Allegato A DOCUMENTO DI SLA (Service Level Agreement)

2. Introduzione

Wolters Kluwer Italia S.r.l. (di seguito anche "WKI") ha sviluppato una soluzione innovativa per l'erogazione del proprio applicativo in modalità SaaS, ovvero su piattaforma cloud con alti livelli di affidabilità, sicurezza e scalabilità.

3. 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 WKI garantisce la corretta installazione e funzionamento degli aggiornamenti garantendo tempestivi interventi in caso di errori sul software.

4. SLA relativo alla Infrastruttura

Wolters Kluwer Italia S.r.l. ha definito con Microsoft i livelli di servizio della piattaforma cloud Windows Azure. Si fa pertanto riferimento alle garanzie che Microsoft stessa presta, di cui si riportano le caratteristiche più significative:

4.1 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.

4.2 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. Questi data center sono conformi agli standard del settore relativi a protezione fisica e affidabilità, vengono gestiti, monitorati e amministrati da operatori Microsoft e sono situati in località geografiche diverse.

Microsoft utilizza meccanismi di accesso altamente protetti, limitati a un numero molto ristretto di propri operatori ed operatori WKI che sono tenuti a modificare regolarmente le proprie password di accesso amministratore. L'accesso ai data center e l'autorizzazione ad aprire i ticket di accesso per i data center vengono sottoposti al controllo del responsabile delle operazioni di rete, nel rispetto delle procedure di protezione dei data center locali.

4.3 Protezione delle operazioni e del personale

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.

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.

Controllo

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

4.4 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. Il failover avviene nella maggior parte dei casi in modo automatico, senza necessità di intervento umano, e la rete viene monitorata dal Network Operations Center (NOC) 24 ore al giorno, 7 giorni su 7, per rilevare eventuali anomalie o potenziali problemi di rete.

4.5 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.

4.6 Dati di Targa infrastruttura

Si riportano i dati di targa garantiti da Microsoft che sono alla base del servizio offerto e di cui beneficerà il cliente durante l'utilizzo del prodotto applicativo oggetto del contratto:

La disponibilità dell'infrastruttura è garantita per il 99.9% per 24 ore al giorno, 365 giorni l'anno.

Per indisponibilità s'intende una interruzione della rete sull'infrastruttura Windows Azure che impedisca il raggiungimento dei servizi di Wolters Kluwer Italia S.r.l. ospitati sulla piattaforma cloud Windows Azure da una postazione esterna per un periodo di almeno cinque (5) minuti.

Essa non include sospensioni programmate per interventi tecnici, interruzioni parziali, degrado del servizio, interruzioni dovute a catastrofi, sommosse, eventi di carattere eccezionale.

5. SLA sulle applicazioni WKI

WKI offre le proprie garanzie relativamente al funzionamento dei servizi applicativi ospitati sulla piattaforma Windows Azure.

5.1 System monitoring

I servizi sono costantemente monitorati dal personale WKI al fine di:

- 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.

A fronte del flusso di eventi generato dai server, gli operatori WKI applicano le procedure operative di gestione, sia generali, sia, eventualmente, specifiche per il singolo servizio.

Gli scopi del servizio di monitoraggio sono:

1. L'individuazione, preventiva o reattiva, degli eventuali problemi di funzionamento dei servizi (troubleshooting)
2. Misurazione continua ed in tempo reale dei valori garantiti contrattualmente, al fine di assicurare il rispetto del Service Level Agreement (SLA).

5.2 System management

Le componenti del Servizio Base di System Management sono:

Problem solving

- Gestione dei contratti di manutenzione con i fornitori HW/SW, relativamente alle componenti gestite, in caso di failure
- 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

5.3 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 quotidiane di MANUTENZIONE ordinaria (patching, ecc). Questa fascia di indisponibilità del SERVIZIO SOFTWARE dovrà avere una durata non superiore ai 60 minuti, collocata nella fascia 18.00 – 08.00 e segnalata tramite apposita pagina di cortesia.
- 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 tramite apposita pagina di cortesia.

5.4 Dati di targa servizio software

Nelle tabelle seguenti sono riportati i gradi di severity del "guasto" ed il relativo tempo di ripristino.

Per "guasto" si intende una anomalia del software che ne impedisca il corretto funzionamento.

Livelli di Severity	
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.

Tempi di ripristino del servizio			
Tempo di Ripristino	Guasti rilevati nella finestra temporale 8.00 - 17.00 nei giorni lavorativi	Guasti rilevati nella finestra temporale 17.00 - 8.00 nei giorni lavorativi dal lunedì al giovedì	Guasti rilevati nella finestra temporale 17.00 - 8.00 del venerdì e nei giorni non lavorativi
SEVERITY 1 85% dei casi	4+1 ore	Entro le 12.00 del giorno successivo	Entro le 12.00 del primo giorno lavorativo successivo alla segnalazione
SEVERITY 1 15% dei casi	48 ore a partire dalla giornata lavorativa successiva alla segnalazione		
SEVERITY 2 100% dei casi	4+1 ore	Entro le 12.00 del giorno successivo	Entro le 12.00 del primo giorno lavorativo successivo alla segnalazione

6. Limiti di applicabilità degli SLA

Oltre alle ipotesi contrattualmente previste, sono di seguito riportate ulteriori fattispecie giustificative del mancato rispetto da parte di WKI degli SLA sopra indicati e di conseguente esclusione di responsabilità di WKI:

1. indisponibilità delle linee d'accesso del Cliente;
2. anomalie che comportano il blocco di una specifica funzionalità, in tale caso il Cliente sarà avvisato tramite apposita pagina di cortesia;
3. inaccessibilità logica alle risorse della infrastruttura dovute a cambiamenti dei controlli di accesso fatte dal provider Microsoft e non comunicate a WKI;
4. indisponibilità del servizio causata da azioni non direttamente imputabili a WKI;
5. interruzioni del Servizio dovute ad indisponibilità di reti di altri provider (es: ISP di accesso dell'utente);
6. indisponibilità del servizio Internet dovuta a disservizi sugli Upstream Provider o Peering pubblici e privati;
7. guasti e/o disservizi comunicati dal Cliente ma non riscontrati da WKI;
8. indisponibilità del Servizio per aggiornamenti dei database degli enti ufficiali che gestiscono regole, infrastrutture e protocolli Internet (Ripe, Nic, ecc.)

I valori di SLA quivi illustrati potranno subire variazioni, nel corso della durata del Contratto, previa comunicazione scritta al Cliente con preavviso di 15 (quindici) giorni.