

Servizio in cloud dedicato caratteristiche generali

Ver. 1.9

Introduzione

Il presente documento riguarda le caratteristiche generali del servizio in cloud dedicato denominato “Virtualspace” su cui poggieranno il sito/app/webapp ed in generale i servizi Internet commissionati e relativa manutenzione, alle misure di sicurezza adottate a livello infrastrutturale, nonché alle procedure per la conservazione dei dati quale parte integrante della normativa sul trattamento dei dati personali.

Tutte le misure di sicurezza applicate sono state prese in seguito ad un’analisi dei rischi, dello stato dell’arte tecnologico e dei costi di attuazione e sono finalizzate a garantire un livello di sicurezza adeguato al rischio.

Tutto quanto qui esposto si applica a caratteristiche e procedure standard, attuate come predefinite in mancanza di ulteriori richieste specifiche. Eventuali variazioni vengono integrate con un Addendum e condivise con il committente.

Infrastruttura Hardware e Software

Il servizio in cloud dedicato denominato “Virtualspace” è un servizio di cloud computing professionale dedicato a hosting di siti e applicativi web, fornito sotto forma di “Software as a Service” (SaaS).

I server utilizzati per la fornitura del servizio sono server privati virtuali (VPS) forniti e gestiti da Akamai Technologies per mezzo della sede svizzera Akamai Technologies International AG e commercializzati sotto il brand Linode, Internet Service Provider (ISP) Statunitense.

Fisicamente i server utilizzati da I.T.S. Planet S.r.l. sono locati presso le web-farm di Francoforte in Germania o Milano in Italia, gestiti dal medesimo provider.

In merito alla documentazione legale, termini di utilizzo, caratteristiche del servizio, ed in particolare alle policy di privacy e sicurezza adottate da Akamai Technologies si rimanda alla seguente sezione del portale online: <https://www.akamai.com/it/legal>

In particolare in merito alle certificazioni e compliance di sicurezza si rimanda al seguente link: <https://www.akamai.com/it/legal/compliance>

In merito al brand Linode ulteriori informazioni vengono fornite dalla sezione Legal & Compliance Center del relativo portale, raggiungibile online al seguente link: <https://www.linode.com/legal/>

Specifiche tecniche generali del servizio

- I server adottati sono server cloud virtuali che vengono eseguiti su un supervisore KVM, configurati e gestiti autonomamente da I.T.S. Planet S.r.l. a seconda dei servizi deputati a svolgere.

- Ogni server virtuale è dedicato al committente e non condivide dati con alcun altro cliente.
- *Le risorse dedicate ai server dipendono dal piano concordato con il committente e variano in base a diversi fattori, quali carico di elaborazione, memoria RAM consumata, spazio disco necessario, traffico richiesto, etc. In caso di necessità possono variare nel corso della vita operativa di ciascun server. Le dotazioni hardware si basano su componenti di ultime generazioni, in particolare:*
 - Processori dedicate di classe minima Intel Xeon o AMD EPYC
 - Memoria DRAM dedicata di ultima generazione
 - Storage su SSD ridondato in RAID 1
 - Connessione tramite Gbit Ethernet

Software di sistema e management

Di seguito le specifiche tecniche generiche generali sui software di sistema adottati.

- Sistema operativo di classe Linux.
- Server web di ultima generazione (NginX).
- Server di database relazionale di ultima generazione di classe MySQL (MariaDB).
- Interprete PHP v. 7.x o 8.x a seconda delle esigenze del committente.

Sicurezza e Business continuity

Provvedimenti generali di sicurezza

Per la conservazione e l'integrità dei dati nonché la sicurezza delle trasmissioni tra server/server e server/client, vengono inoltre adottati i seguenti provvedimenti tecnici.

- Firewall DDoS al perimetro.
- Firewall di sistema su tutte le porte dei servizi attivi per il monitoraggio in real-time dei tentativi di accesso non autorizzati.
- Blocco delle porte di accesso al server agli indirizzi IP dopo un numero predefinito di tentativi di accesso falliti (ad es. account ftp, accesso a database, etc.).
- Accesso ai servizi di database permesso solo ai servizi applicativi tramite doppia verifica (server richiedente ed autenticazione a livello applicativo).
- Backup giornaliero di tutto il server, mantenimento a rotazione di 1 backup giornaliero e 2 settimanali.
- Aggiornamento settimanale delle patch di sistema/sicurezza ufficiali su sistema operativo ed applicativi di sistema.
- Connessione criptata client-server su tutti i servizi aperti, in particolare https con cifratura TLS per l'accesso alle pagine Web. Il livello di sicurezza delle ciphersuites sono di tipo "intermediate" secondo la configurazione raccomandata dalla Mozilla Foundation.
- Eliminazione dai server di tutti i dati trattati secondo le istruzioni ricevute dal Titolare dei Trattamenti a conclusione dell'incarico. In assenza di istruzioni impartite i dati verranno cancellati entro 30 gg dalla sua conclusione.

- Verifiche scadenzate tramite Vulnerability Assessment mirati (solo per server di lungo termine).

Business Continuity

In merito all'infrastruttura hardware, essendo i server ed in generale tutta l'architettura presso provider esterno, per il livello di servizio (SLA) si rimanda al Master Service Agreement di Akamai Technologies.

Eventuale SLA con I.T.S. Planet Srl che esuli dalla suddetta documentazione deve essere concordata di volta in volta in base alle effettive esigenze del cliente e valutazione dei rischi.

Interventi tecnici dovuti ad eventuali malfunzionamenti riconducibili alla nostra area di intervento vengono presi in carico il prima possibile e generalmente nel giro di 120 minuti in orario lavorativo (h. 9-18 dal lunedì al venerdì).

In caso di corruzione hardware tale da rendere necessario un ripristino dati, questi verrà effettuato tramite ultimo backup utile (generalmente la perdita di dati si attesta all'interno delle 24h). L'attivazione di policy di backup differenti deve essere concordata di volta in volta in base alle effettive esigenze del cliente e valutazione dei rischi.

Software Web

Tutti i software web commissionati, sviluppati, testati ed installati da I.T.S. Planet S.r.l. per il committente, quali siti internet, applicativi web, webapp, gestionali, etc. vengono sviluppati sin dalle fondamenta con grande attenzione alla sicurezza. Tutto

il codice “core” è sviluppato internamente ad I.T.S. Planet S.r.l. senza l'utilizzo di framework precostituiti utilizzando come riferimento le linee guida dell'OWASP(*) (open web application security project).

Tutti i software e relativa logica sono conformi alle normative GDPR.

A seguito dello sviluppo vengono condotti una serie di test per individuare eventuali vulnerabilità del software. In caso di individuazione di una vulnerabilità che possa compromettere la conservazione o l'integrità dei dati questa viene risolta nel più breve tempo possibile. In caso di allungamento dei tempi di risoluzione del rischio i dati vengono messi off-line e resi non più accessibili da internet sino alla risoluzione del rischio.

() Le linee guida prevedono che venga conseguito un livello di sicurezza adeguato al livello di rischio ritenuto accettabile dal committente; quale sia tale livello di rischio dipende dalle esigenze del committente e può essere valutato adeguatamente solo con un'analisi dei rischi. In caso di mancanza di indicazioni specifiche, verranno applicati gli accorgimenti considerati standard e in proporzione ai costi per applicativi web i quali non trattino dati particolari ai sensi del GDPR, e la cui eventuale diffusione a causa di data-breach non costituisca danno di immagine od economico rilevante per il committente.*

Quanto espresso sopra non è applicabile a software installato, modificato o realizzato da parti esterne e non ufficialmente sviluppate da I.T.S. Planet S.r.l.