

Allegato A DOCUMENTO DI SLA (Service Level Agreement) – HRgo

1. Introduzione

Il presente documento illustra l'organizzazione, le modalità di erogazione nonché i livelli di servizio per la soluzione indicata.

Il presente documento non tratta dell'assistenza applicativa.

2. Descrizione del servizio

Il servizio viene erogato tramite un'infrastruttura basata sulla piattaforma cloud Windows Azure di Microsoft, che garantisce elevati livelli di servizio in merito a:

- Sicurezza fisica dei server
- Protezione da interruzioni di alimentazione
- Ridondanze di apparati
- Banda con profilo dinamico
- Duplicazione delle istanze applicative e dei dati su base geografica.

Rimane facoltà di WKI, in qualsiasi momento della durata del Contratto, di cambiare il soggetto titolare dell'infrastruttura, senza previo avviso al Cliente, garantendo comunque a quest'ultimo gli stessi SLA di Servizio di cui al presente documento.

Nel contempo viene garantita la corretta installazione e funzionamento degli aggiornamenti garantendo tempestivi interventi in caso di errori sul software.

3. SLA relativo alla Infrastruttura

3.1 Protezione per l'ambiente di hosting

L'ambiente della piattaforma Windows Azure è costituito da computer, sistemi operativi, applicazioni e servizi, reti, apparecchiature per le operazioni e il monitoraggio e hardware specializzato, oltre dagli operatori e dal personale amministrativo necessari per eseguire e gestire i servizi. L'ambiente include, inoltre, centri operativi fisici che ospitano i servizi e che richiedono protezione da eventuali danni intenzionali e accidentali.

Punti di progettazione architetturale principali

La piattaforma Windows Azure è progettata per fornire una "difesa in profondità" e ridurre il rischio che il guasto di un singolo meccanismo di protezione comprometta la sicurezza dell'intero ambiente. I livelli di difesa in profondità includono:

- **Router di filtraggio:** i router di filtraggio respingono i tentativi di comunicazione tra indirizzi e porte non configurati nel modo consentito. Questa soluzione consente di prevenire gli attacchi più comuni che utilizzano “droni” o “zombie” per la ricerca di server vulnerabili. Benché siano relativamente facili da bloccare, questi tipi di attacchi restano il metodo preferito dagli utenti malintenzionati in cerca di vulnerabilità. I router di filtraggio supportano, inoltre, la configurazione dei servizi back-end in modo che siano accessibili solo dai corrispondenti front-end.
- **Firewall:** i firewall limitano le comunicazioni di dati da e verso porte, protocolli e indirizzi IP di destinazione (e di origine) noti e autorizzati.
- **Gestione delle patch di protezione del software:** la gestione delle patch di protezione costituisce parte integrante delle operazioni che garantiscono la protezione dei sistemi dalle vulnerabilità note. La piattaforma Windows Azure utilizza sistemi di distribuzione integrati per gestire la distribuzione e l'installazione delle patch di protezione per il software Microsoft.
- **Monitoraggio:** la protezione viene monitorata con l'ausilio di sistemi di monitoraggio, correlazione e analisi centralizzati in grado di gestire l'elevato volume di informazioni generato dai dispositivi all'interno dell'ambiente, fornendo monitoraggio e avvisi pertinenti e tempestivi.
- **Segmentazione di rete:** Microsoft utilizza diverse tecnologie per creare barriere contro il traffico non autorizzato in corrispondenza dei principali punti di giunzione verso i data center e al loro interno, tra cui firewall, caselle NAT (Network Address Translation) (bilanciamento del carico) e router di filtraggio. La rete di back-end è costituita da reti locali (LAN) partizionate per server applicazioni e Web, archiviazione dei dati e amministrazione centralizzata. Tali server sono raggruppati in segmenti di indirizzi privati protetti da router di filtraggio.

3.2 Protezione fisica

La protezione fisica va di pari passo con le misure di protezione basate sul software e a entrambe si applicano analoghe procedure di valutazione e attenuazione dei rischi.

I servizi della piattaforma Windows Azure vengono forniti ai clienti attraverso una rete di data center globali, progettati per l'esecuzione 24 ore su 24, 7 giorni su 7 e per l'utilizzo di diverse misure per proteggere le operazioni da eventuali interruzioni di alimentazione, intrusioni fisiche e interruzioni della rete.

3.3 Protezione delle operazioni e del personale

3.3.1 Progettazione dei servizi

La piattaforma Windows Azure è progettata per l'esecuzione senza accesso di routine ai dati dei clienti da parte del personale Microsoft; solo un numero limitato di operatori può accedere alle informazioni dei clienti.

3.3.2 Risposta agli eventi imprevisti

I servizi della piattaforma Windows Azure dispongono di operatori che lavorano 24 ore al giorno, 7 giorni su 7. Se l'evento imprevisto è legato alla protezione, le procedure documentate da seguire vengono implementate dal personale addetto. È inoltre disponibile un piano di comunicazione completo che viene implementato nel caso di un evento imprevisto legato alla protezione.

3.3.3 Controllo

Le operazioni amministrative di Microsoft sono sottoposte a controlli. È possibile visualizzare l'audit trail per determinare la cronologia delle modifiche.

3.4 Tolleranza di errore e ridondanza

La piattaforma Windows Azure è progettata per garantire tolleranza di errore e ridondanza.

Ogni livello dell'infrastruttura della piattaforma Windows Azure è progettato per consentire il proseguimento delle operazioni in caso di errore, inclusi dispositivi di rete ridondanti a ogni livello e doppi provider di servizi Internet in ciascun data center.

3.5 Servizio di Backup dell'infrastruttura

Il servizio di backup ha come obiettivo la protezione dei dati finalizzato al ripristino degli stessi in caso di disaster recovery.

La piattaforma Windows Azure garantisce il ripristino dei dati a fronte dell'ultimo evento di disaster.

3.6 Dati di Targa infrastruttura

La disponibilità dell'infrastruttura è garantita per il 99.5% per 24 ore al giorno, 365 giorni l'anno.

4. SLA sulle applicazioni WKI

4.1 System monitoring

- Sovrintendere, senza interruzioni, al funzionamento di tutte le componenti del servizio erogato ai clienti
- Gestire l'esecuzione delle procedure operative e il mantenimento della documentazione relativa all'operatività
- Interfacciare le terze parti (es. fornitori, partner, clienti) coinvolte nel processo di erogazione e governance dei servizi.

Gli scopi del servizio di monitoraggio sono:

- L'individuazione, preventiva o reattiva, degli eventuali problemi di funzionamento dei servizi (troubleshooting)
- Misurazione continua ed in tempo reale dei valori garantiti contrattualmente

4.2 System management

Problem solving

- Gestione dei contratti di manutenzione con i fornitori HW/SW
- Risoluzione di eventi dei software registrati nel system-log file

Gestione ordinaria

- Tuning dei parametri prestazionali
- Segnalazione di procedure operative da notificare al cliente

Manutenzione

- Pianificazione ed esecuzione degli interventi di manutenzione ordinaria e straordinaria sulle applicazioni

4.3 Disponibilità del servizio software

- Il servizio software sarà di norma disponibile 24 ore al giorno, 365 giorni l'anno, fatta salva una FINESTRA DI MANUTENZIONE per le attività di MANUTENZIONE ordinaria (patching, ecc). Questa fascia di indisponibilità del SERVIZIO SOFTWARE sarà notificata con almeno 24 ore di anticipo a mezzo e-mail.
- Gli interventi di MANUTENZIONE straordinaria effettuati al di fuori della FINESTRA DI MANUTENZIONE e/o per una durata superiore ai 60 minuti saranno segnalati con 3 gg di anticipo

4.4 Dati di targa servizio software

Livelli di Severity	Descrizione		
Severity 1	Grave indisponibilità del servizio che ha un serio impatto sulle attività del cliente e non può essere aggirata. Impossibilità di utilizzo del servizio.		
Severity 2	Anomalie parziali a cui è possibile applicare soluzioni temporanee per garantire l'erogazione del servizio.		
Tempo di Ripristino	8.00 - 17.00	17.00 - 8.00	Weekend/Festivi
SEVERITY 1 85%	4+1 ore	Entro le 12.00 del giorno successivo	Entro le 12.00 del primo giorno lavorativo successivo alla segnalazione
SEVERITY 1 15%	48 ore a partire dalla giornata lavorativa successiva alla segnalazione		
SEVERITY 2 100%	4+1 ore	Entro le 12.00 del giorno successivo	Entro le 12.00 del primo giorno lavorativo successivo alla segnalazione

5. Limiti di applicabilità degli SLA

- indisponibilità delle linee d'accesso del Cliente;
- anomalie che comportano il blocco di una specifica funzionalità;
- inaccessibilità logica alle risorse della infrastruttura;
- indisponibilità del servizio causata da azioni non direttamente imputabili a WKI;
- interruzioni del Servizio dovute ad indisponibilità di reti di altri provider;
- indisponibilità del servizio Internet;
- guasti e/o disservizi comunicati dal Cliente ma non riscontrati;
- indisponibilità del Servizio per aggiornamenti dei database degli enti ufficiali (Ripe, Nic, ecc.)

I valori di SLA quivi illustrati potranno subire variazioni, nel corso della durata del Contratto. La versione aggiornata di questo documento sarà disponibile in apposita sezione del Software.

Con riferimento all'Allegato SLA Infrastruttura, allegato alle Condizioni Generali di Acquisto di HRgo, si precisa e si chiarisce che Wolters Kluwer Italia S.r.l. non presta alcuna garanzia in ordine al puntuale e corretto "funzionamento" dei livelli di servizio ivi indicati, i quali riflettono esclusivamente standard di servizio definiti da fornitori terzi dell'infrastruttura.

Conseguentemente, Wolters Kluwer Italia S.r.l. non potrà essere ritenuta responsabile di eventuali disservizi connessi al mancato rispetto degli SLA infrastrutturali, né sarà tenuta a rispondere delle eventuali conseguenze pregiudizievoli, dirette o indirette, che dovessero derivarne, salvi i soli casi di dolo o colpa grave.

Resta in ogni caso espressamente fermo che, come previsto dalle Condizioni Generali di Contratto sottoscritte, e salvi i casi di dolo o colpa grave, la responsabilità complessiva di Wolters Kluwer Italia S.r.l. sarà in ogni caso limitata a un importo massimo pari ai corrispettivi effettivamente pagati dal Cliente per i Programmi e per i Servizi di Assistenza nell'ultimo anno di vigenza del Contratto.

WOLTERS KLUWER ITALIA SRL

Versione di marzo 2026