



Sicurezza dell'infrastruttura e dei servizi SaaS

Informativa tecnica - settembre 2026

MINIMIZZAZIONE

stack essenziale

CONTROLLO

software proprietario

SEGREGAZIONE

dati e servizi

CONTINUITA

replica e backup

Finalità e impostazione della sicurezza

ItalSenior srls adotta un'architettura tecnologica progettata per ridurre la superficie di attacco, mantenere il controllo diretto dello stack applicativo e garantire continuità operativa e protezione dei dati. La sicurezza non è affidata a un singolo prodotto, ma a una combinazione di minimizzazione dei componenti, segregazione, filtraggio di rete, software proprietario, replica dei sistemi, backup e procedure operative consolidate.

La piattaforma è destinata all'erogazione di applicazioni e servizi SaaS sviluppati e gestiti direttamente da ItalSenior. L'approccio privilegia componenti conosciuti, configurazioni essenziali e dipendenze limitate, così da rendere più semplice il controllo delle versioni, l'aggiornamento e l'analisi dell'esposizione.

Stack essenziale Sistema operativo Linux, Apache HTTP Server e MariaDB; installazione dei soli componenti necessari al servizio.	Software proprietario Applicazioni sviluppate internamente in Perl, senza CMS o framework applicativi general-purpose installati sui sistemi di produzione.
Firewall restrittivo Politiche di filtraggio consolidate, basate sul principio default deny e sull'apertura dei soli servizi necessari.	Dati segregati Database non pubblicamente esposti e accessibili solo dai sistemi/applicazioni autorizzati.
Ridondanza Server primari affiancati da sistemi gemelli sincronizzati e predisposti al subentro.	Backup separato Copie di sicurezza aggiuntive mantenute anche presso la sede ItalSenior di Roma.

DATA CENTER

Infrastruttura fisica e di rete

I servizi sono erogati da server fisici di proprietà ItalSenior, non condivisi con altri soggetti, collocati in armadio dedicato presso la web farm IT2 di Aruba S.p.A. ad Arezzo. La connettività disponibile è a 1 Gbps e l'infrastruttura dispone di indirizzamento IP pubblico dedicato.

L'hardware impiegato è di classe professionale. L'amministrazione dei sistemi è svolta direttamente da personale autorizzato ItalSenior, riducendo il numero di soggetti che possono intervenire sullo stack applicativo e sull'ambiente di esercizio.

Minimizzazione del software e gestione delle dipendenze

Sui server di produzione viene installato esclusivamente il software necessario all'erogazione dei servizi. Lo stack di base è volutamente contenuto e comprende Linux come sistema operativo, Apache HTTP Server per l'erogazione web e MariaDB per la gestione dei database, oltre alle utilità di sistema strettamente necessarie all'amministrazione e al funzionamento.

ItalSenior evita l'installazione di CMS, framework applicativi general-purpose e componenti non necessari. Questa scelta riduce il numero di dipendenze e di superfici applicative da mantenere e monitorare; non elimina tuttavia la necessità di aggiornamenti, hardening e verifica continua delle vulnerabilità dei componenti utilizzati.

- Aggiornamento: mantenimento delle versioni di sistema e dei componenti server secondo le esigenze di sicurezza e compatibilità.
- Servizi minimi: disabilitazione dei demoni e dei servizi non indispensabili.
- Esposizione controllata: pubblicazione verso Internet dei soli endpoint necessari al servizio.
- Controllo delle modifiche: gli aggiornamenti applicativi sono realizzati e distribuiti direttamente da ItalSenior.

PROTEZIONE PERIMETRALE

Firewall, filtraggio e accessi amministrativi

L'infrastruttura utilizza un firewall software e politiche di filtraggio sviluppate e affinate operativamente da oltre vent'anni. La configurazione segue un'impostazione restrittiva: il traffico non esplicitamente necessario è bloccato e vengono consentite esclusivamente le comunicazioni previste dall'architettura del servizio.

- Default deny: apertura selettiva delle porte e dei flussi autorizzati.
- Accessi amministrativi limitati: gli accessi ai server sono riservati ai soggetti autorizzati e alle modalità operative previste.
- Monitoraggio: controllo operativo dei sistemi e delle anomalie rilevanti.
- Database non esposti: i servizi database non sono resi direttamente raggiungibili dalla rete Internet pubblica.

APPLICATION SECURITY

Software applicativo proprietario

Il software applicativo erogato da ItalSenior è sviluppato internamente, prevalentemente in Perl, ed è di proprietà ItalSenior. La disponibilità del codice sorgente e la conoscenza diretta dell'architettura consentono di intervenire senza dipendere dai cicli di rilascio di framework o CMS di terze parti.

Lo sviluppo applicativo prevede misure specifiche contro classi di attacco tipiche delle applicazioni web, comprese SQL Injection e Cross-Site Scripting (XSS), attraverso validazione e normalizzazione degli input, corretta gestione dei dati destinati al database e codifica/controllo dell'output nei contesti web.

Segregazione dei dati e protezione delle risorse

I database applicativi sono mantenuti su sistemi non direttamente accessibili dall'esterno. Le applicazioni costituiscono il livello autorizzato di accesso ai dati e applicano i controlli previsti per utenti, profili e funzioni.

Per documenti e risorse non destinate alla pubblicazione diretta, ItalSenior utilizza meccanismi applicativi proprietari di identificazione e risoluzione delle risorse. Gli identificativi esposti all'utente non devono corrispondere direttamente alla struttura fisica di memorizzazione e vengono interpretati dal software applicativo, riducendo l'esposizione dei percorsi e della struttura interna degli archivi.

Tale meccanismo è una misura aggiuntiva di segregazione e controllo e non viene considerato sostitutivo dei normali controlli di autorizzazione, delle protezioni del filesystem, del filtraggio di rete e delle altre misure di sicurezza.

BUSINESS CONTINUITY

Continuità operativa, replica e ripristino

I server principali sono affiancati da sistemi gemelli mantenuti sincronizzati. In caso di guasto hardware o indisponibilità del sistema primario, il servizio può essere trasferito al sistema di riserva mediante le procedure di subentro previste, compresa la riallocazione dell'indirizzo IP quando applicabile.

- Replica: sincronizzazione dei sistemi di riserva rispetto ai server primari.
- Riduzione dei tempi di ripristino: disponibilità di una macchina già predisposta per il servizio.
- Backup separato: ulteriore copia di programmi e dati mantenuta presso la sede ItalSenior di Roma.
- Resilienza geografica: la copia esterna al data center costituisce un ulteriore livello di protezione rispetto a guasti o indisponibilità della sede primaria.

EVIDENZA STORICA

Esperienza operativa e storico di sicurezza

L'architettura e le politiche descritte derivano da un modello operativo consolidato nel tempo. Per quanto risulta dai sistemi e dalle evidenze operative nella disponibilità di ItalSenior, non sono state rilevate intrusioni riuscite nei server o nei servizi SaaS gestiti con questa architettura.

Questo dato storico costituisce un elemento positivo di esperienza operativa, ma non viene presentato come garanzia di invulnerabilità futura: la sicurezza informatica richiede manutenzione continua, aggiornamenti e adattamento alle nuove tecniche di attacco.

SINTESI

Principi di sicurezza adottati

- Riduzione della superficie di attacco mediante installazione dei soli componenti necessari.
- Controllo diretto dello stack grazie allo sviluppo applicativo proprietario e alla gestione interna dell'infrastruttura.
- Difesa per livelli: firewall, segregazione, autorizzazioni applicative, protezione delle risorse, replica e backup.
- Segregazione dei dati e assenza di esposizione diretta dei database alla rete pubblica.
- Continuità operativa mediante sistemi gemelli sincronizzati e procedure di subentro.
- Backup separato geograficamente rispetto alla web farm primaria.
- Indipendenza tecnologica da CMS, framework e piattaforme SaaS di terzi non indispensabili.
- Manutenibilità attraverso uno stack ridotto, conosciuto e direttamente controllato.

NOTA TECNICA

Ambito e precisazioni

La presente informativa descrive l'impostazione tecnica generale adottata da Italsenior per la protezione dei server e dei servizi SaaS. Le misure effettivamente applicabili a uno specifico servizio possono variare in funzione dell'architettura, dei dati trattati, dei requisiti contrattuali e delle integrazioni richieste dal cliente.

La sicurezza è un processo continuo. Nessuna architettura informatica può garantire l'assenza assoluta di vulnerabilità o incidenti; Italsenior adotta pertanto un approccio basato sulla riduzione del rischio, sul controllo diretto dei sistemi e sulla capacità di ripristino.

Roma, 4 settembre 2026

Il Legale Rappresentante

Ing. Alvise Valsecchi

ITALSENIOR SRLS

Dati societari

Sede	Via Donato Menichella 282 - 00156 Roma
PEC	italsenior@pec.it
P. IVA	14083161001
REA	RM-1495115
IBAN	IT23 U030 6984 8101 00000004379

Sito	www.italsenior.it
------	--