

CLUB ALPINO ITALIANO



MATTEO
CANALI
21.10.2026
16:42:12
GMT+02:00

CAPITOLATO TECNICO

PROCEDURA APERTA PER L’AFFIDAMENTO DI SERVIZI PER LA MANUTENZIONE E GESTIONE DELLA PIATTAFORMA DEL CLUB ALPINO ITALIANO DI PRENOTAZIONE ONLINE DEI RIFUGI

*Portale “Prenota Rifugi CAI”
www.prenotarifugi.cai.it*

C.I.G. BD75BDB0BB
Durata prevista: 36 mesi

Sommario

Premessa e finalità

Art. 1 - Oggetto e perimetro dell'appalto

Art. 2 - Definizioni e principi di esecuzione

Art. 3 - Descrizione funzionale e tecnica del sistema attuale

Art. 4 - Presa in carico, trasferimento e avvio del servizio

Art. 5 - Servizi di hosting e gestione infrastrutturale

Art. 6 - Manutenzione correttiva, adeguativa, preventiva ed evolutiva

Art. 7 - Gestione operativa del marketplace e dei pagamenti

Art. 8 - Assistenza, help desk e supporto agli utenti

Art. 9 - Sicurezza, privacy, continuità operativa e conformità

Art. 10 - Livelli di servizio (SLA)

Art. 11 - Monitoraggio, reportistica e governance

Art. 12 - Proprietà, diritti sul software, dati e sviluppi

Art. 13 - Obblighi di documentazione, repository e reversibilità

Art. 14 - Team di lavoro e modalità operative

Art. 15 - Verifica di conformità, penali e rimedi

Art. 16 - Durata, cronoprogramma e consegne

Art. 17 - Contenuti minimi dell'offerta tecnica

Allegato A - Matrice degli SLA

Allegato B - Inventario tecnico di presa in carico

Allegato C - Deliverable e report periodici

Allegato D - Clausole tecniche su proprietà e riuso

Premessa e finalità

Il presente Capitolato disciplina i servizi necessari ad assicurare continuità, sicurezza, manutenzione, gestione ed evoluzione della piattaforma web “Prenota Rifugi CAI”, già operativa e accessibile al pubblico. L’affidamento non riguarda la realizzazione ex novo del portale, ma la presa in carico e la gestione di un sistema esistente, comprensiva del trasferimento su infrastruttura messa a disposizione dall’aggiudicatario, senza soluzione di continuità per utenti, rifugisti e strutture aderenti.

La piattaforma supporta la ricerca delle strutture, la verifica delle disponibilità, la prenotazione online, la consultazione di cammini e percorsi, l’accesso all’area riservata e i servizi di assistenza. Il portale presenta strutture ricettive diverse, comprese strutture lungo percorsi escursionistici, e permette di individuare quelle aperte e prenotabili. La descrizione è funzionale all’appalto e non sostituisce l’inventario tecnico che dovrà essere consegnato in fase di subentro.

Finalità principali dell’affidamento:

- garantire disponibilità, integrità, riservatezza e prestazioni adeguate del servizio;
- assicurare la manutenzione dell’intero stack applicativo e infrastrutturale;
- gestire il ciclo operativo delle prenotazioni e, ove previsto dagli atti di gara, le attività del marketplace e dei pagamenti;
- evitare dipendenze dal fornitore e assicurare piena portabilità tecnica e dei dati;
- consentire al CAI di disporre degli sviluppi e delle personalizzazioni realizzati nel periodo contrattuale;
- garantire un passaggio ordinato a CAI o a un successivo affidatario al termine del contratto
- permettere a CAI la verifica periodica delle attività e delle prestazioni.

Art. 1 - Oggetto e perimetro dell'appalto

L'appalto ha per oggetto l'erogazione integrata dei servizi di presa in carico, migrazione, hosting, conduzione, manutenzione, assistenza e supporto operativo della piattaforma "Prenota Rifugi CAI", per tutta la durata contrattuale:

- trasferimento completo della piattaforma, sull'infrastruttura messa a disposizione dall'aggiudicatario;
- configurazione degli ambienti di produzione, collaudo/pre-produzione, sviluppo e disaster recovery, ove previsto;
- gestione sistemistica, applicativa, database, domini, certificati, componenti middleware e servizi collegati;
- manutenzione correttiva, preventiva, adeguativa ed evolutiva;
- monitoraggio tecnico e applicativo continuativo;
- help desk e supporto a CAI, rifugisti/gestori e utenti finali secondo i livelli indicati;
- gestione delle integrazioni e delle interfacce con sistemi CAI, servizi di pagamento, posta elettronica, cartografia, analytics e servizi terzi effettivamente presenti;
- gestione operativa delle prenotazioni, delle transazioni e degli adempimenti espressamente previsti dal contratto;
- formazione e aggiornamento della documentazione;
- reversibilità e trasferimento finale senza vendor lock-in.

Il corrispettivo si intende onnicomprensivo di personale, infrastruttura, traffico, backup, monitoraggio, licenze, certificati, ambienti, strumenti, assistenza e ogni attività necessaria al rispetto degli SLA, salvo le sole voci espressamente escluse negli atti di gara.

L'aggiudicatario dovrà impegnarsi a:

- garantire che la piattaforma sia conforme a quanto prescritto dalle norme AgID sull'accessibilità dei siti della Pubblica Amministrazione (rif. Linee Guida sull'Accessibilità degli strumenti informatici

<https://www.agid.gov.it/it/design-servizi/accessibilità>);

- rispettare i requisiti di accessibilità definiti dalla legge n. 4 del 9 gennaio 2004 e ss.mm.ii.;

- rispettare quanto previsto nel D.Lgs.82/2005 (CAD);

- garantire che il trattamento dei dati inseriti nella piattaforma sia improntato ai principi del GDPR e, pertanto, che i dati siano raccolti e trattati esclusivamente per le finalità connesse alla presente procedura.

L'aggiudicatario ha l'obbligo di mantenere riservati i dati e le informazioni di cui venga in possesso e a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione delle prestazioni oggetto del contratto.

Art. 2 - Definizioni e principi di esecuzione

Ai fini del presente Capitolato si applicano le seguenti definizioni.

Termine	Definizione
CAI / Stazione appaltante	Club Alpino Italiano, titolare del servizio e dei dati.
Piattaforma	Insieme di portale pubblico, area riservata, back office, booking engine, marketplace, database, integrazioni, configurazioni e componenti necessari al servizio.
Aggiudicatario	Operatore economico responsabile dell'esecuzione dei servizi.
Incidente	Evento che determina o può determinare degrado, indisponibilità, perdita di dati o compromissione della sicurezza.
Richiesta di servizio	Richiesta non riconducibile a malfunzionamento, inclusi supporto, configurazione e informazione.
RTO	Tempo massimo obiettivo per il ripristino del servizio a seguito di evento grave.
RPO	Massima perdita di dati temporalmente ammissibile rispetto all'ultimo punto di ripristino.
Manutenzione evolutiva	Interventi che introducono o modificano funzionalità, integrazioni o flussi applicativi.

L'esecuzione deve rispettare i principi di continuità del servizio, sicurezza by design e by default, tracciabilità, interoperabilità, accessibilità, documentazione, portabilità, separazione degli ambienti.

Art. 3 - Descrizione funzionale e tecnica del sistema attuale

La piattaforma è attualmente un servizio web pubblico responsive con area riservata e funzionalità di ricerca e prenotazione. In base alle fonti istruttorie disponibili, l'architettura esistente comprende componenti web/CMS, un gestionale applicativo per strutture e prenotazioni, database relazionale, servizi di invio e-mail, integrazioni applicative e componenti di marketplace. La composizione definitiva dovrà essere accertata nel periodo di presa in carico mediante inventario congiunto.

3.1 Moduli funzionali da mantenere

- home page, contenuti informativi, news e pagine editoriali;
- ricerca delle strutture per località, regione, date, ospiti, caratteristiche e stato di apertura;
- mappa e schede delle strutture con servizi, disponibilità, immagini, condizioni e informazioni utili;
- cammini, percorsi e itinerari a più tappe;
- booking engine e carrello, inclusa la prenotazione di più strutture quando prevista;
- registrazione, autenticazione, area personale e gestione delle prenotazioni;
- back office dei rifugisti/gestori per disponibilità, listini, camere/posti letto, prenotazioni e contenuti;
- back office CAI/amministrativo per configurazione, controllo, reporting e gestione delle strutture;
- notifiche e-mail e comunicazioni automatiche;
- processi di caparra, pagamento, rimborso, ripartizione e rendicontazione nei limiti previsti dagli atti contrattuali;
- FAQ, contatti e gestione delle richieste di assistenza;
- strumenti di analisi, log applicativi e audit trail.

3.2 Architettura tecnica

Ambito	Elementi minimi da censire
Front end e CMS	Tecnologie, temi, componenti, plugin, lingue, accessibilità, dipendenze.
Applicazione booking	Framework, moduli, API, codebase, scheduler, processi asincroni.
Dati	DBMS, schema, volumi, cifratura, retention, procedure di export/import.
Infrastruttura	Server/VM/container, OS, web server, storage, rete, firewall, bilanciamento, CDN.
Integrazioni	SSO CAI, servizi anagrafici, gateway pagamento, e-mail, mappe, analytics, sistemi esterni tramite API.
DevOps	Repository, branching, build, test, CI/CD, gestione rilasci.
Sicurezza	IAM, ruoli, logging, vulnerabilità, hardening, backup, audit.
Licenze	Open source, commerciali, SaaS, certificati e relative scadenze.

3.3 Architettura applicativa attuale

La configurazione descritta nel presente articolo rappresenta lo stato attuale della piattaforma e costituisce la baseline tecnica per la presa in carico. L'aggiudicatario dovrà mantenerne tutte le funzioni durante la migrazione; eventuali soluzioni equivalenti o migliorative dovranno essere motivate, documentate e preventivamente approvate dal CAI.

3.3.1 Utenti e punti di accesso

- Escursionisti: consultano rifugi e itinerari, verificano le disponibilità, prenotano posti letto ed effettuano pagamenti online.
- Gestori e amministratori CAI: accedono al backoffice per gestire strutture, disponibilità, listini, prenotazioni, pagamenti e payout.

3.3.2 Schema applicativo

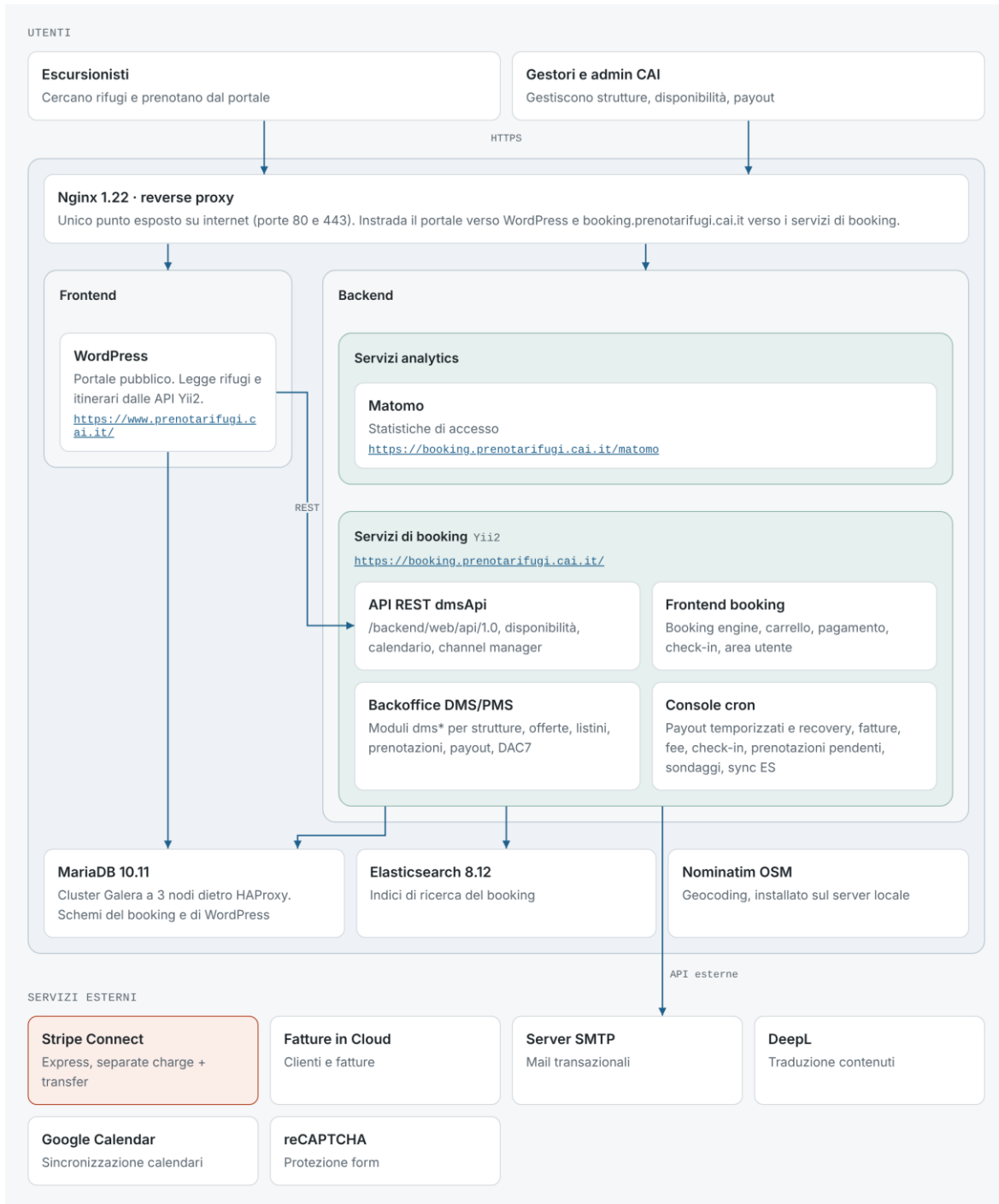


Figura 1 - Componenti applicativi e comunicazioni della piattaforma attuale.

3.3.3 Componenti applicativi

Componente	Configurazione e funzione
Reverse proxy	Nginx 1.22, unico componente esposto su internet alle porte 80 e 443; termina HTTPS e instrada il portale WordPress, i servizi di booking e Matomo.
Portale pubblico	WordPress con PHP 8.2 e Nginx 1.22. Presenta rifugi, itinerari e contenuti; legge i dati di rifugi e disponibilità tramite API REST e usa Nominatim per la ricerca geografica.
Backend booking	Applicazione PHP 8.2 basata su Yii2, articolata in API REST, frontend booking, backoffice DMS/PMS e processi pianificati.
Frontend booking	Ricerca disponibilità, carrello, pagamento, check-in online e area riservata dell'utente.
Backoffice DMS/PMS	Gestione strutture, offerte, listini, prenotazioni, payout e statistiche per gestori e amministratori.
Analytics	Matomo 5.10 per la raccolta delle statistiche di accesso.
Database	MariaDB 10.11 in cluster Galera a tre nodi, raggiunto tramite HAProxy 2.6; booking e WordPress usano schemi separati.
Ricerca	Elasticsearch 8.12 per indicizzazione e ricerca dei contenuti booking.
Geocoding	Nominatim con PostgreSQL 16, installato su server della piattaforma e usato dal portale per la ricerca per località.
Monitoraggio	Zabbix 6.0, tramite proxy dedicato.

3.3.4 Servizi esterni integrati

Servizio	Utilizzo
Stripe Connect	Incasso dei pagamenti con account Express dei rifugi, modello separate charge + transfer, rimborsi, contestazioni e payout.
Fatture in Cloud	Creazione dei clienti ed emissione delle fatture.
Server SMTP	Invio delle email transazionali: conferme, notifiche, sondaggi.
DeepL	Traduzione automatica dei contenuti multilingua.
Google Calendar	Sincronizzazione dei calendari di disponibilità.
Google reCAPTCHA	Protezione dei form pubblici dallo spam.

3.3.5 Comunicazioni tra componenti

Da	Verso	Descrizione
Utenti	Reverse proxy	Richieste HTTPS al portale e al booking.
Reverse proxy	WordPress	Pagine del portale pubblico.
Reverse proxy	Backend	Booking engine, backoffice, API e Matomo.
WordPress	API REST	Lettura di rifugi, itinerari e disponibilità.
WordPress	Nominatim	Ricerca geografica per località.
WordPress	MariaDB	Contenuti del portale.
Servizi di booking	MariaDB	Dati applicativi.
Servizi di booking	Elasticsearch	Indicizzazione e ricerca.
Servizi di booking	Servizi esterni	Pagamenti, fatture, email, traduzioni, calendari, reCAPTCHA.

3.3.6 Processi pianificati

L'aggiudicatario dovrà censire, migrare, testare e monitorare almeno i seguenti processi schedulati, preservandone frequenze, dipendenze e tracciabilità:

Frequenza	Processo
Ogni minuto	Eliminazione degli ordini rimasti in sospeso senza pagamento.
Ogni giorno alle 02:00	Importazione dell'anagrafica dei rifugi.
Ogni giorno alle 03:00	Calcolo delle fee della piattaforma.
Ogni giorno alle 03:30	Sincronizzazione dei calendari con Google Calendar.
Ogni giorno alle 11:00	Invio del sondaggio di soddisfazione per gli ordini recenti.
Ogni giorno alle 23:00	Invio delle schedine degli ospiti.
Ogni domenica alle 04:00	Importazione dei sentieri.

Ogni lunedì alle 04:00	Importazione dei cammini.
Primo lunedì del mese alle 08:00	Emissione delle fatture.

Art. 4 - Presa in carico, trasferimento e avvio del servizio

L'aggiudicatario dovrà trasferire la piattaforma su una propria infrastruttura, ubicata nello Spazio Economico Europeo, assicurando piena continuità, sicurezza e reversibilità. Il trasferimento è incluso nel corrispettivo e deve comprendere tutti gli elementi necessari al funzionamento autonomo del servizio.

1. Kick-off e definizione del piano di subentro entro 5 giorni lavorativi dall'avvio.
2. Acquisizione e verifica di sorgenti, dump dati, file, configurazioni, segreti, certificati, licenze, DNS, log e documentazione.
3. Predisposizione degli ambienti e installazione della piattaforma.
4. Migrazione dei dati con controlli di completezza, consistenza e riconciliazione.
5. Test funzionali, prestazionali, di sicurezza, backup e ripristino.
6. Esecuzione di almeno una prova generale di migrazione e di rollback.
7. Passaggio in produzione in finestra concordata, con presidio rafforzato.
8. Periodo di stabilizzazione di massimo 20 giorni lavorativi e chiusura delle anomalie di subentro.

Il piano deve indicare responsabilità, dipendenze, finestre di fermo, criteri di successo, rollback, comunicazioni agli utenti e rischi. L'eventuale indisponibilità pianificata per il cut-over non potrà superare le 8 ore e dovrà essere autorizzata dal CAI in una fascia oraria con minor carico del sistema.

L'avvio a regime è subordinato al verbale di esito positivo della presa in carico. I dati dell'ambiente di origine non potranno essere cancellati prima dell'autorizzazione scritta del CAI e dell'esito positivo della verifica di ripristino.

Art. 5 - Servizi di hosting e gestione infrastrutturale

L'aggiudicatario fornisce e gestisce l'infrastruttura necessaria a sostenere i carichi ordinari e i picchi stagionali, con possibilità di crescita senza modifiche sostanziali all'applicazione. L'architettura proposta deve evitare single point of failure incompatibili con gli SLA.

- ambienti separati di produzione e collaudo;
- dimensionamento, capacity planning e scalabilità;
- sistemi operativi e middleware supportati e aggiornati;
- certificati TLS, DNS, firewall/WAF ove opportuno, protezione da attacchi volumetrici secondo l'architettura proposta;
- monitoraggio 24x7 di disponibilità, prestazioni, risorse, code, errori applicativi e scadenze;
- backup cifrati, segregati e verificati;
- gestione centralizzata dei log, alert e audit trail;
- gestione delle credenziali con principio del minimo privilegio e autenticazione forte per gli amministratori;
- supporto alla gestione dei domini e sottodomini del CAI, che restano intestati al CAI;
- piano di continuità e disaster recovery testato almeno annualmente.

I servizi cloud e le risorse essenziali devono essere intestati al CAI oppure configurati in modo da poter essere trasferiti senza oneri o impedimenti tecnici. Sono vietate dipendenze non dichiarate da account personali o da licenze non cedibili che compromettano la continuità.

5.1 Infrastruttura attualmente in esercizio

La piattaforma è attualmente ospitata presso un provider europeo su due server fisici dedicati collocati in datacenter distinti dislocati in aree geograficamente distinte su territorio UE, più un server virtuale di quorum. I server fisici costituiscono un cluster Proxmox VE e ospitano le macchine virtuali dei servizi. Tale configurazione è riportata a fini di consistenza iniziale e per consentire il dimensionamento della soluzione di subentro.

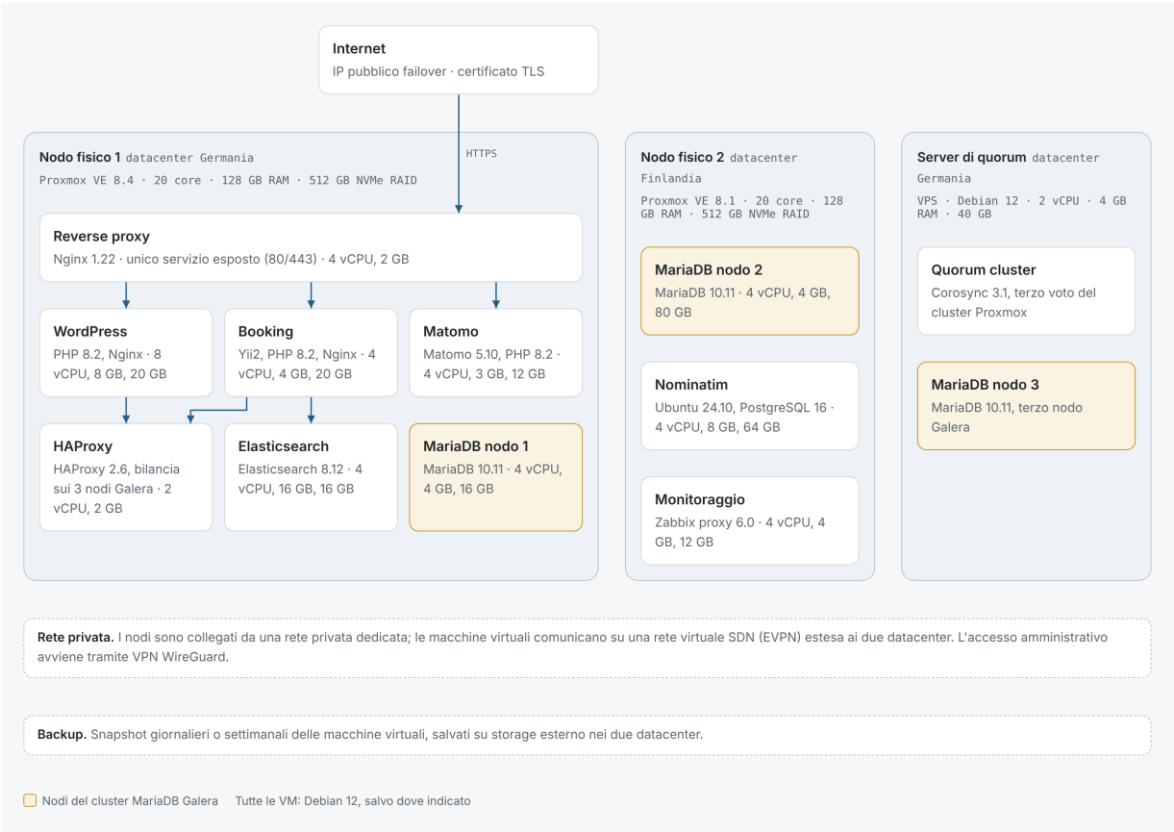


Figura 2 - Server fisici, macchine virtuali e servizi ospitati nella configurazione attuale.

5.1.1 Server fisici e quorum

Server	Datacenter	Caratteristiche
Nodo fisico 1	Area 1 EU	Proxmox VE 8.4, CPU Intel Core i5-13500 (20 core, 1 socket), 128 GB RAM, 512 GB NVMe in RAID.
Nodo fisico 2	Area 2 EU	Proxmox VE 8.1, CPU Intel Core i5-13500 (20 core, 1 socket), 128 GB RAM, 512 GB NVMe in RAID.
Server di quorum	Area 1 EU	Server virtuale Debian 12, 2 vCPU, 4 GB RAM, 40 GB disco. Fornisce il terzo voto al cluster Proxmox (Corosync 3.1) e ospita il terzo nodo MariaDB.

5.1.2 Macchine virtuali e software

Le macchine virtuali utilizzano Debian 12, salvo Nominatim che utilizza Ubuntu 24.10, e memorizzano i dati su disco locale NVMe.

Macchina	Nodo	vCPU / RAM / disco	Software
Reverse proxy	Nodo 1	4 / 2 GB / 8 GB	Nginx 1.22
WordPress	Nodo 1	8 / 8 GB / 20 GB	WordPress, PHP 8.2, Nginx 1.22
Booking	Nodo 1	4 / 4 GB / 20 GB	Applicazione Yii2, PHP 8.2, Nginx 1.22, processi pianificati
Matomo	Nodo 1	4 / 3 GB / 12 GB	Matomo 5.10, PHP 8.2, Nginx 1.22
Elasticsearch	Nodo 1	4 / 16 GB / 16 GB	Elasticsearch 8.12
HAProxy	Nodo 1	2 / 2 GB / 6 GB	HAProxy 2.6, bilanciamento verso il cluster MariaDB
MariaDB nodo 1	Nodo 1	4 / 4 GB / 16 GB	MariaDB 10.11, Galera
MariaDB nodo 2	Nodo 2	4 / 4 GB / 80 GB	MariaDB 10.11, Galera
Nominatim	Nodo 2	4 / 8 GB / 64 GB	Nominatim, PostgreSQL 16, Python 3.12, Nginx 1.26
Monitoraggio	Nodo 2	4 / 4 GB / 12 GB	Zabbix proxy 6.0

MariaDB nodo 3	Server di quorum	condivide il server	MariaDB 10.11, Galera
----------------	------------------	---------------------	-----------------------

5.1.3 Rete e accessi

- I nodi fisici e il server di quorum sono collegati da una rete privata dedicata.
- Le macchine virtuali comunicano su rete virtuale SDN EVPN estesa ai due datacenter e possono essere spostate senza cambio di indirizzo.
- È esposto un solo indirizzo IP pubblico failover, assegnato al reverse proxy, sul quale è installato il certificato TLS del dominio.
- L'accesso amministrativo ai server avviene tramite VPN WireGuard.

5.1.4 Regole di firewall attuali

Macchina	Traffico consentito
Reverse proxy	In ingresso da internet solo sulle porte 80 e 443. Accesso alla rete interna.
WordPress	Verso il database, verso il server di booking (porte 80 e 443), verso il server SMTP e il repository del codice. Verso internet solo HTTP/HTTPS, DNS, NTP e ICMP.
Booking	Verso il database, Elasticsearch, il server SMTP e il repository del codice. Verso internet HTTP/HTTPS, SMTP sulla porta 587, DNS, NTP e ICMP.
Nominatim	Verso internet solo HTTP/HTTPS, DNS, NTP e ICMP.
Altre macchine	Accesso alla rete interna e a internet.

5.1.5 Alta affidabilità

- Database: cluster MariaDB Galera multi-master su tre nodi distribuiti su tre server e due datacenter; HAProxy distribuisce le connessioni sui nodi attivi.
- Virtualizzazione: il cluster Proxmox usa il server di quorum come terzo voto, consentendo a un nodo di restare operativo quando l'altro non è raggiungibile.
- Altri servizi: reverse proxy, WordPress, booking, Matomo, Elasticsearch e Nominatim sono ciascuno su una singola VM; in caso di guasto del nodo la VM può essere riavviata sull'altro nodo del cluster.

5.1.6 Backup attuali

I backup correnti consistono in snapshot completi delle macchine virtuali salvati su storage esterno nei due datacenter. L'aggiudicatario dovrà acquisire e verificare tali configurazioni e adeguarle ai requisiti più stringenti del presente Capitolato.

Macchine	Frequenza	Copie conservate
MariaDB nodo 2	Ogni giorno alle 02:00	1
Booking, WordPress, MariaDB nodo 1, Matomo, Elasticsearch	Ogni giorno alle 04:00	5
Reverse proxy, HAProxy	Ogni sabato alle 11:00	5
Monitoraggio	Ogni domenica alle 05:00	2
Nominatim	Ogni giovedì alle 01:00	1

5.1.7 Quadro tecnologico della baseline

Ambito	Tecnologia
Virtualizzazione	Proxmox VE 8 in cluster, con server di quorum
Sistemi operativi	Debian 12; Ubuntu 24.10 per Nominatim
Reverse proxy e web server	Nginx 1.22
Portale pubblico	WordPress, PHP 8.2
Backend applicativo	PHP 8.2, framework Yii2

Database	MariaDB 10.11 in cluster Galera, HAProxy 2.6
Ricerca	Elasticsearch 8.12
Geocoding	Nominatim con PostgreSQL 16
Analytics	Matomo 5.10
Monitoraggio	Zabbix 6.0
Pagamenti	Stripe Connect (account Express)

Le versioni sopra indicate descrivono la baseline rilevata. L'aggiudicatario dovrà verificare lo stato di supporto e sicurezza di ciascun componente, proporre gli aggiornamenti necessari e assicurare la compatibilità dell'intero sistema prima di ogni variazione.

Art. 6 - Manutenzione correttiva, adeguativa, preventiva ed evolutiva

Il servizio comprende tutte le attività necessarie per conservare e migliorare il corretto funzionamento del sistema.

Tipologia	Prestazioni richieste
Correttiva	Diagnosi e rimozione di errori, regressioni, blocchi, incongruenze dati e malfunzionamenti di integrazioni.
Adeguativa	Aggiornamenti necessari per norme, sicurezza, browser, sistemi operativi, servizi terzi, API, gateway e standard tecnici.
Preventiva	Refactoring mirato, aggiornamento dipendenze, tuning, pulizia log/dati, revisione job, test di ripristino e riduzione del debito tecnico.
Evolutiva	Nuove funzionalità e modifiche richieste dal CAI, previa analisi, stima, approvazione e pianificazione; gli sviluppi sono di proprietà del CAI secondo l'art. 12.
Perfettiva	Miglioramenti a usabilità, accessibilità, prestazioni, qualità del codice e osservabilità senza alterare la finalità del servizio.

Ogni rilascio deve essere versionato, sottoposto a test, accompagnato da note di rilascio e da procedura di rollback. Le modifiche urgenti devono essere ricondotte successivamente al normale processo di documentazione e versionamento.

Il servizio deve comprendere due pacchetti ore annui destinati alla manutenzione evolutiva e all'aggiornamento redazionale (inserimento di nuovi contenuti nel sito web) della durata di non meno di 40 ore ciascuno, utilizzabile su ordine del CAI. Le stime devono distinguere analisi, sviluppo, test, documentazione e rilascio; le ore non autorizzate non sono contabilizzabili.

Art. 7 - Gestione operativa del marketplace e dei pagamenti

L'aggiudicatario assicura le attività operative connesse al marketplace nei termini stabiliti dal contratto e dalle condizioni di utilizzo, comprese le configurazioni dei profili delle strutture, il supporto ai flussi di pagamento e rimborso, la riconciliazione, la reportistica, azioni di marketing proattivo verso i rifugisti e tutti i gestori.

Di seguito una lista di azioni da svolgere:

- configurazione e gestione tecnica degli account delle strutture sul gateway di pagamento;
- supporto tecnico ai gestori nella creazione degli account e nella gestione del CMS;
- presidio dei flussi di incasso delle caparre e degli eventuali pagamenti completi;
- ripartizione e disposizione degli importi ai soggetti aventi diritto secondo le regole contrattuali;
- gestione dei rimborsi e delle anomalie di pagamento;
- riconciliazione tra prenotazioni, transazioni, storni, commissioni e bonifici;
- produzione delle evidenze contabili e fiscali previste;
- report mensile al CAI con prenotazioni e transazioni, suddivise secondo le dimensioni concordate;
- tracciabilità delle operazioni e segregazione dei ruoli;
- coperture assicurative e garanzie richieste negli atti di gara;
- copertura di azioni di marketing a favore di gestori e rifugisti finalizzate ad incrementare il numero di adesioni delle strutture.

L'aggiudicatario non può modificare commissioni, condizioni, flussi finanziari o soggetti beneficiari senza preventiva autorizzazione del CAI.

Art. 8 - Assistenza, help desk e supporto agli utenti

L'aggiudicatario attiva un servizio di assistenza multicanale in lingua italiana, tracciato mediante sistema di ticketing accessibile ai referenti CAI. Il servizio deve distinguere richieste del CAI, dei gestori/rifugisti e degli utenti finali.

- canale web/e-mail sempre disponibile per apertura ticket;
- numero telefonico per criticità P1 e P2 e per supporto operativo negli orari di servizio;
- orario ordinario: giorni lavorativi 09:00-18:00;
- reperibilità per incidenti P1: 24x7;
- knowledge base e FAQ aggiornate;
- presa in carico, classificazione, escalation, comunicazioni periodiche e chiusura concordata;
- report mensile con volumi, categorie, tempi e problemi ricorrenti;
- assistenza rafforzata nei periodi di apertura delle strutture e nelle finestre di rilascio.

L'aggiudicatario deve evitare che l'utente sia rinviato tra CAI, rifugio, gateway e fornitore senza una chiara responsabilità di gestione. I ticket relativi a dati personali o pagamenti devono essere trattati da personale autorizzato e secondo procedure dedicate.

8.1 Fascia e canale per l'assistenza ordinaria

Per l'assistenza funzionale a escursionisti e gestori, il servizio è garantito dalle 09:00 alle 18:00, sette giorni su sette, tramite e-mail. I tempi sono espressi in ore lavorative conteggiate esclusivamente nella fascia di assistenza. Restano fermi gli SLA tecnici e la reperibilità per incidenti critici disciplinati dall'art. 10.

8.2 SLA verso i clienti finali

Ambito	Priorità	Presa in carico	Risoluzione
Problemi durante il processo di prenotazione	Alta	4 ore lavorative	8-24 ore lavorative
Anomalie relative ai pagamenti	Alta	4 ore lavorative	8-24 ore lavorative
Mancata ricezione della conferma di prenotazione	Alta	4 ore lavorative	8-24 ore lavorative
Problemi di accesso o utilizzo della piattaforma	Media	8 ore lavorative	24-48 ore lavorative
Richieste informative sulle funzionalità della piattaforma	Bassa	8 ore lavorative	24-48 ore lavorative
Richieste relative a disponibilità, servizi e condizioni del rifugio	Esterna	Entro 8 ore lavorative per l'eventuale inoltro al gestore	Dipendente dai tempi di risposta del gestore
Richieste di rimborso relative a prenotazioni e pagamenti	Alta	4 ore lavorative	8-24 ore lavorative per la verifica iniziale e l'avvio della procedura
Anomalie tecniche che impediscono l'esecuzione di un rimborso	Alta	4 ore lavorative	8-24 ore lavorative
Verifica dello stato di una richiesta di rimborso	Media	8 ore lavorative	24-48 ore lavorative per fornire un aggiornamento
Gestione delle comunicazioni tra cliente finale e gestore del rifugio	Esterna	8 ore lavorative	24-48 ore lavorative per la presa in carico e il coordinamento
Richieste di chiarimento su modifiche, cancellazioni o condizioni della prenotazione	Esterna	8 ore lavorative	24-48 ore lavorative per fornire un riscontro o indirizzare la richiesta
Mancata risposta del gestore a una richiesta del cliente finale	Esterna	8 ore lavorative	24-48 ore lavorative per l'eventuale sollecito e aggiornamento al cliente

8.3 SLA verso i gestori dei rifugi

Ambito	Priorità	Presa in carico	Risoluzione
Indisponibilità complessiva della piattaforma	P1 – Critica	1 ora lavorativa	8 ore lavorative
Impossibilità di effettuare o gestire prenotazioni	P1 – Critica	1 ora lavorativa	8 ore lavorative
Anomalie relative a pagamenti o transazioni	P2 – Alta	4 ore lavorative	8-24 ore lavorative
Errori nella gestione di calendari e disponibilità	P2 – Alta	4 ore lavorative	8-24 ore lavorative
Problemi relativi a camere, posti letto e tariffe	P3 – Media	8 ore lavorative	24-48 ore lavorative
Problemi di accesso all'area di gestione	P3 – Media	8 ore lavorative	24-48 ore lavorative
Anomalie o richieste di aggiornamento dei dati del rifugio	P4 – Bassa	8 ore lavorative	24-48 ore lavorative
Richieste informative e assistenza ordinaria	P4 – Bassa	8 ore lavorative	Entro 48 ore lavorative

Per i rimborsi, il tempo di risoluzione riguarda la verifica e l'avvio della procedura, non l'effettivo accredito bancario. Per le richieste che coinvolgono un gestore, i tempi si riferiscono alla presa in carico e al coordinamento dell'assistenza e non garantiscono il tempo di risposta del gestore.

Art. 9 - Sicurezza, privacy, continuità operativa e conformità

La piattaforma deve essere gestita nel rispetto della normativa vigente, delle istruzioni del CAI e delle misure tecniche e organizzative concordate. L'aggiudicatario opera quale responsabile del trattamento, ove nominato, e assicura che eventuali sub-responsabili siano autorizzati.

Misure tecniche da rispettare:

- inventario aggiornato di asset, dati, utenti privilegiati e dipendenze;
- hardening, gestione delle patch e vulnerability management;
- scansioni automatiche almeno mensili e penetration test annuale condotto da soggetto qualificato o indipendente dal team di sviluppo;
- correzione delle vulnerabilità critiche entro 72 ore e alte entro 10 giorni, salvo misura compensativa approvata;
- MFA per accessi amministrativi e separazione degli account nominativi;
- cifratura del traffico e dei backup;
- logging degli accessi amministrativi e delle operazioni rilevanti;
- notifica al CAI di incidenti di sicurezza entro 1 ora dalla rilevazione e supporto agli adempimenti;
- procedure di backup, restore, continuità operativa e disaster recovery;
- gestione data breach, conservazione, cancellazione e restituzione dei dati;
- accessibilità digitale, compatibilità con browser supportati e progressivo allineamento alle linee guida applicabili.

Art. 10 - Livelli di servizio (SLA)

Gli SLA si applicano dal termine del periodo di stabilizzazione. I tempi decorrono dall'apertura del ticket o dalla rilevazione automatica, se anteriore. Per "ripristino" si intende il ritorno a condizioni operative, anche mediante workaround sicuro; la soluzione definitiva resta dovuta nei tempi concordati.

Priorità	Definizione	Presa in carico	Ripristino	Aggiornamenti
P1 Critica	Servizio indisponibile; prenotazioni o pagamenti bloccati; perdita/compromissione dati; incidente di sicurezza grave.	15 min, 24x7	4 ore	ogni 30 min
P2 Alta	Funzione essenziale fortemente degradata senza alternativa adeguata; impatto su più strutture/utenti.	30 min in orario; 60 min fuori orario	8 ore lavorative	ogni 2 ore
P3 Media	Malfunzionamento circoscritto con workaround; impatto limitato.	4 ore lavorative	3 giorni lavorativi	giornaliero
P4 Bassa	Richiesta informativa, configurazione, difetto cosmetico o miglioramento non urgente.	1 giorno lavorativo	10 giorni lavorativi o piano concordato	alla variazione dello stato

10.1 Disponibilità e prestazioni

Indicatore	Valore minimo	Modalità
Disponibilità mensile del portale e booking	99,8%	Misurazione 24x7, escluse sole manutenzioni autorizzate.
Disponibilità dei pagamenti	99,8% al netto di indisponibilità documentate del gateway	Monitoraggio transazione sintetica o verifica equivalente.
Tempo risposta pagine principali	95° percentile <= 3 secondi	Misura server-side o sintetica da località UE, condizioni concordate.
Successo backup	>= 98% job mensili e nessun ciclo giornaliero privo di copia valida	Report automatico; fallimenti recuperati entro il ciclo successivo.
Test di ripristino	Almeno trimestrale su campione; annuale end-to-end	Verbale con tempi, esito e azioni correttive.

Le indisponibilità pianificate devono essere comunicate almeno 5 giorni lavorativi prima, svolte di norma in fascia a minor traffico e non superare 4 ore al mese, salvo autorizzazione. Non sono escluse dal calcolo le indisponibilità dovute a manutenzione urgente conseguente a ritardi imputabili all'aggiudicatario.

Art. 11 - Monitoraggio, reportistica e governance

La governance prevede un Responsabile del contratto per l'aggiudicatario, un responsabile tecnico e referenti specialistici. Sono previsti almeno: riunione di avvio; riunione operativa mensile; riesame trimestrale; riesame annuale di sicurezza e continuità.

- dashboard condivisa con disponibilità, performance, incidenti e ticket;
- report mensile entro il decimo giorno lavorativo del mese successivo;
- registro problemi, rischi, decisioni e azioni;
- report di capacity e costi infrastrutturali;
- report di sicurezza e patching;
- report su prenotazioni, transazioni, rimborsi e riconciliazioni;
- piano trimestrale di manutenzione ed evoluzione;
- SAL e consuntivo delle ore evolutive autorizzate.

Art. 12 - Proprietà, diritti sul software, dati e sviluppi

La piattaforma oggetto di presa in carico, i dati, i contenuti, le configurazioni specifiche CAI e la relativa documentazione nella disponibilità del CAI devono poter essere trasferiti e gestiti dall'aggiudicatario esclusivamente per l'esecuzione del contratto. Il trasferimento sull'infrastruttura dell'aggiudicatario non comporta alcun trasferimento di titolarità a favore di quest'ultimo.

12.1 Proprietà degli sviluppi contrattuali

Tutte le implementazioni, personalizzazioni, modifiche, configurazioni, connettori, API, script, modelli dati, documentazione, test e ulteriori elaborati realizzati specificamente nell'esecuzione del contratto sono di proprietà esclusiva del CAI dal momento della loro realizzazione e del relativo pagamento, senza limiti territoriali o temporali, fatti salvi i diritti su componenti di terzi dichiarati nell'offerta.

L'aggiudicatario cede al CAI, in via esclusiva e irrevocabile, tutti i diritti di utilizzazione economica sugli sviluppi specifici, inclusi i diritti di riproduzione, modifica, elaborazione, adattamento, integrazione, manutenzione, evoluzione, migrazione, distribuzione interna, messa a disposizione e affidamento a terzi per finalità connesse al servizio istituzionale del CAI.

12.2 Background e componenti di terzi

L'aggiudicatario deve indicare prima dell'uso ogni componente preesistente, open source, commerciale o di terzi, specificandone titolare, versione, licenza, costi, vincoli, dipendenze e condizioni di trasferibilità. Non può incorporare componenti che impediscano al CAI o a un successivo affidatario di esercitare i diritti previsti.

12.3 Sorgenti e repository

Si richiede:

- repository del codice sorgente accessibile in lettura al CAI per tutta la durata del contratto;
- commit frequenti, tracciabili e riferiti ai ticket/change;
- consegna di codice, cronologia, dipendenze, manifest, script di build e deployment, configurazioni parametrizzate, test e documentazione;
- assenza di credenziali in chiaro e consegna separata dei segreti;
- rilasci riproducibili e istruzioni sufficienti a installare il sistema su infrastruttura equivalente;
- divieto di trattenere componenti indispensabili alla continuità per contestazioni economiche diverse da quelle definitivamente accertate.

Art. 13 - Obblighi di documentazione, repository e reversibilità

L'aggiudicatario mantiene la documentazione aggiornata e la rende disponibile al CAI in formati aperti o comunemente utilizzati. La reversibilità è un'obbligazione continuativa e non limitata alla fase finale.

Di seguito la documentazione richiesta:

- architettura logica e fisica;
- inventario applicativo e infrastrutturale;
- schema dati e dizionario dei dati;
- catalogo API e integrazioni;
- manuale di installazione, configurazione, esercizio e troubleshooting;
- procedure di backup, restore, DR e gestione incidenti;
- manuali utente, amministratore e rifugista;
- registro licenze e dipendenze;
- runbook operativi;
- piano e verbali di test;
- repository di codice e documentazione aggiornata;
- aggiornamento documentazione nuovi ingressi di rifugi.

Negli ultimi 90 giorni di contratto, o dalla richiesta del CAI in caso di cessazione anticipata, l'aggiudicatario esegue il piano di uscita e collabora con CAI e nuovo operatore. Sono inclusi almeno due workshop tecnici, export completi, supporto alla migrazione, trasferimento di account e licenze trasferibili, verifica dei dati e periodo di affiancamento.

Art. 14 - Team di lavoro e modalità operative

Il gruppo di lavoro deve essere adeguato a garantire continuità, competenza e segregazione dei compiti. I curricula delle figure chiave devono essere indicati nell'offerta e le sostituzioni devono avvenire con profili di esperienza equivalente o superiore.

Ruolo minimo	Responsabilità
Responsabile del servizio	Governo complessivo, SLA, rischi, comunicazioni e SAL.
Responsabile tecnico/architetto	Architettura, subentro, evoluzione, qualità tecnica.
Sistemista/Cloud engineer	Infrastruttura, sicurezza, monitoraggio, backup e DR.
Sviluppatore applicativo	Manutenzione ed evoluzione front end/back end, API e integrazioni.
DBA/Data specialist	Integrità, performance, backup, migrazione e reporting dati.
Specialista sicurezza e privacy	Vulnerability management, incidenti, compliance e audit.
Help desk specialist	Ticket, supporto utenti e knowledge base.
Specialista marketplace/pagamenti	Flussi economici, riconciliazioni e supporto alle strutture, azioni di marketing.

Art. 15 - Verifica di conformità, penali e rimedi

Il CAI verifica l'esecuzione mediante report, monitoraggio, ticket, verbali e controlli a campione. L'aggiudicatario deve fornire accesso alle evidenze utili, nel rispetto della sicurezza e della riservatezza.

Inadempimento	Penale
Mancato rispetto del tempo di presa in carico P1	€ 150 per ogni intervallo di 15 minuti di ritardo.
Mancato rispetto del tempo di ripristino P1	€ 250 per ogni ora o frazione di ritardo.
Mancato rispetto SLA P2/P3	€ 100 per ogni scadenza superata e ulteriore € 50 per giorno lavorativo.
Disponibilità mensile inferiore al 99,8%	1% del canone mensile per ogni 0,1 punto percentuale o frazione, entro il limite contrattuale.
Ritardo nel subentro o in deliverable essenziale	€ 200 per ogni giorno di ritardo.
Mancata consegna/aggiornamento sorgenti e documentazione	€ 300 per ogni giorno di ritardo dopo diffida.
Mancata o tardiva comunicazione di incidente di sicurezza	€ 1.000 per evento, fatti salvi maggiori danni e obblighi di legge.

Prima dell'applicazione è assicurato il contraddittorio previsto dagli atti di gara.

Art. 16 - Durata, cronoprogramma e consegne

La durata prevista è di massimo 36 mesi con decorrenza dalla sottoscrizione del contratto o dall'esecuzione anticipata, fatte salve le determinazioni definitive degli atti di gara.

Avvio del servizio trasferito e operativo entro il 1° febbraio 2027.

Il piano di subentro deve essere compatibile con la data di avvio e con la continuità del servizio.

Il corrispettivo sarà versato a decorrere dall'avvio operativo del servizio.

Fase	Termine proposto	Esito
Kick-off	T0 + 5 giorni lavorativi	Piano di subentro e governance.
Inventario e ambiente target	T0 + 15 giorni lavorativi	Verbale consistenza e infrastruttura pronta.
Migrazione di prova	T0 + 25 giorni lavorativi	Report test e rollback.
Collaudo	T0 + 35 giorni lavorativi	Verbale test funzionali, prestazionali e sicurezza.
Go-live	T0 + 45 giorni lavorativi	Servizio trasferito e operativo.
Stabilizzazione	20 giorni lavorativi dal go-live	Verbale avvio a regime.
Aggiornamento documentazione	Continuativo e a ogni rilascio	Repository allineato.
Piano di uscita	Entro 90 giorni dalla cessazione	Trasferimento completo e verificato.

Art. 17 - Contenuti minimi dell'offerta tecnica

L'offerta tecnica deve descrivere in modo verificabile come il concorrente intende rispettare il Capitolato e deve includere almeno:

- piano di presa in carico e migrazione, con rischi e rollback;
- architettura di hosting proposta, localizzazione, dimensionamento e scalabilità;
- modello di manutenzione, rilascio e gestione del codice;
- sistema di monitoraggio e modalità di misura degli SLA;
- organizzazione dell'help desk e reperibilità;
- piano di sicurezza, backup, DR e gestione incidenti;
- metodologia di test e qualità;
- team, ruoli, presidio e sostituzioni;
- modalità di gestione marketplace e pagamenti;
- strumenti di reportistica e governance;
- piano di reversibilità;
- elenco completo di licenze e componenti di terzi;
- pacchetti di ore per manutenzione evolutiva e redazionale
- eventuali migliorie senza ulteriori oneri, chiaramente distinte dalle prestazioni minime.

Allegato A - Matrice riepilogativa degli SLA

La matrice seguente sintetizza gli indicatori minimi, da coordinare con lo schema di contratto.

KPI	Target	Fonte dati	Frequenza
Disponibilità portale	>= 99,8% mensile	Monitoring condiviso	Mensile
P1 presa in carico	<= 15 min	Ticket + alert	Per evento
P1 ripristino	<= 4 ore	Ticket + monitoring	Per evento
P2 ripristino	<= 8 ore lavorative	Ticket	Per evento
RPO	<= 4 ore	Log backup/replica	Trimestrale
RTO	<= 8 ore	Test DR	Annuale
Vulnerabilità critiche	Correzione <= 72 ore	Scanner + ticket	Mensile
Report mensile	Entro 10° giorno lavorativo	Protocollo/consegna	Mensile

Allegato B - Inventario tecnico di presa in carico

L'inventario, sottoscritto dalle parti, deve includere almeno le informazioni seguenti:

- codice sorgente, repository, rami, tag, commit e procedure di build;
- domini, DNS, certificati, account, utenze e ruoli;
- server, VM, container, storage, reti e regole di sicurezza;
- applicazioni, framework, CMS, plugin, moduli, versioni e licenze;
- database, schema, volumi, retention, job e procedure;
- API, web service, SSO, pagamenti, e-mail, mappe, analytics e ulteriori integrazioni;
- backup, restore, monitoraggio, logging e alert;
- dati personali trattati, categorie, flussi e sub-responsabili;
- documentazione esistente e gap documentali;
- anomalie note, debito tecnico, vulnerabilità e interventi pendenti.

Allegato C - Deliverable e report periodici

I deliverable sono forniti in formato editabile e, ove opportuno, PDF/A, con versionamento e data.

Deliverable	Periodicità
Piano di subentro e migrazione	Una tantum, aggiornato fino al go-live
Verbale di consistenza tecnica	Iniziale e a ogni variazione sostanziale
Report SLA e ticket	Mensile
Report infrastruttura e capacità	Mensile/trimestrale
Report sicurezza e patching	Mensile
Report prenotazioni e transazioni	Mensile
Piano evolutive e manutenzione	Trimestrale
Test di restore	Trimestrale
Test DR e penetration test	Annuale
Repository e documentazione	Continuativo
Piano di reversibilità	Iniziale, annuale e finale

Allegato D - Clausole tecniche su proprietà e riuso

Ai fini della predisposizione definitiva degli atti, si raccomanda di mantenere congiuntamente le seguenti previsioni:

1. la piattaforma e i dati trasferiti restano nella titolarità o disponibilità del CAI;
2. gli sviluppi specifici realizzati nel nuovo affidamento sono di proprietà esclusiva del CAI;
3. i diritti ceduti comprendono modifica, manutenzione, evoluzione e affidamento a terzi;
4. i componenti preesistenti e di terzi devono essere dichiarati e non possono impedire la continuità;
5. il repository deve essere accessibile al CAI e aggiornato durante il contratto, non solo alla scadenza;
6. devono essere consegnati sorgenti, dipendenze, script, configurazioni, test, documentazione e cronologia;
7. la reversibilità deve essere inclusa nel corrispettivo e verificata con prova tecnica;
8. nessuna licenza, account o componente essenziale deve creare lock-in.