Hi-Logic

Sede Legale: via del Brennero, 322 | 38121 Trento (TN) - Italia
Sede Operativa: via Proner, 32 | 38015 Lavis (TN) - Italia
+39 345 1793243 | info@hi-logic.it | pec@pec.hi-logic.it | www.hi-logic.it
P.Iva \ C.F. \ Reg.Impr. Trento n. 02487210227 | Cap. Soc. 30.000,00 euro i.v.

Microsoft Partner

WHITE PAPER SERVIZI CLOUD

SOMMARIO

1. INTRODUZIONE

Il presente documento ha lo scopo di fornire al cliente dei servizi SaaS erogati da Hi-Logic una dettagliata informativa sulle modalità di gestione delle attività in conformità a quanto previsto dalle linee guida ISO/IEC 27017:2021 e ISO/IEC 27018:2020, con particolare attenzione alle misure introdotte per garantire la disponibilità, riservatezza ed integrità dei dati.

2. LOCALIZZAZIONE GEOGRAFICA

Hi-Logic utilizza per i propri servizi in cloud infrastrutture Microsoft Azure e sceglie di localizzarli, ove possibile, all'interno dello Spazio Economico Europeo e più precisamente in area West Europe.

In alcuni casi, per via della tipologia di servizi scelti, tale localizzazione non è possibile ed in tali scenari vengono scelti comunque servizi che effettuano trasferimenti all'esterno dello SEE solo sulle basi di legittimità stabilite dal GDPR. In particolare, i servizi ad oggi utilizzati che effettuano trasferimenti all'esterno dello SEE sono quelli forniti dal sistema di ticketing in uso Zendesk e del Web Application Firewall fornito da Cloudflare, che possono ospitare i dati, anche personali (sulla base di esistenti accordi di responsabilità), in Stati Uniti (decisione di adeguatezza), Regno Unito (decisione di adeguatezza), Giappone (decisione di adeguatezza) e Australia (clausole contrattuali standard).

Si specifica in questa sede che i tre fornitori descritti sono anch'essi certificati, come Hi-Logic, a fronte della norma ISO/IEC 27001:2022 ed estensioni alle linee guida ISO/IEC 27017:2021 e ISO/IEC 27018:2020, oltre alle ulteriori certificazioni per il cui dettaglio si rimanda alle relative pagine di documentazione:

- Microsoft Azure e Microsoft 365 (erogazione del servizio): https://learn.microsoft.com/it-it/azure/compliance/;
- Zendesk (supporto clienti): https://www.zendesk.com/it/trust-center/;
- Cloudflare (web application firewall): https://www.cloudflare.com/it-it/trust-hub/compliance-resources/).

3. GESTIONE DEGLI ASSET E DELLE UTENZE

3.1 ACCESSI

Hi-Logic regola l'accesso alle applicazioni e ai sistemi con modalità differenti a seconda dei servizi offerti. In tutti i casi, in sede di attivazione del servizio, viene definito dal cliente il contatto responsabile per il servizio e per la variazione degli account.

Nei servizi in cui è possibile una gestione autonoma degli account, a tale responsabile viene assegnata un'utenza di tipo *tenant admin* che gli permette di creare autonomamente ulteriori utenti della tipologia desiderata tra quelle disponibili (diverse a seconda del servizio). Negli altri servizi, è Hi-Logic a fungere da *tenant admin* e solo i suoi dipendenti possono creare gli account di accesso per il cliente. In tale caso, il responsabile per il servizio è l'unico contatto che può richiedere, tramite richiesta scritta via email, variazioni agli account come aggiunta o rimozione.

All'attivazione di una nuova utenza, il sistema invia un'email automatica all'indirizzo indicato per la conferma dell'account e l'impostazione della password, che deve seguire i criteri di *strong* password di default decisi dal sistema di *identity* utilizzato. L'utente ha in ogni momento la possibilità di modificare la password una volta autenticato nel servizio, oltre alla possibilità di ripristinarla autonomamente, senza effettuare l'accesso, consentendo di agire in maniera tempestiva nei casi di dubbi circa eventuali corruzioni o compromissioni di password, come ad esempio i casi di divulgazioni involontarie.

Come ulteriori protezione da accessi indesiderati, nel caso di inserimento di password errata per dieci volte consecutive, il sistema blocca l'accesso per un periodo di tempo che varia da un minuto a cinque ore in base alle politiche di *smart lockout* specificate dal servizio di *identity* utilizzato (https://learn.microsoft.com/en-us/azure/active-directory-b2c/threat-management). Una volta bloccato l'account, è possibile sbloccarlo attendendo il tempo necessario o effettuando un reset della password. Inoltre, è facoltà del responsabile del servizio decidere di attivare l'obbligo di autenticazione multifattore per tutti i propri utenti.

Negli orari lavorativi e in caso di urgenze è possibile contattare l'assistenza tecnica di Hi-Logic all'indirizzo assistenza@hi-logic.it per eventuali necessità legate agli account come controllo degli accessi (è possibile verificare i log fino a 7 giorni precedenti), reset password, revoca delle sessioni e disabilitazione temporanea (operazioni effettuate solo sull'utente che effettua la richiesta o sugli utenti indicati in caso di richiesta da parte del responsabile del servizio).

3.2 RIMOZIONE DEGLI ASSET

Alla chiusura di un contratto con Hi-Logic i servizi in uso al cliente vengono disattivati ma la cancellazione effettiva di tutti i dati, inclusi quelli personali, avviene solo a seguito di comunicazione a mezzo email tra Hi-Logic e il cliente per l'eventuale restituzione dei dati. A restituzione terminata o in assenza di indicazioni a riguardo, e comunque non oltre 60 giorni trascorsa la scadenza del contratto, tutti i dati presenti sui sistemi vengono cancellati definitivamente e non possono più essere recuperati. Alcuni dati potrebbero essere ancora presenti sui sistemi per qualche tempo in base ai tempi di retention dei backup effettuati e descritti nel paragrafo 4.3.

Si specifica che in Hi-Logic di norma non si producono stampe cartacee di alcun tipo e che eventuali stampe sono distrutte immediatamente dopo l'utilizzo.

3.3 PROTEZIONE DATI PERSONALI

In base al servizio cloud offerto, Hi-Logic si configura come titolare del trattamento di alcune tipologie di dati personali (es: utenze di accesso di BMS/Stanza del Sindaco) e come responsabile del trattamento per altre tipologie (es: dati degli utenti che accedono ai chatbot). Caso per caso viene stipulata apposita nomina a responsabile tra il cliente e Hi-Logic ove opportuno e il trattamento avviene per le sole finalità e con le modalità meglio descritte in ciascuna nomina e nelle informative agli utenti.

Hi-Logic conserva gli opportuni registri di legge sul trattamento dei dati personali e, nel caso si rivelasse necessario procedere al ripristino di dati personali, segue la relativa procedura

interna che prevede anche la tracciatura di tale operazione in apposito registro predisposto allo scopo.

3.4 GESTIONE DEI CONSENSI E DELLE RICHIESTE DEGLI UTENTI

Qualora un servizio, per le sue caratteristiche, possa essere offerto agli utenti solo su loro specifico consenso espresso in modo esplicito, Hi-Logic ha cura di mantenere apposito registro dei consensi con la tracciatura dei consensi rilasciati e delle modifiche effettuate nel corso del tempo.

Indipendentemente dalla necessità di mantenere un registro dei consensi, gli utenti finali possono reclamare il proprio diritto di accesso, rettifica o cancellazione dei propri dati personali in qualsiasi momento. Il titolare che ricevesse tale richiesta può inoltrarla tramite richiesta di assistenza ad Hi-Logic per l'evasione per la parte di propria competenza (oltre alla possibilità di contatto diretto da parte degli utenti per cui Hi-Logic effettua il trattamento in qualità di titolare).

4. MISURE OPERATIVE

4.1 CRITTOGRAFIA

Nei servizi cloud i flussi di dati da e verso i sistemi ed i server esposti su internet sono protetti utilizzando il canale TLS 1.2 e le comunicazioni interne avvengono su protocollo HTTPS protetto da certificati SSL rilasciati da fonti attendibili.

4.2 CHANGE MANAGEMENT

Per quanto attiene le eventuali modifiche ai servizi cloud ed ai sistemi che lo compongono, nel caso in cui vengano apportate modifiche sostanziali, Hi-Logic provvederà a comunicarle ai clienti, fornendo i tempi di esecuzione delle variazioni così da minimizzarne gli impatti che potrebbero derivarne.

4.3 BACKUP E BUSINESS CONTINUITY

Viene effettuato regolarmente il backup di tutti i sistemi secondo le procedure interne, generalmente ogni 24 ore, e con tempistiche di retention differenti in base alla tipologia di sistema, in ogni caso di minimo 7 giorni.

Hi-Logic esegue inoltre regolarmente delle verifiche e dei test di ripristino per assicurarsi della regolarità delle operazioni a regime.

Le tempistiche di backup sono state definite anche in relazione alla procedura interna per la *business continuity* e alla *business impact analysis*, dove sono definiti i tempi massimi di RTO (Recovery Time Objective) e RPO (Recovery Point Objective).

4.4 RACCOLTA E MONITORAGGIO LOG

I log applicativi sono conservati da Hi-Logic e sono disponibili per eventuali verifiche che dovessero rendersi necessarie, insieme ai log delle modifiche effettuate ai dati, oltre ai log di accesso già menzionati al paragrafo 3.1.

4.5 SINCRONIZZAZIONE DEGLI OROLOGI

Hi-Logic, per mantenere coerenza degli eventi sul cloud, utilizza le impostazioni di sincronizzazione automatica degli orologi degli host su cui i sistemi sono ospitati. Il fuso orario utilizzato varia a seconda del sistema e può essere UTC oppure quello locale di Roma (UTC +1 o +2 in base all'ora solare/legale).

4.6 GESTIONE DELLE VULNERABILITÀ

Hi-Logic predispone tutte le misure per ricercare, governare e risolvere le vulnerabilità tecniche individuate per evitare che possano comportare impatti negativi sul servizio e sui dati gestiti. Il team tecnico esegue annualmente (o in caso di modifiche e/o richieste specifiche) scansioni di vulnerabilità sugli applicativi; in caso di esiti negativi, provvede ad adottare le necessarie azioni correttive. Considerata la riservatezza di tali informazioni, l'esito dei test non è divulgato all'esterno.

4.7 MONITORAGGIO DEL CLOUD

Hi-Logic effettua il monitoraggio dei servizi cloud attraverso diversi strumenti messi a disposizione dalle piattaforme hosting, tra cui strumenti di segnalazione delle anomalie e raccolta informazioni. Le notifiche ricevute sono analizzate dal team tecnico ed eventualmente prese in carico. I sistemi di monitoraggio sono configurati con sistemi automatici di allarme basati su soglie per le tipologie più frequenti di incidenti o malfunzionamenti. Sono inoltre configurati degli allarmi che avvisano se un sistema supera determinate soglie di carico (oltre alla possibilità per Hi-Logic di visualizzare tali informazioni in ogni momento tramite dashboard dedicate).

4.8 SICUREZZA DELLE RETI

La sicurezza delle reti viene garantita attraverso diverse misure, quali a titolo esemplificativo la crittografia dei dati in transito e rest, l'autenticazione multifattore ove attivabile, i firewall di base e la prossima implementazione di un Web Application Firewall fornito da Cloudflare, la protezione delle Web API tramite chiavi autenticative e autorizzative, il logging, il patching dei sistemi.

Le reti virtuali utilizzate sono definite e le comunicazioni interne avvengono solo tra risorse facenti parte della stessa rete o tra determinati indirizzi IP autorizzati.

Inoltre, la prossima implementazione di Cloudflare già menzionata garantirà ulteriore protezione, non solo nel filtraggio delle richieste, ma anche nei confronti di eventuali attacchi DDoS e di mitigazione bot.

4.9 AGGIORNAMENTI E MANUTENZIONI

I sistemi sono manutenuti sulla base delle necessità o delle richieste di incremento di prestazioni o capacità, di malfunzionamenti o della disponibilità di aggiornamenti dei sistemi operativi o dei middleware. Tutte le attività di manutenzione ordinaria sono pianificate e comunicate ai clienti almeno 7 giorni prima qualora queste prevedano l'interruzione di disponibilità del servizio. Le attività di manutenzione straordinaria o in emergenza sono svolte in modo da limitare il più possibile l'impatto sui sistemi di produzione e sui clienti.

5. GESTIONE DEGLI INCIDENTI

Hi-Logic ha definito una specifica procedura per poter permettere un approccio organizzato e regolato alla gestione degli incidenti come parte della propria strategia di sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza e ai punti di debolezza.

Gli incidenti di sicurezza delle informazioni rilevati dal cliente devono essere segnalati al più presto possibile inviando un'email a assistenza@hi-logic.it. Tutte le segnalazioni pervenute sono gestite dal team tecnico che valuta se classificarle come incidente relativo alla sicurezza delle informazioni, rispondendo coerentemente a quanto previsto dalla procedura interna.

Se l'incidente di sicurezza delle informazioni è in relazione ad informazioni personali viene inoltre attivata sezione apposita della procedura per il data breach, che prevede la notifica al Garante per la privacy nel caso in cui i dati violati risultino essere di titolarità di Hi-Logic. Qualora i dati violati siano di titolarità del cliente sarà esso a dover provvedere alla notifica, informando comunque Hi-Logic in qualità di responsabile del trattamento.

Il livello di impatto di un incidente di sicurezza delle informazioni sarà determinato secondo la strategia di gestione del rischio stabilita in accordo tra Direzione e Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni. Quest'ultimo manterrà una copertura del processo di gestione degli incidenti in relazione ad identificazione, valutazione, gestione e monitoraggio degli incidenti di sicurezza delle informazioni, compresa la raccolta di qualsiasi prova che potrebbe essere richiesta per l'analisi come prova forense.

6. DIVULGAZIONE DELLE INFORMAZIONI

A meno che non sia necessaria per soddisfare requisiti contrattuali non è prevista divulgazione di informazioni personali a terzi. L'eventuale divulgazione può avvenire solo verso dipendenti, fornitori o subfornitori con cui sono stati stipulati opportuni accordi di responsabilità e riservatezza. Fanno eccezione eventuali richieste legalmente vincolanti da parte delle autorità preposte (es: Autorità Giudiziaria).

Qualsiasi eventuale divulgazione di informazioni personali dovesse verificarsi verrà registrata nell'apposito registro come da procedure interne, che comprende i riferimenti alle informazioni personali divulgate, il destinatario, la data e ora, il metodo e il motivo (incluso di riferimento legale nel caso di richiesta da autorità prepose).

7. AUDIT DI TERZE PARTI

Hi-Logic, avendo un sistema di gestione conforme alle norme UNI EN ISO 9001:2015, ISO/IEC 27001:2022 con estensioni alle linee guida ISO/IEC 27017:2021 e ISO/IEC 27018:2020, sostiene regolarmente audit eseguiti da organismi di certificazione accreditati.

8. CANALI DI SUPPORTO E AGGIORNAMENTO PERSONALE

Per qualsiasi necessità legata alla sicurezza o alla risoluzione di problematiche relative agli account, i clienti possono contattare il team di supporto scrivendo a assistenza@hi-logic.it.

Il personale tecnico di Hi-Logic partecipa regolarmente a corsi di formazione annuali per restare aggiornato sulle migliori pratiche di protezione dati e sicurezza informatica, garantendo così risposte tempestive e informate alle richieste di supporto.

9. RUOLI E RESPONSABILITÀ DEL CLIENTE PER L'USO DEI SERVIZI SAAS

Pur garantendo la sicurezza e la protezione dei dati attraverso pratiche certificate, i servizi SaaS di Hi-Logic richiedono alcune responsabilità in capo al cliente per un utilizzo sicuro ed efficiente. Queste includono:

- gestione degli accessi e delle autenticazioni: il cliente è responsabile della gestione delle credenziali dei propri utenti e dell'implementazione di policy di accesso sicuro, inclusa l'abilitazione dell'autenticazione multi-fattore (MFA) per gli account con accesso privilegiato, ove applicabile;
- monitoraggio dell'utilizzo del servizio: è responsabilità del cliente verificare che le modalità d'uso del servizio SaaS rispecchino i requisiti operativi aziendali e che la capacità di servizio soddisfi le proprie esigenze;
- sicurezza delle informazioni e formazione del personale: il cliente deve assicurarsi che il proprio personale riceva un'adeguata formazione sui rischi associati all'uso di servizi cloud, promuovendo consapevolezza sui temi di sicurezza informatica e sugli standard operativi necessari per mantenere sicuro l'ambiente di lavoro;
- gestione della conformità e dei requisiti di sicurezza: anche se la gestione di backup e configurazioni dei servizi cloud sottostanti non è direttamente gestita dal cliente, lo stesso deve segnalare eventuali necessità aggiuntive o particolari, non indicate in questo documento, necessarie per adattarsi alle politiche aziendali interne, in modo da permettere ad Hi-Logic di analizzare la casistica e di informarlo sulle possibilità di implementazione;
- gestione delle vulnerabilità e segnalazione di incidenti: il cliente è responsabile di segnalare prontamente qualsiasi attività sospetta, potenziali vulnerabilità o incidente di sicurezza rilevato, comunicando tramite i canali di supporto, in modo da permettere ad Hi-Logic di intervenire rapidamente per mitigare eventuali rischi.