazione basato su ruoli.	SSO configurato per il riconoscimento di credenziali istituzionali secondo modelli quali Shibboleth e IDEM.	1° livello	Inter data center
Sistema di monitoraggio e report	Sistema atto a monitorare le risorse hardware per la rilevazione di problematiche e anomalie.	Tecnologie consigliate Prometheus e Grafana.	1° livello	Intra data center
Sistema per la sicurezza dell'infrastruttura e dei dati	Sistema per il monitoraggio e la rilevazione delle attività malevole.		1° livello 2° livello	Inter data center

Portale Web	Portale web multilingua (almeno italiano e inglese) che permetta l'accesso ai servizi e ai dati contenuti nell'infrastruttura cloud. Tale portale dovrà necessariamente contenere un marketplace organizzato in cataloghi per l'acceso ai dati e ai servizi. È richiesto di utilizzare una tecnologia di sviluppo lato front end personalizzata, come ad esempio Angular 2+, al fine di offrire una maggiore flessibilità e personalizzazione rispetto ai CMS.	Unico punto di accesso alla piattaforma cloud.	1° livello	Inter data center
REST API	Tutti i servizi web realizzati devono esporre API volte ad abilitare la fruizione di risorse e servizi in maniera programmatica da parte degli applicativi degli utenti.	Conforme alle specifiche OpenAPI.	1° livello 2° livello	Inter data center

L'offerta dell'operatore economico deve rispettare tutte le caratteristiche tecniche, funzionalità e dotazioni minime specificate in questa sezione. La mancata conformità a tali requisiti comporterà l'esclusione dell'operatore dalla procedura di gara, in conformità con il principio di equivalenza stabilito nell'art. 68 del D.Lgs. N° 50/2016 e successive modifiche (di seguito denominato "Codice").
I successivi paragrafi dettaglieranno le esigenze del servizio in termini di applicazioni infrastrutturali e software. La tabella seguente riassume i servizi software richiesti.
In conformità con l'allegato II.5 del D.Lgs. 36/2023 (codice), il fornitore deve dimostrare nell'offerta, utilizzando qualsiasi mezzo appropriato, compresi i mezzi di prova previsti dall'articolo 105 del codice, che le soluzioni proposte rispettano in modo equivalente le prestazioni, i requisiti funzionali e le specifiche tecniche indicate in questo documento.
Nel seguito di questa sezione, presenteremo una visione ad alto livello dei software chiave necessari per il progetto, fornendo indicazioni generali sulle loro funzionalità e sul contributo essenziale che apportano al funzionamento complessivo dei data center.

2.1. Implementazione e gestione della piattaforma Cloud e dei servizi correlati

L'operatore economico è tenuto a fornire una serie di servizi chiave per l'implementazione e la gestione dell'ambiente cloud e dei container. Questi servizi includono:

- **Installazione e Configurazione di Software Abilitanti al Cloud (OpenStack)**
  L'operatore economico dovrà installare e configurare il software OpenStack sui nodi di primo livello per creare un ambiente cloud scalabile e flessibile. La configurazione accurata dei servizi principali di OpenStack, come Keystone (Identity Service), Nova (Compute Service), Neutron (Networking Service) e Glance (Image Service), è fondamentale per garantire la gestione efficiente delle risorse cloud.
- **Gestione di Container (Kubernetes) e Virtual Machine**
  L'operatore economico dovrà implementare e configurare Kubernetes, la piattaforma di gestione dei container, su tutti i nodi. Questo consentirà la distribuzione e la gestione di applicazioni containerizzate nell'ambiente cloud. La configurazione dei componenti principali di Kubernetes, compresi Kubernetes Master e Worker Nodes, è essenziale per fornire un'infrastruttura di containerizzazione affidabile e sicura. Inoltre, tutti i nodi dovranno

essere in grado di gestire le Virtual Machine: quelli di primo livello tramite OpenStack e quelli di secondo livello tramite framework appropriati (Hypervisor).

- **Sviluppo di Servizi per la Sincronizzazione dei Data Center**
  L'operatore economico dovrà sviluppare servizi applicativi e meccanismi per garantire la sincronizzazione e la replica dei dati tra i data center. Questo assicurerà la disponibilità e la ridondanza dei dati nell'ambiente cloud. Tali servizi devono essere progettati per garantire la coerenza e l'integrità dei dati, nonché la capacità di recupero in caso di guasti o interruzioni. È previsto un mirroring tra i nodi di primo livello, che devono essere cloni l'uno dell'altro. Inoltre, i dati salvati nei nodi di secondo livello, in base a politiche configurabili, saranno ridondati sui nodi di primo livello.
- **Servizi di Base**
  L'operatore economico dovrà fornire servizi di base essenziali, compresi servizi per il monitoraggio e la gestione delle risorse cloud, la gestione delle identità e degli accessi, nonché il supporto per il backup e il ripristino dei dati. Tali servizi devono essere configurati e ottimizzati per garantire un funzionamento affidabile e continuo dell'intera piattaforma.

Questi servizi sono fondamentali per la realizzazione e la gestione efficace dell'ambiente cloud e dei container nell'ambito del progetto.

2.1.1. Ottimizzazione delle Risorse Hardware e Garanzia di Disponibilità, Continuità e Ridondanza

L'operatore economico dovrà garantire il migliore utilizzo delle risorse hardware al fine di assicurare l'affidabilità, la disponibilità dei dati e la continuità delle operazioni. Saranno implementate misure appropriate per garantire una corretta gestione delle risorse hardware, la ridondanza dei dati e dei servizi, nonché la continous integration, come descritto di seguito.

- **Ottimizzazione delle Risorse Hardware**
  L'operatore economico sarà responsabile della corretta configurazione e ottimizzazione delle risorse hardware. Ciò includerà la configurazione dei server, dei dispositivi di storage, dell'utilizzo dell'infrastrutture di rete e delle risorse di calcolo in modo da massimizzare l'utilizzo e la performance, garantendo al contempo la stabilità e l'affidabilità.
- **Disponibilità dei Dati**
  Saranno adottate misure per garantire la disponibilità dei dati in modo continuo. Ciò includerà la replica e il backup dei dati in modo appropriato, utilizzando soluzioni di storage ridondanti e meccanismi di failover per prevenire la perdita dei dati in caso di guasti hardware o incidenti. La disponibilità dei dati deve essere garantita in ogni nodo della rete di data center.
- **Continuous Integration**
  L'operatore economico dovrà implementare e mantenere un ambiente di continuous integration che consenta lo sviluppo, il test e il rilascio di software in modo rapido e automatizzato. Saranno utilizzati strumenti e processi di continuous integration per garantire l'integrazione regolare e il testing delle modifiche apportate al sistema, garantendo la stabilità e la sicurezza del software. La continous integration dovrà essere garantita fino alla fine del progetto sia per quanto concerne gli applicativi volti alla gestione dell'infrastruttura che per quelli sviluppati dall'operatore economico su richiesta degli Istituti.

- **Business Continuity**
  L'operatore economico dovrà implementare piani di business continuity per garantire la continuità delle operazioni in caso di criticità, come guasti hardware, disastri naturali o attacchi informatici. Dovrà quindi prevedere meccanismi di disaster recovery e di ripristino per garantire la ripresa tempestiva delle attività in caso di interruzioni critiche.
- **Ridondanza dei Servizi**
  L'operatore economico dovrà prevedere soluzioni di ridondanza per garantire la continuità dei servizi. Ciò potrebbe includere la distribuzione di servizi su server multipli con bilanciamento del carico, la duplicazione dei servizi critici in diversi data center o l'utilizzo di tecnologie di clustering e failover per garantire la continuità operativa.
- **Monitoraggio e Reporting**
  L'operatore economico dovrà implementare meccanismi di monitoraggio delle risorse hardware e dei servizi per rilevare tempestivamente eventuali problemi o anomalie (tramite Prometheus e Grafana). Saranno forniti report periodici riguardanti le prestazioni del sistema e l'utilizzo delle risorse.
- **Test di Stress e Scalabilità**
  L'operatore economico dovrà condurre test di stress e scalabilità per valutare le prestazioni e la capacità di gestione delle risorse hardware e dei servizi. Ciò garantirà che il sistema sarà in grado di gestire carichi di lavoro crescenti senza compromettere le prestazioni e la disponibilità.

2.1.2. Installazione e Configurazione dei Servizi di Load Balancing

L'operatore economico dovrà installare e configurare servizi per il load balancing nella piattaforma cloud al fine di garantire una distribuzione efficiente del carico di lavoro tra le risorse disponibili. Questi servizi di load balancing dovranno essere adeguatamente configurati per ottimizzare le prestazioni del sistema, garantire l'alta disponibilità e migliorare la resilienza dell'infrastruttura.
Caratteristiche dei Servizi di Load Balancing:

- **Selezione del Tipo di Load Balancer**
  L'operatore economico dovrà identificare e selezionare, dopo interfacciamento con la Stazione Appaltante, il tipo di load balancer più adatto alle specifiche esigenze della piattaforma cloud. Saranno considerati load balancer basati su software, hardware o servizi cloud, tenendo conto dei requisiti di prestazioni, scalabilità e flessibilità del sistema.
- **Distribuzione Equa del Traffico**
  L'operatore economico dovrà configurare i servizi di bilanciamento del carico per distribuire in maniera efficiente il traffico tra le risorse disponibili, garantendo un utilizzo bilanciato delle risorse hardware e riducendo i possibili punti di congestione.
- **Algoritmi di Bilanciamento del Carico**
  L'operatore economico dovrà implementare gli algoritmi di bilanciamento del carico più appropriati, come round-robin, least connection, least response time, weight-based, etc., in base alle esigenze dell'infrastruttura e al tipo di applicazioni ospitate.
- **Health Checking e Monitoraggio delle Risorse**
  L'operatore economico dovrà configurare meccanismi di health checking e monitoraggio delle risorse per valutare lo stato e la disponibilità dei server e delle applicazioni. I servizi di bilanciamento del carico dovranno essere in grado di rilevare automaticamente le risorse non

disponibili o malfunzionanti, rimuoverle dalla distribuzione del traffico e notificare al sistema di Health Checking l'identificativo del dispositivo non funzionante.

- **Persistenza delle Sessioni**
  L'operatore economico dovrà prevedere la configurazione della persistenza delle sessioni per consentire il corretto mantenimento dello stato delle connessioni dei client verso le risorse del sistema. Questo garantirà la corretta gestione delle sessioni e la continuità delle attività degli utenti.
- **Scalabilità Orizzontale e Verticale**
  I servizi di load balancing dovranno supportare la scalabilità orizzontale e verticale delle risorse, consentendo l'aggiunta o la rimozione di nodi di elaborazione senza interruzioni del servizio.
- **Sicurezza e Protezione**
  L'operatore economico dovrà adottare misure di sicurezza per proteggere i servizi di load balancing da attacchi informatici, compresi gli attacchi di tipo DDoS (Distributed Denial of Service).

Per massimizzare l'aderenza ai principi di sostenibilità ambientale, il soggetto operante è tenuto a concepire un piano di programmazione energetica di carattere avanzato. Tale approccio consentirà un'ottimizzazione dell'impiego delle risorse informatiche, garantendo che le unità di elaborazione siano operative solamente durante le fasi in cui risulta indispensabile. Attraverso un'articolata gestione intelligente delle risorse, mirata all'accensione e allo spegnimento delle unità in base al carico di lavoro, si assicurerà una notevole riduzione nel consumo di energia nei periodi di minore richiesta di capacità computazionali. Tale prassi, oltre a ridurre il carico ambientale, comporterà un apprezzabile risparmio delle preziose risorse energetiche.
Il nucleo della strategia consisterà nell'utilizzo di sofisticati algoritmi, costantemente operativi nell'analisi del carico di lavoro, consentendo di identificare in tempo reale quali unità di elaborazione siano necessarie per un'efficace gestione delle attività. Ciò determinerà l'eliminazione dell'uso superfluo di energia, traducendosi in una significativa riduzione delle emissioni di gas serra e una concreta integrazione nei confronti della nostra missione volta alla promozione della sostenibilità ambientale.
Tale approccio non solo comporterà un abbattimento dei costi energetici, ma costituirà altresì una dimostrazione tangibile dell'impegno dell'organizzazione nella tutela e nella salvaguardia dell'ambiente.

2.1.3. Gestione dinamica di VM e container

L'operatore economico dovrà garantire la possibilità di una gestione dinamica di macchine virtuali (VM) e container all'interno della piattaforma cloud. La gestione dinamica dovrà consentire l'aggiunta di VM e container in numero crescente, al fine di poter ospitare nuovi servizi e applicativi che verranno sviluppati durante l'avanzamento del progetto.
Caratteristiche della Gestione Dinamica di VM e Container:

- **Scalabilità Orizzontale e Verticale**
  La piattaforma cloud dovrà supportare la scalabilità orizzontale e verticale delle VM e dei container, consentendo l'aggiunta o la rimozione di risorse in modo dinamico. Dovranno essere previste politiche di scaling sia automatico sia manuale, per adattare le risorse alle necessità dell'infrastruttura.

- **Orchestrazione dei Container**
  È necessario implementare un sistema di orchestrazione dei container, come Kubernetes, che consenta la gestione automatizzata dei container. Questo sistema permetterà di distribuire, monitorare e scalare i container in modo efficiente.
- **Allocazione Dinamica delle Risorse**
  La gestione dinamica delle macchine virtuali (VM) e dei container deve includere l'allocazione dinamica di risorse, come CPU, GPU, memoria, storage e larghezza di banda di rete, in base alle richieste e alle esigenze dei servizi e degli applicativi ospitati.
- **Sistema di Monitoraggio e Logging**
  L'operatore economico dovrà implementare un sistema di monitoraggio e logging delle VM e dei container per rilevare eventuali problemi di performance, disponibilità, integrità e sicurezza. Questo sistema permetterà di intervenire tempestivamente in caso di anomalie.
- **Gestione dei Backup e delle Snapshot**
  Dovranno essere previsti meccanismi di gestione dei backup e delle snapshot delle VM e dei container, al fine di garantire la protezione e la disponibilità dei dati in caso di guasti o perdite accidentali.
- **Gestione delle Versioni dei Servizi e Applicativi**
  L'operatore economico dovrà fornire la possibilità di gestione delle versioni parziale dei servizi e degli applicativi ospitati all'interno delle VM e dei container. Questo consentirà di mantenere un registro delle versioni e di effettuare il rollback in caso di necessità.
- **Politiche di Autorizzazione e Accesso**
  Dovranno essere implementati meccanismi per gestire dinamicamente le politiche di autorizzazione e accesso per garantire la sicurezza e il controllo degli attori autorizzati alla gestione e all'uso delle VM e dei container.
- **Conformità agli Standard e Normative**
  La gestione dinamica di VM e container dovrà rispettare gli standard e le normative riguardanti la sicurezza, la privacy e la gestione delle risorse della piattaforma cloud.

2.1.4. Sistema di logging

L'operatore economico dovrà tracciare tutte le attività svolte nella piattaforma cloud mediante un sistema di logging apposito. Tale sistema di logging dovrà essere sviluppato dall'operatore economico o selezionato tra sistemi open source esistenti e adeguatamente installato e configurato. Il tracciamento delle attività attraverso il sistema di logging avrà lo scopo di registrare in modo dettagliato gli eventi e le azioni compiute dagli utenti, dai servizi e dai componenti della piattaforma, al fine di consentire un'analisi approfondita e una risposta tempestiva a eventuali incidenti o problematiche. Saranno presi in considerazione aspetti quali la gestione dei log, la protezione dei dati sensibili e l'accessibilità dei registri per il personale incaricato.
Caratteristiche per il tracciamento delle attività con sistema di logging:

- **Sviluppo o Selezione di un Sistema di Logging Adeguato**
  L'operatore economico dovrà sviluppare un sistema di logging in-house o selezionare un sistema open source esistente che sia adeguato a soddisfare le esigenze di tracciamento delle attività della piattaforma complessiva.
- **Completa Tracciabilità delle Attività**

Il sistema di logging dovrà garantire la completa tracciabilità delle attività svolte sulla piattaforma, registrando gli eventi e le azioni compiute dagli utenti, dai servizi e dai componenti.

- **Dettaglio e Precisione dei Log**
  I log generati dal sistema dovranno essere dettagliati e precisi, includendo informazioni rilevanti sugli eventi registrati, come data e ora, tipo di attività, utente coinvolto, indirizzi IP utilizzati e altre informazioni utili per l'analisi e la gestione degli eventi.
- **Gestione dei Log e Conservazione dei Dati**
  Saranno definiti protocolli di gestione dei log, compresi tempi di conservazione e modalità di backup, per garantire l'integrità e l'accesso alle informazioni registrate nel tempo.
- **Protezione dei Dati Sensibili**
  Il sistema di logging dovrà essere configurato per proteggere i dati sensibili e rispettare le normative sulla privacy, evitando l'inclusione di informazioni sensibili nei log e garantendo l'accesso solo al personale autorizzato.
- **Monitoraggio dei Log e Rilevazione di Anomalie**
  Saranno implementati meccanismi di monitoraggio dei log per rilevare eventuali anomalie o attività sospette nell'infrastruttura, al fine di consentire una risposta tempestiva a potenziali minacce.
- **Accessibilità dei Log per il Personale Autorizzato**
  Il personale incaricato della sicurezza e della gestione della piattaforma dovrà avere accesso ai log e alle informazioni registrate per consentire analisi approfondite e risposte rapide a incidenti o problemi.

2.1.5. Sicurezza della piattaforma

L'operatore economico dovrà garantire la sicurezza della piattaforma cloud adottando strumenti e soluzioni avanzate per proteggere i dati e le risorse. Sarà necessario implementare tool di cifratura dei dati per garantire la protezione e la riservatezza delle informazioni sensibili. Saranno adottati strumenti di monitoraggio e rilevazione delle attività malevole, attacchi e intrusioni (Intrusion Detection System e Anomaly Detection System), al fine di identificare tempestivamente eventuali minacce alla sicurezza e intraprendere azioni correttive. L'operatore economico dovrà assicurarsi che gli strumenti utilizzati siano in linea con le migliori pratiche di sicurezza e siano aggiornati per far fronte alle nuove minacce emergenti.
Caratteristiche per la sicurezza della piattaforma:

- **Strumenti di Cifratura dei Dati**
  Dovranno essere implementati strumenti di cifratura per proteggere i dati durante la trasmissione. I dati sensibili dovranno essere crittografati in modo tale da risultare incomprensibili e inaccessibili in caso di accesso non autorizzato.
- **Monitoraggio Avanzato delle Attività**
  Dovranno essere utilizzati strumenti di monitoraggio adeguati a tenere traccia delle attività svolte sulla piattaforma. Il monitoraggio comprenderà la registrazione degli eventi e delle attività degli utenti, dei servizi e dei componenti della piattaforma.
- **Rilevazione delle Attività Malevole, Attacchi e Intrusioni**

Dovranno essere adottati strumenti per la rilevazione tempestiva di attività malevole, tentativi di attacco e intrusioni nel sistema. Questi strumenti dovranno essere in grado di identificare comportamenti sospetti e segnalarli al personale incaricato della sicurezza.

- **Gestione degli Incidenti di Sicurezza**
  Dovrà essere predisposto un piano per la gestione degli incidenti di sicurezza, che definirà le procedure da seguire in caso di rilevazione di attività malevole o tentativi di attacco. Questo piano dovrà garantire una risposta rapida ed efficace per mitigare eventuali danni o minacce alla sicurezza.
- **Aggiornamenti e Patching**
  Sarà garantito che tutti gli strumenti e le soluzioni di sicurezza siano costantemente aggiornati con le ultime patch e le versioni più recenti per garantire la protezione contro le vulnerabilità note.
- **Protezione degli Accessi**
  Dovranno essere adottate misure di sicurezza per proteggere gli accessi alla piattaforma, come autenticazione a più fattori (MFA) e controllo degli accessi basato sui privilegi, per garantire che solo gli utenti autorizzati possano accedere alle risorse critiche.

2.2. Software per l'accesso al IAAS

L'operatore economico dovrà occuparsi dello sviluppo software relativo ad un portale web, Marketplace, REST API e altri applicativi di vario genere che potranno essere concordati con la Stazione Appaltante in corso di progetto. Questa fase, successiva alla fase infrastrutturale, potrà richiedere lo sviluppo di software eterogeneo nell'arco di tutta la durata del progetto.

2.2.1. Servizi di integrazione, di gestione e di infrastruttura

I servizi cloud si suddividono in tre categorie principali: servizi di integrazione, servizi di gestione e servizi di infrastruttura. Ciascuna di queste categorie fornisce funzionalità specifiche per l'implementazione e la gestione di applicazioni e servizi in ambiente cloud. Di seguito, una panoramica delle tre categorie:

1. **Servizi di Integrazione**
   Questi servizi consentono di collegare applicazioni e servizi tra loro, indipendentemente dalla loro posizione (cloud o on-premise). Forniscono funzionalità come API per consentire la comunicazione tra le applicazioni, servizi di gestione per configurare, monitorare e gestire le integrazioni e servizi di sicurezza per proteggere le integrazioni da minacce e attacchi.
   Esempi: API Gateway, Servizi di Messaggistica, Servizi di Sicurezza delle API.
2. **Servizi di Gestione**
   Questi servizi sono focalizzati sulla configurazione, il monitoraggio e la gestione dell'ambiente cloud. Offrono funzionalità come gestione delle identità e degli accessi per controllare l'accesso alle risorse cloud, gestione delle risorse per monitorare e gestire l'utilizzo delle risorse, orchestrazione e automazione per automatizzare attività di provisioning e amministrazione, sicurezza e conformità per proteggere l'ambiente cloud da minacce.
   Esempi: Servizi di Identità e Accesso, Monitoraggio e Log, Orchestrazione, Sicurezza e Conformità.
3. **Servizi di Infrastruttura**
   Questi servizi forniscono l'hardware e il software necessari per eseguire applicazioni e servizi in ambiente cloud. Includono risorse virtuali come macchine virtuali, container e serverless,

servizi di gestione delle macchine virtuali, storage come servizio per l'archiviazione dei dati, e servizi di rete per garantire la connettività tra risorse cloud e infrastrutture on-premise.
Esempi: Fornitura di Risorse Virtuali, Gestione delle Macchine Virtuali, Storage come Servizio, Rete come Servizio.

Ognuna di queste categorie ha un ruolo specifico nella realizzazione e nella gestione di un ambiente cloud. Nel contesto del progetto FOSSR, saranno necessari servizi da tutte e tre le categorie per garantire l'integrazione, la gestione e l'infrastruttura adeguata al funzionamento del servizio di Infrastructure as a Service (IaaS) e del portale web. La tabella seguente fornisce dettagli aggiuntivi sui servizi identificati all'interno di ciascuna categoria.La tabella non rappresenta un vincolo assoluto; per ragioni di fattibilità e implementazione, l'operatore economico può divergere dalle direttive fornite. In tal caso, è richiesto che l'operatore economico notifichi tempestivamente e formalmente la stazione appaltante delle modifiche apportate.

Tabella 2 - Specifica dei Servizi

Servizio	Descrizione	Tipologia
Fornitura di risorse virtuali	Permette agli utenti di ottenere accesso a risorse virtuali, come server, storage e rete, basate su soluzioni open source. Gli utenti possono provisionare queste risorse in modo flessibile e adattarle alle proprie esigenze senza costi aggiuntivi.	Infrastruttura
Gestione delle macchine virtuali (VM)	Permette agli utenti di creare, avviare e gestire le macchine virtuali basate su software open source. Gli utenti possono selezionare i sistemi operativi open source e le applicazioni da eseguire sulle VM.	Infrastruttura
Storage come servizio	Offre spazio di archiviazione scalabile basato su soluzioni open source come Ceph o GlusterFS. Gli utenti possono anche usufruire di servizi di backup e ripristino dei dati.	Infrastruttura
Rete come servizio	Consente agli utenti di configurare reti virtuali, indirizzamento IP, bilanciamento del carico e VPN utilizzando strumenti open source come Open vSwitch o OpenDaylight.	Infrastruttura
Gestione delle identità e degli accessi	Un sistema di gestione degli utenti e dei ruoli basato su software open source. Ciò garantisce un accesso sicuro alle risorse e alle applicazioni all'interno dell'ambiente.	Gestione
Gestione delle risorse	Ha lo scopo di fornire strumenti di monitoraggio e gestione delle risorse basati su software open source, consentendo agli utenti di tenere traccia dell'utilizzo delle risorse e dell'allocazione delle stesse.	Gestione
Orchestrazione e automazione	Al fine di semplificare l'uso delle risorse, tale servizio offrirà strumenti open source come Kubernetes per automatizzare i processi di provisioning, scalabilità e gestione delle risorse.	Gestione
Sicurezza e conformità	La sicurezza dei dati è una priorità. Sono implementate misure di sicurezza come la crittografia dei dati, l'audit e la conformità alle normative per proteggere le risorse e i dati degli utenti.	Gestione

Supporto e assistenza	Ha lo scopo di aiutare gli utenti a risolvere problemi o rispondere a domande.	Integrazione
API e personalizzazione	Le API aperte permettono agli utenti di integrare l'IaaS con le proprie applicazioni e di personalizzare l'ambiente secondo le proprie esigenze, promuovendo l'interoperabilità.	Integrazione
Alta disponibilità e ridondanza	Gli ambienti FOSSR sono progettati per garantire un'elevata disponibilità e ridondanza dei servizi. Questo evita interruzioni del servizio e si basa su soluzioni open source per la scalabilità orizzontale e verticale.	Integrazione
Scalabilità orizzontale e verticale	Gli utenti di FOSSR possono aumentare o ridurre le risorse in base alle esigenze di carico di lavoro, sfruttando la scalabilità orizzontale e verticale offerta dalle soluzioni open source.	Integrazione
Mobilità delle applicazioni	FOSSR consente la migrazione agevole delle applicazioni tra ambienti on-premises e cloud o tra diversi fornitori di servizi cloud, promuovendo la flessibilità.	Integrazione
Archiviazione dei dati	Servizi open source di archiviazione dei dati permettono agli utenti di conservare i dati a lungo termine in modo efficiente e sicuro all'interno dell'ambiente FOSSR.	Integrazione

2.2.2. Portale web

L'operatore economico avrà il compito di sviluppare un portale web che fungerà da punto di accesso principale alla piattaforma. Inoltre, sarà responsabile della creazione di un marketplace, che includerà un catalogo per la ricerca di dati e metadati da parte degli utenti.
Un elemento cruciale del portale web è la sua natura multilingua. È obbligatorio che il portale sia accessibile in almeno due lingue principali: italiano e inglese. Queste due lingue costituiranno il requisito minimo per l'interfaccia utente e la fruizione del portale. Gli utenti devono poter selezionare tra italiano e inglese come lingua di visualizzazione dell'interfaccia utente. Inoltre, tutti i contenuti presenti sul portale, inclusi testi, menu, etichette e informazioni, dovranno essere disponibili in entrambe le lingue.
L'implementazione multilingua è di fondamentale importanza poiché assicura l'accessibilità alle risorse e alle funzionalità offerte dall'infrastruttura FOSSR. Questo favorisce un approccio aperto e inclusivo per un pubblico diversificato a livello linguistico. L'obiettivo principale di questa implementazione è promuovere l'adozione e l'ampio utilizzo della piattaforma FOSSR da parte di una vasta comunità internazionale. Consentendo a utenti provenienti da diverse nazioni e con varie lingue di trarre pieno vantaggio dalle risorse e dai servizi forniti dalla piattaforma, si migliora significativamente l'accessibilità e l'usabilità su scala globale dell'infrastruttura FOSSR. Tali strumenti, ossia il portale web e il marketplace, dovranno essere resi accessibili attraverso i nodi di primo livello della piattaforma.
Il portale web dovrà essere sviluppato con funzionalità analoghe al portale EOSC (https://eosc-portal.eu/) e D4Science (https://www.d4science.org/). Le caratteristiche primarie potranno essere quindi identificate da:

- **Ricerca di dati**: Il portale, tramite un marketplace, deve poter consentire agli utenti di trovare dati di ricerca scientifica da diverse fonti. Gli utenti dovranno poter effettuare ricerche per parola chiave, argomento o tipo di dato.

- **Ricerca di tool e servizi**: tramite il marketplace gli utenti potranno ricercare tool e servizi riguardanti il settore delle social science. Tali servizi potranno essere localizzati nei repository del cloud FOSSR o esternamente. In ogni caso dovrà essere fornita una descrizione dei servizi e l'accesso agli stessi.
- **Accesso a ambienti di ricerca virtuali**: il portale dovrà consentire agli utenti di accedere a ambienti di ricerca virtuali. Questi ambienti dovranno poter consentire agli utenti di collaborare e condividere dati e risorse.
- **Valutazione della qualità dei dati**: il portale dovrà poter consentire agli utenti di valutare la qualità dei dati di ricerca scientifica.
- **Documentazione dei dati**: Il portale dovrà poter consentire agli utenti di documentare i dati di ricerca scientifica.
- **Documentazione**: Il portale dovrà fornire documentazione sui servizi offerti da FOSSR.
- **Supporto**: il portale offrirà servizi di supporto agli utenti.
- **Possibilità di accesso tramite un sistema di autenticazione SSO**: Tale sistema servirà a fornire funzionalità aggiuntive agli utenti, come la creazione di progetti atti a raggruppare dati e tool di interesse.
- Pagine supplementari per servizi di help desk, monitoraggio dello stato dei server, statistiche di utilizzo, etc.

È importante notare che mentre alcune funzionalità, come il marketplace, saranno definite nella fase iniziale del progetto, altre caratteristiche del portale potrebbero essere soggette a ulteriori definizioni e raffinamenti durante il corso dello sviluppo. Questo approccio mira a garantire la necessaria flessibilità per adattare il portale alle mutevoli esigenze dell'infrastruttura FOSSR e dei suoi utenti. Tale flessibilità è fondamentale per assicurare che il risultato finale sia perfettamente allineato con gli obiettivi e le aspettative del progetto, garantendo così un prodotto finale di qualità che soddisfi appieno le esigenze in evoluzione.
Il portale sarà principalmente dedicato a semplificare l'accesso ai dati di ricerca e ai servizi forniti dall'infrastruttura FOSSR. Inoltre, è progettato per agevolare la ricerca e l'accesso ai dati e ai servizi disponibili in altre infrastrutture di ricerca esterne. Questa strategia è finalizzata a fornire alla comunità scientifica un punto di riferimento italiano per i dati delle scienze sociali, contribuendo notevolmente a migliorare la disponibilità e l'accessibilità di tali risorse per gli utenti interessati.
Lo sviluppo del portale FOSSR dovrà essere effettuato utilizzando le più moderne tecniche di sviluppo e i protocolli di sicurezza più recenti. Tale approccio garantirà che il portale sia sicuro, affidabile e scalabile.
In particolare, lo sviluppo del portale dovrà seguire i seguenti principi:

- **Architettura modulare**
  Il portale dovrà essere progettato come un sistema modulare, in modo da facilitare la manutenzione e l'aggiornamento.
- **Codifica standardizzata**
  Il codice del portale dovrà essere scritto secondo le migliori pratiche di codifica, in modo da ridurre il rischio di vulnerabilità di sicurezza.
- **Test di sicurezza**
  Il portale dovrà essere sottoposto a test di sicurezza rigorosi, al fine di identificare e correggere eventuali vulnerabilità.

Il portale FOSSR costituirà il punto di accesso esclusivo alla piattaforma cloud di FOSSR, offrendo agli utenti un'interfaccia centralizzata per accedere a tutte le risorse e funzionalità disponibili. A tal fine, verrà implementato un processo di autenticazione basato su SSO (Single Sign-On) per semplificare l'accesso degli utenti.
La configurazione del portale FOSSR consentirà agli utenti di utilizzare le proprie credenziali di identità, fornite dagli enti di ricerca e/o università di cui fanno parte, per accedere a tutte le risorse di FOSSR. Questo processo semplificherà notevolmente la gestione delle credenziali degli utenti e migliorare l'esperienza di accesso alle risorse. In particolare, il portale sarà progettato per interfacciarsi con Identity Provider (IdP) di terze parti, consentendo agli utenti di utilizzare le stesse credenziali di identità che già utilizzano per accedere ad altri servizi, come servizi di posta elettronica, risorse accademiche o servizi di cloud computing.
Inoltre, il portale FOSSR includerà un marketplace dedicato alle risorse di ricerca. Questo marketplace sarà uno strumento fondamentale per la ricerca scientifica, consentendo agli utenti di scoprire, esplorare e accedere a una vasta gamma di risorse pertinenti per la ricerca, tra cui dati, dataset, pubblicazioni, strumenti, servizi e altro.
La piattaforma FOSSR sarà progettata per semplificare in modo significativo il processo di scoperta e utilizzo delle risorse di ricerca, fornendo agli utenti un punto di accesso unificato per individuare tutte le risorse di cui hanno bisogno.
Il marketplace FOSSR sarà concepito come un sistema centralizzato, consentendo agli utenti di accedere a risorse provenienti da diverse fonti, sia all'interno del progetto FOSSR che da fonti esterne. Questa strategia garantirà un accesso agevole e unificato a un'ampia varietà di risorse di ricerca, semplificando ulteriormente il processo di scoperta e utilizzo delle risorse. L'interfaccia utente sarà progettata per garantire un'esperienza utente altamente intuitiva e di facile navigazione, assicurando un accesso rapido e agevole alle risorse di interesse.
Le principali funzionalità includeranno:

- **Ricerca avanzata**: gli utenti potranno effettuare ricerche mirate in base a criteri specifici, come parole chiave, data di pubblicazione, tipologia di risorsa e altro ancora.
- **Catalogo organizzato**: il catalogo delle risorse sarà organizzato in sezioni tematiche, garantendo una struttura logica e intuitiva per la ricerca delle risorse desiderate.
- **Ricerca interna ed esterna**: il Marketplace sarà in grado di condurre ricerche sia all'interno dell'infrastruttura FOSSR che al di fuori di essa, collegandosi ad altre infrastrutture di ricerca.
- **Esplorazione dei metadati**: per ciascuna risorsa, sono disponibili metadati dettagliati che consentiranno agli utenti di valutare la pertinenza e l'utilità delle risorse stesse.

Il progetto prevede la necessità di una gestione dinamica del front-end del portale web e del marketplace, con la capacità da parte della Stazione Appaltante di inserire o rimuovere facilmente contenuti.
Il back-end del sistema dovrà implementare interfacce altamente flessibili, basate su OpenAPI, che consentano una facile aggiunta o rimozione di servizi e funzionalità. Queste interfacce dovrebbero essere progettate per permettere personalizzazioni e modifiche agili, adattabili alle esigenze specifiche. Ciò garantirà che la Stazione Appaltante possa integrare nuovi servizi o funzionalità nel sistema o eliminarli senza complicazioni, garantendo una gestione agibile e reattiva delle risorse disponibili.
L'interfaccia utente sarà dinamica e basata su template appositamente progettati per ciascuna categoria di risorsa. Le pagine dedicate alle diverse categorie di risorse saranno in grado di

visualizzare risultati specifici, evidenziando i metadati rilevanti relativi a ciascuna risorsa. Ad esempio, per le pubblicazioni scientifiche, verranno mostrate informazioni quali il Digital Object Identifier (DOI), l'URL per l'accesso alla pubblicazione e i metadati che identificano l'ambito di ricerca associato. Per i servizi, potrebbe essere inclusa una sezione descrittiva esaustiva insieme all'indicazione dell'URL del servizio, che può essere sia interno che esterno all'infrastruttura FOSSR. Questo approccio garantirà una presentazione altamente personalizzata delle risorse, migliorando l'esperienza dell'utente finale e assicurando che le informazioni pertinenti siano rapidamente accessibili in base al tipo di risorsa consultata.
Il portale web fornirà agli utenti una serie di funzionalità essenziali, tra cui:

- **Aggiunta di dati e dataset**
  Gli utenti dovranno poter utilizzare il portale per inserire nella piattaforma nuovi dati e dataset fruibili dalla comunità scientifica.
- **Aggiunta di servizi**
  Gli utenti dovranno poter aggiungere propri applicativi e servizi allocandoli in macchine virtuali e container.
- **Richiesta di container e macchine virtuali**
  Gli utenti dovranno poter richiedere la creazione di macchine virtuali e container per l'allocazione dei propri servizi, conformemente alle proprie esigenze specifiche. Questo processo di creazione dovrà essere altamente flessibile, consentendo una personalizzazione completa.
- **Gestione di container e macchine virtuali**
  Un'altra prerogativa degli utenti è la gestione autonoma delle risorse create. Tale gestione abbraccia la possibilità di apportare modifiche alle configurazioni, avviare o interrompere le risorse e, al momento opportuno, rimuovere risorse non più necessarie al fine di garantire un utilizzo efficiente dell'infrastruttura.
- **Monitoraggio delle risorse**
  Un elemento cruciale è il monitoraggio costante delle risorse create dagli utenti. Tale monitoraggio riveste una rilevanza fondamentale, consentendo agli utenti di tenere sotto controllo l'utilizzo delle risorse e di garantirne l'integrità e l'efficienza.

Il portale web FOSSR dovrà mettere a disposizione degli utenti un'interfaccia utente (UI) altamente intuitiva e usabile. L'interfaccia utente dovrà essere concepita con l'obiettivo di garantire una fruibilità ottimale, consentendo agli utenti di individuare e utilizzare le risorse offerte da FOSSR con celerità e semplicità.
Nel dettaglio, l'interfaccia utente FOSSR dovrà conformarsi ai seguenti principi:

- **Coerenza**
  L'omogeneità rappresenta un requisito fondamentale, poiché l'interfaccia utente dovrà mantenersi uniforme in tutti i settori del portale. Questa uniformità agevolerà il processo di apprendimento e memorizzazione delle operazioni da parte degli utenti, garantendo un'esperienza coerente e fluida.
- **Comprensibilità**
  L'interfaccia utente dovrà offrire una chiarezza esemplare, consentendo agli utenti di comprenderne il funzionamento senza la necessità di istruzioni particolari. La sua struttura e i comandi dovranno risultare immediatamente intuitivi, promuovendo un apprendimento rapido.

- **Accessibilità**
  L'interfaccia utente dovrà garantire l'accessibilità a tutti gli utenti, indipendentemente dalle loro abilità e capacità. Questo significa che dovrà essere progettata tenendo conto delle diverse esigenze degli utenti, inclusi coloro con disabilità, al fine di garantire una fruizione equa e inclusiva del portale.

La fornitura di un'interfaccia utente intuitiva e di buona facilità d'uso riveste un ruolo di rilevanza cruciale nel garantire che il portale FOSSR sia accessibile e utilizzabile da un vasto pubblico di utenti. La progettazione e lo sviluppo del portale web FOSSR dovranno essere condotti adottando le più avanzate tecniche di sicurezza e facendo ricorso ai protocolli di sicurezza più aggiornati. Questo approccio sarà garante della tutela delle informazioni di natura sensibile degli utenti, oltre che della sicurezza complessiva dell'infrastruttura. In particolare, il portale FOSSR dovrà ottemperare ai seguenti stringenti requisiti in materia di sicurezza:

- **Autenticazione e Autorizzazione**
  Il portale dovrà essere equipaggiato con un sistema di autenticazione e autorizzazione di grande robustezza. Ciò garantisce che soltanto gli utenti previamente autorizzati siano in grado di accedere alle risorse ospitate dalla piattaforma. Un rigoroso controllo degli accessi costituisce una barriera cruciale contro potenziali minacce. Le politiche di accesso dovranno essere facilmente configurabili dalla Stazione Appaltante.
- **Crittografia**
  Per la protezione di informazioni delicate, come dati personali e dati identificativi, il portale dovrà implementare un robusto sistema di crittografia. Tale sistema contribuirà a garantire che tali dati siano inaccessibili a terzi non autorizzati, contribuendo all'integrità e alla confidenzialità delle informazioni.
- **Controllo degli Accessi**
  Sarà necessario implementare meccanismi di controllo degli accessi che disciplinino e regolamentino l'accesso alle risorse. Ciò comporterà la necessità di limitare l'accesso solo a utenti e sistemi previamente autorizzati, rafforzando ulteriormente la sicurezza dell'ambiente.
- **Monitoraggio della Sicurezza**
  Sarà essenziale sottoporre il portale a un monitoraggio costante al fine di individuare tempestivamente eventuali attività sospette o intrusioni. Questa pratica consentirà di mantenere la sicurezza a un livello ottimale, intervenendo immediatamente in caso di anomalie.

L'implementazione di un portale che soddisfi rigorosamente questi criteri di sicurezza garantisce che il portale sarà un ambiente affidabile e protetto, adatto alla condivisione di dati e risorse di ricerca in un contesto in cui la sicurezza è di vitale importanza.
Inoltre, il portale includerà una sezione dedicata all'help desk, che fornirà assistenza e supporto agli utenti per risolvere eventuali problemi o ottenere informazioni sull'uso dell'infrastruttura e dei servizi offerti. L'implementazione di un help desk è un prerequisito essenziale per garantire un'esperienza ottimale agli utenti. Un efficiente help desk consentirà agli utenti di superare con successo eventuali ostacoli, assicurando loro la possibilità di un utilizzo efficace e produttivo.
L'attuazione di un help desk efficiente rappresenta un investimento significativo per il progetto, contribuendo notevolmente al miglioramento complessivo dell'esperienza degli utenti e al successo dell'infrastruttura FOSSR.

2.3. Ulteriori caratteristiche del servizio

L'operatore economico è tenuto ad installare, configurare e testare tutti i software sviluppati sia per quanto concerne il lato infrastrutturale che applicativo, rispettando le decisioni prese in fase di progettazione dalla Stazione Appaltante riguardo alla distribuzione delle componenti nei data center. Saranno presi in considerazione i requisiti specificati nell'architettura di riferimento, con particolare attenzione alla ridondanza, all'alta disponibilità e alla scalabilità. Tutti i software dovranno essere adeguatamente testati per garantire il corretto funzionamento e la compatibilità con l'ambiente operativo dell'infrastruttura.

2.3.1. Requisiti Preliminari per l'Installazione del Software

L'installazione di qualsiasi software necessario per l'esecuzione delle operazioni oggetto di questo capitolato è subordinata al completo e corretto allestimento dell'infrastruttura fisica, come specificato e messo a disposizione dalla stazione appaltante. Prima di procedere con l'installazione del software, l'operatore economico dovrà effettuare una verifica dell'idoneità dell'infrastruttura fisica e ricevere una conferma da parte della stazione appaltante che quest'ultima sia pronta per accogliere il software. La mancata conformità dell'infrastruttura fisica alle specifiche richieste dovrà essere segnalata tempestivamente e risolta prima dell'installazione del software.

2.3.2. Installazione e avvio operativo

Il software oggetto della presente procedura dovrà essere installato sulle apparecchiature hardware che saranno presenti all'interno dei locali indicati dalla Stazione Appaltante provvedendo alle opportune configurazioni e test per la verifica del corretto funzionamento. L'aggiudicatario dovrà garantire che il software prodotto sia esente da difetti e perfettamente funzionante.
Caratteristiche dell'installazione, configurazione e test dei software:

- **Aderenza alle Decisioni di Progettazione**
  L'operatore economico dovrà seguire le decisioni prese in fase di progettazione dalla Stazione Appaltante prevedendo delle attività atte alla verifica dell'aderenza dei software progettati rispetto alla configurazione prevista. Sarà garantita l'aderenza all'architettura di riferimento per ottimizzare la distribuzione e il funzionamento delle componenti.
- **Installazione e Configurazione dei Software**
  L'operatore economico dovrà installare e configurare tutti i software sviluppati e utilizzati sull'infrastruttura. La configurazione dovrà essere accurata per garantire un corretto funzionamento e una sicura interazione tra le diverse componenti.
- **Test di Funzionamento e Compatibilità**
  Dovranno essere condotti test approfonditi sui software sia a livello infrastrutturale che applicativo, per verificare il loro corretto funzionamento e la compatibilità con l'ambiente operativo della piattaforma cloud. I test dovranno essere svolti su diverse configurazioni e scenari per garantire la stabilità e l'affidabilità delle soluzioni. I test dovranno essere di diverse tipologie, tra cui:

    - **Test di Generazione di Eventi**
      Saranno creati eventi di prova che simuleranno attività tipiche svolte nell'ambito dell'infrastruttura, come accessi di utenti, esecuzione di servizi o avvio di processi.

Questi eventi di prova saranno inviati al sistema di logging e sarà verificato se essi saranno registrati correttamente nei log.

- **Test di Rilevazione delle Anomalie**
  Verranno creati eventi di prova che simuleranno attività malevole o anomalie, come tentativi di accesso non autorizzati o comportamenti sospetti. L'obiettivo sarà verificare se il sistema di logging sarà in grado di rilevare tali eventi e di generare avvisi o notifiche appropriate.
- **Test di Scalabilità**
  Viene eseguito un test di scalabilità per verificare la capacità del sistema di logging di gestire un carico di lavoro crescente senza compromettere le prestazioni e la qualità del tracciamento delle attività.
- **Test di Archiviazione e Gestione dei Log**
  Si verificano i meccanismi di archiviazione e gestione dei log, inclusi i tempi di conservazione e l'accessibilità delle informazioni per il personale autorizzato.
- **Test di Analisi dei Log**
  Si effettuano test per verificare la facilità di analisi dei log e la capacità di identificare eventi rilevanti o anomalie tramite gli strumenti di analisi e ricerca.
- **Test di Ripristino**
  Viene eseguito un test di ripristino per verificare la capacità di recuperare i log in caso di guasti o interruzioni.
- **Test di Allarme e Notifica**
  Si verifica la capacità del sistema di logging di generare avvisi e notifiche in tempo reale per segnalare eventi critici o situazioni anomale.
- **Test di Conformità agli Standard**
  Si verifica la conformità del sistema di logging agli standard e alle normative di sicurezza applicabili.

- L'operatore economico dovrà fornire un piano di test completo relativamente alle componenti degli applicativi software sviluppati (back-end, front-end). Il piano di test dovrà includere le seguenti fasi:

  - **Test di unità**
    I test di unità vengono eseguiti su ogni unità di codice individuale per verificare che funzioni correttamente. I test di unità dovrebbero concentrarsi sulla validità dei dati, sulla conformità ai requisiti e sul rispetto delle linee guida di sviluppo.
  - **Test di integrazione**
    I test di integrazione vengono eseguiti per verificare che le unità di codice funzionino correttamente insieme. I test di integrazione dovrebbero concentrarsi sull'interazione tra le diverse funzionalità della piattaforma cloud e del portale web. **Test di sistema**
    I test di sistema vengono eseguiti per verificare che il portale web funzioni come previsto nel suo insieme. I test di sistema dovrebbero concentrarsi sulle funzionalità principali del portale web.
  - **Test di accettazione**

I test di accettazione vengono eseguiti dalla Stazione Appaltante per verificare che il portale web soddisfi i requisiti. I test di accettazione dovrebbero concentrarsi sulla facilità d'uso, l'accessibilità e l'usabilità del portale web.

2.3.3. Allocazione di risorse umane per lo sviluppo, installazione e configurazione di software

L'accordo contrattuale tra l'operatore economico e la Stazione Appaltante includerà una specifica allocazione di risorse umane per soddisfare le ulteriori esigenze che potrebbero presentarsi durante le successive fasi del progetto. Pertanto, sarà necessario prevedere la possibilità di dedicare risorse umane per seguire specifiche tecniche più dettagliate fornite dalla Stazione Appaltante. L'accordo stabilirà che i pagamenti saranno correlati esclusivamente alle ore persona effettivamente utilizzate per l'esecuzione delle eventuali attività concordate.
Caratteristiche del requisito di allocazione di risorse:

- **Definizione dei Ruoli e Competenze**
  L'accordo contrattuale specificherà i ruoli e le competenze richieste per le risorse umane assegnate al progetto. Sarà necessario definire le responsabilità di ciascun ruolo e assicurarsi che le competenze del personale siano adeguate alle attività richieste.
- **Durata del Contratto**
  L'accordo specificherà la durata del contratto, che comprenderà il periodo di tempo in cui il personale sarà impegnato nello sviluppo, installazione e configurazione del software.
- **Flessibilità nell'Utilizzo delle Risorse**
  L'accordo prevedrà la possibilità di utilizzare le risorse in modo flessibile durante il progetto, consentendo ad esempio la concentrazione delle risorse in fasi critiche o l'allungamento dei tempi in caso di necessità.
- **Rendicontazione delle ore persona utilizzate**
  Le ore persona effettivamente utilizzate durante il progetto per soddisfare eventuali esigenze dovranno essere richieste dalla Stazione Appaltante a mezzo PEC.
- **Sospensione e Risoluzione del Bando e/o Contratto**
  La Stazione Appaltante si riserva la possibilità di sospendere e/o revocare il bando o il contratto oni ottemperanza alle norme di legge.

2.3.4. Formazione

L'aggiudicatario dovrà garantire un programma di addestramento all'uso dei software installati (sia infrastrutturali sia applicativi) di durata minima effettiva di almeno 3 giornate, fatta salva l'offerta migliorativa presentata in sede di gara: il programma dovrà essere tenuto preferibilmente on-site presso la sede di consegna ed installazione, da personale specializzato, secondo un calendario che dovrà essere concordato con la Stazione Appaltante. Detto programma dovrà essere avviato entro 30 (trenta) giorni solari dal superamento della verifica di conformità della strumentazione, salvo diverso accordo. Il corso e la documentazione di addestramento dovranno essere in lingua italiana e/o inglese.

2.3.5. Garanzia

La garanzia fornita dall'aggiudicatario dovrà coprire un periodo di almeno 12 (dodici) mesi dalla data dal superamento della verifica di conformità della strumentazione, fatta salva l'offerta

migliorativa presentata in sede di gara[Errore. Il segnalibro non è definito.]. Tale garanzia deve comprendere le riparazioni o sostituzioni di parti (con esclusione delle parti c.d. "consumabili" chiaramente individuabili nella documentazione a corredo) necessarie al funzionamento ottimale della strumentazione. Devono ritenersi, inoltre, comprese nella garanzia le spese di trasferta ed i costi della manodopera dei tecnici presso la sede di consegna ed installazione. Per l'intero periodo di vigenza della garanzia, l'aggiudicatario dovrà impegnarsi a fornire gratuitamente gli eventuali upgrade alle licenze software.

2.3.6. Assistenza tecnica, supporto e manutenzione

In caso di guasto l'aggiudicatario dovrà essere in grado di intervenire tempestivamente dalla segnalazione effettuata a mezzo PEC entro un massimo di 3 (tre) giorni lavorativi, fatta salva l'offerta migliorativa presentata in sede di gara[Errore. Il segnalibro non è definito.]. Tale intervento è finalizzato alla immediata assistenza ed al ripristino delle funzionalità dei software o, nel caso in cui ciò non sia possibile, alla valutazione delle criticità e degli interventi necessari.
L'assistenza tecnica, supporto e manutenzione fornita dall'aggiudicatario dovrà coprire un periodo di almeno 12 (dodici) mesi dalla data dal superamento della verifica di conformità della strumentazione, fatta salva l'offerta migliorativa presentata in sede di gara.

3. MODALITÀ DI ESECUZIONE DEL SERVIZIO

3.1. Luogo di svolgimento/consegna e installazione

I software dovranno essere installati e configurati presso la sede principale dell'Istituto ICAR del CNR sita in via Pietro Castellino 111, 80131, Napoli e presso le sedi secondarie dell'Istituto ICAR del CNR sita in Via Ugo La Malfa, 153, 90146, Palermo, dell'Istituto ISTC sita in Via Paolo Gaifami n. 18, 95126 Catania e dell'Istituto IRCRES del CNR sito in Str. delle Cacce, 73, 10135 Torino. Ove possibile sarà possibile procedere alle fasi di installazione e configurazione in remoto.

3.2. Termini di svolgimento/consegna e installazione

I servizi software richiesti dovranno essere installati e configurati entro 365 (trecento sessantacinque) giorni naturali e consecutivi decorrenti dalla data di stipula del contratto di appalto, ovvero dalla data di sottoscrizione del verbale di avvio anticipato dell'esecuzione del contratto e comunque non oltre la data del 31 gennaio 2025. Tale data potrà subire una proroga in accordo con eventuali proroghe de progetto stesso.

4. MODALITÀ DI ESECUZIONE DEL CONTRATTO

4.1. Avvio dell'esecuzione

Il Direttore dell'esecuzione del contratto (DEC) appositamente nominato, sulla base delle disposizioni del Responsabile Unico del Procedimento (RUP), darà avvio all'esecuzione del contratto, fornendo all'Aggiudicatario tutte le istruzioni e direttive necessarie e redigendo, laddove sia indispensabile in relazione alla natura e al luogo di esecuzione delle prestazioni, apposito verbale come meglio disciplinato all'art. 31, c.2, lett. c) dell'Allegato II.14 del D.Lgs. 36/2023. È ammesso l'avvio del contratto nelle more della verifica dei requisiti previsti dal disciplinare, ai sensi dell'art.8, c.1, lett.a) della L.120/2020.

4.2. Sospensione dell'esecuzione

In tutti i casi in cui ricorrano circostanze speciali che impediscano in via temporanea l'esecuzione dell'appalto si applicano le disposizioni di cui all'art. 121 del D. Lgs. 36/2023 e s.m.i. e all'art.8 dell'Allegato II.14 del D.Lgs. 36/2023.

4.3. Termine dell'esecuzione

Ai sensi dell'art.31, c.2, lett.n) dell'Allegato II.14 del D.Lgs. 36/2023, dopo la comunicazione dell'esecutore di intervenuta ultimazione delle prestazioni, il DEC effettua, entro cinque giorni, i necessari accertamenti in contraddittorio e nei successivi cinque giorni elabora il certificato di ultimazione delle prestazioni, da inviare al RUP, che ne rilascia copia conforme all'esecutore.

5. PENALI

Per ogni giorno naturale e consecutivo di ritardo rispetto ai termini previsti per l'esecuzione dell'appalto di cui all'art.8, si applicherà una penale pari all'1‰ (uno per mille) dell'importo contrattuale, al netto dell'IVA e dell'eventuale costo relativo alla sicurezza sui luoghi di lavoro derivante dai rischi di natura interferenziale.
Ai sensi dell'art.47, comma 6 del DL77/2021, convertito in L.108/2021, verrà applicata una penale calcolata in misura giornaliera pari all'1 ‰ (uno per mille) dell'ammontare netto contrattuale complessivo in caso di ritardo nella consegna della certificazione e della relazione che chiarisca l'avvenuto assolvimento degli obblighi previsti a carico delle imprese dalla Legge 12 marzo 1999, n. 68 rispetto alla scadenza dei sei mesi dalla conclusione del Contratto (per gli operatori tenuti a tale adempimento).
La violazione dell'obbligo di cui al comma 3 dell'art.47 L.108/2021, determina, altresì, l'impossibilità per l'operatore economico di partecipare, in forma singola ovvero in raggruppamento temporaneo, per un periodo di dodici mesi ad ulteriori procedure di affidamento afferenti agli investimenti pubblici finanziati, in tutto o in parte, con le risorse previste dal Regolamento (UE) 2021/240 del Parlamento europeo e del Consiglio del 10 febbraio 2021 e dal Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, nonché dal PNC.
Nell'ipotesi in cui l'importo delle penali applicabili superi l'importo pari al 20% (venti per cento) dell'importo contrattuale, al netto dell'IVA e dell'eventuale costo relativo alla sicurezza sui luoghi di lavoro derivante dai rischi di natura interferenziale, l'Ente risolverà il contratto in danno all'Aggiudicatario, salvo il diritto al risarcimento dell'eventuale ulteriore danno patito.
Gli eventuali inadempimenti contrattuali che daranno luogo all'applicazione delle penali sopra elencate saranno contestati al Fornitore per iscritto. Il Fornitore dovrà comunicare, in ogni caso, per iscritto, le proprie deduzioni, supportate da una chiara ed esauriente documentazione, nel termine massimo di 5 (cinque) giorni lavorativi dalla ricezione della contestazione stessa. Qualora le predette deduzioni non pervengano al Direttore dell'Esecuzione nel termine indicato, ovvero, pur essendo pervenute tempestivamente, non siano idonee, a giudizio del CNR, a giustificare l'inadempienza, saranno applicate al Fornitore le penali a decorrere dall'inizio dell'inadempimento.
La richiesta e/o il pagamento delle penali non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.
Ferma restando l'applicazione delle penali previste nei precedenti comma, il Committente si riserva di richiedere il maggior danno, sulla base di quanto disposto all'articolo 1382 cod. civ., nonché la risoluzione del presente Contratto nell'ipotesi di grave e reiterato inadempimento.

Fatto salvo quanto previsto ai precedenti comma, l'Impresa si impegna espressamente a rifondere al Committente l'ammontare di eventuali oneri che il CNR dovesse applicare, anche per cause diverse da quelle di cui al presente articolo, a seguito di fatti che siano ascrivibili a responsabilità della Impresa stessa.
Il Committente, per i crediti derivanti dall'applicazione delle penali di cui al presente articolo, potrà, a sua insindacabile scelta, avvalersi della cauzione definitiva senza bisogno di diffida o procedimento giudiziario, ovvero compensare il credito con quanto dovuto all'Impresa a qualsiasi titolo, quindi anche per i corrispettivi maturati; in questo caso il Fornitore dovrà emettere una nota di credito pari all'importo della penale o decrementare la fattura del mese in corso di un valore pari all'importo della penale stessa.

6. MODALITÀ DI RESA

Per operatori economici appartenenti a Stati membri dell'Unione europea, si applica la regola Incoterms 2020 - DPU (Delivered At Place Unloaded) presso il luogo di destinazione (sede di consegna) indicato al paragrafo § 3.1 del presente Capitolato tecnico.
Per operatori economici non appartenenti a Stati membri dell'Unione europea, si applica la regola Incoterms 2020 - DDP (Delivered Duty Paid) presso il luogo di destinazione (sede di consegna) indicato al paragrafo § 3.1 del presente Capitolato tecnico.
In aggiunta l'operatore economico è tenuto a provvedere allo scarico della merce nel luogo di destinazione, a sua cura e spesa.
Tutti gli operatori economici sono obbligati, incluso nel prezzo contrattuale d'appalto:

- A stipulare un contratto di assicurazione per la parte di trasporto sotto la loro responsabilità;
- All'installazione della fornitura ed ai servizi addizionali indicati nel presente Capitolato tecnico.

7. ONERI ED OBBLIGHI DELL'AGGIUDICATARIO

L'Aggiudicatario:
Si impegna ad eseguire le prestazioni oggetto dell'appalto, senza alcun onere aggiuntivo, salvaguardando le esigenze della Stazione Appaltante e di terzi autorizzati, senza recare intralci, disturbi o interruzioni all'attività lavorativa in atto.
Rinuncia a qualsiasi pretesa o richiesta di compenso nel caso in cui lo svolgimento delle prestazioni dovesse essere ostacolato o reso più oneroso dalle attività svolte dalla Stazione Appaltante e/o da terzi.
È direttamente responsabile dell'inosservanza delle clausole che saranno contenute nel contratto anche se queste dovessero derivare dall'attività del personale dipendente di altre imprese a diverso titolo coinvolto.
Deve avvalersi di personale qualificato in regola con gli obblighi previsti dai contratti collettivi di lavoro e da tutte le normative vigenti, in particolare in materia previdenziale, fiscale, di igiene ed in materia di sicurezza sul lavoro.
Risponderà direttamente dei danni alle persone, alle cose o all'ambiente comunque provocati nell'esecuzione dell'appalto che possano derivare da fatto proprio, dal personale o da chiunque chiamato a collaborare. La Stazione Appaltante è esonerata da ogni responsabilità per danni, infortuni o qualsiasi altra cosa accadesse al personale di cui si avvarrà l'Aggiudicatario nell'esecuzione delle prestazioni relative all'appalto.

Si fa carico, intendendosi remunerati con il corrispettivo contrattuale, di tutti gli oneri ed i rischi relativi alle attività ed agli adempimenti occorrenti all'integrale espletamento dell'oggetto contrattuale, ivi compresi, a mero titolo esemplificativo e non esaustivo, gli oneri relativi alle spese di trasporto, di viaggio e di missione per il personale addetto alla esecuzione della prestazione, nonché i connessi oneri assicurativi.

Si impegna ad eseguire le prestazioni oggetto dell'appalto a perfetta regola d'arte e nel rispetto di tutte le norme e le prescrizioni tecniche e di sicurezza in vigore e di quelle che dovessero essere emanate nel corso della procedura di gara e fino alla sua completa conclusione, nonché secondo le condizioni, le modalità, i termini e le prescrizioni contenute negli atti di gara e relativi allegati;
Si impegna a consegnare gli elaborati progettuali e tutte le dichiarazioni e/o certificazioni discendenti da specifici obblighi normativi e legislativi correlati con l'oggetto della prestazione.

8. SICUREZZA SUL LAVORO

L'Aggiudicatario si assume la responsabilità per gli infortuni del personale addetto, che dovrà essere opportunamente addestrato ed istruito.
La valutazione dei rischi propri dell'Aggiudicatario nello svolgimento della propria attività professionale resta a carico dello stesso, così come la redazione dei relativi documenti e la informazione/formazione dei propri dipendenti.
L'Aggiudicatario è tenuto a garantire il rispetto di tutte le normative riguardanti l'igiene e la sicurezza sul lavoro con particolare riferimento alle attività che si espleteranno presso l'Ente.
In relazione alle risorse umane impegnate nelle attività oggetto del presente contratto, l'Aggiudicatario è tenuto a far fronte ad ogni obbligo previsto dalla normativa vigente in ordine agli adempimenti fiscali, tributari, previdenziali ed assicurativi riferibili al personale dipendente ed ai collaboratori.
Per quanto riguarda i lavoratori dipendenti, l'Aggiudicatario è tenuto ad osservare gli obblighi retributivi e previdenziali previsti dai corrispondenti CCNL di categoria, compresi, se esistenti alla stipulazione del contratto, gli eventuali accordi integrativi territoriali.
Gli obblighi di cui al comma precedente vincolano l'Aggiudicatario anche qualora lo stesso non sia aderente alle associazioni stipulanti gli accordi o receda da esse, indipendentemente dalla struttura o dimensione del medesimo e da ogni altra qualificazione giuridica, economica o sindacale.

9. DIVIETO DI CESSIONE DEL CONTRATTO

È vietata la cessione del contratto ai sensi dell'art. 119, comma 1 del D. Lgs. 36/2023 e ss.mm.ii.
Per quanto riguarda le ristrutturazioni societarie, che comportino successione nei rapporti pendenti riguardanti l'Aggiudicatario, si applicano le disposizioni di cui all'art. 120, c.1 lett. d) del D. Lgs. 36/2023 e ss.mm.ii.
L'Aggiudicatario è tenuto a comunicare tempestivamente alla Stazione Appaltante ogni modificazione intervenuta negli assetti proprietari e nella struttura organizzativa.

10.VERIFICA DI CONFORMITÀ DI SERVIZI/FORNITURE

Il servizio sarà oggetto di verifica di conformità da svolgersi conformemente a quanto previsto nell'art. 36 dell'Allegato II.14 del D. Lgs. 36/2023 e ss.mm.ii., al fine di accertarne la regolare esecuzione, rispetto alle condizioni e ai termini stabiliti nel contratto, alle eventuali leggi di settore e

alle disposizioni del codice. Le attività di verifica hanno, altresì, lo scopo di accertare che i dati risultanti dalla contabilità e dai documenti giustificativi corrispondano fra loro e con le risultanze di fatto, fermi restando gli eventuali accertamenti tecnici previsti dalle leggi di settore.
La verifica di conformità è avviata entro trenta giorni dall'ultimazione della prestazione, salvo un diverso termine esplicitamente previsto dal contratto ed è conclusa entro il termine stabilito dal contratto e comunque non oltre sessanta giorni dall'ultimazione della prestazione. È effettuata direttamente dal RUP o dal direttore dell'esecuzione del contratto. È effettuata da un soggetto ovvero da una commissione composta da due o tre soggetti, in possesso della competenza tecnica necessaria in relazione al tipo di fornitura o servizio da verificare.
Durante le suddette operazioni, la Stazione Appaltante ha altresì la facoltà di chiedere all'Aggiudicatario tutte quelle prove atte a definire il rispetto delle specifiche tecniche e strumentali dichiarate.
L'esito positivo della verifica non esonera l'Aggiudicatario dal rispondere di eventuali difetti non emersi nell'ambito delle attività di verifica di conformità e successivamente riscontrati; tali difetti dovranno essere prontamente eliminati durante il periodo di garanzia.
Il certificato di verifica di conformità è sempre trasmesso dal soggetto che lo rilascia al RUP. Il RUP, ricevuto il certificato di verifica di conformità definitivo, lo trasmette all'esecutore, il quale lo sottoscrive nel termine di quindici giorni dalla sua ricezione, ferma restando la possibilità, in sede di sottoscrizione, di formulare eventuali contestazioni in ordine alle operazioni di verifica di conformità. Il RUP comunica al soggetto incaricato della verifica le eventuali contestazioni fatte dall'esecutore al certificato di conformità. Il soggetto incaricato della verifica di conformità riferisce, con apposita relazione riservata, sulle contestazioni fatte dall'esecutore e propone le soluzioni ritenute più idonee, ovvero conferma le conclusioni del certificato di verifica di conformità emesso.

11.FATTURAZIONE E PAGAMENTO

Ai fini del pagamento del corrispettivo contrattuale il Fornitore, se stabilito e/o identificato ai fini IVA in Italia, dovrà emettere fattura elettronica ai sensi e per gli effetti del Decreto del Ministero dell'Economia e delle Finanze N. 55 del 3 aprile 2013, inviando il documento elettronico al Sistema di Interscambio che si occuperà di recapitare il documento ricevuto alla Stazione appaltante. Il Consiglio Nazionale delle Ricerche è soggetto all'applicazione del meccanismo dello "Split Payment". In caso di Fornitore straniero la fattura dovrà essere in formato cartaceo.
È prevista un'anticipazione sul prezzo contrattuale pari al venti (20%) da corrispondere all'aggiudicatario, previa emissione di fattura, entro quindici giorni dall'effettivo inizio della prestazione, sul conto corrente dedicato di cui alla tracciabilità dei flussi finanziari. L'erogazione dell'anticipazione è subordinata alla costituzione di garanzia fideiussoria bancaria o assicurativa di importo pari all'anticipazione maggiorato del tasso di interesse legale applicato al periodo necessario al recupero dell'anticipazione stessa secondo il cronoprogramma della prestazione, rilasciata da imprese bancarie autorizzate ai sensi del decreto legislativo 1° settembre 1993, n. 385, o assicurative autorizzate alla copertura dei rischi ai quali si riferisce l'assicurazione e che rispondano ai requisiti di solvibilità previsti dalle leggi che ne disciplinano la rispettiva attività. La garanzia può essere, altresì, rilasciata dagli intermediari finanziari iscritti nell'albo degli intermediari finanziari di cui all'articolo 106 del decreto legislativo 1° settembre 1993, n. 385. L'importo della garanzia è gradualmente e automaticamente ridotto nel corso della prestazione, in rapporto al progressivo recupero dell'anticipazione da parte delle stazioni appaltanti. Il beneficiario decade dall'anticipazione, con obbligo di restituzione, se l'esecuzione della prestazione non procede, per ritardi a lui imputabili,

secondo i tempi contrattuali. Sulle somme restituite sono dovuti gli interessi legali con decorrenza dalla data di erogazione della anticipazione.

Secondo quanto disposto dall'art.37, c.6 dell'Allegato II.14 al D. Lgs. 36/2023, il pagamento della rata di saldo e lo svincolo della cauzione definitiva, di cui all'articolo 117 del codice, saranno effettuati a seguito dell'emissione del certificato di verifica di conformità definitivo, e dopo la risoluzione delle eventuali contestazioni sollevate dall'esecutore.
I prezzi si intendono fissi ed invariabili per l'intera durata contrattuale.
Le fatture dovranno contenere i seguenti dati:

- Intestazione: Istituto di Calcolo e Reti ad Alte Prestazioni - ICAR - UOS Napoli Via Pietro Castellino 111 - 80131 Napoli, NA, Campania, Dott.ssa Ivana Marra;
- Il Codice Fiscale 80054330586;
- La Partita IVA 02118311006 (solo per Aggiudicatari stranieri)
- Il riferimento al contratto (N° di protocollo e data);
- Il CIG A03B49C208;
- Il CUP B83C22003950001;
- Il CUU (Codice Univoco Ufficio) dell'Ente: 018.001 MCHOZ6 0I-J8W (solo per i soggetti stabiliti e/o identificati ai fini IVA in Italia);
- L'importo imponibile; (solo per i soggetti stabiliti e/o identificati ai fini IVA in Italia)
- L'importo dell'IVA (solo per i soggetti stabiliti e/o identificati ai fini IVA in Italia);
- Esigibilità IVA "S" scissione dei pagamenti (solo per i soggetti stabiliti e/o identificati ai fini IVA in Italia);
- L'importo totale;
- L'intestazione del contratto;
- Il codice IBAN del conto corrente dedicato;
- Il "Commodity code" (solo per Aggiudicatari stranieri).

Ai fini del pagamento del corrispettivo la Stazione Appaltante procederà alle verifiche di legge.
In caso di inadempienza risultante dal documento unico di regolarità contributiva relativo a personale dipendente dell'affidatario o del subappaltatore o dei soggetti titolari di subappalti e cottimi, impiegato nell'esecuzione del contratto, il CNR tratterrà l'importo corrispondente all'inadempienza per il successivo versamento diretto agli enti previdenziali e assicurativi, ai sensi dell'articolo 11, comma 6 del D. Lgs. n. 36/2023.

In attuazione dell'articolo 48-bis del DPR n. 602/1973 e ss.mm.ii., recante disposizioni in materia di pagamenti da parte delle Pubbliche Amministrazioni, i pagamenti di importo superiore ad € 5.000,00 saranno effettuati previa verifica presso Agenzia delle Entrate–Riscossione del regolare pagamento delle cartelle esattoriali eventualmente notificate all'Impresa.

Nell'ipotesi di raggruppamenti temporanei di imprese o di consorzi, la liquidazione del corrispettivo avverrà esclusivamente a favore della mandataria o designata quale capogruppo o del consorzio stesso.

In sede di liquidazione delle fatture potranno essere recuperate le spese per l'applicazione di eventuali penalità (di cui al paragrafo § 5); la Stazione Appaltante potrà sospendere, ferma restando l'applicazione delle eventuali penali, i pagamenti all'Aggiudicatario cui sono state contestate

inadempienze nell'esecuzione della fornitura, fino al completo adempimento degli obblighi contrattuali.

12.TRACCIABILITÀ DEI FLUSSI FINANZIARI

L'Aggiudicatario assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3 della legge 13
agosto 2010 n. 136 e successive modificazioni ed integrazioni.
Il mancato utilizzo del bonifico bancario o postale ovvero degli altri strumenti di incasso o pagamento idonei a consentire la piena tracciabilità delle operazioni costituisce causa di risoluzione del contratto ai
sensi dell'art. 3, comma 9-bis, della legge 13 agosto 2010 n.136.
L'Aggiudicatario si impegna a dare immediata comunicazione alla Stazione Appaltante ed alla prefettura
ufficio territoriale del Governo della provincia di Roma della notizia dell'inadempimento della propria
controparte (subappaltatore/subcontraente) agli obblighi di tracciabilità finanziaria.

13.RISOLUZIONE DEL CONTRATTO

In adempimento a quanto previsto dall'art. 122 del D. Lgs. 36/2023 e s.m.i. la Stazione Appaltante risolverà
il contratto nei casi e con le modalità ivi previste.
Per quanto non previsto nel presente paragrafo, si applicano le disposizioni di cui al Codice civile in materia
di inadempimento e risoluzione del contratto.
In ogni caso si conviene che la Stazione Appaltante, senza bisogno di assegnare previamente alcun termine
per l'adempimento, potrà risolvere di diritto il contratto ai sensi dell'art. 1456 c.c., previa dichiarazione da
comunicarsi all'Aggiudicatario tramite posta elettronica certificata nei seguenti casi:

- mancata reintegrazione della cauzione eventualmente escussa entro il termine di 10 (dieci) giorni lavorativi dal ricevimento della relativa richiesta da parte della Stazione Appaltante;
- nel caso in cui l'UTG competente rilasci la comunicazione/informazione antimafia interdittiva;
- nei casi di cui ai precedenti paragrafi relativi a:
  - Penalità;
  - Oneri ed obblighi dell'Aggiudicatario;
  - Sicurezza sul lavoro;
  - Divieto di cessione del contratto.